جامعة 20 أوت 1955 – سكيكدة

كلية الحقوق والعلوم السياسية

قسم الحقوق

إجراءات المعاينة، التفتيش، والحجز داخل المنظومة المعلوماتية

مذكرة مكملة لنيل شهادة الماستر تخصص: القانون الجنائي والعلوم الجنائية.

من تقديم الطالب(ة):

- بوفروك هند
- سعيود بشرى

تحت إشراف:

- **د.** خطابي فارس

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
بوصيدة أمحمد	أستاذ محاضر	رئيسا
خطابي فارس	أستاذ محاضر	مشرفا ومقررا
صافي عبد الله	أستاذ مساعد	مناقشا

دورة جوان 2025

شكر وتقدير

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

ونخص بالتقدير والشكر لأوليائنا اللذين علمونا السلوك القويم، وأناروا حياتنا بقبسات الهداية وعلمونا أيضا أن الصبر هو طريق النجاح كما أخص بالشكر لأستاذنا ومشرفنا الذي سخر جهوده من أجلنا وأخص بالشكر الى زوج أختي الدكتور محمد قطاف الذي كان داعما لنا طوال فترة بحثنا.

الإهداء

إلى العزيز الذي حملت اسمه فخرًا، إلى من كلّله الله بالهيبة والوقار، إلى من حصد الأشواك عن دربي وزرع لي الراحة بدلاً منها، إلى أبي...

لم يحنِ ظهر أبي ما كان يحمله، لكن ليحملني، من أجليّ انحنى. وكنت أحجب عن نفسي مطالبها فكان يكشف عمّا أشتهي الحُجبا. فشكرًا لكونك أبي!

إلى من علّمتني الأخلاق قبل أن أتعلمها، إلى الجسر الصاعد بي إلى الجنة، إلى اليد الخفية التي أزالت عن طريقي العقبات ومن ظلت دعواتها تحمل اسمي ليلًا ونهارًا...

أمي، محبوبتي وملهمتي.

وإلى من وهبني الله نعمة وجودهم، إلى مصدر قوتي، وأرضي الصلبة، وجدار قلبي المتين...

إخوتي وأخواتي.

وإلى من إن ضاقت بي الدنيا وسعت بخُطاهم، وإن سقطت، كانوا أول من رفعوني بكلماتهم،

إلى من رافقني بالقلب قبل الدرب. أصحابي وأحبتي.

ها أنا اليوم طويت صفحة من التعب وسجلت في تاريخي فخرا لا ينسى. لم أعد أتساءل عن ملامح الوصول فقد رأيتها في عيوني. تلاشت غيوم التعب وابتسم الأفق بعد عتمة الانتظار. ها هي الخطى التي كانت تتعثر أحيانًا قد وجدت مستقرها في قمة الإنجاز، وبين طيات الطريق تنفست سلامًا وفرحًا وامتنانً.

(وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ)

– بشرى –

لا يطيب الليل إلا بشكره ولا يطيب النهار إلا بطاعته.... ولا يطيب اللحظات إلا بذكره.

-الله جل جلاله –

انتهت الرحلة ولم تكن سهلة وليس من المفترض أن تكون كذلك. ومهما طالت فستمضي بحلوها ومرها وها أنا الآن وبعوض الله تعالى أتمم هذا العمل.

إلى قدوتي الأولى ومعنى الحب والتفاني إلى بسمة الحياة وسر الوجود إلى من كان دعاؤها سر نجاحي وحنانها بلسم جراحي ..... إلى من أرشدتني و رافقتني في كل مشاعر حياتي و لا تزال تفعل إلى الآن.. اللهم أحفظها وأرزقها الصحة والعافية ..... أمي الغالية.

وإلى النور الذي شع ضياءه على قلبي ودربي وكل حياتي من سقوا الفؤاد دوماً بطيب كلماتهم وعطاياهم السخية وبوجودهم استشعرت معنى أن يكون للمرء وجهه يستمد منها بهجته وشغاف الحياة وايقنت معهم إني حظيت بخير اخوة ورفاق وسند... أخواني الغاليين.
والى رفيقة الخطوة الأولى والخطوة ما قبل الأخيرة التي كانت خلال السِنين العِجاف سحابًا ممطرًا، زنزونتي.

والى صديقتي التي رافقتها في طريقٍ صارت بعد الطريقِ خيرُ رفيقة، نُورْ.

والى أعظم عائلة الى نعيمي ونعمتي من أمنوا بقدراتي وراهنوا على نجاحي وكانوا لأحلامي سندا ولأمالي عونا ولحياتي أنسا وسرورا ونورا.

الحمد لله

– هند–

مقدمة

مقدمة:

في عصر التحول الرقمي، أصبحت الجرائم المعلوماتية تشكل تهديدا متناميًا لأمن الأفراد والمؤسسات، مما استدعى تطوير أدوات قانونية متخصصة لمواجهتها. تأتي هذه الدراسة لتحليل إجراءات المعاينة والحجز والتفتيش في المنظومة المعلوماتية كآليات أساسية للكشف عن الأدلة الرقمية ومكافحة الجرائم الإلكترونية. وتبحث هذه الورقة في الإطار القانوني المنظم لهذه الإجراءات، مع التركيز على التحديات العملية الناتجة عن طبيعة البيئة الرقمية غير الملموسة، والتي تختلف جذريًا عن الإجراءات التقليدية في القانون الجنائي. وبالتالي جريمة الأمس ليست كجريمة اليوم، إلا أن المشرع الجزائري تدارك ذلك بإصدار القانون 04/115 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، والذي جاء كمولود جديد في التشريع الجنائي الجزائري، كما اصطلح عليه بالجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات.

أصبحت تقنية الحاسوب تستعمل كوسيلة لارتكاب الجرائم تارة وكموضوع للجريمة تارة أخرى، وأصبح هذا النوع من الجرائم يرتكب في وسط افتراضي غير متعارف عليه ولا يشبه الوسط التقليدي للجرائم التقليدية، مما دفع المشرع الجزائري مرة أخرى في سنة 2006 بتعديل بعض أحكام قانون العقوبات، بحيث أصدر الأمر 06/23 المعدل والمتمم لقانون العقوبات الجزائري، إلا أن كل هذا لم يكن كافيا لإعطاء حماية جزائية إجرائية لمكافحة الجرائم المعلوماتية.

وأول قانون إجرائي ينظم إجراءات مكافحة الجرائم المعلوماتية كان ضمن قانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي جاء ببعض الإجراءات التي من شأنها إن صح التعبير أن تكمل ما جاءت به القواعد الإجرائية العامة التي نص عليها قانون الإجراءات الجزائية، كل هذا تحت ظل أزمة

القانون الجنائي في مواجهة واقع المعلوماتية والذي فرض حلها البحث عن الأوضاع القانونية والإجراءات اللازمة مع مدى ملاءمتها في مواجهة هذه المشاكل.

أهمية الدراسة:

تبرز أهمية موضوع مذكرتنا من خلال ما يقدمه من معلومات وأفكار متنوعة وشاملة عن الجرائم الماسة بالنظام المعلوماتي والإجراءات المتبعة داخل المنظومة المعلوماتية، وذلك من خلال تسليط الضوء على ماهية النظم المعلوماتية وخصائصها هذا من جهة، ومن جهة أخرى الوقوف على بعض صور جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتحديد العقوبة المقررة لكل جريمة كألية ردعية بهدف الحد من انتشار هذا النوع من الجرائم خاصة في ظل الثورة التكنولوجية الواسعة.

وتكمن أهمية موضوع "إجراءات المعاينة التفتيش والحجز داخل المنظومة المعلوماتية" أساسا في كون الجريمة المعلوماتية جريمة جديدة حديثة النشأة وبالتالي لا يكفي تطبيق الإجراءات المطبقة على الجرائم التقليدية، حيث نجد القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية لا يمكن أن تطبق عليها كونها تقع في عالم افتراضي، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال التي تستعمل في جميع مجالات الحياة سواء من طرف الأفراد أو المؤسسات، إذ تجعل التعاملات معها صعبا ومعقدا مما يحتم إلى إيجاد إجراءات تحري جديدة.

ونظرا للأهمية البالغة التي تكتسيه مكافحة الجريمة المعلوماتية وما فرضته من تحديات خاصة في عصرنا الحالي، الذي يعرف تطورا سريعا في مجال تكنولوجيا الإعلام والاتصال، حيث أصبحت هذه الأخيرة الركيزة التي تقوم عليها مختلف القطاعات سواء الخاصة أو العامة، حاولنا في دراسة موضوعنا وضع الخطوط العريضة بالتعرف على الإجراءات الإلكترونية للمعاينة الحجز والتفتيش داخل المنظومة المعلوماتية.

أهداف الدراسة:

نسعى من خلال موضوع مذكرتنا إلى تحقيق جملة من الأهداف تتمثل فيما يلي:

- بيان أنواع الجرائم التي تمس بأنظمة المعالجة الآلية للمعطيات.
- تحديد العقوبات المقررة لمرتكبي هذه الجريمة، سواء كانوا أشخاص طبيعيين أو معنويين.
- الضوابط القانونية والفنية لإجراءات المعاينة والحجز التفتيش في الفضاء الرقمي.
- القيمة العلمية للدليل الالكتروني ومدى تأثيره على قناعة القاضي الجزائي.

وعليه فالهدف المبتغى من دراسة هذا الموضوع هو معرفة إجراءات التحري المستحدثة داخل المنظومة المعلوماتية للمعاينة المتمثلة في معاينة مسرح الجريمة الإلكترونية وإجراءات التفتيش والحجز في النظم المعلوماتية وحجية الدليل الإلكتروني في الإثبات.

أسباب اختيار الموضوع:

هناك أسباب ذاتية وأخرى موضوعية دفعتنا إلى اختيار هذا الموضوع والتي يأتي ذكرها فيما يلي:

أ -الأسباب الذاتية:

تعود الأسباب الذاتية إلى رغبتنا الشخصية لدراسة هذا الموضوع والغوص فيه ومعرفة بعض السلوكيات التي تعد جريمة تمس بالمعطيات المنظمة آليا، بالإضافة إلى ذلك ميولنا الذاتي إلى مجال تكنولوجيا الإعلام والاتصال لما له من تأثير على حياة الفرد والمجتمع.

ب -الأسباب الموضوعية:

تعود الأسباب الموضوعية التي دفعتنا لاختيار موضوع مذكرتنا إلى كون موضوع جرائم المساس بأنظمة المعالجة الآلية للمعطيات يعتبر من المواضيع الحديثة التي تعالج جانب من

الجريمة الإلكترونية والتي تعد من أوسع وأخطر الجرائم التي تنتهك سيادة الدول واقتصادها الدولي، وهو الأمر الذي دفع بالمشرع الجزائري إلى علاجها نظرا للاستغلال المتزايد للتكنولوجيا وتقنية المعلومات لأغراض إجرامية و ما يترتب عليه من خطورة على الفرد والمجتمع، و لهذا عمل المشرع الجزائري على توفير حماية شاملة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلال نصوص المواد من 394 مكرر إلى 394 مرر 7.

الاشكالية:

الى أي مدى وفق المشرع الجزائري آليات إجراءات المعاينة الحجز والتفتيش في الجرائم الماسة بالأنظمة المعلوماتية؟

ويتفرع عن هذه الاشكالية عدت أسئلة فرعية يستوجب الإجابة عنها من خلال هذه الدراسة وهي:

- ماهي القوانين الجزائرية الحالية التي تجرم المساس بأنظمة المعالجة الآلية للمعطيات؟
- ماهي الآليات المتبعة من قبل الجهات القضائية والامنية للتعامل مع هذه الجرائم؟

المنهج المتبع:

للإجابة على الإشكالية المطروحة اتبعنا المنهج الوصفي والمنهج التحليلي، وذلك من خلال وصف وتعريف النظام المعلوماتي وإبراز خصائصه والجرائم التي تقع على مستواه ومن جانب آخر بيان كيفية القيام بإجراءات المعاينة الحجز والتفتيش في البيئة الإلكترونية ومدى حجية دليلها الإلكتروني على قناعة القاضي الجزائي.

خطة الدراسة:

لقد تم تقسيم موضوع مذكرتنا إلى فصلين رئيسيين، حيث خصصنا الفصل الأول لدراسة الطبيعة الخاصة للنظم المعلوماتية، وقد قسمناه إلى مبحثين ، المبحث الأول نتطرق من خلاله إلى ماهية النظم المعلوماتية، بينما نتحدث في المبحث الثاني عن تقسيم الجرائم المعلوماتية، هذا من جهة و من جهة أخرى نتطرق في الفصل الثاني والذي سميناه بإجراءات المعاينة الحجز و التفتيش في المنظومة المعلوماتية حيث قمنا بتقسيمه إلى مبحثين .المبحث الأول نبين فيه إجراءات المعاينة و الحجز ،ثم بعد ذلك درسنا في المبحث الثاني إجراءات التفتيش الإلكتروني و حجيته . وفي الأخير نختم موضوع بحثنا بخاتمة تنطوي على مجموعة من النتائج التي توصلنا إليها، وبمجموعة من التوصيات التي بادر المشرع الجزائري باتخاذها من أجل مكافحة الجرائم المعلوماتية.

الفصل الأول

الطبيعة الخاصة للنظم المعلوماتية

في عصرنا الحديث، أصبحت المعلومات تمثل اهم الموارد الاستراتيجية التي تعتمد عليها المؤسسات في تحقيق أهدافها ة اتخاذ قراراتها. ومع هذا التحول، برزت نظم المعلومات كأدوات حيوية تمكن المؤسسات من جمع ومعالجة وتخزين واسترجاع المعلومات بشكل فعال وسريع.

تتسم النظم المعلوماتية بطبيعة خاصة تميزها عن غيرها من الأنظمة، حيث تجمع بين العناصر البشرية والتقنية والتنظيمية في إطار واحد متكامل. فهي ليست مجرد برامج او أجهزة، بل هي منظومة تتفاعل فيها التكنولوجيا مع السياسات والإجراءات والأشخاص، بهدف دعم عمليات المؤسسة وتحقيقي ميزة تنافسية.

تعد هذه النظم العمود الفقري لأي منظمة تسعى للابتكار والتطور في بيئة تتسم بالتغير المستمر وسرعة التفاعل مع المتغيرات، مما يجعل فهم طبيعتها الخاصة امرا ضروريا لفهم كيفية توظيفها والاستفادة منها بأقصى قدر ممكن. سنتطرق في هذا الفصل الى ماهية النظم المعلوماتية(المبحث الاول) والى تقسيم الجرائم المعلوماتية(المبحث الثاني) .

المبحث الأول: ماهية النظم المعلوماتية

تعد النظم المعلوماتية أحد الركائز الأساسية في العصر الرقمي، حيث تلعب دورا حيويا في جمع، معالجة، تخزين، وتحليل البيانات لتحويلها الى معلومات مفيدة تدعم اتخاذ القرارات في مختلف المجالات سنتطرق في هذا المبحث الى مفهوم النظم المعلوماتية(المطلب الأول) والى مكونات وخصائص نظم المعلومات(المطلب الثاني) .

المطلب الأول: مفهوم النظم المعلوماتية

نظم المعلومات هو اصطلاح نشأ منذ السبعينات من القرن الماضي بهدف وصف الحالة التي نشأت باندماج تقنية عملاقة هي تقنية نظم المعلومات، وتقنية الاتصالات عن بعد وهندسة التحكم، وقد أدى هذا التزاوج إلى اختراع تقنيات باهرة ساعدة بشكل كبير على تطوير أنظمة معالجة البيانات بمختلف أشكالها وأنواعها وأصبحت بالفعل عمالا حاسما فقي تحديد مصير عالمنا بدوله وأفراده، وأثرت ولا تزال تؤثر في شتى مناحي الحياة المعاصرة[1]. سنتطرق في هذا المطلب الى التعريف بالنظم المعلوماتية (الفرع الأول) والى مكونات النظم المعلوماتية (الفرع الثاني).

الفرع الاول: تعريف النظم المعلوماتية:

سنذكر في هذا الفرع التعريف اللغوي والاصطلاحي وكذلك التشريعي للنظم المعلوماتية.

أولا: التعريف اللغوي:

يتضمن التعريف اللغوي مصطلح النظام وكذا مصطلح المعلوماتية.

[1] أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 2014، ص 23.

1. تعريف النظام:

هناك تعاريف عديد حول النظام وسنتطرق لبعض التعريفات كالاتي:

يعرف النظام مجموعة العناصر والأجزاء والمكونات التي ترتبط وتتفاعل مع بعضها تعمل على نحو متكامل لتحقيق هدف أو أهداف محددة[1].

ويعرف النظام كذلك بأنه عبارة عن إطار عام متكامل يحقق عدة أهداف، حيث يتولى تنسيق الموارد اللازمة لتحويل المدخلات الى المخرجات، وهذه الموارد تتراوح من الموارد الى الدلالات وعناصر الطاقة الإنتاجية حسب نوعية كل نظام.[2]

ومنه نستنتج ان النظام هو إطار متكامل يضم مجموعة من العناصر المترابطة والمتفاعلة فيما بينها بهدف تحقيق أهداف محددة ومشتركة، سواء كانت أساسية او ثانوية. ويتألف النظام من مكونات مادية كالأجهزة التقنية وخطوط الاتصال، ومكونات معنوية كقواعد البيانات والبرمجيات.

2. تعريف المعلوماتية:

المعلوماتية او المعالجة الالية للمعلومات هي كلمة مكونة من مقطعين، المقطع الأول كلمة Information، والمقطع الثاني كلمة Automatique، والكلمة على هذا النحو قد لا يستسيغها القارئ العربي للوهلة الأولى، ولكن من الاجدر الاخذ بها على هذا النحو لما لها من شيوع في المجال الدولي.

---

[1] بن الصغير الربيع، خلاف محمد زكرياء، نظم المعلومات الإدارية وأثرها على استراتيجية المؤسسة دراسة حالة مؤسسة الصندوق الوطني للتأمينات الاجتماعية للعمال الاجراء وكالة ميلة، مذكرة مكملة لنيل شهادة الماستر، المركز الجامعي عبد الحفيظ بالصوف، معهد العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، تخصص إدارة أعمال، 2022-2023، ص 11.

[2] بودواب سمير، لبديوي فؤاد، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة ماستر، جامعة 20اوث 1955، كلية الحقوق والعلوم السياسية، قسم الحقوق، سكيكدة، 2024، ص 09.

وقد صاغت الأكاديمية الفرنسية تعريفا للمعلوماتية في جلستها المنعقدة بتاريخ 6 أبريل سنة 1967 م، تضمن انها: "علم التعامل العقلاني على الأخص بواسطة الات اوتوماتكية –مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعمادا للاتصالات في ميادين التقنية والاقتصاد والاجتماع.

وخلاصة الامر نشير الى ان مصطلح المعلوماتية يسير في فضاء واسع من الحقول والتخصصات المتنوعة، ويرتبط بأبعاد وعلاقات ومداخل متباينة منها ما هو مرئي واضح وملموس ومنها ما هو غير مرئي ومؤثر وحيوي، وهذا ما يجعل مفهوم المعلوماتية غير واضح تماما وغير محدد بالإطلاق لأسباب تتعلق باتساع نطاق تطبيق واستخدام المعلوماتية من جهة، وللتفنن اللغوي في إطلاق الكثير من المصطلحات المرادفة للمعلوماتية من جهة أخرى.[1]

ثانيا: التعريف الاصطلاحي:

لقد عرفها أحد المتخصصين في مجال نظم المعلومات بأنها:« إخضاع المعلومات في حصرها وتبويبيها وتحليلها الى مجموعة من نظم التشغيل والمعالجة الحسابية والمنطقية لاستخلاص النتائج » .

وفي تعريف اخر بأنها:« مجموعة من الإجراءات التي يتم من خلالها تجميع واسترجاع أو تشغيل وتخزين ونشر المعلومات بغرض دعم عمليات صنع القرار وتحقيق الرقابة داخل الجهة الإدارية أو أيا كانت شكل تلك المنظمة ».[2]

ثالثا: التعريف التشريعي:

[1] طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية الامن المعلوماتي النظام القانوني لحماية المعلوماتية Système Judicaire Pour La Protection de L'information، دار الجامعة الجديدة، الإسكندرية، 2015، ص 46.

[2] ايمن عبد الله فكري، المرجع السابق، ص 23.

لقد عرف المشرع الجزائري المنظومة المعلوماتية في المادة 2 من قانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".[1] وقد عرف قانون الاونيسترال النموذجي بشأن التجارة الالكترونية مصطلح نظام المعلومات بالمادة 2 الفقرة السادسة بأنها:" النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها أو استلامها أو تحويلها أو لتجهيزها على أي وجه آخر". [2]

كما تم تعريف نظم المعلومات بمعاهدة بودابست الدولية بأنها : « كل آلة بمفردها او مع غيرها من الآلات المتصلة أو المرتبطة ، و التي يمكن أن تقوم بمفردها أو مع مجموعة عناصر أخر تنفيذا لبرنامج معين ، بأداء معالجة آلية للمعلومات »، توضح هذه الاتفاقية بأن محل الجريمة هو نظام المعلوماتي ، و هو جهاز يتكون من مكونات مادية و مكونات منطقية و ذلك بهدف المعالجة الآلية للبيانات ، و هو يشتمل على وسائل لإدخال و إخراج و معالجة و تخزين المعلومات ، و هذا الجهاز قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة إلكترونية بدون تدخل بشري.

و عرفتها منظمة التعاون الاقتصادي و التنمية بأنها: « تشمل الحاسبات الالية و وسائل الاتصالات و شبكات المعلومات و البيانات و المعلومات التي يمكن تخزينها و معالجتها و

[1] المادة 02 من قانون رقم 09-04، 14المؤرخ في شعبان عام 1430 الموافق ل 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخة في 25 شعبان عام 1430هـ الموافق ل 16 غشت 2009م.

[2] المادة 02 من قانون الاونيسترال النموذجي بشأن التجارة الالكترونية مع دليل التشريع 1996 ومع المادة الإضافية 5 مكررا بصيغتها المعتمدة في عام 1998، قرار الجمعية العامة 162/51 المؤرخ في 16 ديسمبر 1996، الأمم المتحدة، نيويورك، سنة 2000.

استرجاعها و نقلها بوساطة هذه الحاسبات و وسائل الاتصالات أو شبكات المعلومات بما في ذلك برامج الحاسبات الالية وجميع القواعد اللازمة لتشغيل هذه الأنظمة و المحافظة عليها ».[1]

المطلب الثاني: مكونات وخصائص نظم المعلومات

ان للنظم المعلوماتية مكونات وخصائص تهدف الى معالجة المعلومات وتسهيل حلها ومنه سنتطرق في هذا المطلب الى مكونات نظم المعلومات(الفرع الاول) وخصائصها (الفرع الثاني).

الفرع الأول: مكونات نظم المعلومات:

سنتطرق في هذا الفرع الى أهم المكونات المادية للنظام المعلوماتي والتي تتمثل في الحاسب الالي ولاهم المكونات غير المادية والمتمثلة في المعطيات.

أولا: المكونات المادية (الحاسب الالي):

يعرف الحاسب الالي بانه آلة او جهاز الكتروني لديه القدرة على استقبال البيانات او المعطيات وتخزينها ومعالجتها، للحصول على النتائج المطلوبة بسرعة ودقة، وله استخدامات متعددة.[2] ويعرف الحاسب الالي أيضا بانه: " مجموعة الطرق او البرامج المتعلقة بتشغيل الحاسوب".[3] وتنقسم المكونات المادية للحاسب الالي الى ست وحدات هي: المدخلات–الذاكرة الرئيسية– التحكم–المخرجات.

1– وحدة المدخلات:

[1] ايمن عبد الله فكري، المرجع السابق، ص25.

[2] بليردوح ثليثة، "الحاسوب ودوره في العملية التعليمية والتعلمية"، مجلة العربية، جامعة العربي بن مهيدي، المجلد07، عدد خاص01، 2020/03/02، ص 153.

[3] أسامة بن يطو، حمزة عبدلي، " حماية برامج الحاسب الالي في ضوء التشريع الجزائري والمواثيق الدولية"، مجلة معارف، قسم العلوم القانونية، السنة التاسعة، العدد 19، 2015، ص 127.

وهي الوسائل التي تستخدم في ادخال البيانات والبرامج الى وحدة التشغيل المركزية وذلك بتوجيه من وحدة التحكم منها: لوحة المفاتيح–الفأرة–الميكروفون–الكاميرا–الماسح الضوئي...الخ.

2–وحدة الذاكرة الرئيسية (M.M) Main Memory:

تستخدم الذاكرة الرئيسية لحفظ البيانات والمعلومات والبرامج حفظاً دائما أو مؤقتا وهي بهذا المعنى تتكون من نوعين.

النوع الاول لنوع الأول ذاكرة القراءة فقط Read only memory (ROM) والنوع الثاني ذاكرة القراءة والكتابة Random Access Memory (RAM). [1]

3– وحدة المعالجة المركزية Central Processing Unit:

وتعتبر مركز الأنشطة في الحاسوب وتحتوي على دوائر كهربائية تترجم وتنفذ تعليمات برامج التشغيل.

4–وحدة المخرجات (وحدات الإخراج)Output Units :

وهي الأجزاء والوحدات التي يتم من خلالها اخراج البيانات المعالجة من وحدة المعالجة المركزية على الخارج ومن اهم وحدات اخراج: الشاشة والطابعة.[2]

ثانيا: المكونات غير المادية (المعطيات):

لقد أفرزت الثورة المعلوماتية كيانات جديدة لم يكن للإنسان عهد بها قبل وقت قريب، ولعل أهم هذه الكيانات هي المعطيات وما تقدمه من معلومات، ولقد بات لزاماً على القانون أن يحدد

[1] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص ص90–94.

[2] سحنين طارق، بوسماحة صارة، إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية، مذكرة التخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة يحي فارس، كلية الحقوق والعلوم السياسية، المدية، 2021/2020، ص 11.

موقفه من هذه المعطيات، وأهم إشكال يواجه رجال القانون في التحري حول هذا الموقف هو تحديد مفهوم لهذه المعطيات، وذلك بوضع تعريف لها يجمع خصائصها كلها ويمنع من دخول غيرها فيها، ولعل أهم ما يلتبس بالمعطيات من مفاهيم هي المعلومات وكذا البرامج والمعرفة ولا يستقيم تعريف المعطيات إلا إذا تم تمييزها عن كل ذلك.

I- –تعريف المعطيات وتمييزها عما يتلبس بها:

المعطيات في اللغة تقابل " البيانات "، و" البيان " في اللغة من مشتقات كلمة " بين " ومن معانيه فيها ما يتبين به الشيء من الدلالة وغيرها وقد جاء في لسان العرب " البيان ما بين به الشيء من الدلالة وغيرها". ويقابل هذا في اللغة اللاتينية كلمة " Datum " وتعني شيئا معطى أو مسلم به، أو شيء ما معروف أو مسلم بصحته كحقيقة أو واقعة، وجمعها "Data" وهي التي تستخدم كلاسيكيا في اللغة الإنجليزية، بينما تستخدم اللغة الفرنسية مقابلا لها كلمة معطيات "Données"وهي الكلمة التي أثر استعمالها المشرع الجزائري في مقابل كلمة "بيانات".[1]

أ- المعطيات والمعلومات:

المعلومات هي كل ما يصلح لتقديمه فائدة او كل ما يصلح ان يكون محلا للتبادل او التصرف فيه الكترونيا سواء بالتخزين او الارسال باي شكل كان من رموز او صور او بيانات يتم ارساله وتبادله عبر النظام المعلوماتي، يهدف الى امر معين ويكون ذا قيمة ما (علمية، ثقافية، مالية، اجتماعية...).[2]

[1] خليفة محمد، جريمة التواجد غير المشروع في الانظمة المعلوماتية. اطروحة دكتوراه، كلية الحقوق جامعة عنابة ،2012/2011، صفحة 86.

[2] بن فردية محمد، الاثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، كلية الحقوق، 07-12-2015، ص 32.

فالمعطيات والمعلومات عبارة عن فكرة أو معرفة أو علم، لكنها في الأولى تكون معالجة آليا وتأخذ شكلاً محدداً لا تأخذه الثانية، أي أن للمعطيات طبيعة شكلية Formel وللمعلومات طبيعة ذهنية أو فكرية. ويمكن القول بعد هذا أن كل معطيات هي معلومات وليس كل معلومات هي معطيات، ذلك أن المعلومات لا تصبح معطيات إلا بعد معالجتها آليا. وإن كان الكثير من الباحثين يطلق مصطلح " المعلومات " على الاثنين معا.

ب- المعطيات والبرامج:

الفرق بين المعطيات والبرامج يكمن في الوظيفة التي يؤديها كل واحد منهما، فالغاية من وجود المعطيات تكمن فيها في حد ذاتها، إذ ليس لها دور معين في تشغيل الحاسب الآلي، وإنما يعتبر هذا الأخير بمثابة المستودع الذي يتم فيه معالجة هذه المعطيات وتخزينها، ثم إتاحتها عند طلبها واسترجاعها، وذلك للاطلاع عليها وتكوين معرفة أو دراية توفرها هذه المعطيات. أما البرامج فالغاية منه هو الوظيفة التي يقدمها، فليس مجرد الاطلاع على البرنامج وأخذ فكرة هو الهدف منه، بل أن وجوده بالحاسب له دور وهو القيام بمختلف العمليات التي تحتويها نظام الحاسب، فهذا الأخير لا يقوم بعمله إلا عن طريق مجموعة من البرامج والتي تسمح بالقيام مختلف العمليات عند إعطائها أوامر بذلك. فقيمة المعطيات إذا والغابة منها تكمن فيما تحويه هي ذاتها، أما قيمة البرنامج فتكمن فيما يقوم به من وظائف في تشغيل الحاسب الآلي والقيام بإدخال المعطيات ومعالجتها وتخزينها واسترجاعها يتطلب وجود برنامج خاص لمختلف هذه العمليات، فلا غنى للمعطيات عن البرامج إذن.[1]

الفرع الثاني: خصائص نظم المعلومات:

من الخصائص الأساسية الواجب توفرها في نظم المعلومات نذكر منها:

[1] خليفة محمد، المرجع السابق، ص 92.

1. المرونة والديناميكية: بحيث يمكن لمستخدميه احداث التعديلات والتصحيحات اللازمة على النظام كلما أقتضى لأمر ذلك بهدف مواجهة الاحتياجات الجديدة للمنظمة من المعلومات.
2. التكامل بين العناصر: هذا يعني أن نظام المعلومات يشكل وحدة واحدة متكاملة الأمر الذي يسهل التفاعل السريع للمنظمة مع كل التغيرات الخارجية.
3. تحديد التغيرات البيئية: ويكون ذلك من خلال عملية الترصد واليقظة المستمرة لمساعدة المنظمة على اتخاد القرارات التي يمكنها من استغلال الفرص المتاحة وفي نفس الوقت تجنب العراقيل والتهديدات الخارجية.
4. التواصل: حيث يعتبر نظام المعلومات بالمنظمة شبكة اتصال داخلية تضمن ربط جميع الأقسام والمصالح ببعضها البعض وخارجية تسمح بتسهيل عملية الاتصال مع كل المتعاملين مع المنظمة.

ان توفر نظام المعلومات على هذه الخصائص، يسمح للمؤسسة بالتسيير الجيد والنجاح لأقسامها ومصلحتها، مع إمكانية حصول المسيرين لهذه الأقسام على المعلومات اللازمة والكافية بطريقة فعالة لاتخاذ القرارات المناسبة.[1]

[1] بن الصغير الربيع، خلاف محمد زكرياء، المرجع السابق، ص 16.

المبحث الثاني: تقسيم الجرائم المعلوماتية

تعتبر الجرائم المعلوماتية من أخطر الجرائم واعقدها، والتي ظهرت نتيجة تطور التقنيات والأساليب التكنولوجية، بحيث ساهمت الثورة المعلوماتية في بروز جرائم جديدة تستهدف جرائم الحاسوب وتضر بأنظمتها المعلوماتية، وعلى هذا الأساس وجب العمل على سن قوانين تقر الحماية الجنائية للمعلومات المدخلة والمرتبطة بالحواسيب. اذ أن الجرائم المعلوماتية فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الاجرام الذي بات يهدد امن المجتمعات، كونه يتميز بامتداده وانه عابر للأوطان ولا يقتصر على مكان ارتكابه فقط، والجزائر بدورها ركزت على الجريمة المعلوماتية وحاولت وضع مجموعة من الاليات الموضوعية والإجرائية لمواجهة هذا النوع من الاجرام[1]، وقد اعتمد التعريف القانوني للجريمة المعلوماتية على معيار محل الجريمة والوسيلة المستعملة فيها.

سنتطرق في هذا المبحث الى بعض الجرائم الالكترونية الواقعة على النظام المعلوماتي (المطلب الاول) وكذلك الى بعض الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي (المطلب الثاني).

المطلب الأول: الجرائم الالكترونية الواقعة على النظام المعلوماتي:

تتنوع الجرائم الماسة بالنظام المعلوماتي كمحل، ومنه سنتطرق في هذا المطلب الى الجرائم الواقعة على المكونات المعنوية أو المعلومات المسجلة بالنظام المعلوماتي (الفرع الأول).

الفرع الأول: الجرائم الواقعة على المكونات المعنوية أو المعلومات المسجلة بالنظام المعلوماتي:

[1] وهيبة رابح، " الجريمة المعلوماتية في التشريع الاجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، العدد الرابع، 2014، ص 320.

سنذكر في هذا الفرع جريمة الدخول أو البقاء عن طريق الغش المعلوماتي وكذلك الى جريمة التعامل في معطيات غير مشروعة.

أولا: جريمة الدخول أو البقاء عن طريق الغش المعلوماتي:

ان ربط أجهزة الحاسبات الالكترونية مع بعضها البعض عن طريق الشبكات المعلوماتية أدى الى سرعة انتقال المعلومات فيما بينها من جهة، و الى سهولة التطفل عليها عن طريق الدخول الى الحاسبات من جهة أخرى، فنظام المعالجة الالية قد يتعرض الى اختراق افراد غير مسرح لهم بالدخول اليها او البقاء فيها و تعد جريمة الدخول او البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات من اهم الجرائم الالكترونية و اكثرها انتشارا، لان معظم الجرائم لا يمكن اقترافها الا بعد الدخول الى نظام المعالجة الالية للمعطيات، فجريمة الدخول او البقاء هي الخطوة الأولى و الحد الفاصل بين الجاني و بين اقترافه للجرائم الالكترونية الأخرى.[1]

ولقد ورد ذكر جريمة الدخول أو البقاء عن طريق الغش الى جزء أو كل نظام المعالجة الالية للمعطيات في المادة 394 مكرر من قانون العقوبات الجزائري المعدل والتمتم.

- **جريمة الدخول عن طريق الغش الى النظام المعلوماتي:**

تضمن قانون العقوبات الجزائري هذه الصورة من الجرائم في نص المادة 394 مكرر ومدلول كلمة الدخول ينصرف الى كل الأفعال التي تسمح بالولوج الى النظام المعلوماتي او السيطرة على المعطيات والمعلومات التي يتكون منها، لكن فعل الدخول الى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع وانما يتخذ هذا الوصف انطلاقا من كونه قد تم دون وجه حق، ولا يتطلب لقيام ركنها المادي توافر نتيجة معينة وهي كذلك من الجرائم المستمرة لان سلوك الجاني يمتد فيها طالما ضل يستغل النظام بطريقة غير مشروعة.

[1] نعمان عبد الكريم، "الدخول او البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات"، حوليات جامعة الجزائر 1، كلة الحقوق ساعد حمدين، المجلد 38، العدد 02، 2024، ص 36.

- **جريمة البقاء غير المصرح به في النظام المعلوماتي:**

تناول المشرع الجزائري هذه الصورة من الجرائم كذلك في المادة 394 مكرر من قانون العقوبات، ويقصد بالبقاء التواجد داخل نظام المعالجة الالية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، يتحقق هذا البقاء مجتمعا مع الدخول الغير مشروع للنظام أو مستقلا عنه. [1]

ثانيا: أركان جريمة الدخول أو البقاء عن طريق الغش المعلوماتي:

يرتبط السلوك الاجرامي المتعلق بالدخول او البقاء في كل جزء من نظام معالجة الاليات للمعطيات عن طريق الغش بالنتيجة الاجرامية التي تظهر في صورة أثر مادي ضار لكن في أحيان أخرى يتمثل الضرر في الاعتداء على حق يحميه القانون، و يسمى النوع الأول بالجرائم المادية أو ذات النتيجة أو جرائم الضرر و هذا النوع من الجرائم يعتبر حقيقة مادية بينما يسمى النوع الثاني بالجرائم الشكلية أو غير ذات النتيجة أو جرائم الخطر، و ان الركن المادي لجريمة الدخول أو البقاء عن طريق الغش في كل او جزء من نظام المعالجة الالية للمعطيات يختلف ما اذا كانت الجريمة بسيطة أو مشددة، فإذا كانت بسيطة فإن المشرع لا يشترط تحقق النتيجة، و إذا كانت مشددة فإن المشرع يشترط توافر نتيجة الحذف أو تغيير لمعطيا المنظومة.[2]

1- الركن المادي للجريمة:

لم يحدد المشرع الجزائري الوسائل التي تتم بها عملية الدخول، معنى ذلك أن أية وسيلة تقنية تستعمل الغرض الدخول إلى النظام تتحقق بها الجريمة، فقد يتم الدخول مثلا باستخدام الجاني كلمة السر الحقيقية المملوكة للغير بعد الحصول عليها بطريقة غير مشروعة أو باستخدام

[1] حابت أمال، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15 و09-04"، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 25، 2023، ص 53.

[2] حديدان سفيان، " الدخول او البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الثاني، العدد الثامن، 2017، ص 676.

برنامج أو شيفرة خاصة. ويستوي أن يتم الدخول إلى النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فقد يعمد الجاني إلى الدخول مباشرة إلى جهاز الحاسب الآلي للضحية، كما من الممكن أن يدخل إليه بطريقة غير مباشرة أي عن بعد من خلال جهاز آخر متصل مع جهاز الضحية بواسطة شبكة الأنترنت. وقد ذهب القضاء إلى تأييد ذلك.[1]

فنص المادة 394 من قانون العقوبات الجزائري جاء عامة ولم يحدد طريق معين للدخول أو البقاء عن طريق الغش في جزء أو كل من نظام المعالجة الالية للمعطيات، فإمكانية الدخول تكون عن طريق أبواب و منافذ تقنية ممسوحة آليا يتم من خلالها استخدام برنامج مخصص، أو عن طريق عدد معين من عناوين بروتوكول الانترنت IP بهدف فحص الأبواب المفتوحة في كل جهاز للإعلام الالي و استغلال الثغرات الأمنية للدخول لنظام المعالجة الالية للمعطيات كما يستخدم مسح الأبواب من طرف مسؤولي النظام للتحقق من الثغرات الأمنية او ببساطة الأشخاص الذين يرغبون في التحقق من ان الالة التي تستضيف البيانات مؤمنة جدا و الأبواب هي نقاط دخول من خلالها يستطيع الحاسوب التواصل و تبادل المعلومات مع أجهزة الحاسوب الأخرى، يفتح الباب الافتراضي في حالة الاستعمال و يعتبر كل باب مفتوح ثغرة للنفاذ و الولوج عن طريق أي جهاز، و هو فرصة للقراصنة لدخول أو البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات.[2]

وتبرز أهمية تجريم البقاء داخل النظام المعلوماتي في الفرض الذي لا يدخل فيه الدخول في حد ذاته في دائرة التجريم، كأن يقع الدخول مثلا بطريق الصدفة أو الخطأ ويستغل الجاني الفرصة بعد ذلك ويبقى داخل النظام دون أن يكون من حقه ذلك.

[1] بطيحي نسيمة،" جريمة الدخول او البقاء غير المشروع الى النظام المعلوماتي"، مجلة الفقه القانوني والسياسي، جامعة سطيف 2، المجلد 01، العدد 01، 01-06-2016، ص 78.

[2] حديدان سفيان، المرجع السابق، ص 675.

يمكن التنويه إلى أن عبارات المادة 394 مكرر من قانون العقوبات جاءت عامة، حيث جرم المشرع الجزائري فعل البقاء دون أن يُحدد حالاته، الأمر الذي يمكن من احتواء حالات البقاء في الفرض الذي يلجأ فيه الجاني إلى البقاء داخل النظام بعد أن كان قد ولج إليه بطريق الخطأ أو الصدفة، بالإضافة إلى حالات البقاء التي تتم بعد عمليات الولوج القانونية أيضا، كمن يقدم على الدخول بطريقة قانونية إلى النظام المعلوماتي، غير أنه يتجاوز فيما بعد حدود المرخص به من طرف صاحب النظام المعلوماتي بتجاوزه للمدة المحددة مثلا أو للحدود المرخص بها.[1]

2- الركن المعنوي للجريمة في صورتها البسيطة:

وسنتكلم عن القصد الجرمي العام وكذلك مدى توافر القصد الجرمي الخاص كما يلي:

أ- القصد الجنائي العام:

يتمثل في العلم والإرادة كالتالي:

- **العلم:**

لقيام القصد الجرمي لابد ان يتصرف علم الجاني الى واقعة ذات أهمية قانونية في تكون الجريمة، أي كل واقعة يتطلبها لبناء اركان الجريمة واستكمال عناصرها، وإضافة الى ذلك لا بد ان يشمل العلم أيضا التكييف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون، بحيث إن عددا من الوقائع التي تقوم بها الجريمة لا يمثل أهمية في نظر القانون الا إذا اكتسبت وصفا معينا، فإن تجرد من هذا الوصف فقد تجرد من الأهمية القانونية ولم يعد صالحا لتقوم به الجريمة.

[1] بطيحي نسيمة، المرجع السابق، ص 79.

فإذا انتفى العلم بأحد عناصره انتفى تبعا له القصد الجرمي، كأن يعتقد بناء على أسباب معقولة أنه يقوم مثلا ببعض العمليات الحسابية عن طريق نظام المعالجة الالية ولا يعلم أنه يدخل في نظام المعالجة الالية بما يحويه من معلومات فإن القصد الجرمي في هذه الحالة يعد منتفيا لديه، كما ينتفي القصد أيضا إذا كان يعتقد أن له تصريح بالدخول أو البقاء أو ان الموقع مفتوح للجمهور، وكذلك هو الامر إذا كان الدخول عن طريق الصدفة أو السهو الخطأ، لكن في هذه الحالة ينبغي على الجاني أن يخرج فورا من النظام عند علمه بأن دخوله غير مصرح به او بقاءه، فإذا امتنع عن ذلك وقع تحت طائلة العقاب لقيام القصد الجرمي لديه منذ اللحظة التي تحقق فيها العلم.[1]

- **الإرادة:**

تتمثل الإرادة في كونها: « حالة ذهنية و نفسية يكون عليها الجاني ساعة إقدامه على ارتكاب الجريمة، و يمكن تصور هذه الحالة بعزم الجاني على ارتكاب الجريمة أو اتخاذ قرار بتنفيذها، ثم اصدار الامر الى أعضاء جسمه للقيام بالأفعال المكونة لها، و قيادة هذه الأعضاء الى تحقيق النتيجة المطلوبة. و إرادة الجاني في القصد الجرمي على هذا النحو يجب ان تتجه الى ارتكاب الفعل، و لكن في الجرائم ذات النتيجة لا يتكون القصد الجرمي الا إذا اتجهت الإرادة أيضا الى إحداث النتيجة » .

وعلى ذلك، فاذا توافر القصد الجرمي بعنصريه العلم والإرادة، فانه لا محل للاعتداد بالباعث على ارتكاب الجريمة بسبب من أن الباعث لا أثر له في قيام الجريمة – كأصل عام إعمالا للقواعد العامة – ، و لذلك تقوم الجريمة في حق الجاني بتوافر القصد الجرمي و لو كان باعثه على الدخول – كما رأينا – مجرد محاولة قهر النظام و التفوق على الوسائل التقنية.[2]

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 235.

[2] رشيدة بوكر، نفس المرجع، ص 236.

3- العقوبات المقررة للجريمة في التشريع الجزائري:

قرر المشرع الجزائري في المادة 394 مكرر من قانون العقوبات لجريمة الدخول أو البقاء داخل النظام عقوبة تقدر ب الحبس من ثلاث(3) أشهر الى سنة(1) وغرامة مالية تقدر ب 50000 دج الى 1000000 دج. [1]

حيث نصت المادة 394 مكرر6 من قانون العقوبات على عقوبات تكميلية لهذه الجريمة تتضمن ما يلي : « مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على اغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها» .

كما ان المشرع الجزائري عاقب على الاعمال التحضيرية للجريمة تنص المادة 394 مكرر 5 من قانون العقوبات على انه: « كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم(التي من بينها جريمة الدخول أو البقاء) و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها» .[2]

و نصت المادة 394 مكرر من قانون العقوبات الجزائري على انه« يعاقب ب..، كل من يدخل او يبقى عن طريق الغش ...أو يحاول ذلك » ،كما ذكرت المادة 394 مكرر7 من قانون العقوبات على أن عقوبة الشروع في الجريمة هي نفس العقوبة المقررة للجريمة التامة.

---

[1] المادة 394 مكرر من قانون العقوبات أمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966، القسم السابع مكرر الذي يتضمن المساس بأنظمة المعالجة الالية للمعطيات، جريدة رسمية عدد 49 صادر في 21 صفر عام 1386 الموافق 11 يونيو 1966، معدّل ومتمم.

[2] المادة 394 مكرر5 من نفس القانون.

حيث تضمنت كذلك المادة 394 مكرر4 على مساءلة الشخص المعنوي على أنه« يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم (و التي من بينها جريمة الدخول أو البقاء داخل النظام) بغرامة تعادل خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي » .

و لقد نصت المادة 394 مكرر فقرة 2 من قانون العقوبات على أنه« تضاعف العقوبة إذا ترتب على ذلك (أي على فعل الدخول أو البقاء) حذف أو تغيير لمعطيات المنظومة » كما نصت ذات المادة في الفقرة الثالثة 3 على أنه« و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر الى سنتين و الغرامة من 50.000 دج الى 150.000 دج » ، بالإضافة الى ما أقرته المادة 394 مكرر3 من قانون العقوبات و المتعلق بالمساس بمؤسسات الدولة.[1]

ثانيا: جريمة التعامل في معطيات غير مشروعة:

تعرف جريمة التعامل في معطيات غير مشروعة في القانون الجزائري بانها: أي حيازة او تداول او استخدام لبيانات او معلومات تم الحصول عليها بطريقة غير قانونية وهي مجرمة في المادة 394 مكرر من قانون العقوبات الجزائري.

1- الركن المادي:

يتكون الركن المادي من مجرد السلوك الإجرامي دون النتيجة الإجرامية.

أ- السلوك الإجرامي:

يقوم الركن المادي لجريمة التعامل في معطيات غير مشرعة على مجرد توافر السلوك الإجرامي الذي يتخذ صورتين اثنتين يمكن توضيحهما بشكل مختصر كالاتي:

[1] المادة 394 مكرر، المادة 394 مكرر2، المادة 394 مكرر4، من قانون العقوبات الجزائري.

- **التعامل في معطيات صالحة لارتكاب جريمة:**

تجرم المادة 394 مكرر 02 في البند الأول منها مجموعة من الأفعال الخطرة التي لو تركت بدون تجريم لأدت إلى حدوث جرائم أخرى، هذه الأفعال تشمل كافة أشكال التعامل الواقعة على معطيات لاسيما المتعلقة بقطاع البنوك، والتي تسبق عملية استعمال هذه المعطيات في ارتكاب الجريمة، فالمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل إلى يد الجاني فيرتكب بها جريمته وهذه المراحل تبدأ من تصميم هذه المعطيات والبحث فيها وتجميعها وصولا إلى جعلها في متناول الغير وتحت تصرفه وذلك بتوفيرها أو نشرها أو الاتجار فيها. ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداهما فقط، وهذه الأفعال هي التصميم والبحث والتجميع والتوفير (الوضع تحت التصرف أو العرض) والنشر والاتجار. [1]

- **التعامل في معطيات متحصلة من جريمة:**

هي الصورة الثانية من جريمة التعامل في معطيات غير مشروعة، وتتحقق بواحد من أربعة أفعال هي حيازة معطيات متحصلة من جريمة (دخول أو بقاء غير مصرح بهما أو التلاعب بالمعطيات) أو إفشاء هذه المعطيات أو نشرها أو استعمالها، أي أنه يكفي تحقق واحد من هذه الأفعال فقط حتى تقوم الجريمة.

ب- النتيجة الإجرامية:

جريمة التعامل في معطيات غير مشروعة هي من جرائم الخطر لا يتطلب لقيامها حدوث نتيجة معينة، فالمشرع جرم تلك الأفعال بوصفها أفعال خطرة يمكن أن تؤدي إلى ضرر فعلي.[2]

[1] محمد خليفة، " خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها"، دراسات وأبحاث، جامعة 08 ماي 1945-قالمة، المجلد1، العدد 1، 15-09-2009، ص 384.

[2] محمد خليفة، نفس المرجع، ص 385.

2- الركن المعنوي:

جريمة التعامل في معطيات غير مشروعة جريمة عمدية، ويستفاد ذلك من عبارة المادة 394 مكرر02 "عمدا وعن طريق الغش".

ولدينا أن الجريمة في صورتها الأولى (التعامل في معطيات صالحة لارتكاب جريمة) تتطلب قصدا خاصا هو قصد الإعداد أو التمهيد لاستعمالها في ارتكاب جريمة.

أما الجريمة في صورتها الثانية (التعامل في معطيات متحصلة من جريمة) فلدينا أنه يكفي لقيامها توافر القصد الجنائي العام.[1]

3- العقوبة المقررة لجريمة التعامل في معطيات غير مشروعة:

تعاقب المادة 394 مكرر 2 من قانون العقوبات على هذه الجريمة بالحبس من شهرين إلى 03سنوات وبالغرامة من مليون(1000000) إلى خمسة ملايين(5000000) دينار جزائري. كما يعاقب عليها بالعقوبة التكميلية المقررة على كل الجرائم السابقة.[2]

المطلب الثاني: بعض الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي:

تجسد الاستعمالات الواسعة للنظم المعلوماتية خاصية للحياة اليومية للأفراد ونشاط المؤسسات، وإزاء ما يعرقل السير الحسن لتلك الأنظمة أو يحولها عن الغرض منها، تقف الجرائم الالكترونية التي وسيلتها النظام المعلوماتي، حيث تتنوع هذه الجرائم ما بين الجرائم الاقتصادية، أو قرصنة المعلومات أو ذات طابع سياسي، وقد تقع هذه الجرائم على أشخاص طبيعية وأخرى معنوية،[3] ومنه سنتطرق في هذا المطلب الى بعض الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي.

---

[1] محمد خليفة، المرجع السابق، ص 385.

[2] المادة 394 مكرر 2 من قانون العقوبات الجزائري.

[3] مونة مقلاتي، راضية مشري، " الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية"، مجلة أبحاث قانونية وسياسية، جامعة 8 ماي 1945–قالمة، المجلد 06، العدد 01، جوان 2021، ص 502.

الفرع الأول: جريمة تبييض الأموال المرتكبة على الانترنت:

بالنسبة للمشرع الجزائري فلم يعرف جريمة تبييض الأموال في النصوص التشريعية والتنظيمية التي أصدرها، بحيث استعمل مصطلح تبييض الأموال بدلا من مصطلح غسيل الأموال حيث نصت المادة (389 مكرر) من القانون رقم 04-15 على: "يعتبر تبييض للأموال":

- تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروع لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته.

- إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، مع علم الفاعل بأنها عائدات إجرامية.

- اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية.

- المشاركة في ارتكاب أي من الجرائم المقرر وفقا لهذه المادة، أو التواطؤ أو التآمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه.[1]

كما نص أيضا على تجريم نفس الأفعال المكونة للجريمة في المادة (02) من القانون رقم 05-01 مؤرخ في 2005/02/06، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.[2] وتقوم هذه الجريمة على ركنين أساسيين هما: الركن المادي والركن المعنوي.

1- الركن المادي للجريمة:

[1] المادة 389 مكرر من قانون رقم 04-15، المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية رقم 71/2004.

[2] المادة 2 من قانون رقم 05-01، المؤرخ في 27 ذي الحجة 1425 الموافق 6 فبراير 2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، الجريدة الرسمية رقم 83/2004.

ينحصر السلوك الإجرامي وفق نص المادة (389 مكرر) في أربعة صور نتناولها كما يأتي:

الصورة الأولى: تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصادر غير المشروعة لتلك الممتلكات أو مساعدة أي شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعلته. تتألف هذه الصورة من عنصرين هما: العنصر الأول فعل إيجابي يتمثل في تحويل ممتلكات عائدة من جريمة أو نقلها وتختلف طريقة تحويل المال أو نقله باختلاف طبيعة المال محل الجريمة، فإذا كان المال نقدا يتم تحويله عن طريق صرفه بتحويله إلى عملة أجنبية، أو في شراء شقة...إلخ، كما يمكن أن يكون المال في صيغة إلكترونية يتم تحويله إلكترونيا من حساب إلى آخر. أما العنصر الثاني يتمثل في الغرض من تحويل الممتلكات أو نقلها فيستهدف الجاني من وراء ذلك غايتين هما: إما إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات، وإما مساعدة شخص متورط في ارتكاب الجريمة الأصلية التي تأتت منها هذه الممتلكات على الإفلات من الآثار القانونية لفعله. وقد يتمثل التحويل في كل تصرف يقع على الأموال أو الممتلكات أو المتحصلات النقدية أو العينية، ومثال ذلك الإيداع، البيع، الإقراض، المبادلة...إلخ.[1]

الصورة الثانية: إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو الحقوق المتعلقة بها، اذ ان المشرع الجزائري يشترط ان يكون الغرض من فعلي التحويل او النقل هو إخفاء مصدرها غير المشروع او التمويه عن المصدر غير المشروع لتلك الأموال، ومن بين صور ذلك نجد اقتناء الأموال الناتجة عن جريمة او

[1] يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، سنة 2019، ص 287.

اكتسابها عن طريق الهبة او الوديعة، او ادخال أموال غير مشروعة ضمن نتائج او أرباح شركة قانونية للتمويه عن مصدر الأموال محل التبييض.[1]

الصورة الثالثة: اكتساب الممتلكات أو حيازتها أو استخدامها مع علم الشخص القائم بذلك وقت تلقيها أنها تشكل عائدات إجرامية. إن المقصود باكتساب الممتلكات هو تلقي الأموال أو المتحصلات على سبيل التكسب أو الترويج كما أن لفظ الاكتساب هنا عام، فلا يشترط أن يكون الحصول على المال من الجريمة المصدر بطريق مباشر، بل يمكن الحصول عليها بطريق غير مباشر مثل الأرباح الناتجة من الأموال المتحصلة من الجريمة المصدر، أما الحيازة فهي الاستئثار بالشيء على سبيل الملك دون الحاجة للاستيلاء عليه، فيكفي لاعتبار الشخص حائزا ولو لم تكن له السيطرة المادية مثل إجراء قروض وهمية.

الصورة الرابعة: المشاركة في ارتكاب أي من الجرائم المقرر وفقا لهذه المادة، أو التواطؤ أو التأمر على ارتكابها ومحاولة ارتكابها والمساعدة والتحريض على ذلك وتسهيله وإسداء المشورة بشأنه بعد تبييضا للأموال وأن كل فعل من هذه الأفعال يصلح أن يشكل صورة من صور هذه الجريمة.

كما تتفق جل التشريعات المجرمة لظاهرة تبييض الأموال، أن هذه الجريمة تابعة تتطلب لاكتمال بنيانها القانوني وقوع جريمة أولية أو أصلية هي مصدر الأموال غير المشروعة، وهي العنصر المفترض لجريمة تبييض الأموال، وعلى ضوء ذلك فإن الجريمة الأولية هي: كل نشاط إجرامي فعل أو امتناع عن فعل تحصلت منه بطريقة مباشرة أو غير مباشرة أموالا غير مشروعة تعتبر محلا لجريمة غسيل الأموال، هذه الجريمة السابقة هي المصدر الجريمة التبييض.[2]

---

[1] خفيف جمال، "قراءة قانونية لجريمة تبييض الأموال (خصوصية أركانها وإجراءات مواجهتها)"، مجلة صوت القانون، كلية الحقوق، السعيد حمدين، جامعة الجزائر، المجلد التاسع، العدد 01، 2022، ص 434.

[2] يزيد بوحليط، المرجع السابق، ص 289.

2- الركن المعنوي للجريمة:

فجريمة تبييض الأموال لا تختلف عن الجرائم الأخرى، فهي لا تتطلب لقيامها أن يأتي الجاني فحسب أحد صور السلوك الإجرامي التي بتوافر من خلالها الركن المادي وإنما ينبغي أيضا توفر الركن المعنوي، الذي يتطلب القصد الجنائي بالدرجة الأولى سواء القصد العام أو القصد الخاص باعتبار أن هذه الجريمة من الجرائم العمدية تقوم على أساس القصد الجنائي فمن المتعذر وقوعها عن طريق الخطأ أو الإهمال، بمعني أنه يستوجب لغرض مسائلة الجاني أن يثبت لديه توافر القصد العام والقصد الخاص لكي تقوم المسؤولية القصدية، فنجد المشرع اخذ بالقصد العام بعنصريه العلم و الإرادة، و القصد الخاص و يظهر ذلك من خلال نص المادة 389 مكرر من قانون العقوبات.[1]

3- العقوبات المقررة للجريمة:

تنصت المادة (389 مكرر1) على أنه:" يعاقب كل من قام بتبييض الأموال بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 1.000.000 دج إلى 3.000.000دج".

لقد تبعت العقوبات الاصلية عقوبات تكميلية حيث تنص المادتان (389 مكرر5 و389 مكرر6) على تطبيق عقوبة واحدة أو أكثر من العقوبات التكميلية على الشخص الطبيعي.[2]

أ- الظروف المشددة:

نصت المادة (389 مكرر2) على أنه:" يعاقب كل من ارتكب جريمة تبييض الأموال على سبيل الاعتياد أو باستعمال التسهيلات التي يمنحها نشاط مهني أو في إطار جماعة إجرامية،

[1] حداوي صبرينة، زرورو عمر، اركان جريمة تبييض الأموال، مذكرة لنيل شهادة الماستر في القانون، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، قسم القانون، تيزي وزو، 2017/09/26، ص 54.

[2] المواد 389 مكرر1، 389 مكرر5 و389 مكرر6، من قانون العقوبات الجزائري.

بالحبس من عشر (10) سنوات إلى خمس عشر (15) سنة وبغرامة من 4.000.000 الى 8.000.000 دج".

- **المصادرة:**

طبقا للمادة (389 مكرر4) من قانون العقوبات حيث تنص: " تحكم الجهة القضائية المختصة بمصادرة الأملاك موضوع الجريمة المنصوص عليها في هذا القسم، بما في ذلك العائدات والفوائد الأخرى الناتجة عن ذلك في أي يد كانت، إلا إذا أثبت مالكها أنه يحوزها بموجب سند شرعي وأنه لم يكن يعلم بمصدرها غير المشروع..." [1].

الفرع الثاني: جريمة التعدي الالكتروني على حرمة الحياة الخاصة:

لقد اختلفت أساليب ارتكاب الجرائم في ظل الثورة الرقمية لشبكات التواصل الاجتماعي، فعلى الرغم من وجود مزايا لهذه الشبكات، إلا لأنها ساهمت في ظهور طابع جديد من الجرائم، فانتقلت من جرائم تقليدية إلى جرائم المعلوماتية التي لم تعد منحصرة في السرقة والاحتيال المعلوماتي، بل وصلت إلى جرائم من نوع أخر.[2]

سنتطرق الى أحد هذه الجرائم في هذا الفرع كما يلي:

1- جريمة التقاط الأحاديث والصور دون رخصة:

نصت المادة (303 مكرر) من قانون العقوبات الجزائري على...، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:

– بالنقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

---

[1] المواد 389 مكرر2، 389 مكرر4 من قانون العقوبات الجزائري.

[2] زروقي عاسية،" جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، مجلة القانون والعلوم السياسية، جامعة غرداية، المجلد 08، العدد 02، 2022، ص 13.

– التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه...".[1]

أ– الركن المادي للجريمة:

يتمثل الركن المادي لجريمة التقاط الأحاديث والصور دون رخصة في العناصر الآتية:

– تعلق الأفعال بالحياة الخاصة للفرد.

–التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية.

– التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص.

–استخدام الوسائل التقنية مهما كان نوعها وحدوث الفعل بغير رضا المجني عليه.[2]

عرفته المادة 8/02 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه:" مشاهدة البيانات أو المعلومات أو الحصول عليها". وبهذا المعنى ينصرف فعل الالتقاط إلى الحصول على ما جرى بين الأشخاص من كلام أو ما تفوه به الفرد سر او دون علمه، أما التسجيل يعني حفظ الحديث على جهاز أو أي وسيلة أخرى معدة لذلك، بقصد الاستماع إليه فيما بعد، أما النقل في قصد به نقل الحديث أو المكالمة الذي يتم الاستماع إليهما أو تسجيلهما من المكان الذي تم فيه إلى مكان آخر غيره، وذلك بأي وسيلة تقنية كما تتم هذه الأفعال دون رضا المجني عليه حال وجوده في مكان خاص.[3]

من جهة أخرى لقد اشترط المشرع الجزائري المكان الذي تقع فيه هذه الجريمة مكانا خاصا، وبالتالي تجد أنه قد اعتنق فكرة المكان الخاص كمعيار التحديد نطاق الحماية الجزائية، وهو نفس المسلك الذي انتهجه المشرع الفرنسي في نص المادة 226–1 من قانون العقوبات

[1] المادة 303 مكرر من قانون العقوبات الجزائري.

[2] يزيد بوحليط، المرجع السابق، ص 222.

[3] فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الاخوة منتوري قسنطينة، الجزائر، 2012، ص 251.

الجديد. فما دام القانون يحمى حرمة للشخص فهي لا تتوافر إلا في المكان الخاص. وتنسحب حماية القانون على كل من يوجد في هذا المكان أيا كانت صفته، أي سواء كان مالكا أو مستأجرا أو زائرا أو موجودا فيه بصفة عارضة لأي سبب كان.[1]

أما بخصوص الوسائل المستعملة، لم يشترط المشرع الجزائري في جريمة التقاط الصورة كما في جريمة التقاط الأحاديث الخاصة وسيلة معينة أو جهاز أياً كان نوعه لارتكاب الأفعال التي تشكل السلوك الإجرامي، إذ نص في الفقرة الأولى من نص المادة 303 مكرر أن فعل الالتقاط يحصل:" بأية تقنية كانت ...". وقد أخذ ذلك من التشريع الفرنسي في نص المادة 226-1 بعد تعديله لقانون العقوبات. فالمشرع يكون بذلك قد وسع من نطاق الحماية الجنائية للحق في الصورة.

ومما تجدر الإشارة إليه، أن الرضاء بالتصوير لا يعنى ضرورة الرضاء بنشرها إلى الجمهور، ذلك للاختلاف بين الأمرين، فقد يرضى الشخص بتصويره ولا يرضى بنشر صورته، لكن قد يستنتج رضاء ضمني بالنشر من الظروف التي تمت فيها عملية التصوير، ومن طبيعة الشخص التي التقطت صورته، وطبيعة الصورة ومكان التصوير وعلى أنه ليس كل رضاء بالنشر ولو كان صريحاً يكون مشروعاً، فكل رضاء بنشر الصورة التي تكون مخالفة للنظام والآداب العامة يقع باطلاً مطلقاً كأن لم يكن، بل يعتبر حريمة معاقب عليها.[2]

ب- الركن المعنوي للجريمة:

جريمة التقاط الأحاديث والصور بدون رخصة جريمة عمدية بدليل قول المشرع:" ... كل من تعمد المساس بحرمة الحياة الخاصة ..."، إذ تتطلب القصد الجنائي العام الذي يقوم على

[1] عبد القادر رحال،" البناء القانوني لجريمة التقاط الصورة ونشرها في التشريع الجزائري والفرنسي-دراسة موضوعية إجرائية مقارنة "، مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر1، المجلد 15، العدد 01، 2022، ص 354.

[2] عبد القادر رحال، نفس المرجع، ص ص 255-256.

عنصر العلم الجاني بأن هذه الأفعال تشكل جريمة، إضافة إلى اتجاه إرادته للقيام بالسلوك المجرم.[1]

والعنصر الثاني للقصد الجنائي يتمثل في الإرادة، فينبغي أن تتجه مباشرة إلى السلوك الإجرامي فلا يكفي لقيامها بطريق الخطأ، وعليه فلا تقع الجريمة وفقاً لنص المادة 303 مكرر من يترك سهواً جهازاً للتصوير أو البث التلفزيوني، فيحصل النقاط الصور الأشخاص.[2]

ت- العقوبات المقررة للجريمة:

الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000دج إلى 300.00 دج.

- **العقوبة على الشروع:**

معاقب عليه بنص المادة (303 مكرر الفقرة 3):"... يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة ويضع صفح الضحية حدا للمتابعة الجزائية".[3]

- **العقوبات التكميلية:**

نصت عليها المادة (303 مكرر2):" يجوز للمحكمة أن تحظر على المحكوم عليه من أجل الجرائم المنصوص عليها في المادتين (303 مكرر -303 مكرر1) ممارسة حق أو أكثر من الحقوق المنصوص عليها في المادة (09 مكرر1) لمدة لا تتجاوز خمس (5) سنوات. كما

[1] دكتور يزيد بوحليط، المرجع السابق، ص 223.

[2] عبد القادر رحال، المرجع السابق، ص 357.

[3] المادة 303 مكرر الفقرة 3 من قانون العقوبات الجزائري.

يجوز لها أن تأمر بنشر حكم الإدانة طبقا للكيفيات المبينة بالمادة (18) من هذا القانون، ويتعين دائما الحكم بمصادرة الأشياء التي استعملت لارتكاب الجريمة.[1]

[1] المواد 09 مكرر 1، 303 مكرر-303 مكرر 1، 303 مكرر 2، من نفس القانون.

الفصل الثاني

إجراءات المعاينة، الحجز والتفتيش في الجرائم المعلوماتية

في ظل التطور المتسارع للمنظومات المعلوماتية واتساع نطاق الجرائم الالكترونية، برز أهمية الإجراءات الرقابية والتحقيقية كأدوات حيوية لضمان أمن السيبراني وحماية الحقوق والمصالح، وتأتي إجراءات المعاينة والحجز والتفتيش ضمن الإطار القانوني والفني الذي يهدف الى مواجهة التحديات الأمنية المعقدة في البيئة الرقمية، حيث تتطلب هذه الإجراءات دقة متناهية في التنفيذ لضمان فعاليتها من ناحية، واحترامها للضوابط القانونية وحقوق الافراد من ناحية أخرى.

وتكسب هذه الإجراءات طابعا خاصا في البيئة الرقمية، نظرا لطبيعة الأدلة الالكترونية الهشة وقابليتها للتعديل أو الاتلاف، مما يستلزم تبني اليات تقنية وقانونية دقيقة للحفاظ على سلامة الأدلة وضمان قبولها أمام القضاء. كما يجب أن تنفذ هذه الإجراءات في إطار موازنة بين متطلبات التحقيق ومكافحة الجريمة من جهة أخرى.

لذا، فان ضبط هذه الإجراءات وفق معايير قانونية واضحة واليات تنفيذ محكمة يعد ركيزة أساسية لتعزيز الثقة في المنظومة العدلية الرقمية، وضمان فعالية التدخلات الأمنية دون تجاوز الحدود المرسومة قانونيا وأخلاقيا. سنتطرق في هذا الفصل الى دراسة إجراءات المعاينة، الحجز (المبحث الاول) و الى التفتيش الالكتروني و حجية الدليل الالكتروني (المبحث الثاني).

المبحث الأول: إجراءات المعاينة والحجز

حققت الثورة التكنولوجية قفزة هائلة في مجال تقنية المعلومات، وبالمقابل أدى سوء استخدامها الى ظهور جرائم مستحدثة عرفت بالجرائم المعلوماتية، مما صعب من مكافحتها نظرا لطبيعتها وخصوصية إجراءات التحقيق فيها، عبر هذه البيئة الافتراضية لتعقب المجرم المعلوماتي.

في هذا الصدد، يتضمن نص القانون رقم: 09-04 المؤرخ في 05 اوث 2009 القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، على جملة من القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية وحجز المعطيات[1]. سنتطرق في هذا المبحث الى اجراء المعاينة(المطلب الأول)و الى اجراء الحجز(المطلب الثاني).

المطلب الأول: اجراء المعاينة:

المعاينة من اهم مراحل البحث والتحقيق في الجرائم المستحدثة نظرا لما يمكن ان توفره من ادلة اثبات، وتزداد أهميتها عند اثبات الجرائم الالكترونية لكونها تقوم على معاينة جملة من البرمجيات أو الأقراص وكل ما يتعلق بجهاز الحاسب الالي، حيث تكتسي طبيعة خاصة في هذا المجال لكونها تقوم على فحص حسي مباشر لمكان او شخص او أي شيء له علاقة بالجريمة لإثبات حالته، والتحفظ على كل ما يفيد من أشياء في كشف الحقيقة.

الا انه ورغم تلك الأهمية، فان السلطات المختصة التي تقوم بها لا تزال تواجه صعوبات في بعض الأحيان، كون الجرائم الالكترونية قد تطول فيها الفترة الزمنية بين وقوعها واكتشافها مما يعرض الاثار الناجمة عنها الى المحور او التلف او العبث[2]. وسنتطرق في هذا المطلب الى

---

[1] يزيد بوحليط، " تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري"، التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة، العدد 48، ديسمبر 2016، ص 82.

[2] ديابلو محمد نجيب، الجريمة الالكترونية وحجية الدليل الرقمي في الاثبات الجنائي، الطبعة الأولى، المركز المغاربي- شرق أدنى للدراسات الاستراتيجية، المملكة المتحدة -بريطانيا-، جانفي 2024، ص 132.

مفهوم الانتقال و المعاينة (الفرع الاول) و الى الانتقال و المعاينة التقنية لمسرح الجريمة الالكترونية (الفرع الثاني).

الفرع الأول: مفهوم الانتقال والمعاينة:

لم يتطرق المشرع الجزائري الى مفهوم الانتقال و المعاينة، و بالرجوع الى الفقه الجنائي، يعتبر الانتقال عملا هاما من اعمال التحقيق يتم بقصد جمع الأدلة و فحصها لكشف حقيقة الجريمة و يتطلب ذلك ان ينتقل المحقق من مقر عمله الى مكان اخر قد يكون مسرح الجريمة لإجراء عمل من أعمال التحقيق، حيث يتم الانتقال بهدف اجراء معاينة او بهدف القيام بعمل اخر كالتفتيش و الضبط و سماع اقوال الشهود في بعض الأحوال، اما بخصوص المعاينة فهناك عدة تعاريف لها، فيقصد بها:" اثبات حالة الأماكن و الأشخاص و كل ما يفيد في كشف الحقيقة " او هي :" اثبات حالة الأشياء و الأشخاص و غيرها و هي تستلزم الانتقال الى محل وجود الشيء او الشخص الذي ينبغي معاينته "، كما تعرف أيضا على انها:" رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته و ضبط كل ما يلزم لشف الحقيقة "، كما اعتبرها جانب من الفقه على انها:" اثبات مباشر و مادي لحالة الأشخاص و الأمكنة ذات الصلة بالحادث عن طريق رؤيتها او فحصها فحصا حسيا مباشرا ".[1]

تعرف المعاينة بأنه إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في الكشف عن الحقيقة، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز السلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت في ذلك ضرورة لإجلاء الحقيقة أو بناء على طلب من الخصوم، والأصل أن تجري المعاينة بحضور أطراف الدعوى الجزائية

[1] يزيد بوحليط، المرجع السابق، ص 320.

غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة.[1]

ان للمعاينة أهمية بالغة في الكشف عن الحقيقة حيث تتلخص في البحث عن العلاقة بين اثار الجريمة والانسان الذي تركها وتسبب فيها، حيث تعتبر شاهدا شكليا وموضوعيا له وزنه في التحقيق.

ان الأصل في المعاينة هي اجراء من إجراءات التحقيق، باستثناء حالات التلبس بارتكاب جناية اين يجوز لضباط الشرطة القضائية القيام بالانتقال الى مسرح الجريمة واتخاذ التحريات اللازمة. كما يمكن للمحكمة ان تقوم بإجراء المعاينة إذا ما رات في ذلك سبيلا لكشف الحقيقة سواء كان ذلك من تلقاء نفسها او بناء على طلب الخصوم. وحتى تأتي المعاينة بثمارها المرجوة سواء ما تعلق باكتشاف الأدلة او اثبات حالة الأشخاص والأمكنة، نصت جل التشريعات على توقيع جزاءات جنائية على كل من يحدث تغييرا او تعديلا في مسرح الجريمة قبل قيام سلطات التحقيق بإجراء المعاينة.[2]

الفرع الثاني: الانتقال والمعاينة التقنية لمسرح الجريمة الالكترونية:

تتم المعاينة في جرائم الانترنت كأي جريمة أخرى عن طريق الانتقال الى محل واقعة الاجرامية، الا ان الانتقال هنا لا يكون الى العالم المادي، وانما الى العالم الافتراضي، وهذا ما يطرح اشكال اخر هو: كيف يتم ذلك الانتقال والمعاينة؟.[3] سنتطرق في هذا الفرع الى الإجراءات

[1] رزيق محمد، إجراءات المعاينة التفتيش والحجز داخل المنظومة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة آكلي محند أولحاج، كلية الحقوق والعلوم السياسية، قسم القانون العام، البويرة، 2018-2019، ص 09.

[2] يزيد بوحليط، المرجع السابق، ص 322.

[3] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دون طبعة نشر، دار الفكر الجامعي، الإسكندرية، 2013، ص 217.

المتبعة اثناء المعاينة والى كيفية الانتقال الى مسرح الجريمة الالكترونية وكذلك الى المعاينة التقنية لمسرح الجريمة الالكترونية.

أولا: الإجراءات المتبعة اثناء المعاينة:

قصد نجاح المعاينة لابد من مراعاة الجوانب الفنية الاتية [1]:

- تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز على تصوير الأجزاء الخلفية للحاسوب وتسجيل وقت وتاريخ ومكان التقاط كل صورة.
- العناية البالغة بملاحظة الطريق التي تم بها اعداد النظام، واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، حتى يمكن اجراء عمليات المقارنة والتحليل.
- حصر أجهزة الحاسوب الموجودة في مكان المعاينة بصفة دقيقة، وفي حالة وجود شبكة للاتصالات، يجب البحث أولا على خادم الملف (File Server) وذلك لأجل تعطيل حركة الاتصالات.
- عدم نقل أي معلومة من مسرح الجريمة، الا بعد التأكد من خلو المحيط الخارجي لموقع الحاسوب من أي مجال مغناطيسي يمكن ان يتسبب في محو البيانات المسجلة.
- التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والأشرطة والأقراص المضغوطة...إلخ.
- التحفظ على مستندات الادخال والمخرجات الورقية للحاسوب ذات الصلة بالجريمة.
- ربط الأقراص الكمبيوترية التي تحتوي على الأدلة مع جهاز يمنع الكتابة والتسجيل عليها بما يسمح للمحققين قراءة البيانات الموجودة فيها دون تعديلها.

[1] يزيد بوحليط، المرجع السابق، ص 326.

- قصر مباشرة المعاينة على المحققين الذين تتوفر لديهم الكفاءة العلمية والخبرة التقنية في مجال المعلوماتية واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحتويها مسرح الجريمة الالكترونية.
- ضبط وتحريز الدعائم الاصلية للبيانات وعدم الاكتفاء بضبط النسخ، كما يجب مراعات ظروف تخزينها كعدم وضعها على مقربة من محطة ارسال لاسلكي أو وضعها في أماكن تحتوي على الغبار، بما يؤدي الى اتلافها.
- منع أي ادخال جديد على الجهاز او ذاكرته، وضبط برنامج التغذية الخاصة (Software) بالاستعانة بنظام التحميل (Downloading).

إن المعاينة التقليدية لمسرح الجريمة الإلكترونية غير كافية، فدائما ما يكون الدليل الجنائي في الجريمة التقليدية مرئيا ذو طبيعة مادية ، بحيث يمكن للقائمين على عملية التحقيق بمعاينة مسرح الجريمة وضبط أي دليل يفيد في الكشف عن ملابساتها ، ولكن في الجريمة المعلوماتية تقع في بيئة مختلفة تماما عن بيئة الجريمة التقليدية ، إذ تكون فيها الأدلة عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية مشكلة معلومات وبيانات رقمية في العالم الافتراضي ومنه فعدم رؤية الدليل الجنائي الرقمي يشكل العديد من الصعوبات من خلال جمعه وتحليله مما يتوجب توفر لدى المحققين الفنيين دراية كافية ومهارة كبيرة في التعامل مع هذا النوع من الأدلة.[1]

ثانيا: كيفية الانتقال الى مسرح الجريمة الالكترونية:

تتم معاينة الجريمة الالكترونية بالانتقال الى مسرح الجريمة الالكترونية، غير ان الانتقال لا يتم بالضرورة عبر العالم المادي، وانما عبر العالم الافتراضي (Cyber Space). وعليه

[1] خطوي مسعود، عكوش حنان،" خصوصية الدليل الالكتروني"، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الاغواط، مجلد السابع، العدد الأول، 2023، ص 1066.

يستطيع ضابط الشرطة القضائية الانتقال الى العالم الافتراضي لمعاينة الجريمة الالكترونية كما يأتي[1]:

- يستطيع ضابط الشرطة القضائية الانتقال الى العالم الافتراضي لمعاينة مسرح الجريمة من خلال حاسوبه الموجود بمكتبه.
- يمكن لضابط الشرطة القضائية اللجوء إلى مقهى الانترنت.
- يمكن لضابط الشرطة القضائية اللجوء الى مزود خدمة الانترنت (Internet Server Provider)الذي يعتبر أفضل مكان يمكن من خلاله اجراء المعاينة.

ثالثا: المعاينة التقنية لمسرح الجريمة الالكترونية:

ان معاينة مسرح الجريمة الالكترونية يختلف عن غيره من الجرائم بسبب طبيعة الدليل الالكتروني غير المرئي والقابل للمحو، لذا ينبغي قبل الانتقال لمسرح الجريمة القيام بالخطوات الاتية [2]:

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها فنيا.
- اعداد خريطة للموقع المتوقع الاغارة عليه والتأكد من تأمين وصلاحية الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة.
- اعداد فريق متخصص من الخبراء ورجال الامن والضباط واعطائهم الوقت الكافي للاستعداد فنيا عن طريق وضع خطة عملية لضبط أدلة الجريمة وقت معاينتها.

[1] قلات سومية، عبد العالي حاحة، " مقتضيات المعاينة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية، جامعة بسكرة، المجلد 11، العدد 1، الجزائر، 2023، ص 534.

[2] يزيد بوحليط، المرجع السابق، ص 325.

- الحصول على الاحتياجات الضرورية من أجهزة و برامج للاستعانة بها في الفحص والتشغيل مثل: برامج معالجة الملفات (Xtree Pro Gold)و برامج النسخ (Lap Link)و برامج انتاج صور مطابقة عن القرص الصلب (Encase)، و الذي تستخدمه المباحث الفدرالية الامريكية في التحقيقات الجنائية و يطلق عليه الخبراء (حقيبة الأدلة الرقمية) .
- تأمين عدم انقطاع التيار الكهربائي المفاجئ لان ذلك يتسبب في محو المعلومات من الذاكرة، وبالتالي ضياع كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة.

المطلب الثاني: إجراء الحجز

لقد تناول المشرع الجزائري القواعد الخاصة بضبط البيانات المعلوماتية وفقا للقانون09-04 تحت تسمية " حجز المعطيات المعلوماتية"، الذي يعتبر الخلاصة النهائية التي ينتهي الى التفتيش، و اثره المباشر الذي يسفر عنه الاجراء، و تحصيل الأدلة في الجرائم الالكترونية قد يرتبط بالعناصر المادية كجهاز الحاسوب الالي و ملحقاته، الأقراص الصلبة ..... حيث لا يطرح أي اشكال في عملية حجز هذه المكونات، اما الحجز الالكتروني للمكونات المعنوية للحاسب الالي كالبرامج و البيانات المعالجة التي هي فالأصل شيء معنوي غير ملموس[1]. و عليه سنتطرق في هذا المطلب الى تدابير الحجز(الفرع الأول) و الى الحجز عن طريق منع الوصول الى المعطيات و حدود استعماله (الفرع الثاني).

[1] فلاح عبد القادر، " حجز وحفظ المعطيات في الجريمة الالكترونية"، مجلة صوت القانون، جامعة الجلالي بو نعامة، العدد 1، المجلد 8، خميس مليانة، 2021، ص 179.

الفرع الأول: تدابير الحجز:

يقصد بالحجز في قانون الإجراءات الجزائية:" وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها". يمكن تخزين المعطيات في ذاكرة الحاسوب أو في برامجه إذ تعتبر كيانات غير مادية مما شكل اختلافا في التشريعات العالمية حول مدى اعتبارها قابلة للحجز.[1]

في حين أضفى المشرع الجزائري حماية قانونية لقواعد البيانات بموجب نص المادة (05) من الامر رقم: 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة التي تنص على:" تعتبر أيضا مصنفات محمية الاعمال الاتية:

- عمال الترجمة والاقتباس، والتوزيعات الموسيقية، والمراجعات التحريرية، وباقي التحويرات الاصلية للمصنفات الأدبية والفنية.
- المجموعات والمختارات من المصنفات، مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة او بأي شكل من الاشكال الأخرى، والتي تأتي أصالتها من انتقاء مواد أو ترتيبها...".[2]

وطبقا لنص المادة (06) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها التي تنص على:" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات اللازمة

[1] يزيد بوحليط، المرجع السابق، ص 486.

[2] المادة (05) من الامر رقم: 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44، المؤرخ في 23 جمادى الأولى 1424 هـ، الموافق ل 23 يوليو 2003 م.

لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي يجري بها العملية. غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط ان لا يؤدي ذلك الى المساس بمحتوى المعطيات".[1]

وهو نفسه ما ذهبت اليه المادة (27) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تحت عنوان:" ضبط المعلومات المخزنة" التي تنص على:" تلتزم كل دولة ظرف يتبنى الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول اليها حسب الفقرة(1) من المادة السادسة والعشرين من هذه الاتفاقية، هذه الإجراءات تشمل صلاحيات:

أ- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات.

ب- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.

ت- الحفاظ على سلامة تقنية المعلومات المخزنة.

ث- إزالة أو منع الوصول الى تلك المعلومات في تقنية المعلومات التي يتم الوصول اليها...". [2]

و الملاحظ أن المشرع الجزائري استعمل مصطلح دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحراز مثل: القرص المرن و القرص الصلب و القرص المضغوط و الذاكرة

[1] المادة 06 من القانون رقم 09-04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

[2] المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تحت عنوان ضبط المعلومات المخزنة، بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 2014/09/08، جريدة رسمية 57 سنة 2014.

الوميضية و الأشرطة المغناطيسية...إلخ، و ترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة، إذ أنه لا يمكن التعامل مع تلك المعطيات في شكلها الأولى المعنوي و هي عبارة عن نبضات أو ذبذبات الكترونية أو إشارة ممغنطة الا بعد نسخها على هذه الدعامات كما تتم عملية الحجز وفقا للقواعد المقررة في نص المادة (84) من قانون إجراءات جزائية كالاطلاع على المستندات المبحوث عنها و الاحترام التام لمقتضيات التحقيق و خاصة احترام سر المهنة و حقوق الدفاع بما يكفل أمن و سرية و سلامة المعطيات في المنظومة المعلوماتية وفقا لنص المادة (2/06) من القانون رقم: 09-04 .

من ناحية ثانية حرص المشرع الجزائري على سلامة المعطيات المحجوزة من أي حذف أو تغيير بما لا يضر بالدليل الرقمي، وأيضا إعادة تشكيل هذه المعطيات بما يخدم التحقيق بشرط عدم المساس بمحتواها وفقا لنص المادة (3/06) من القانون نفسه، وهذا تحت طائلة العقوبات وفقا لنص المادة(85) من قانو إجراءات جزائية وهو نفس ما نصت عليه المادتان(07) و (09) من القانون رقم: 09-04 كما سنرى لاحقا. إضافة الى إجراء الحجز، نص قانون العقوبات في المادة (394 مكرر06) على تدابير أخرى كمصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع التي تكون محلا للجريمة. [1]

الفرع الثاني: الحجز عن طريق منع الوصول الى المعطيات وحدود استعمالها:

سنتطرق في هذا الفرع الى الحجز عن طريق منع الوصول الى المعطيات وكذلك الى حدود استعمال المعطيات كالاتي:

أولا: الحجز عن طريق منع الوصول الى المعطيات:

[1] يزيد بوحليط، المرجع السابق، ص 489.

يخلق تتبع المجرم المعلوماتي صعوبات تقنية بالغة تحول أحيانا دون الكشف عنه، وبالتالي إتلافه من العقاب، فاذا أمرت السلطة القضائية المختصة بإجراء تحقيق في جريمة ما يكون المجرم الالكتروني طرفا فيها، فسيحاول محو آثار جريمته ليصعب على المحققين تعقبه، وبالتالي اختفاء الدليل الرقمي الذي يدينه. لذلك نص المشرع في المادة(07) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها:" إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (06) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول الى المعطيات التي تحتويها المنظومة المعلوماتية او الى نسخها...". وهو ما نصت عليه المادة (1/27-د) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سالفة الذكر.

و الملاحظ ان المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، لأن نظم الحواسيب الحديثة يغلب ان تكون جزء من شبكات واسعة و معقدة يصعب على السلطات المختصة مباشرة الحجز دون تعاون كامل (full co-operation) من القائم على تشغيل النظام، أو ما تعلق بعملية نسخ المعطيات بسبب التطور الدائم في هذه التقنيات، و ما يتطلبه ذلك من متابعة و تكوين دوري لأعضاء الأجهزة القضائية المختصة في مجال التحقيق و الكشف عن الجرائم المعلوماتية. لذلك نص على ضرورة اجراء تدابير احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية لاستعمالها او نسخها او الاطلاع عليها، لأن هذه المعطيات تشكل محل الجريمة تحتوي على أدلة قد يتمكن المجرم من تهريبها أو تدميرها.[1]

[1] بشرى عواطة، حجية الدليل الالكتروني في الاثبات الجنائي، مذكرة الماستر في قانون الاعمال، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، 2017-2018، ص 181.

ثانيا: حدود استعمال المعطيات:

نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة، إلا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة (09) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومعالجتها:" تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، الا في الحدود الضرورية للتحريات أو التحقيقات القضائية".[1]

في هذا الشأن نصت المادة (85) من قانون إجراءات جزائية على:" يعاقب بالحبس من شهرين الى سنتين وبغرامة من 2000 الى 20.000 دينار كل من أفشي او اذاع مستندا متحصلا من تفتيش شخص لا صفة له قانونا في الاطلاع عليه، وكان ذلك بغير اذن من المتهم او من خلفه او من الموقع بإمضائه على المستند او الشخص المرسل اليه وكذلك كل من استعمل ما وصل الى عمله ما لم يكن ذلك من ضروريات التحقيق القضائي".[2]

من خلال ما سبق ذكره، نص المشرع الجزائري على اجراء تفتيش المنظومة المعلوماتية وحجز المعطيات، وهذا تماشيا مع التشريعات الحديثة والاتفاقيات المبرمة في هذا المجال، رغم صعوبة البحث والتحري عن الجرائم الالكترونية بسبب التطورات التقنية المذهلة الحاصلة في مجال الحوسبة ونظم الاتصالات، مما يخلق معه صور وأنماط مستحدثة لجرائم جديدة، فهي جرائم حديثة تقع في بيئة افتراضية يصعب اكتشافها والتحقيق فيها وبالتالي يسهل على المجرم المعلوماتي الإفلات من العقوبة. وعليه لابد من الاهتمام بالتكوين النظري والتدريب العملي

[1] بشرى عواطة ، نفس المرجع، ص 182.

[2] المادة 85 من قانون رقم قانون رقم 01-08 مؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، جريدة رسمية 34/2001.

للمكلفين من السلطة القضائية المختصة بالتحريات والتحقيقات في الجرائم الالكترونية قصد اكتساب المهارات الفنية اللازمة ومسايرة التطورات التقنية المتلاحقة.[1]

المبحث الثاني: إجراءات التفتيش الالكتروني وحجيته

تعبر إجراءات التفتيش الالكتروني من بين أهم الإجراءات المتبعة في الكشف عن الجرائم الالكترونية الماسة بالأنظمة المعلوماتية. ومنه سنتطرق في هذا البحث الى التفتيش الالكتروني (المطلب الأول) والى حجية دليله الالكتروني (المطلب الثاني).

المطلب الأول: التفتيش الالكتروني:

لقد شهد العالم تقدما علميا وتطورا للأنظمة المعلوماتية في مختلف مجالات الحياة مما أدى الى ظهور أنواع جديدة من الجرائم تستغل هذا التطور المعلوماتي والتي تعرف بما يسمى بالجرائم الالكترونية والتي تعد ذات طابع عابر للحدود، يصعب تتبعها والكشف عنها بأساليب التحري والتحقيق التقليدية، لذلك فقد بات من الضروري تكييف المنظومة التشريعية بغرض استحداث أساليب جديدة لمكافحة هذه الجريمة واثباتها. ومن بين هذه الأساليب التفتيش الالكتروني كآلية إجرائية مستحدثة. [2]

الفرع الأول: ماهية التفتيش الالكتروني:

يعتبر التفتيش الالكتروني إجراء من الإجراءات التي تهدف الى البحث عن ملابسات الجريمة كما يعد من أهم وأخطر إجراءات التحقيق في جرائم المعلوماتية ذلك من خلال مساسه بالحريات الخاصة للأفراد المكفولة دستوريا.

[1] يزيد بوحليط، المرجع السابق، ص492.

[2] ديابلو محمد، المرجع السابق، ص 78.

لقد سن المشرع الجزائري جملة من التعديلات لمواجهة الجرائم المعلوماتية من خلال التفتيش والضبط.

لا يوجد تعريف قانوني للتفتيش، لكن التعريف الفقهي عرفه باعتباره إجراء التحقيق التي تهدف الى البحث عن الأدلة المادية للجريمة الالكترونية كما يعد من أهم وأخطر إجراءات التحقيق، ولهذا سوف نتطرق الى مفهوم التفتيش الالكتروني أولا وخصائصه ثانيا.[1]

أولا: مفهوم التفتيش الالكتروني:

ان المشرع الجزائري لم يضع تعريف تشريعي للتفتيش الالكتروني في القانون رقم 04/09 المتعلق بالجرائم المتصلة بتكنولوجيات المعلومات، وانما تطرق أولا لتنظيم احكامه وضوابطه، تاركا ذلك للفقه. وقد تم تعريف التفتيش بصفة عامة بأنه اجراء من إجراءات التحقيق لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه، أو البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها الى المتهم، كما عرفه البعض الاخر بأنه إجراء من إجراءات التحقيق هو ليس عملا إداريا من أعمال الضبط الإداري وإنما هو عمل من أعمال التحقيق والضبط القضائي لجمع الأدلة عن جريمة معينة بعد قيام الاتهام ضد شخص معين.

وهناك من عرفه بأنه البحث والتحري داخل سر الافراد عن أدلة تفيد لإثبات جريمة معينة أو ارتكبت فعلا، وهو إجراء من إجراءات التحقيق أما فيما يتعلق بالتفتيش الالكتروني، فقد عرفه بعض الفقهاء بأنه الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع صاحبه يستوفي أن يكون هذا المحل جهاز الحاسب الالي أو أنظمة أو شبكة الانترنت.

[1] عربوز فاطمة الزهراء، "التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية"، مجلة جيل الأبحاث القانونية المعمقة، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 34، الجزائر، 2019، ص 103.

وعرفه المجلس الأوروبي بأنه اجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني.[1]

ثانيا: خصائص التفتيش الالكتروني:

من خلال التعريف الذي تم تقديمه من طرف الفقه يتعين ان التفتيش في نظم المعلوماتية يتميز بعدة خصائص أهمها:

1- يسمح التفتيش او البحث في الشبكات الالكترونية من الجرائم المعلوماتية باستخدام قواعد وأساليب التحقيق الجنائي المعروفة بتقنيات خاصة فريدة أو غير مسبوقة، فهو يعكس التفتيش في معناها التقليدي أي الكلاسيكي، بحيث لا يتطلب في كثير من الأحيان الانتقال الى مساكن الأشخاص الذين يشتبه في انهم ساهموا في الجريمة وانما قد يتم عن بعد، أو ما يعرف بالتفتيش على الخط Perquisition en ligne.

2- كما يتطلب فيمن يباشر التحقيق في الجريمة أن يكون متخصصا في التحقيق الجنائي ومعالجة البيانات والمراجعة والحسابات.

3- وكذلك من بين مميزاته أن التفتيش في المنظومة المعلوماتية أن المحتوى المعلوماتي يتميز بطبيعة لامادية وتجاوزه الحدود المادية وسهولة إتلافه او مسحه. لأنه تفتيش أو تحقيق لقضاء افتراضي.

كما يتميز بأنه عملية معقدة ومتشابكة تقتضي من القائمين عليها أن يكونوا على دراية واسعة وكفاءة عالية في البحث عن المعلومة وفي معالجة المعطيات وتحليلها وفك طلاسمها، ويزداد الامر صعوبة في ظل التزايد المتسارع في حجم الأقراص الصلبة للحاسوب كما أن تفتيش الأنظمة المعلوماتية فيه مساس خاص بالحياة الخاصة لأنه يتطلب وضع ترتيبات خاصة

[1] كيحول عبد القادر، التفتيش الالكتروني كإجراء للتحقيق في الجرائم الالكترونية، مذكرة ماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، جامعة زيان عاشور –الجلفة، كلية الحقوق والعلوم السياسية، 2019–2020، ص 6.

وتقنيات لمراقبة الاتصالات الالكترونية وتسجيلها الفوري وكذا القيام بعملية التفتيش والحجز داخل المنظومة المعلوماتية [1].

ثالثا: الضوابط الشكلية للتفتيش الالكتروني:

تهدف هذه الشروط الشكلية ليس فقط إلى تحقيق العدالة من خلال ضمان صحة إجراءات جمع الأدلة، بل تسعى أيضًا إلى وضع إطار يحمي الحقوق والحريات الفردية، بما يتماشى مع متطلبات كل إجراء، وتتمثل هذه الضوابط الشكلية في:

1. إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الاطمئنان على سلامة الإجراء غني عن البيان أن التفتيش فيه اطلاع على أسرار الغير. فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن، ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه أو المتهم عند 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.

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم 06-22 المادة 45 منه، حيث استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني، خاصة وأن

[1] ديابلو محمد، المرجع السابق، ص 80.

هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد. كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بنظام التفتيش عن بعد، أو ما يطلق عليه الفقه الفرنسي التفتيش على المباشر (perquisition en ligne) [1].

2. الميعاد الزمني لإجراء التفتيش الإلكتروني:

يقصد بشرط الميعاد الزمني في التفتيش أن يجربه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن. إن القانون الجزائري يحظر تفتيش المنازل وما في حكمهما في وقت معين، وهو محدد في القانون الإجراءات الجزائية من خلال المادة 47 من الساعة الخامسة صباحا على الساعة الثامنة مساء. وهناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد ويصح إجراء التفتيش في أي ساعة من ساعات الليل والنهار.

وأن المشرع الجزائري قد أورد في قانون الإجراءات الجنائية المادة 3/64 « أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 3/47 من هذا القانون تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر حيث أجاز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص » وجاء في نص المادة 3/47 من قانون الإجراءات الجزائية، حيث استثنى تطبيق هذه الضمانات على طائفة الجرائم المذكورة في هذه المادة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والملاحظ أن المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتباره مستودع أسرارهم، إلا أن ما يبرره ويقل من خطورته الطبيعة

[1] ليندة بن طالب، " التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة مولود معمري–تيزي وزو، العدد 16، جوان 2017، ص 493.

الخاصة لهذه الجرائم خاصة الجريمة الإلكترونية وطبيعة الدليل لإثباتها فهو قابل للمحو والتعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية وما يزيد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوة الجنائية. أما بالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل معه مكونات الحاسوب سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.[1]

3. محضر التفتيش الالكتروني:

باعتبار أن التفتيش من أعمال التحقيق، لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة.

والقانون لم يتطلب شكلا خاصا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكونا مكتوبا باللغة الرسمية وأن يكون

مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية.[2]

الفرع الثاني: إجراءات التفتيش الالكتروني

تعد إجراءات التفتيش و الضبط من إجراءات التحقيق التي تختص بها سلطة التحقيق ويناط لضابط الشرط القضائية القيام بها في حالات استثنائية ويعتبر التفتيش وسيلة للحصول من خلاله على أدلة في بيان و ظهور الحقيقة و لا يكفي في التفتيش مجرد توافر شروطه سواء الموضوعية أو الشكلية، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية و التي يتمثل أهمها في

[1] عربوز فاطمة الزهراء، المرجع السابق، ص 103.

[2] ليندة بن طالب، المرجع السابق، ص 494.

ضرورة التقيد بالغرض من التفتيش أثناء تنفيذه وفقا لما نص عليه قانون الإجراءات الجزائية و الذي يقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلقة بالجريمة موضوع التحقيق، ويلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش والضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه.

وبعد حضور أشخاص معنيين في أثناء إجراء التفتيش من قبل الشخص المكلف الضمانات المهمة التي تكفل إجراءه بشكل صحيح، ويبعد الشك حول إمكانية إخفاء الدليل من قبل القائمين به، وبعد ضمانة للقائم بالتفتيش به.[1]

ويقوم المفتش في إطار البحث عن الجرائم الماسة بأنظمة الاتصال والمعلوماتية بمجموعة من الإجراءات بذلك قانوناً منها:

أولا: إجراءات تفتيش النظام المعلوماتي الخاص بالمتهم:

إذا كان محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون لزوم التدخل في نظام معلوماتي لشخص آخر، وفي هذا الفرض إذا كانت الشروط الإجرائية للتفتيش صحيحة وفقا لما نص عليه القانون فإن التفتيش و ما يسفر عنه من ضبط أي من الأدلة، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر أم أحد الوسائط المتعددة، يكون مشروعا، وهذا الحال يكثر في جرائم التزوير و التزييف حيث يتم التفتيش وملحقاته من طابعات ملونة أو أجهزة ماسح ضوئي و يتم نقل البرنامج الداخلي الذي يوجد عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعددة وبذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما

[1] عز الدين عثماني، " إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة، العدد الرابع، جانفي 2018، ص 60.

يتم أيضا في الجرائم النسخ والتقليد حيث يتم ضبط الوسائط المتعددة المحملة بالبرنامج المنسوخة والأجهزة المستخدمة في ذلك.[1]

ثانيا: إجراءات تفتيش في نظام معلوماتي غير خاصة بالمتهم:

يظهر هذا الفرض في الجرائم التي ترتكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي جهاز من أجهزة الحاسبات الآلية الأخرى المتصلة بالحاسب الذي ارتكبت في انظامه المعلوماتي الجريمة و في هذا الفرض فإن إجراءات التفتيش و الضبط تتطلب الدخول في نظام معلوماتي لشخص آخر، ويلاحظ أن قانون الإجراءات الجزائية نص على أنه لا يجوز لرجال الشرطة القضائية الدخول في أي محل مسكون إلا في الأحوال المبينة في القانون، أو في حالة طلب المساعدة من الداخل، وهو ما دعا المشرع إلى من تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن وكذلك السيارة الخاصة إذا كانت توجد في مسكن للمتهم. أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانونا.[2]

ثالثا: تطبيقات في 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 نضام المعلومات وما يحويه من خصوصيات للأشخاص تخضع أيضا وبالتبعية المعيار الخصوصية من حيث عدم جواز التدخل فيها بدون إذن من وكيل الجمهورية.

ورغم أن المشرع وفي جل القوانين التي نصها حاول حماية خصوصية الأفراد بما فيها البيانات والمعلومات الشخصية وكذلك السجلات والدفاتر أو الحاسبات الآلية والملحقات السرية بعدم

---

[1] ديابلو محمد، المرجع السابق، ص 85.

[2] عز الدين عثماني، المرجع السابق، ص 61.

جواز الاطلاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون، وهذا ما أكده أيضا بامتداد الحق في التفتيش إلى سجلات البيانات التي تكون في موقع إلكتروني آخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.

وكذلك ذهب جانب آخر من الفقه بأن البيانات لها طابع مادي على أساس أنها نبضات أو ذبذبات إلكترونية وإرشادات أو موجات كهرومغناطيسية قابلة لأن تسجل وتخزين على وسائط متعددة ويمكن قياسها ولأن البحث عن الدليل على ارتكاب الجريمة، من حيث كونه وسيلة للإثبات ومحلا للاقتناع وفقا لنظرية الإثبات الجنائي يتطلب الإقرار بإمكانية أن تكون المعلومات محلا للتفتيش وضبط الأدلة المتحصل عليها.[1]

المطلب الثاني: حجية الدليل الالكتروني

نتناول في هذا المطلب ماهية الدليل الالكتروني (الفرع الأول) وكذلك تأثير الدليل الالكتروني على قناعة القاضي (الفرع الثاني).

الفرع الأول: ماهية الدليل الالكتروني:

من القواعد المستقرة في مجال الإثبات الجنائي أن القاضي لا يمكنه أن يقضي بعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة، ومن هنا يبدو الدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته، ولهذه الأهمية التي يتمتع بها الدليل عموماً حظيت باهتمام المشرع في مختلف الأنظمة القانونية من حيث تحديد شروط مشروعيته وتقدير قيمته الإثباتية. [2]

[1] ديابلو محمد، المرجع السابق، ص 86.

[2] سمير شبلاق، حجية الدليل الرقمي في الكشف عن الجريمة، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور مولاي الطاهر-سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019-2020، ص 10.

أولا: تعريف الدليل الالكتروني:

يعرف الدليل الالكتروني بأنه الدليل المأخوذ من أجهزة الكمبيوتر والذي يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقعي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم من أجل اعتماده أمام أجهزة إنفاذ القانون وتطبيقه. كما عرفته المنظمة العالمية لدليل الكمبيوتر في أكتوبر 2001 بأنه: " المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية".

وهناك من عرف الدليل الالكتروني بانه: "كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقعي بحيث تمكن الحاسوب من انجاز مهمة ما".

وعليه يتضح أن الدليل الالكتروني هو مجموع البيانات داخل العالم الافتراضي بجميع صورها تأخذ شكل أرقام ويتم تحويلها عند عرضها الى صور أو تسجيلات أو نصوص، وهو الوسيلة المستخلصة من البيئة الرقمية لإثبات الجريمة الالكترونية.[1]

ثانيا: استخلاص الدليل الالكتروني بطريقة مشروعة:

لكي يُعتد بالدليل الإلكتروني أمام القضاء، يجب أن يُستخلص بوسائل مشروعة، وتتوفر فيه شروط قانونية محددة.

وسنتناول ذلك من خلال بيان مراحل استخلاصه، تليها إجراءات جمعه.

1- مراحل استخلاص الدليل الالكتروني:

[1] عائشة عبد الحميد، " الدليل الرقمي كحجية للإثبات امام القاضي الجزائي في المعاملات الالكترونية"، مجلة صوت القانون، جامعة الطارف، المجلد السابع، العدد01، ماي 2020، ص 483.

تتطلب عملية استخلاص الدليل الالكتروني إتباع خطوات من طرف المحققين لكي يعتد بهذا الدليل أمام القاضي الجزائي. ويتعين إتباع المراحل التالية:

أ- مرحلة التعرف على الدليل الالكتروني:

ويتم ذلك بمناظرة جهاز الكمبيوتر الخاص بالمشتبه فيه، وفحصه بطريقة فنية، والاطلاع على وحدة الذاكرة هارد ديسك وبيان البرامج الوسيطة التي يستعملها ويستخدمها، وإمكانية استخدام هذه البرامج في الجريمة المرتكبة.[1]

ب- مرحلة الاحتفاظ بالدليل الالكتروني:

يتم في هذه المرحلة تجنب حدوث أي تغييرات على البيانات الموجودة على الجهاز الذي استخلصت منه الوقائع والبيانات المجرمة.

ت- مرحلة إعادة بناء الدليل الالكتروني وتوثيقه:

هنا يتم التمييز بين الأدلة الالكترونية الصحيحة والأدلة التي تم العبث بها أو محوها، ثم يتم تصنيفها بحسب أهميتها، ويتم تحليل الدليل الالكتروني من خلال استخلاص البيانات والتعرف عليها ونوعية المعلومات المتحصل عليها.

باتباع المراحل المذكورة أعلاه يتم استخلاص الدليل الالكتروني بطريقة سليمة وموثوقية وتكون له قوة ثبوتية في إثبات الجرائم الالكترونية والأكثر من ذلك تكون له مقبولية كافية من طرف القاضي الجزائي في تكوين عقيدته والحكم على الجاني اما بالبراءة واما بالإدانة.[2]

الفرع الثاني: تأثير الدليل الالكتروني على قناعة القاضي:

---

[1] أسامة حسين محي الدين عبد العال، " حجية الدليل الرقمي في الاثبات الجنائي للجرائم المعلوماتية دراسة تحليلية مقارنة"، مجلة البحوث القانونية، العدد 76، يونيو 2021، ص 663.

[2] ديابلو محمد، المرجع السابق، ص 156.

بعدما تم التوصل من خلال إجراءات تحقيق البحث، التحري وحجز المعطيات وتفتيشها، كل ذلك يتم تقديمه في المرحلة الأخيرة من مراحل الإجراءات الجزائية وهي مرحلة المحاكمة أمام قاضي الموضوع لأجل تحميصها ولأجل ادانة او تبرئة المتهم في الجريمة المعلوماتية، والتي يستمد فيها القاضي الجنائي الى الدليل الالكتروني، ومدى حجيته وقناعته بالنسبة للقاضي الجنائي؟

تطورت وسائل الاثبات الجنائي بشكل يمكن اعتماده في التحقيق الجنائي فلم تعد الوسائل التقليدية قادرة على كشف ملابسات بعض الجرائم ما استدعى اعتماد وسائل علمية حديثة من بينها الدليل الالكتروني.[1] وعليه سنعالج مصداقية الدليل الالكتروني وقيمته الفنية والعلمية في تأثيرها على قناعة القاضي.

أولا: مصداقية الدليل الالكتروني في الاثبات:

للدليل الالكتروني في مجال الاثبات توافر شروط في مصداقيته وكذا صحة الإجراءات المتبعة في الحصول عليه من جهة أخرى وهي:

1- يقينية الدليل الالكتروني:

اليقين هو عبارة عن حالة ذهنية أو عقلية تؤكد وجود الحقيقة، ويتم الوصول الى ذلك عن طريق ما نستخلصه من وسائل الإدراك المختلفة للقاضي ما يقدم اليه من وقائع الدعوى، وما ينطبع في ذهنه من تخيلات ذات درجة عالية لذلك عندما يصل القاضي إلى اليقين فإنه يصبح في المرحلة مقتنعا بالحقيقة.

[1] آسية ذنياب، "مشروعية استخدام الوسائل العليمة الحديثة في الاثبات الجنائي"، مجلة أبحاث قانونية وسياسية، جامعة محمد الصديق بن يحيى، جيجل–الجزائر–، المجلد 07، العدد 02، 2022، ص 235.

ويصل القاضي إلى يقينية المخرجات المقدمة ذكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينتها لهذه المخرجات وعن طريق المعرفة العقلية التي يتم كمن خلالها استخلاص واستقراء الحقيقة التي تهدف إليها. ويجب أن يصدر حكمه استنادا اليها.

ونظرا لطبيعة التقنية التي يتميز بها الدليل الالكتروني الا انه هناك قواعد محددة، تم وضعها من طرف المختصين التي تحكم يقينيتها ومن بينها استعمال الوسائل الفنية، تكون من طبيعة هذا الدليل تكمن في فحص سلامة وصحة الإجراءات المتبعة للحصول عليه.[1]

أ- تقييم الدليل من حيث سلامة العبث به:

للتأكد من سلامة العبث بالدليل الرقمي يجب أن تتبع عدة طرق منها:

- علم الكمبيوتر يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقعي، وهذا النوع من العلوم تتم الاستعانة به في الكشف عن مدى تلاعب بمضمون هذا الدليل، وفكرة التحليل التناظري الرقعي تبدوا من الوسائل المهمة للكشف عن مدى مصداقية الدليل، ومن خلالها يتم التأكد من مدى إمكانية حصول العبث في النسخة المستخرجة ام لا.
- وهناك نوع من الأدلة الالكترونية والتي تسعى بالأدلة المحايدة، وهو من الأدلة التي لا علاقة بموضوع الجريمة، إلا أنه يساعد من التأكد من سلامة الدليل الالكتروني، يجعله يقيني ولا مجال للشك فيه حتى تتم مراجعة المتهم به هذا من ناحية ومن ناحية أخرى ضمان حقوق المتهم المعلوماتي.

[1] مرغاد شهيرة، حداد عيسى، " حجية الدليل الالكتروني امام القاضي الجزائي"، دائرة البحوث والدراسات القانونية والسياسية، جامعة باجي مختار-عنابة، المجلد 07، العدد 02، الجزائر، 2023/06/01، ص 309.

- في حالة عدم حصول الدليل على نسخة الاصلية، أو أن الدليل وقع في حالة عبث، وقد وقع على النسخة الاصلية، فيمكن التأكد من سلامة الدليل الالكتروني من العبث.[1]

ب- تقيم الدليل الالكتروني من حيث القيمة الفنية:

من بين الإجراءات الفنية التي يمكن الاعتماد عليها لتأكد من سلامة الدليل الالكتروني في الاثبات:

- **التأكد من دقة الأدوات المستخدمة في استخلاص الدليل الجنائي الالكتروني:**

يتم التأكد من صحة الأدوات المستخدمة في استخلاص الدليل الالكتروني بالتحقيق من مدى قدرة هذه الأدوات على عرض كافة البيانات المتعلقة بالدليل الالكتروني، وكذلك خضوعها لأدوات الاختيار. فمن خلاله يمكن أن تتأكد من أن الأدلة لا تعرض بيانات إضافية جديدة.

ومن خلال هذا الاختبارين نتأكد من الأدلة المستخدمة عرضت على البيانات المتعلقة بالدليل الالكتروني، وبالتالي لم يضف اليه أي بيان جديد ويعطي نتائج مقدمة عن طريق جهاز الكمبيوتر مصداقية في التدليل على الواقع.

- **الاعتماد على الأدوات التي اثبتت الدراسات العلمية كفاءتها في تقديم أفضل:**

لقد بينت الدراسات العلمية في مجال تقنية المعلومات على الطريقة الواجب اتباعها في الحصول على الدليل الالكتروني وفي المقابل أوضحت الدراسات الأدوات المشكوك في كفاءتها، وهذا ساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.[2]

2- مناقشة الدليل:

[1] ديابلو محمد، المرجع السابق، ص 173.

[2] ديابلو محمد، نفس المرجع، ص 174.

تتم مناقشة الدليل بناء على مبدأ شفوية المرافعات، وهذا طبقا لنص المادة 212 قانون إجراءات جزائية التي تنص على انه " لا يسوغ القاضي أن يبني قراره إلا على الأدلة المقدمة له في المرافعات والتي حصلت المناقشة فيها حضوريا أمامه ".[1]

من خلال هذه نجد أن القاضي يعتمد في الحكم على الاجتهاد، ولا يعتمد على رأي الغير إلا إذا كان ذلك من الخبراء المتخصصين.[2]

ثانيا: القيمة العلمية على الدليل الالكتروني وتأثيرها على قناعة القاضي:

للقاضي الجنائي سلطة قبول أي دليل مشروع حقق لديه اليقين، وهو كذلك الذي يقدر قيمة الدليل وقوته في الإثبات، وتحتاج عملية تقدير الدليل أن يلتزم القاضي في تكوين إقناعته إتباع أسلوب عقلي ومنطقي، يعتمد على الاستقرار والاستنباط لتجميع صورة ذهنية حقيقية بهدف الوصول إلى الحقيقة.

وبالرغم من أن الأدلة الجنائية تخضع لمبدأ تكافؤ الأدلة إلا أن سلطة القاضي الجنائي في تقدير الأدلة العلمية الحديثة، لا نقول تقيد أو تحد من هذه السلطة، الا أنه يجب على القاضي أن يراعي خصوصية هذه الأدلة باعتبارها مسائل علمية دقيقة ومراعاة ذلك يكون ضمن مجالين أساسيين هما:

- القيمة العلمية للدليل.
- الظروف والملابسات التي وجد فيها الدليل.[3]

[1] المادة 212 من قانون الإجراءات الجزائية الجزائري.

[2] مرغاد شهيرة، حداد عيسى، المرجع السابق، ص 310.

[3] خوري عمر، بن لاغة عقيلة، " الرقابة على سلطة القاضي الجنائي في تقدير الدليل العلمي"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر 1، العدد الحادي عشر، سبتمبر 2018، ص 549.

كما أن المادة 215 قانون إجراءات جزائية تؤكد على: "ألا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك".[1]

وهو الأمر الذي أخذ به المشرع الجزائري حيث بموجبه يقرر مبدأ الشخصي للقاضي الجزائي يجعله يبسط سلطاته على جميع الأدلة دون استثناء بما فيها تقرير الخبير.

بحيث قضت المحكمة العليا هذا الاتجاه في أحد أحكامها: " إن تقرير الخبرة ليس إلا عنصر من عناصر الاقتناع يخضع لمناقشة الأطراف والتقدير قضاة الموضوع وكما أكدت في حكم آخر لها: " إن تقرير الخبرة لا يقيد لزوما قضاة الموضوع وانما هو كغيره من أدلة الإثبات قابل للمناقشة والتمحيص، ومتروك لتقديرهم وقناعتهم".

وكما يلزم القاضي بالحقائق العلمية لا يسلب منه سلطة الرقابة القانونية على عناصر الدعوى بما فيها طرق الحصول على الدليل والظروف التي وجد فيها، فهي تدخل ضمن الاختصاصات الأصلية للقاضي، كما إنها تخضع أيضا لمبدأ تكافي الأدلة بحيث يمكن للقاضي استبعاد أي دليل علمي لا يتناسب مع ظروف الواقعة أو الجريمة.

وكما يمكن الاستعانة بمعطيات التطور العلمي في إطار الكشف عن الجريمة ويبقى للقاضي حرية مطلقة في تقرير الدليل المعروض أمامه، والأخذ بما هو مناسب مع الواقع.

نستخلص موقف المشرع الجزائري من خلال أحكام المادة 212 من قانون الإجراءات الجزائية التي تنص على انه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وعلى القاضي أن يصدر حكمه تبعا لاقتناعه الخاص، وهنا يتبين اتجاه المشرع الجزائري في تبني مقومات النظام اللاتيني في الإثبات، ومن ثمة ترك حرية للقاضي في تكوين اقتناعه الشخصي.[2]

[1] المادة 215 من قانون الإجراءات الجزائية الجزائري.

[2] ديابلو محمد، المرجع السابق، ص 176.

خاتمة

خاتمة:

سعى هذا البحث من خلال موضوع "إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية" إلى تسليط الضوء على خصوصية الإجراءات المتبعة في مجال مكافحة الجريمة المعلوماتية، وذلك بالاعتماد على أحكام قانون الإجراءات الجزائية الجزائري، بالإضافة إلى القانون رقم 09/04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها. وقد تبيّن أن قانون الإجراءات الجزائية يقتصر في مجمله على تنظيم القواعد العامة الخاصة بالجرائم التقليدية، بينما جاء القانون 09/04 ليتناول بعض الإجراءات الخاصة التي تتلاءم مع طبيعة الجريمة المعلوماتية، على غرار حجز البيانات، ومراقبة الاتصالات الإلكترونية، وحفظ المعطيات.

وفي ختام الدراسة، يمكن القول إن المنظومة التشريعية الجزائرية لا تزال تفتقر إلى إطار قانوني شامل وفعال يُمكّن من التصدي للأخطار المتزايدة التي تفرزها الجرائم المعلوماتية، سواء من حيث النصوص القانونية، أو من حيث توفر الكفاءات البشرية والتقنية المتخصصة. كما أن تشتت النصوص القانونية ذات الصلة بين قانون العقوبات وقانون الإجراءات الجزائية والقوانين المكملة لهما، وما يرافقه من تناقض بين القواعد العامة والخاصة وصعوبة تطبيقها عمليًا، يشكل عقبة حقيقية أمام عمل أجهزة الضبطية القضائية، ويساهم في اتساع دائرة إفلات مرتكبي هذه الجرائم من العقاب.

وعليه، فإن غياب الأطر التقنية المتخصصة في مجال مكافحة الجرائم السيبرانية على مستوى الأجهزة الأمنية يمثل أحد أبرز العوائق التي تحول دون تحقيق حماية فعالة للمعطيات الرقمية، كما أن القانون 09/04 يظل دون جدوى إذا لم يُفعّل من خلال تطبيق صارم ودقيق لمضامينه، خاصة فيما يتعلق بإجراءات المعاينة والتفتيش والحجز داخل النظم المعلوماتية.

كما ختمنا هذه الدراسة ببعض النتائج والتوصيات والتي تتمثل في:

النتائج:

– إجراءات معاينة الأنظمة المعلوماتية لابد ان تكون من طرف شرطة قضائية متخصصة في الجرائم المعلوماتية.

– السلطة المختصة بالتفتيش والحجز تضمن سلامة البيانات في الأنظمة المعلوماتية أثناء العملية دون المساس بمحتواها الاصلي.

– إجراءات التفتيش لابد لها ان تتوافر على الشروط الشكلية المنصوص عليها في قانون الإجراءات الجزائية، زيادة عن الدقة في التفتيش عن البيانات الالكترونية.

– حجز الدليل الالكتروني لابد ان يكون دقيقا وسليما.

– للدليل الالكتروني أهمية بارزة في اثبات الجرائم بصفة عامة والجريمة المعلوماتية على وجه الخصوص.

التوصيات:

– إعادة النظر في المنظومة القانونية بما يشمل توحيد النصوص الخاصة بالجريمة المعلوماتية ضمن قانون واحد شامل ومتكامل.

– وضع آليات تنسيق بين الجهات المختصة (القضائية، الأمنية، والتقنية لضمان تدخل فعال عند حدوث الجرائم المعلوماتية.

– تطوير بنية تحتية رقمية آمنة ودعم البحث العلمي في مجال أمن المعلومات والتحقيق الرقمي.

–تكوين ضباط شرطة وقضاة حكم ونيابة مختصين في الجرائم المعلوماتية.

-إنشاء محاكم خاصة بالجرائم المعلوماتية.

-تدعيم التعاون الدولي ما بين الدول في إجراءات المعاينة الحجز والتفتيش.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع:

أولا: المصادر

1- الاتفاقيات الدولية:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تحت عنوان ضبط المعلومات المخزنة، بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 2014/09/08، جريدة رسمية 57 سنة 2014.

- قانون الاونيسترال النموذجي بشأن التجارة الالكترونية مع دليل التشريع 1996 ومع المادة الإضافية 5 مكررا بصيغتها المعتمدة في عام 1998، قرار الجمعية العامة 162/51 المؤرخ في 16 ديسمبر 1996، الأمم المتحدة، نيويورك، سنة 2000.

2-القوانين:

- قانون العقوبات الصادر بموجب أمر رقم 66-156 مؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966، القسم السابع مكرر الذي يتضمن المساس بأنظمة المعالجة الالية للمعطيات، جريدة رسمية عدد 49 صادر في 21 صفر عام 1386 الموافق 11 يونيو 1966، معدّل ومتمم.

- قانون رقم قانون رقم 01-08 مؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، جريدة رسمية 34/2001.

- الامر رقم: 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44، المؤرخ في 23 جمادى الأولى 1424 هـ، الموافق ل 23 يوليو 2003 م.

- قانون رقم 09-04، المؤرخ في 14 شعبان عام 1430 الموافق ل 05 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المؤرخة في 25 شعبان عام 1430هـ الموافق ل 16 غشت 2009م.

ثانيا: المراجع

1- الكتب:

-أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 2014.

- ديابلو محمد نجيب، الجريمة الالكترونية وحجية الدليل الرقمي في الاثبات الجنائي، الطبعة الأولى، المركز المغاربي-شرق أدنى للدراسات الاستراتيجية، المملكة المتحدة – بريطانيا-، جانفي 2024.

- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.

- طارق إبراهيم الدسوقي عطية، الموسوعة الأمنية الامن المعلوماتي النظام القانوني لحماية المعلوماتية Système Judicaire Pour La Protection de L'information، دار الجامعة الجديدة، الإسكندرية، 2015.

- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، د.ط.ن، دار الفكر الجامعي، الإسكندرية، 2013.

- يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، سنة 2019.

2- المقالات:

- أسامة بن يطو، حمزة عبدلي، " حماية برامج الحاسب الالي في ضوء التشريع الجزائري والمواثيق الدولية"، مجلة معارف، قسم العلوم القانونية، السنة التاسعة، العدد 19، 2015.
- أسامة حسين محي الدين عبد العال، " حجية الدليل الرقمي في الاثبات الجنائي للجرائم المعلوماتية دراسة تحليلية مقارنة"، مجلة البحوث القانونية، العدد 76، يونيو 2021.
- آسية ذنياب، "مشروعية استخدام الوسائل العليمة الحديثة في الاثبات الجنائي"، مجلة أبحاث قانونية وسياسية، جامعة محمد الصديق بن يحيى، جيجل-الجزائر-، المجلد 07، العدد 02، 2022.
- بطيحي نسيمة،" جريمة الدخول او البقاء غير المشروع الى النظام المعلوماتي"، مجلة الفقه القانوني والسياسي، جامعة سطيف 2، المجلد 01، العدد 01، 01-06-2016.
- بليردوح ثليثة، "الحاسوب ودوره في العملية التعليمية والتعلمية"، مجلة العربية، جامعة العربي بن مهيدي، عدد خاص01، المجلد07، 2020/03/02.
- حابت أمال، "الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 04-15 و09-04"، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 7، العدد 25، 2023.
- حديدان سفيان، " الدخول او البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد الثاني، العدد الثامن، 2017.
- خطوي مسعود، عكوش حنان،" خصوصية الدليل الالكتروني"، مجلة الفكر القانوني والسياسي، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي، الاغواط، العدد الأول، مجلد السابع، 2023.
- خفيف جمال، "قراءة قانونية لجريمة تبييض الأموال (خصوصية أركانها وإجراءات مواجهتها)"، مجلة صوت القانون، كلية الحقوق، السعيد حمدين، جامعة الجزائر، المجلد التاسع، العدد 01، 2022.

– خوري عمر، بن لاغة عقيلة، " الرقابة على سلطة القاضي الجنائي في تقدير الدليل العلمي"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة الجزائر 1، العدد الحادي عشر، سبتمبر 2018.

– زروقي عاسية،" جرائم الاعتداء على الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات الحماية"، مجلة القانون والعلوم السياسية، جامعة غرداية، المجلد 08، العدد 02، 2022.

– عائشة عبد الحميد، " الدليل الرقمي كحجية للإثبات امام القاضي الجزائي في المعاملات الالكترونية"، مجلة صوت القانون، جامعة الطارف، المجلد السابع، العدد01، ماي 2020.

– عبد القادر رحال،" البناء القانوني لجريمة التقاط الصورة ونشرها في التشريع الجزائري والفرنسي–دراسة موضوعية إجرائية مقارنة "، مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر 1، المجلد 15، العدد 01، 2022.

– عربوز فاطمة الزهراء، "التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية"، مجلة جيل الأبحاث القانونية المعمقة، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، العدد 34، الجزائر، 2019.

– عز الدين عثماني، " إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، جامعة تبسة، العدد الرابع، جانفي 2018.

–فلاح عبد القادر، " حجز وحفظ المعطيات في الجريمة الالكترونية"، مجلة صوت القانون، جامعة الجلالي بو نعامة، العدد 1، المجلد 8، خميس مليانة، 2021.

– قلات سومية، عبد العالي حاحة، " مقتضيات المعاينة المعلوماتية في التشريع الجزائري"، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية، جامعة بسكرة، العدد 1، المجلد 11، الجزائر، 2023.

– ليندة بن طالب، " التفتيش في الجريمة المعلوماتية"، مجلة العلوم القانونية والسياسية، جامعة مولود معمري–تيزي وزو، العدد 16، جوان 2017.

- محمد خليفة، " خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها"، دراسات وأبحاث، جامعة 08 ماي 1945-قالمة، المجلد1، العدد 1، 15-09-2009.

- مرغاد شهيرة، حداد عيسى، " حجية الدليل الالكتروني امام القاضي الجزائي"، دائرة البحوث والدراسات القانونية والسياسية، جامعة باجي مختار-عنابة، العدد 02، المجلد 07، الجزائر، 2023/06/01.

- مونة مقلاتي، راضية مشري، " الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية"، مجلة أبحاث قانونية وسياسية، جامعة 8 ماي 1945-قالمة، المجلد 06، العدد 01، جوان 2021.

- نعمان عبد الكريم، "الدخول او البقاء عن طريق الغش في نظام المعالجة الالية للمعطيات"، حوليات جامعة الجزائر 1، كلة الحقوق ساعد حمدين، المجلد 38، العدد 02، 2024.

- وهيبة رابح، " الجريمة المعلوماتية في التشريع الاجرائي الجزائري"، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، العدد الرابع، 2014.

- يزيد بوحليط، " تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري"، التواصل في الاقتصاد والإدارة والقانون، جامعة باجي مختار، عنابة، العدد 48، ديسمبر 2016.

3- الرسائل الجامعية:

- **أطروحات الدكتوراه:**

- بن فردية محمد، الاثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، كلية الحقوق، 07-12-2015.

-خليفة محمد، جريمة التواجد غير المشروع في الانظمة المعلوماتية. اطروحة دكتوراه، كلية الحقوق جامعة عنابة ،2012/2011.

– فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الاخوة منتوري قسنطينة، الجزائر، 2012.

- **مذكرات الماستر:**

–بشرى عواطة، حجية الدليل الالكتروني في الاثبات الجنائي، مذكرة الماستر في قانون الاعمال، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، 2017–2018.

– بن الصغير الربيع، خلاف محمد زكرياء، نظم المعلومات الإدارية وأثرها على استراتيجية المؤسسة دراسة حالة مؤسسة الصندوق الوطني للتأمينات الاجتماعية للعمال الاجراء وكالة ميلة، مذكرة مكملة لنيل شهادة الماستر، المركز الجامعي عبد الحفيظ بالصوف، معهد العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، تخصص إدارة أعمال، 2022–2023.

– بودواب سمير، لبديوي فؤاد، جرائم المساس بأنظمة المعالجة الالية للمعطيات، مذكرة ماستر، جامعة 20اوث 1955، كلية الحقوق والعلوم السياسية، قسم الحقوق، سكيكدة، 2024.

– حداوي صبرينة، زرورو عمر، اركان جريمة تبييض الأموال، مذكرة لنيل شهادة الماستر في القانون، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، قسم القانون، تيزي وزو، 2017/09/26.

– رزيق محمد، إجراءات المعاينة التفتيش والحجز داخل المنظومة المعلوماتية، مذكرة لنيل شهادة الماستر في القانون العام، تخصص القانون الجنائي والعلوم الجنائية، جامعة آكلي محند أولحاج، كلية الحقوق والعلوم السياسية، قسم القانون العام، البويرة، 2018–2019.

– سحنين طارق، بوسماحة صارة، إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية، مذكرة التخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، جامعة يحي فارس، كلية الحقوق والعلوم السياسية، المدية، 2021/2020.

- سمير شبلاق، حجية الدليل الرقمي في الكشف عن الجريمة، مذكرة تخرج لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة الدكتور مولاي الطاهر-سعيدة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2019-2020.
- كيحول عبد القادر، التفتيش الالكتروني كإجراء للتحقيق في الجرائم الالكترونية، مذكرة ماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، جامعة زيان عاشور-الجلفة، كلية الحقوق والعلوم السياسية، 2019-2020.

الملاحق

الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
وزارة الداخلـيـــة والجماعات المحلية
والتهيئة العمرانية
المديريـــة العامـــة للآمـــن الوطنـــي
أمـــن ولايـــة
المصلحـــة الولائيـــة للشرطـــة القضائيـــة
رقـم / أوج/م و ش ق/ق غ/

- محضـــر تفتيـش إلكتروني -

قضيـــة ضـد المدعو/ - ب . ع .

- / إنه في: يوم ..... **الموافق** ..... **من شهر** .....**---- / السنة:**------
- / الساعة: .....ابط الشرطة / ب ع، رئيس ..... بالمصلحة الولائية للشرطة القضائية بأمن ولاية -------
---------- / **ضابط الشرطة القضائية** بقطاع إختصاص محكمة ---------- / بمساعدة مفتش الشرطة / ب.ن التابع للمصلحة---------- / **عملا بنص المواد 44 إلى 48** من قانون الإجراءات الجزائية ونصوص القانون 04/09 المتعلق بجرائم تكنولوجيا الإعلام و الإتصال /---------- تنفيذا للإذن بالتفتيش الصادر تحت رقم..../.. المؤرخ في ../../.... عن السيد/ وكيل الجمهورية لدى محكمة .....، الرامي إلى التفتيش الإلكتروني للهاتف من نوع SAMSUNG Galaxy S23 أزرق اللون ، المثبت به شريحة موبيليس رقم: ** ** ** **06 والحامل لقم الإيماي ********** ملك للمسمى : ب. ع، من مواليد 1978/05/22 الجزائر، إبن **********، جزائري الجنسية، بدون مهنة، الكائن مقره برقم 10 شارع حلوش سليمان بولاية الجزائر، الماتابع في قضية التهديد بإستعمال تكنولوجيا الإعلام و الإتصال).----------

الموضـوع:
محضر تفتيش إلكتروني لهاتف المدعو/ب ع المقيم بالجزائر

- / نقول أنه بالتاريخ و الساعة المذكورين أعلاه باشرنا عملية التفتيش الإلكتروني على الهاتف النقال الحامل للمواصفات التقنية المبينة أعلاه أين وقفنا على ما يلي /----------

01/-خصائص الهاتف محل التفتيش ----------

التكييـف
التهديد بإستعمال تكنولوجيا الإعلام والإتصال

02/ أثناء عملية الولوج لذات المنظومة المعلوماتية المشار إليها أعلاه ، قمنا بتفحص حساب المعني بموقع التواصل الاجتماعي فايسبوك ، و بالضبط بتطبيقة مسنجر الحامل للاسم المستعار ********** رابط ملف الشخصي على الفايسبوك https ://www.facebook.com******** مع الضحية كما هوم بين أدناه ----------

.../...

-

03 / رصدنا محاثة بين المهني والضحية خلال شهر *****، تتمحور على تبادل عبارات التهديد والسب والشتم أين تلفظ المعني بعبارة (نحكمك كي تجي **********)، اين قامت الضحية بالرد على المعني قائلة (ضرك نقول لبابا بلي أنت *******) ----------

تابع لمحضر تفتيش إلكتروني للمدعو / (ب . ع)

- / إنتهت عملية التفتيش على الساعة..... من نفس اليوم. --------- / بعد تلاوة المحضر على المعني بالأمر أكد ما جاء فيه ووقع المساعدون ووقعنا معه. ----------
----

- المعني بالأمر- - المساعدون - - ضابط الشرطة –

الجمهوريـــة الجزائريـــة الديمقراطيـــة الشعبيـــة
وزارة الداخلـــيـــة والجماعات المحلية
و التهيئة العمرانية
المديريـــة العامـــة للآمـــن الوطنـــي
أمـــن ولايـــة
المصلحـــة الولائيـــة للشرطـــة القضائيـــة
رقم / أوج/م و ش ق/ق غ/

– محضـــــر إستفارغ لذاكرة وميضية (flashdisque) –

قضيـــة

ضد المدعو/

- ب . ع .

- / إنه في: يوم ..... **الموافق** ..... **من شهر** .....---- /

السنة:.----------

- / **الساعة:** .....ابط الشرطة / ب ع، رئيس ..... بالمصلحة الولائية للشرطة القضائية بأمن ولاية - ---------- / **ضابط الشرطة القضائية** بقكطاع إختصاص محكمة ---------- / بمساعدة مفتش الشرطة / ب.ن التابع للمصلحة---------- / **عملا** بنصوص القانون 04/09 المتعلق بجرائم تكنولوجيا الإعلام و الإتصال /---------- ---------- تنفيذا للتعليمة النيابية الصادر تحت رقم..../.. المؤرخ في ../../.... عن السيد/ وكيل الجمهورية لدى محكمة .....، الرامي إلى إجراء عملية إستفراغ لذاكرة وميضية (flashdisque) من نوع Flash Disque ADATA 32GB USB 2.0 C906 أسود اللون ، ملك للمسمى : ب. ع، من مواليد 1978/05/22 الجزائر، إبن **********، جزائري الجنسية، بدون مهنة، الكائن مقره برقم 10 شارع حلوش سليمان بولاية الجزائر، الماتابع في قضية التهديد بإستعمال تكنولوجيا الإعلام و الإتصال).--------- ----------

الموضـــوع:

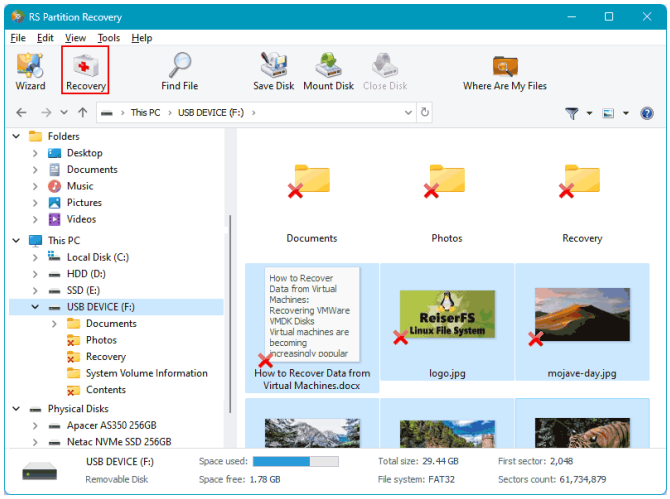
محضر تفتيش إلكتروني لهاتف المدعو/ب ع المقيم بالجزائر

- / نقول أنه بالتاريخ و الساعة المذكورين أعلاه باشرنا عملية إستفراغ إلكتروني على لذاكرة وميضية (flashdisque) الحامل للمواصفات التقنية المبينة أعلاه أين وقفنا على ما يلي /-01/- خصائص الهاتف محل التفتيش ----------

التكييـــف

التهديد بإستعمال تكنولوجيا الإعلام و الإتصال

.../... 02 / أثناء عملية الولوج لذات الذاكرة الوميضية flashdisque المشار إليها أعلاه ، قمنا بتفحص الملفات الموجودة على الذاكرة و التي كانت كما هومبين أدناه ----------



03 / رصدنا خمسة ملفات تحمل التسميات الآتية /----------

04 / الملف الأول يحمل تسمية Systeme و الذي سعته MO 400 و يحتوي بداخله على ملفات و تعريفات برمجية للذاكرة الوميضية /----------

05 / الملف الثاني يحمل تسمية DCIM و الذي سعته MO 700 و يحتوي بداخله على ملفات 20 صورة تخص المعنية في مختلف الأماكن ، بالإضافة إلى 03 فيديوهات تخص الضحية رفقة المعني في منطقة بحرية /----------

تابع لمحضر الإستفراغ الإلكتروني للذاكرة الوميضية flashdisque للمدعو/ (ب . ع)

- / إنتهت عملية الإستفراغ على الساعة..... من نفس اليوم.--------- / بعد تلاوة المحضر على المعني بالأمر أكد ما جاء فيه و وقع ووقع المساعدون و وقعنا معه.-----

---

- المعني بالأمر- **- المساعدون -** **- ضابط الشرطة -**

الجمهوريــة الجزائريــة الديمقراطيــة الشعبيــة

وزارة الداخلــيــة والجماعات المحلية

و التهيئة العمرانية

المديريــة العامــة للآمــن الوطنــي

أمــن ولايـــــة

المصلحــة الولائيــة للشرطــة القضائيــة

رقـم / أوج/م و ش ق/ق غ/

- محضـــــر إستقراء لفيديو إلكتروني -

قضيـــة

ضد المدعو/

- ب . ع .

- / إنه في: يوم **..... الموافق ..... من شهر .....---- /**

السنة:----------

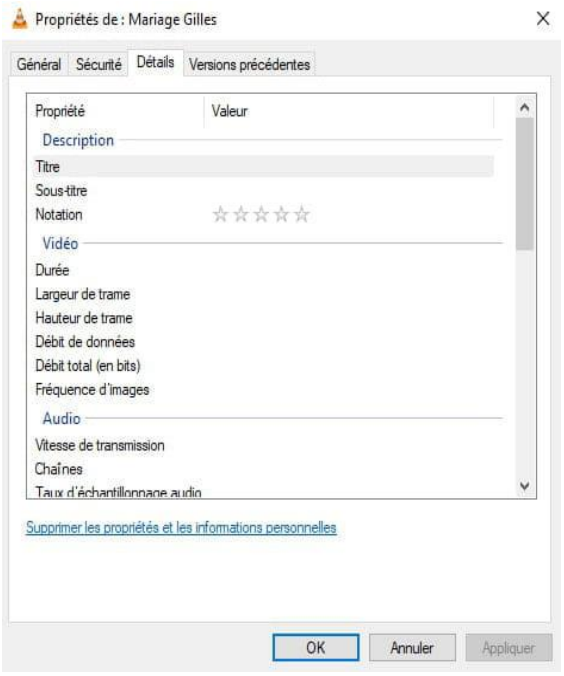
- / الساعة: .....ابط الشرطة / ب ع، رئيس ..... بالمصلحة الولائية للشرطة القضائية بأمن ولاية ------- ---------- **/ ضابط الشرطة القضائية** بقطاع إختصاص محكمة ---------- / بمساعدة مفتش الشرطة / ب.ن التابع للمصلحة---------- **/ عملا** بنصوص القانون 04/09 المتعلق بجرائم تكنولوجيا الإعلام و الإتصال /---------- -------- تنفيذا للتعليمة النيابية الصادر تحت رقم..../../.. المؤرخ في ../../.... عن السيد/ وكيل الجمهورية لدى محكمة .....، الرامي إلى إجراء عملية إستقراء لفيديو يحمل التسمية VID00012CEمن صيغة WMV مثبت على قرص مضغوط من نوع DVD ADATA بسعة 08 GO أبيض اللون ، ملك للمسمى : ب. ع، من مواليد 1978/05/22 الجزائر، إبن **********، جزائري الجنسية، بدون مهنة، الكائن مقره برقم 10 شارع حلوش سليمان بولاية الجزائر، الماتابع في قضية التهديد بإستعمال تكنولوجيا الإعلام و الإتصال).----------

الموضـوع:

محضر تفتيش إلكتروني لهاتف المدعو/ب ع المقيم بالجزائر

- / نقول أنه بالتاريخ و الساعة المذكورين أعلاه باشرنا عملية إستقراء لفيديو يحمل التسمية VID00012CEمن صيغة WMV مثبت على قرص مضغوط من نوع DVD ADATA الحامل للمواصفات التقنية المبينة أعلاه أين وقفنا على ما يلي----------

/-01- خصائص الفيديو محل الإستقراء ----------



التكييـف

التهديد بإستعمال تكنولوجيا الإعلام و الإتصال

.../... 02 / أثناء عملية الولوج لذات الفيديو المشار إليه أعلاه ، قمنا بتفحص الملف الموجودة على القرص و التي كانت كما هومبين أدناه ----------

03 / رصدنا فيديو بحجم 01 GO بصيغة wmv بطول 15 دقيقة يخص المعني رفقة الضحية في رحلة سياحية على متن حافلة تابعة لشركة الأسفار المسماة *********و التي تقوم بتنظيم رحلات مختلطة إلى ولاية *********من أجل التنزه ، حيث يظهر في الفيديو المعني وهو يتحدث مع المجنية حيث يقول(شفتي رانا زاهيين **********) في حين تقوم هذه الأخيرة بالرد عليه قائلة (أنا كنت نسخف نروح نحوس **********) ، كما أننا نلاحظفي الدقيقة 05د و 20ثا نجد أن المعني خاطب الضحية قائلا (المرة الجاية نروحو لدزاير *********) أين تقوم هذه الأخيرة بالرد عليه (دزايربعيدة ونخاف يسمعو**********) /----------

تابع لمحضر الإستقراء إلإكتروني للفيديو يحمل التسمية VID00012CE من صيغة WMV مثبت على قرص مضغوط من نوع DVD ADATA للمدعو/ (ب . ع)

- / إنتهت عملية الإستقراء على الساعة..... من نفس اليوم.--------- / بعد تلاوة المحضر على المعني بالأمر أكد ما جاء فيه و وقع ووقع المساعدون و وقعنا معه.----------
---

- المعني بالأمر- **- المساعدون -** **- ضابط الشرطة -**

الفهرس

الفهرس:

الفصل الثاني: إجراءات المعاينة، الحجز والتفتيش في الجرائم المعلوماتية

الملخص

الملخص:

تعتبر الجرائم المعلوماتية من الجرائم المستحدثة التي ترتكب في بيئة إلكترونية افتراضية ما جعل آليات مكافحتها كالمعاينة الحجز والتفتيش تخضع لإجراءات خاصة تتلاءم مع الواقع الإلكتروني.

تضمنها المشرع الجزائري في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 09-04.

Abstract:

Cybercrimes are recognized as emerging offenses committed in a virtual electronic environment, necessitating specialized countermeasures—such as digital forensics, seizure, and search procedures—that align with the technical nature of cyberspace.

The Algerian legislature has codified these provisions in Law No. 09-04 on the Prevention and Suppression of Crimes Related to Information and Communication Technologies.

Résumé:

Les cybers crimes sont considérés comme des infractions nouvelles commises dans un environnement électronique virtuel, ce qui a conduit à l'adoption de mécanismes de lutte spécifiques tels que la perquisition, la saisie et la perquisition, soumis à des procédures particulières adaptées à la réalité numérique. Le législateur algérien a

encadré ces dispositions dans la Loi n° 09-04 relative à la prévention des infractions liées aux technologies de l'information et de la communication et à leur répression.

الملخص