الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعـــــة عباس لغرور خنشلة
كلية الحقوق و العلوم السياسية

قسم : الحقوق

إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية

مذكرة مكملة لنيل شهادة الماستر في شعبة الحقوق
تخصص: قانون جنائي والعلوم الجنائية

إعـــــداد الطالبة :
بدغيو نوال

إشـــــــراف الأستاذة:
قابوش وهيبة

أعضاء لجنة المناقشة:

الإسم واللقب	الرتبـــــة	الجامعة	الصفـــــــــة
بوكربوعة أحلام	محاضر أ	جامعة خنشلة	رئيسا
قابوش وهيبة	أستاذ مساعد أ	جامعة خنشلة	مشرفا ومقررا
سلامي نادية	محاضر أ	جامعة خنشلة	عضوا ممتحنا

السنة الجامعية 2025/2024

شكر وعرفان

عملا بقوله تعالى" لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ"

إن الشكر الله وحده لا شريك له الذي لا يطيب الليل إلا بشكره، و لا النهار إلا بذكره و لا تطيب اللحظات إلا بطاعته، و لا تطيب الآخرة إلا بعفوه، ولا تطيب الجنة إلا برؤيته، أحمده و أشكر فضله في توفيقي لإنجاز هذا البحث.

أتقدم بجزيل الشكر وعظيم العرفان للأستاذة الفاضلة " قابوش وهيبة" لقبولها الإشراف على هذا البحث وعلى توجيهاتها القيمة التي كانت محل تقدير وامتنان لا ينسى . كما أنها لم تدخر جهدا لأجله وكل ذلك بطلاقة وجه ورحابة صدر، فجزاها عني خير الجزاء، وبارك الله في وقتها و عملها، مع التمني لها دوام النجاح و التوفيق في مشوارها العلمي.

كما أتقدم بجزيل الشكر إلى الأساتذة الأفاضل "أعضاء لجنة المناقشة" الذين تحملوا عناء قراءة وتفحص هذه المذكرة، وعلى ملاحظاتهم التي ستكون نبراساً لي في مسيرتي القادمة.

كما لايفوتني في هذا المقام أن أتقدم بأسمى عبارات الشكر والتقدير لجميع أساتذة كلية الحقوق والعلوم السياسية . و أخص بالذكر الأستاذ "لخذاري عبد المجيد"، الأستاذ" مرداسي حمزة"، وكذا الأستاذة الرائعة " تكواشت جدة.. الذين قدمو لي الكثير أسأ ل المولى أن يسدد خطاهم ويوفقهم في مسارهم المهني.

إهداء

إلى من علمني كيف أمسك بالقلم وكيف أخط الكلمات بلا ندم. إلى قدوتي الأولى ونبراسي الذي أنار دربي وكان لي نعم السند والعون إلى من غاب عن الدنيا "**أبي الغالي** "رحمه الله وأسكنه فسيح جناته.

إلى من ساندتني في صلاتها ودعائها وحاكت سعادتي بخيوط من قلبها. إلى قرة عيني "**أمي الحبيبة** "أطال الله في عمرها.

إلى الذين ظفرت بهم هدية من الله إخوة فعرفوا معنى الأخوة "**إخوتي وأخواتي** " الأحباء حفظهم الله.

إلى من مددن لي يد العون فجسدن معنى المحبة "**زوجتي أخوي** " أسأل المولى أن يحفظهن ويسعدهن في حياتهن.

إلى براعم العائلة ونورها وبهجة الأيام..."**أبناء اخوتي وابن أختي**". أسأل الله أن يحفظهم ويرعاهم.

إلى من لم تلدهن أمي بل ولدتهن لي الأيام "**صديقاتي**" أتمنى لهن التوفيق والنجاح.

قائمة المختصرات

أولا: باللغة العربية

ق إ ج: قانون الإجراءات الجزائية

ق ع : قانون العقوبات

دج: دينار جزائري

ج ر ج ج: الجريدة الرسمية للجمهورية الجزائرية

ج: جزء

ط: طبعة

م: مجلد

تح: تحقيق

ع: عدد

ف: فقرة

ص: صفحة

ص ص: من صفحة إلى صفحة

د س ن : دون سنة نشر

د ب ن: دون بلد نشر

ثانيا: باللغة الأجنبية

IP : Adresse Internet Protocole
TCP : Trams Commission Protocol
P: page

مقدمة

مقدمة

أصبح استخدام الحواسيب وشبكات الأنترنت جزء أساسيا في حياتنا اليومية، وذلك لما تقدمه من تســـهيلات في مجالات متعددة، فتحولت عديد مظاهر الحياة من الطابع التقليدي والمادي إلى أسلوب حديث ورقمي.

غير أن هذا التطور أفرز تحديات جديدة خاصة فيما يتعلق بالأمن السيبراني، وذلك من خلال ظهور جرائم تمس بالمنظومة المعلوماتية، يطلق عليها قانونا "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، التي أضـــافها المشـــرع الجزائري بعد تعديله لقانون العقوبات سنة 2004، من أجل مكافحة هذا النوع من الإجرام، الذي يعتبر من أخطر الجرائم على الإطلاق في الوقت الراهن، نظرا لسهولة ارتكابها من قبل مجرمين أذكياء يمتلكون أدوات متطورة ويتمتعون بمهارات وخبرات عالية.

إلا أن ذلك لم يغطي الصـــرح الكبير الذي تكتسيه الجرائم الواقعة داخل البيئة الرقمية، الأمر الـــذي دفع بـــالمشـــرع مرة أخرى لتعـــديل بعض أحكام قانون العقوبات وقانون الإجراءات الجزائيـــة، وذلك ســـنة 2006 من أجل ســـد الفراغ القانوني الذي اعترى المنظومـــة القـــانونيـــة، أين جاء بقواعد إجرائية خاصـــة بالبحث والتحري في الجرائم المستحدثة ومنها "الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات " كما ذكرنا آنفا.

وباعتبار أن الإجرام المعلوماتي في تطور مســـتمر، كان لزاما على المشرع الجزائري مواكبة التطور الحاصـــل، حيث عمد إلى استحداث قانون يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سنة 2009، وهو القانون رقم 09-04 الذي تضـــمن جملة من الإجراءات تتماشى والطبيعة التقنية للجرائم الواقعة داخل المنظومة المعلوماتية.

وبما أن هذه الجرائم لها خصـــوصـــية في ارتكابها، فإنه وللتصـــدي لها لابد من القيام بإجراءات كالمعاينة المعلوماتية وإجراءات تفتيش المنظومات، إضافة إلى حجز المعطيات المعلوماتية، وقد إقتصرت دراستنا في التشريع الجزائري دون التشريعات الأخرى.

أهمية الدراسة

أصـــبح موضـــوع البحث يكتسي أهمية بالغة بالنظر لحجم الانتهاكات الواقعة على الأنظمة المعلوماتية في ظل التطورات التكنولوجية الراهنة، وظهور ما يســـمى "بالمجرم المعلومـــاتي"، وبـــالتالي فإن القواعد الإجرائية المألوفة في قانون الإجراءات الجزائية لا تتوافق وهذه الجرائم.

باعتبار أن الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات تعد من بين الجرائم العابرة للحدود الوطنية، فإن دراستنا لموضوع "إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية " له أهمية بارزة، وتكمن أســـاسا في كون أن هذه الإجراءات تشكل آلية فعالة في الكشـــف عن الجرائم الواقعة في الوسط الرقمي، إضافة إلى الحد أو محاولة التقليل منها.

أسباب اختيار الموضوع

ترجع أســـباب اختيارنا لهذا الموضوع إلى اهتماماتنا وشغفنا الذي ينصب على كل ما يتعلق بمجال البحث والتحري، وجهاز الضبطية القضائية على وجه الخصوص، أضف إلى ذلك رغبتنا في التعمق والبحث في ثنايا الموضوع.

من بين الأســـباب كذلك حداثة الموضـــوع إذ لم ينل حظه بالبحث، ذلك أن معظم الدراســـات اقتصـــرت على الجانب الموضـــوعي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات دون الشـــق الإجرائي، الأمر الذي شجعنا على الاجتهاد -كمحاولة منا-لإثراء هذا الموضوع والبحث فيه أكثر.

أهداف الدراسة

نسعى من خلال هذه الدراسة إلى تحقيق بعض الأهداف، منها:

- إبراز القواعد الإجرائية المتبعة لمعاينة مسرح الجريمة المعلوماتية.
- محاولة تحليل النصوص القانونية الخاصة بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.

- الوقوف على أهم الطرق والبرامج لجمع الدليل الرقمي، إضافة إلى إبراز الصعوبات التي تواجه السلطة المختصة أثناء حجزه.

صعوبات الدراسة

- اتجاه أغلب الدراسات إلى دراسة الظاهرة الاجرامية من حيث السلوك الإجرامي والعقوبات المقررة لها دون التركيز على الجانب الإجرائي.
- واجهنا صعوبة نوعا ما فيها يخص دراسة " القواعد الإجرائية للمعاينة داخل المنظومة المعلوماتية"، ذلك أن المشرع الجزائري اكتفى بالنص في القانون رقم 09 -04 على القواعد التي تنظم إجراءات المراقبة الالكترونية، إجراءات تفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية دون إجراء المعاينة المعلوماتية.

الدراسات السابقة

باعتبار أن موضوع "إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية" من بين المواضيع المستحدثة نوعا ما، الأمر الذي دفع بناء إلى البحث فيه، وذلك بالاعتماد على العديد من الدراسات، نذكر منها:

01- دراسة بعنوان " آليات البحث والتحقيق في الجرائم المعلوماتية"، للباحث ربيعي حسين، مقدمة لنيل شهادة الدكتوراه، بجامعة باتنة 1، سنة 2016.

أين تناول الموضوع في ثلاث فصول، خصص الأول منها لدراسة " الإطار المفاهيمي للجريمة المعلوماتية "، أما الثاني تطرق فيه " لمسألة شرعية إجراءات البحث والتحقيق في الجرائم والجهات المختصة بتنفيذها " في حين تطرق "للإجراءات الخاصة بالبحث والتحقيق في الجرائم المعلوماتية وذلك في الفصل الثالث.

حيث توصل الباحث فيما يتعلق بالبحث والتحقيق في الجرائم الواقعة داخل المنظومة المعلوماتية، إلى أنه لا مجال لإعمال الإجراءات الخاصة بالبحث والتحقيق في الجرائم التقليدية لمواجهة الجرائم المعلوماتية؛ ذلك أن هذه الأخيرة تستلزم إجراءات من نوع خاص .وهذا ما تؤكده دراستنا.

2. دراســـة بعنوان " إجراءات المعــاينة، التفتيش والحجز داخل المنظومة المعلوماتية"، للطالب محمد رزيق، مذكرة مقدمة لنيل شـــهادة الماســـتر في القانون العام، بجامعة آكلي محند أولحاج البويرة، سنة 2009.

حيث شـــملت دراسته لهذا الموضوع فصلين، تناول في الأول "إجراءات التحري التقليدية للكشـــف عن الجرائم داخـــل المنظومة المعلوماتية، كما تطرق في الثاني إلى "إجراءات التحري المستحدثة للكشف عن الجرائم داخل المنظومة المعلوماتية ".

يهـــدف من خلالها الطالب إلى إبراز إجراءات التحري التقليدية المتبعة في الكشـــف عن الجرائم الواقعة داخل المنظومة المعلوماتية، إضافة إلى معرفة الإجراءات المستحدثة مثل "التفتيش والحجز الالكتروني".

إلا أننا تناولنا هذه الإجراءات بشكل من التفصيل من خلال استقراء النصوص القانونية التي تنظم كل إجراء على حدى.

إشكالية الدراسة

مع التطور التكنولوجي المتســـارع، تصـــاعد خطر الجرائم التي تســـتهدف الأنظمة المعلومـــاتيـــة، وفي إطار مكافحتها نص المشـــرع الجزائري في قوانينه على إجراءات المعاينة، التفتيش والحجز الالكتروني، التي تعد وسيلة جوهرية لجمع الأدلة الرقمية، ومنه تحقيق الغـــايـــة المرجوة وعدم إفلات المجرمين من العقاب، ونظرا للدور المحوري لهذه الإجراءات، فإن الإشكالية هنا تتمحور حول دور الضبطية القضائية في إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية؟

تندرج تحت هذه الإشكالية تساؤلات فرعية، ومن ذلك:

- فيما تكمن أهم الخطوات الواجب مراعاتها لمعاينة مسرح الجريمة المعلوماتية؟
- فيمـــا تتمثـــل الإجراءات الخـــاصـــة بالتفتيش والحجز الالكتروني في ظل قانون الإجراءات الجزائية والقانون رقم 09-04؟

- ماهي الطرق المعتمدة لجمع الدليل الرقمي؟ فيما تتمثل العراقيل التي تعترضـــه أثناء عملية الحجز؟

منهج الدراسة

فرضـــت علينا طبيعة الموضوع اتباع المنهج الاستقرائي وذلك من خلال تحليل النصوص القانونية الخاصـــة بإجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية، كما اقتضـــت بعض جزئيات الدراسة اعتماد المنهج الوصفي، وذلك من خلال تناولنا لمختلف التعاريف المقدمة بشأن هذه الإجراءات.

تقسيم الدراسة

للإجابة عن إشكالية الموضوع اعتمدنا خطة ثنائية شملت فصلين، خصصنا الأول لدراسة الإطار القانوني للمعاينة المعلوماتية، تطرقنا فيه إلى مبحثين تضـــمن الأول مفهوم المعاينة المعلومـــاتية في حين عنون الثاني بالقواعد الإجرائية للمعاينة داخل المنظومة المعلوماتية، أمـــا الفصـــل الثـــاني جاء تحت عنوان الإطار القانوني للتفتيش والحجز داخل المنظومة المعلومـــاتية، احتوى على مبحثين، تناولنا في الأول " التفتيش داخل المنظومة المعلوماتية" أما الثاني عالجنا من خلاله الحجز داخل المنظومة المعلوماتية.

الفصل الأول

الإطار القانوني للمعاينة المعلوماتية

تمهيد وتقسيم

شهدت العقود الأخيرة تطورا سريعا في مجال التكنولوجيا مما أثر بشكل كبير على جميع جوانب الحياة، ومع التقدم التكنولوجي ظهرت تحديات جديدة تتعلق بالأمن السيبراني الأمر الذي أدى إلى ظهور جرائم ماسة بالمنظومة المعلوماتية، والمقصود بهذه الأخيرة حسب ما ورد في الفقرة "ب" من المادة 02 من القانون 09-04[1] أنها": أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة، آلية للمعطيات تنفيذا لبرنامج معين"، كما يقصد بها وفقا لما جاء في المادة الأولى، فقرة "أ" من الاتفاقية المتعلقة بالجريمة الإلكترونية والمؤرخة في 23 نوفمبر 2001 ببودابست أنها:" أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحدا منها أو أكثر، وفقا لبرنامج بالمعالجة الآلية للبيانات" .[2]

ومع تفاقم الاعتداءات على المنظومة المعلوماتية، أصبحت الحاجة ملحة لتطبيق إجراءات فعالة من أجل حمايتها ومكافحة هذا النوع من الإجرام المستحدث، وتعتبر المعاينة أحد أهم إجراءات التحقيق خاصة في الكشف عن الجرائم الواقعة في البيئة الرقمية والتي نحن بصدد دراستها من خلال هذا الفصل، لذا ارتأينا تقسيمه إلى مبحثين، نتطرق في الأول إلى مفهوم المعاينة المعلوماتية، أما الثاني نتناول ضمنه القواعد الإجرائية للمعاينة المعلوماتية.

---

[1] قانون رقم 09-04 . المؤرخ في 05 غشت سنه 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، الصادرة في 16 غشت سنة2009، ص 05.

[2] هذا النص الأصلي كما ورد في الإتفاقية:

Article 01 paragraphe a" of convention Cybercrime"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

المبحث الأول: مفهوم المعاينة المعلوماتية

تعتبر المعاينة أهم إجراءات التحقيق في جميع الجرائم، كونها نقطة البداية التي يتوقف على دقتها صحة كافة الإجراءات الموالية لها، ومع تزايد الاعتماد على التكنولوجيا ووسائل الاتصال الحديثة أصبح الفضاء السيبراني ساحة لنوع جديد من الجرائم والتي تعددت تسمياتها، فالبعض يطلق عليها "**الجريمة الالكترونية**" أما البعض الآخر يسميها "**جرائم تقنية المعلومات**" في حين يفضل البعض الآخر تسميتها "**بالجرائم المعلوماتية**"، وبما أن الجرائم الواقعة داخل المنظومة المعلوماتية في تزايد مستمر فإن المعاينة تزايدت أهميتها في الكشف عن هذه الجرائم كونها الوسيلة الفعالة للوصول إلى الحقيقة.

ومن هذا المنطلق سنتطرق في هذا المبحث إلى تحديد تعريف المعاينة المعلوماتية في المطلب الأول، في حين سنتناول ضمن المطلب الثاني الطبيعة القانونية للمعاينة المعلوماتية وأهميتها.

المطلب الأول: تعريف المعاينة المعلوماتية

تعد المعاينة أحد إجراءات التحقيق التي تجري عقب الإبلاغ بوقوع جريمة معينة، وبالنظر للدور الفعال الذي تلعبه في الإثبات ومعرفة الحقيقة كما ذكرنا آنفا، كان لابد لنا من تحديد المقصود من "المعاينة المعلوماتية" سواء من الناحية اللغوية أو الاصطلاحية وهو ما سندرسه ضمن هذا المطلب.

الفرع الأول: التعريف اللغوي للمعاينة المعلوماتية

من خلال هذا الفرع سنتطرق إلى المدلول اللغوي" للمعاينة المعلوماتية"، المكونة من شطرين، تتناول كل شطر على حدى:

لفظ "معاينة" عاين معاينة وعيانا (ع ي ن ه): رآه بعينه[1].

[1] جبران، مسعود. *الرائد – معجم اللغوي عصري رتبت مفرداته وفقا لحروفها الأولى-*. ط7، بيروت: دار العلم للملايين، 1992، ص 537.

والعين والمعاينة: النَّظَر وقد عايَنهُ مُعاينة وعِيانًا: لم يشك في رؤيته إياه [1].

ولقيتــه عيــانًا، ومعاينة وفي المثل: «ليس الخبر كالعيَان»[2] والمعاينة: هي المُشــاهَدَةُ بالعْينِ– الأخوَّةُ بَيْنَ الأَعْيَانِ[3].

أما المدلول اللغوي لكلمة "المعلوماتية" فهي: إســم منســوب إلى معلومات، وهي مَجْمُوع التِقْنيَّات المُتعلِّقة بالمَعْلُومات ونَقْلِها خَاصــَّةً مُعَالَجتِها الآلِيَّة والعَقْلِيَّة بِحَسَب العِلْم الإِلكْترونيّ النِّصــف الثــَّاني من القَرْن العِشــْرين مطْبوع بــالثَّوْرة التي جــاءَت بِها المَعْلُوماتِيَة[4].

بعــد أن عرجنا على المدلول اللغوي "للمعاينة" وكذا "المعلوماتية"، ســنتطرق في الفرع الموالي للمدلول الإصطلاحي.

الفرع الثاني: التعريف الإصطلاحي للمعاينة المعلوماتية

لم يتنــاول المشــرع الجزائري تعريف "المعاينة المعلوماتية"، تاركا المجال للفقه، حيث تعددت التعريفات الفقهية لكلا المصطلحين والتي سنوضحها كالتالي:

---

[1] إبن منظور، محمد بن مكرم بن علي. *لسان العرب*، م1، بيروت: دار صادر، د س ن، ص 302. منشور على الرابط-https://waqfeya.net/books/%D9%84%D8%B3%D8%A7%D9%86-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8-%D8%B7-%D8%B5%D8%A7%D8%AF%D8%B1-95f4323034d049229a15f5df1f2fb8ae آخر اطلاع بتاريخ 2025/02/01 على الساعة 14:32.

[2] أنيس، إبراهيم وآخرون. *المعجم الوســيط*. مكتبــة الشــروق الدولية، د ب ن، 2004، ص 641، منشــور على الرابط-https://waqfeya.com/books/%D8%A7%D9%84%D9%85%D8%B9%D8%AC%D9%85-%D8%A7%D9%84%D9%88%D8%B3%D9%8A%D8%B7-3385fa57ca9e415d96a9a25cf012e664 آخر إطلاع بتاريخ 2025/02/01 على الساعة 16:00.

[3] بن هادية، علي وآخرون. *القاموس الجديد للطلاب– معجم عربي مدرســي ألفبائي–* . ط7، الجزائر: المؤسسة الوطنية للكتاب، 1991، ص 1160.

[4] حموي، صــبحي. *المنجد في اللغة العربية المعاصرة*. تح ، الحموي، مأمون وآخرون. بيروت: دار المشرق، 2000، ص 1015.

يقصـــد "بالمعاينة" رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشـــف الحقيقة، عرفها" **علي شـــملال** "بأنها:" انتقال ضابط الشرطة القضائية إلى مكان وقوع الجريمة إذ تطلب الأمر ذلك من أجل إثبات حالة الأماكن، ومعاينة مخلفات الجريمة، وضـــبط الأشـــياء المتحصـــلة أو المتخلفة عنها أو التي تفيد في تنفيذ الجريمة"[1]، أوهي" مشـــاهدة مســـرح الجريمة وإثبات الحالة فيه أي مشاهدة وإثبات الآثار التي خلفها الجاني لارتكاب الجريمة، للمساعدة على كشف الحقيقة"[2].

رغم إختلاف وتعـــدد التعاريف المقدمة للمعاينة، إلا أننا نجدها تتصـــب في معنى واحد فالمعاينة هي "مشاهدة مسرح الجريمة وإثبات الحالة التي يكون فيها والمحافظة على الآثار للوصول إلى الحقيقة".

أما "**المعلوماتية**" فهي كلمة مشـــتقة في اللغتين الإنجليزية والفرنســـية /Informatique Infomatics من المقطع الأول من كلمـــة "معلومات"information والمقطع الأخير من كلمـــة آليAutomatic/Automatique ، وذلـــك للتعبير عن المعالجة الآلية للمعلومات وهي تعبير في مجملها عن الإدماج والتزاوج بين تلك، المستحدثات التقنية المتقدمة للتحكم في المعلومات وجمعها ثم معالجتها واختزالها وتحســـين الانتفاع بها كالاقراص الليزرية

[1] شـــملال، علي. *الجديد في شـــرح قانون الإجراءات الجزائية–الاســـتدلال والإلهام*–. ج 1، ط3، الجزائر: دار هومة، 2017.ص 39.

[2] بواط، محمد. *محاضـــرات في قانون الإجراءات الجزائية*. دروس ألقيت على طلبة السنة الثانية ليسانس، كلية الحقوق والعلوم الســـياســـية، جامعة حســـيبة بن بوعلي، الشلف، 2021 –2022، ص 136، محاضرات منشورة على الرابط https://www.univ-chlef.dz/fdsp/wp-content/uploads/2023/05/Droit_Procedure_Penal_BOUAT.pdf، آخر إطلاع بتاريخ 2025/02/03 على الساعة 15:12 .

ووسائط الإدخال[1]، وقد شاع إستعمال كلمة "المعلومة" في الخمسينات في القرن الماضي في مجالات مختلفة[2].

وعليه، يمكن تعريف المعلوماتية أو ما يسمى" بعلم المعلومات" على أنه ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلوم وتجميعها وتنظيمها وتخزينها واسترجاعها وكذا تحويلها واستخدامها[3].

ويمكن لنا تعريف المعاينة المعلوماتية على أنها:" فحص الآثار التي يخلفها مستخدم الشبكة المعلوماتية والتي تشمل الرسائل المرسلة من والتي تم استقبالها وكذا كافة الاتصالات التي تمت من خلال الحاسب الآلي".

المطلب الثاني: الطبيعة القانونية للمعاينة المعلوماتية وأهميتها

نخصص هذا المطلب لدراسة الطبيعة القانونية للمعاينة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى إبراز أهميتها، وذلك وفقا لفرعين.

الفرع الأول: الطبيعة القانونية للمعاينة المعلوماتية

إن المعاينة إجراء يضطلع به كل من ضباط الشرطة القضائية، واللذين حدتهم المادة 15[4]وما يليها من ق إ ج، تحت إشراف النيابة العامة صاحبة الاختصاص الأصيل في البحث والتحري وكذلك قاضي التحقيق والمحكمة في سبيل الكشف عن الحقيقة ،كل

---

[1] بن فردية، محمد. *الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية*. أطروحة دكتوراه، جامعة الجزائر1، 2015، ص 26.

[2] بوخبزة، عائشة. *الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري*. مذكرة ماجستير، جامعة وهران، 2012 – 2013، ص 08.

[3] سعيداني، نعيم. *آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري*. مذكرة ماجستير جامعة باتنة، 2012–2013، ص 12.

[4] راجع أحكام المادة 15 من الأمر رقم 66–155. المتضمن ق إ ج، المؤرخ في 8 يونيو1996،ج رج ج، ع 48، الصادرة في 10يونيو 1966، المعدل والمتمم بالقانون 19–10. المؤرخ في11 ديسمبر سنة 2019، ج ر ج ج، ع 78، الصادرة في 18 ديسمبر سنة 2019، ص 11.

حسب اختصاصه الإقليمي والنوعي[1]، حيث يتحدد الاختصاص الإقليمي لضباط الشرطة القضـــائية حســـب ما ورد في المادة 16 من ق إ ج، في الحدود التي يباشـــرون ضمنها وظائفهم المعتادة[2]، غير أنه فيما يتعلق ببحث ومعاينة الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات فإن اختصاصهم يمتد إلى كافة الإقليم الوطني[3].

وبالرجوع لمضمون المادتين 37 و40 من ق 04-14[4]، فقد حددتا ضوابط إنعقاد الإختصـــاص المحلي لكل من وكيل الجمهورية وقاضـــي التحقيق، بمكان وقوع الجريمة ومحل إقامة أحد الأشـــخاص المشـــتبه في مســـاهمتهم فيها أو بالمكان الذي تم في دائرته القبض على أحـــدهم[5]، غير أنه في حالة وقوع الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات، فقد أجاز المشرع تمديد الإختصاص المحلي لوكيل الجمهورية وقاضي التحقيق إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم[6].

---

[1] قلات، ســـومية، حاحة، عبد العالي. "مقتضيات المعاينة المعلوماتية". *مجلة الحقوق والحريات*، جامعة بسكرة، م 10، ع1، أفريل 2022، ص 524. مقال منشور على الرابط https://asjp.cerist.dz/en/article/219038آ آخر إطلاع بتاريخ 2025/02/04، على الساعة 14:58 .

[2] جاء في الفقرة الأولى من المادة 16 ق إ ج "يمارس ضـــباط الشـــرطة القضائية إختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة".

[3] ورد في المـــادة 16/ ف 07 "غير أنـــه فيمـــا يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، يمتد إختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

[4] الأمر رقم 66-155، المتضـــمن قانون الإجراءات الجزائية، المصدر السابق، المعدل والمتمم بالقانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، ج ر ج ج، ع71، المؤرخ في 10 نوفمبر سنة 2004، ص 04.

[5] راجع الفقرة الأولى من المادتين 37 و40 من القانون 04-14، المصدر نفسه، ص 05.

[6] أنظر المادة الأولى من المرسوم التنفيذي رقم 06-348. المؤرخ في5 أكتوبر سنة2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج رج ج ،ع 63 ،الصادرة في 8 أكتوبر سنة 2006 ،ص 30

دون إغفال دور الهيئة الوطنية للوقاية من الجرائم المتصـــلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، وهو ما ورد في الفقرة الثانية من المادة14 [2]من القانون رقم 09-04، والتي من مهامها مســاعدة الســلطات القضــائية ومصالح الشرطة القضـــائية في التحريات التي تجريها بشـــأن الجرائم ذات الصـــلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية[3].

من خلال نص المادة أعلاه نســتنتج أن لهذه الهيئة صــلاحية إجراء المعاينة في ســبيل الكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

كما يقوم ضــباط الشــرطة القضــائية، وتحت رقابتهم أعوان الشرطة القضائية، بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة، إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء أنفسهم، حسب ما نصت عليه المادة 63 ق إ ج.

لقاضي التحقيق كذلك صلاحية إجراء المعاينة وهو ما يتضح من خلال نص المادة 79 من ق إ ج، بحيث يجوز له أن ينتقل إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته[4].

---

[1] جاء في نص المادة13/ف1 من القانون 09-04 "تنشـــأ هيئة وطنية للوقاية من الجرائم المتصـــلة بتكنولوجيا الإعلام والاتصال ومكافحته"

[2] نصت المادة 14 من القانون 09-04 أنه "تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام الآتية:

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

ب- مســاعدة الســلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات والخبرات.

ت- تبادل المعلومات مع نظيرتها في الخارج قصـــد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم."

[3] انظر المادة 04 من المرسوم الرئاسي رقم. 261-15 المؤرخ في 8 أكتوبر سنة .2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، ع53 ، الصادرة في8 أكتوبر سنة2015 ،ص16.

[4] تنص المادة 79 من ق إ ج "ويجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها. ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته. ويستعين قاضي التحقيق دائما بأمين ضبط التحقيق ويحرر محضر بما يقوم به من إجراءات".

وعليه، فإن المعاينة المعلوماتية وطبقا لطبيعتها القانونية ينظر لها بين كونها "إجراء تحقيق إبتـــدائي" يبدأ تنفيذه عقب تلقي أجهزة الشـــرطة البلاغ بوقوع الجريمة والانتقال الســـريع لمســـرح الجريمة لمشاهدتها والحصول على أدلة لإثبات[1]،وهو ما نصت عليه الفقرة الأولى من المادة 235ق إ ج "يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة "،وبين كونها الوســـيلة لاســـتنطاق مسرح الجريمة والحصول على الأدلة لإثبات الجريمة وبالتالي فهي من الناحية القانونية "وسيلة إثبات في المادة الجزائية[2].

الفرع الثاني: أهمية المعاينة المعلوماتية

للمعاينة في الجرائم التقليدية أهمية بالغة، إذ تعطي صـــورة ووصف دقيق لمكان الجريمة والآثار المادية ذات الصـــلة بالجريمة، وكل ما من شـــأنه الإيصال للحقيقة، وهي من أهم الإجراءات التي تساعد في كشف الغموض عن الجريمة [3]، ومن هنا يمكن اختصار هذه الأهمية كما يلي:

- تنقل المعاينة صـــورة مجملة وواضحة لموقع الجريمة بكل ما يحويه من تفصيلات سواء تعلقت هذه التفصيلات بمكانه أو وصفه من الداخل أو الآثار الموجودة فيه[4].

---

[1] بن لاغة، عقيلة. "الطبيعة القانونية المعاينة". بحث منشور على الرابط https://mail.almerja.com/reading.php?idm=92644 آخر إطلاع بتاريخ 2025/02/04 على الساعة 17:05.

[2] المسعد، عبد الله عبد العزيز. *إجراءات المعاينة الفنية لمسرح الأحداث الإرهابي*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006،ص 91.

[3] نجم، محمد صبحي. *الوجيز في قانون أصول المحاكمات الجزائية*. م01، الأردن: دار الثقافة للنشر والتوزيع، 2006، صص (251-252).

[4] حجـــازي، عبد الفتاح بيومي. *مبادئ الإجراءات الجنائية في جرائم الكمبيوتر*. مصـــر: دار الكتب القانونية، 2007، ص180.

- الكشف عن الكيفية التي تمت بها ارتكاب الجريمة؛ أي أن المعاينة تعمل على إبراز الطريقة أو الأسلوب الذي اتبعه الجاني في ارتكاب جريمته مما يؤدي إلى سهولة التعرف على الجاني أو الجناة والقبض عليهم[1].

- كما تبدو الأهمية القانونية للمعاينة في الجرائم العادية من عدة نواحي: تأكيد وقوع الجريمة ونفيها بالإضافة إلى أنها تساعد المحقق على تحديد وقت ارتكاب الجريمة[2].

- تساهم النتائج المستخلصة من إجراء المعاينة في إرساء خطة عمل مناسبة تمكن المحقق من تحديد الإجراءات التي يجب أن يسرع في اتخاذها كالتفتيش أو القبض أو استجواب المشتبه فيه، وكذا تحديد الخبراء الذين قد يحتاجون إليهم من أجل رفع الآثار المتواجدة بمسرح الجريمة.

- تؤدي المعاينة الدقيقة إلى تحديد شخصية الجاني وذلك من خلال الآثار التي تركها بمسرح الجريمة [3].

إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية لا يرقى إلىالدرجة ذاتها من الأهمية كما هو الحال عليه في الجرائم التقليدية، ويمكن رد ذلك إلى أن هناك مسرح للجريمة التقليدية جرت عليه الأحداث، وتركت آثارها المادية فيه والذي تنبثق منه الأدلة؛ فالمعاينة في مسرح الجريمة العادية تتيح المجال أمام المحقق للكشف عن الآثار المادية التي خلفها ارتكاب الجريمة والتحفظ على الأشياء التي تفيد في التحقيق[4]، بينما لا يوجد عادة مسرح

---

[1] حسين، أحمد رمضان. *مسرح الجريمة وأدلته من منظور البحث الجنائي –دراسة تحليلية مقارنة –*. رسالة ماجستير، جامعة الشرق الأدنى، نيقوسيا، 2022، ص 22.

[2] ممدوح، خالد إبراهيم. *فن التحقيق الجنائي في الجرائم الإلكترونية*. الإسكندرية: دار الفكر الجامعي،2009، ص 152.

[3] قادة، عبد الهادي. *دور المعاينة الجنائية في الإثبات الجنائي*. مذكرة مكملة لنيل شهادة الماستر، جامعة مستغانم، 2023 – 2024، ص ص(17-18).

[4] حجازي، عبد الفتاح بيومي. المرجع السابق، ص 101.

مماثل للجريمة المرتكبة عبر الأنترنت، وهذا المسرح يقلل إلى حد كبير من فرص إفصاحه عن الحقائق المراد التوصل إليها من وراء معاينته[1]،وذلك لعده أسباب نذكر منها:

- أن الجرائم التي تقع بواسطة الأنظمة المعلوماتية نادرا ما تترك آثارا مادية[2].
- أن عددا كبيرا من الأشخاص قد يترددون على مكان ومسرح الجريمة خلال الفترة الزمنية التي تتوسط عاده ارتكاب الجريمة واكتشافها، مما يهيئ فرصة لحدوث تغيير وإتلاف أو عبث بالآثار المادية[3].

[1] الصغير، يوسف. *الجريمة المرتكبة عبر الأنترنت*. رسالة ماجستير، جامعة تيزي وزو، 2013، ص ص(84-85).

[2] المومني، نهلا عبد القادر. *الجرائم المعلوماتية*. ط2، عمان: دار الثقافة للنشر والتوزيع، 2010، ص 57.

[3] العزيزي، فؤاد حسن. *الجرائم المعلوماتية – دراسة مقارنة*–.الإسكندرية: دار الفكر الجامعي، 2015، ص 195.

المبحث الثاني: القواعد الإجرائية للمعاينة داخل المنظومة المعلوماتية

باعتبار أن المعاينة تعد من بين الإجراءات المهمة في الكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه ثمة شروط وقواعد تعد وجوبية للقيام بمعاينة مكونات الحاسب الآلي سواء المادية أو المعنوية ومنه تحقيق الغاية المرجوة.

وعليه فإن دراستنا لهذا المبحث تقتضي التطرق لمعاينة مسرح الجريمة المعلوماتية في المطلب الأول، إضافة إلى دراسة نطاق المعاينة المعلوماتية من خلال المطلب الثاني.

المطلب الأول: معاينة مسرح الجريمة المعلوماتية.

خصصنا هذا المطلب لدراسة "مفهوم مسرح الجريمة المعلوماتية " في الفرع الأول في حين سنبرز من خلال الفرع الثاني" الخطوات المتبعة قبل وأثناء الانتقال للمعاينة المعلوماتية".

الفرع الأول: مفهوم مسرح الجريمة المعلوماتية

إذا كانت المعاينة في الجرائم التقليدية تتم على مسرح مادي، فإن المعاينة داخل المنظومة المعلوماتية تتم على مستويين:

الفقرة الأولى: المسرح التقليدي

يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، وقد يترك فيه الجاني آثارا عدة كالبصمات وغيرها، حيث يتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل حسب اختصاصه [1].

[1] السرحاني، محمد بن نصير. *مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض،2004، ص 77.

الفقرة الثانية: المسرح السيبراني

يقع هذا المسرح داخل بيئة الحاسوب، ويتمثل في البيانات الرقمية التي تتواجد وتنتقل داخل شبكات الحاسوب في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع[1].

وبالتالي فإن معاينة مسرح الجريمة في المنظومة المعلوماتية يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر.

ويلاحظ أن الآثار الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جدا فيما تحتويه من معلومات مثل البريد الالكتروني Email، الفيديو الرقمي vidéo digital، الصوت الرقمي digital audioالملفات المخزنة في الكمبيوتر الشخصي files stored on personal computer، الصور المرئية Digtized Still Images [2].

كما أن الانتقال للمعاينة في المنظومة المعلوماتية يتم عبر العالم الافتراضي، من خلال عدة طرق، ومن ذلك:

- يمكن لضابط الشرطة القضائية اللجوء إلى مقهى الانترنت Internet Café
- وأيضا من مكتبة بالمحكمة من خلال الحاسب الآلي الخاص به .

---

[1] بن طالب، ليندا. *الدليل الإلكتروني ودوره في الإثبات الجنائي –دراسة مقارنة–*. أطروحة دكتوراه، جامعة تيزي وزو، 2019، ص 47.

[2] ممدوح، خالد إبراهيم." *معاينة مسرح الجريمة الإلكترونية* .مقال منشور على الرابط http://kenanaonline.com/users/KhaledMamdouh/posts/81659 آخر إطلاع بتاريخ 10/02/2024، على الساعة 10:35.

- كما يجوز له اللجوء إلى مقر عمل مزود بخدمة الانترنت Internet SewerProvider والذي يعتبر أفضل مكان يمكن إجراء المعاينة فيه[1].

الفرع الثاني: الخطوات المتبعة قبل وعند الانتقال للمعاينة المعلوماتية

قبل التطرق للخطوات المتبعة قبل وعند الانتقال للمعاينة المعلوماتية، لا بد أن نتعرض للشروط القانونية لصحة المعاينة داخل المنظومة المعلوماتية، وبناء عليه سنقسم دراستنا لهذا الفرع على النحو التالي:

الفقرة الأولى: الشروط القانونية لصحة المعاينة المعلوماتية

تتمثل هذه الشروط أساسا في إخطار وإذن وكيل الجمهورية (أولا)؛ أوقات المعاينة المعلوماتية (ثانيا)، رضا الشخص(ثالثا) ومحضر المعاينة المعلوماتية (رابعا).

أولا: إخطار وإذن وكيل الجمهورية

ألزم المشرع الجزائري ضباط الشرطة القضائية –بعد التأكد من وقوع الجريمة فعلا – إخطار وكيل الجمهورية باعتباره المسؤول المباشر عنهم، وباعتبار أننا بصدد دراسة إجراء المعاينة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنها لا تتم إلا بإذن مسبق من قبل وكيل الجمهورية المختص، وهو ما يستشف من الفقرة الثالثة من المادة 47[2] من القانون 06–22 [3].

---

[1] شنتير، خضرة. *الآليات القانونية لمكافحة الجريمة الإلكترونية –دراسة مقارنة–*. أطروحة دكتوراه، جامعة أدرار، 2020 –2021، ص 66.

[2] جاء في نص المادة 47 فقرة03:"وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

[3] الأمر رقم 66 –155. المتضمن ق إ ج ، المصدر السابق، المعدل والمتمم بالقانون رقم 06–22 المؤرخ في 20 ديسمبر سنة 2006 ، ج ر ج ج، ع 84، الصادرة في24 ديسمبر سنة 2006، ص 6.

والملاحظ أن إخطار وإذن وكيل الجمهورية لمباشرة المعاينة سواء في الجرائم التقليدية أو المعلوماتية إجراء جوهري، وبمفهوم المخالفة فإن انتقال ضابط الشرطة القضائية للمعاينة في البيئة الرقمية، دون إذن مسبق من وكيل الجمهورية المختص يترتب عنه بطلان كافة الإجراءات.

ثانيا: أوقات المعاينة المعلوماتية

بالنسبة للمواعيد القانونية فإن القاعدة العامة لإجراء المعاينة في الجرائم العادية أن لا تكون قبل الساعة الخامسة صباح ولا بعد الساعة الثامنة مساء، وهو ما جاء في الفقرة الأولى من نص المادة 47 [1]من القانون 06 – 22، غير أن المشرع الجزائري خرج عن هذه القاعدة وأجاز المعاينة في كل ساعة من ساعات النهار أو الليل، بناء على إذن مسبق من وكيل الجمهورية المختص-كما سبق الإشارة-عندما يتعلق الأمر بطائفة معينة من الجرائم والمحددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حسب ما جاء في الفقرة الثالثة[2] من المادة المذكورة أعلاه.

ثالثا: رضا الشخص بالمعاينة المعلوماتية.

طبقا لنص المادة 64 من ق إ ج، فإنه لا يجوز معاينة المساكن إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، على أن يكون الرضا بتصريح مكتوب[3].

وتطبق الأحكام الواردة في الفقرة الأولى من المادة السالفة الذكر عندما يتعلق الأمر

---

[1] جاء في الفقرة الأولى من المادة 47 من القانون 06-22 "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة (05) صباحا، ولا بعد الساعة الثامنة (08) مساء...".

[2] راجع نص المادة 47/ف03 من القانون 06-22، السابق ذكرها في الصفحة 19، المرجع السابق، ص 06.

[3] تنص المادة 47/ف01 ق إ ج "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه الإجراءات ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الإستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الإشارة صراحة على رضاه".

بالجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات بناء على ما ورد الفقرة الثالثة من ذات المادة [1].

رابعا: محضر المعاينة المعلوماتية

بعد إتمام المعاينة في الجرائم التقليدية، يتم تحرير محاضر من قبل ضباط الشرطة القضـــائية عن أعمالهم التي يقومون بها وهو ما أكدته المادة 18 من ق إ ج، مع ضرورة توقيعه من قبل الضابط أو عونه، كما يجب إثبات الوقت الذي حرر فيه والتاريخ والتوقيع من طرف الأطراف، وإذا امتنع أحد الأفراد ينوه في المحضـــر عن ذلك، وعليه فإنه لا يكون للمحضر قوة إثبات إلا إذا كان صحيحا في الشكل ومحررا أثناء مباشرة الوظيفة من طرف ضابط مختص أورد فيه ما رآه أو عاينه بنفسه[2]، وهذا ما جاءت به المادة 214[3] من ق إج.

---

[1] ورد في الفقرة الثالثة من64 ق إج "غير أنه عند ما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكور في المادة 47 فقرة03 من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر".

و بدورها تنص المادة 47 مكرر من ذات القانون على " إذا حدث أثناء التحري في جريمة متلبس بها أو تحقيق متعلق بإحدى الجرائم المذكورة في المادة 47 الفقرة 3 من هذا القانون إن كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر أو الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام أو لإحتمال فراره أو اختفاء الأدلة خلال المدة اللازمة لنقله، يمكن أن يجري التفتيش بعد الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق وبحضور شاهدين مسخرين طبقا لأحكام المادة 45 من هذا القانون أو بحضور ممثل يعنيه صاحب المسكن محل التفتيش" .

[2] شنة، محمد. *إجراءات البحث والتحري*. محاضرات ألقيت على طلبة السنة أولى ماستر، تخصص قانون جنائي وعلوم جنائية، كليه الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، 2023 –2024، ص15.محاضرات منشورة على الرابط http://dspace.univ-khenchela.dz:4000/items/794bad18-521b-4574-aa4d-993a88f600b9/full آخر إطلاع بتاريخ 15/02/2025 من الساعة 10:46

[3] جاء في المادة 214 ق إ ج "لا يكون للمحضر أو التقرير قوة الإثبات إلا إذا كان صحيحا في الشكل ويكون قد حرره واضعه أثناء مباشرة أعمال وظيفته وأورد فيه عن موضوع داخل في نطاق اختصاصه ما قد رآه أو سمعه أو عاينه بنفسه."

وبالنسبة لهذا الشرط –**محضر المعاينة المعلوماتية**– فإن المطلع على قانون الإجراءات الجزائية لا يجد نصاً صريحا بوجوب تحرير محضر في الجرائم الماسة بأنظمة

المعالجة الآلية للمعطيات، وبالتالي يمكننا إسقاط – قلنا إسقاط وليس القياس إعمالا بالمبدأ السائد، فإن القياس محضور في القانون الجزائي– الشروط الشكلية لمحضر المعاينة في الجرائم العادية على محضر المعاينة المعلوماتية إلا أن الاختلاف هنا يكمن في موضوع الجريمة من حيث سرد سلوكها الإجرامي.

بعد أن عرجنا على الشروط القانونية التي تخضع لها المعاينة في الجرائم الماسة بالمنظومة المعلوماتية، كان لا بد من تكملة هذا الجانب بجانب آخر والمتمثل في القواعد والخطوات الواجب مراعاتها قبل وعند الانتقال لمعاينة مسرح الجريمة المعلوماتية والتي سنوضحها كما يلي:

الفقرة الثانية: الخطوات المتبعة قبل المعاينة المعلوماتية

1–وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة وشبكاتها المتوقع مداهمتها لتحديد إمكانية التعامل معها[1].

2–إعداد خريطة للموقع الذي سيتم الانتقال إليه مع ضرورة وضع خطة وتقسيم الأدوار على فريق التحقيق المختصين، وتحديد المهام واختصاص كل واحد منهم حتى لا تتداخل الاختصاصات[2].

---

[1] سحتوت، نادية. "التنظيم القانوني للجريمة المعلوماتية –أدلة إثبات الجريمة المعلوماتية". *مجلة دراسات وأبحاث*، جامعة الجلفة، ع01،سبتمبر2009، ص 50. مقال منشور على الرابط https://asjp.cerist.dz/en/article/4417 آخر إطلاع بتاريخ 2025/02/20 على الساعة 13:50.

[2] ربيعي، حسين. *آليات البحث والتحري في الجرائم المعلوماتية*.أطروحة دكتوراه، جامعة باتنة 1، 2015 –2016، ص 239.

3- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للإستعانة بها في الفحص والتشغيل مثل برنامج معالجة الملفات Xtree Pro Gold وبرنامج النسخ Lap link وبرنامج En Case الذي ينتج صوره مطابقة من القرص الصلب[1].

4- قطع التيار الكهربائي من موقع المعاينة لشل فاعلية الجاني من القيام بأي فعل من شأنه التلاعب أو تخريب الآثار[2].

5-مراجعة الخطة واستحضار الإذن القضائي[3].

الفقرة الثالثة: الخطوات المتبعة عند معاينة مسرح الجريمة المعلوماتية.

بعـــد أن عرجنا على القواعد والخطوات المتبعة قبل الشـــروع في المعاينة ســـنتطرق للخطوات الواجب مراعاتها عند الوصول لمسرح الجريمة والمتمثلة في:

1-السيطرة على الدائرة والمناطق المحيطة بمسرح الجريمة مراقبة التحركات ورصد الاتصالات الهاتفية من وإلى مسرح الجريمة، مع وضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات[4].

2-تصوير جهاز الحاسوب والأجهزة المتصلة به ومحتوياته ووضعية المكان الموجود فيه مع التركيز على الأجزاء الخلفية للحاسوب وملحقاته، دون إغفال تسجيل وقت وتاريخ ومكان التقاط كل صورة[5].

---

[1] بن قـــارة مصـــطفى، عائشـــة. *حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن*.الإسكندرية: دار الجامعة الجديدة، 2016، ص 85.

[2]البشيري، محمد الأمين. *التحقيق في الجرائم المستحدثة*. دار الأكاديميون للنشر والتوزيع، 2014، ص 113.

[3]ربيعي، حسين. المرجع السابق، ص 239.

[4]يوسف، أمير فرج. *الجرائم المعلوماتية على شبكة الأنترنت*. الإسكندرية: دار المطبوعات الجامعية،2010، ص 222.

[5]عميمر، عبد القادر. *آليات إثبات الجريمة المعلوماتية في التشريع الجزائري –دراسة مقارنة* .أطروحة دكتوراه، جامعة الجزائر،2019-2020، ص 237.

3-إثبات الحالة التي تكون عليها توصـــيلات الكابلات (الخيوط الكهربائية للحاســـب) والتي تكون متصلة بمكونات النظام حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة [1].

4-عدم التسرع في نقل أي مادة معلوماتية خارج مسرح الجريمة إلا بعد أن يتم التأكد من عدم وجود القوى المغناطيســـية في المحيط الخارجي، لكي لا يتســـبب ذلك في إتلاف البيانات المسجلة أو محوها أو تخريبها[2].

5-حفظ ما تحويه ســـلة المهملات، والقيام بفحص الملفات والشـــرائط المتواجدة فيها ورفع البصمات التي تكون لها صلة بالجريمة المرتكبة[3].

6-التحفظ على مســـتندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضـــاهاة ما قد يوجد عليها من بصـــمات، واقتصـــار عملية المعاينة على المحققين الذين تتوافر فيهم الخبرة الفنية والكفاءة العلمية في مجال الحاسبات[4].

7-ملاحظة بطريقة مدققة لكيفية إعداد نظام الحاسب والآثار الالكترونية وبوجه خاص السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريق الولوج إلى النظام.

---

[1] النعيمي، محمد يوســـف. "صعوبات التعامل مع مسرح الجريمة الالكترونية –دراسة مقارنة–". *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة، م01، ع72، يونيو 2020، ص16. مقال منشور على الرابط: https://mjle.journals.ekb.eg/article_259606_e8106720214fd9fa0fb7bc6872deedcb.pdf آخر إطلاع بتاريخ 2025/02/22، على الساعة 17:02.

[2] جرار، محمد باسل صالح. *معاينة مسرح الجريمة الالكتروني ودوره في الإثبات الجنائي وفق التشريع الفلسطيني*.رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، 2022، ص 87.

[3] بن قارة مصطفى، عائشة. المرجع السابق، ص 87.

[4] مليانى، دلال مولاي. *إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري* .أطروحة دكتوراه، جامعة تلمسان، 2017-2018، ص 160.

8- حفظ الموقع باستخدام خاصيةsave as أو تحميل الدليل أو نسخة منه أو استخراجه في هيئة ورقية أو قرص صلب أو مرن[1].

إن نجاح المعاينة داخل المنظومة المعلوماتية من قبل السلطة المخول لها إجرائها قائم على التكامل بين الشروط القانونية، وكذا القواعد والخطوات المتبعة قبل وأثناء معاينة مسرح الجريمة المعلوماتية.

وعلى الرغم من أهمية المعاينة في البيئة الرقمية، إلا أن المشرع لم ينص على هذه الخطوات قانونا، كما أن عدم وجود نصوص قانونية واضحة تنظم إجراءات المعاينة داخل المنظومة المعلوماتية يعد قصورا ملحوظا في التشريع الجزائري، وبالتالي لا تتحقق الحماية الفعالة للمنظومة المعلوماتية من الجرائم الماسة بها وهو ما يتطلب تدارك هذا الأمر من قبله.

المطلب الثاني: نطاق إجراء المعاينة المعلوماتية.

بما أننا بصدد جريمة تقع في البيئة الرقمية، فإن المعاينة فيها تختلف عن تلك الموجودة في الجرائم التقليدية، ذلك أن الحاسب الآلي في مثل هذه الجرائم يعد الوسيلة لإرتكابها أو محل وقوعها، ولعل التساؤل الذي يتبادر إلى أذهاننا، كيف يمكن إجراء المعاينة في وسط الكتروني لا يمكن أن تدركه الحواس؟

وللإجابة عن هذا التساؤل يتعين علينا التطرق إلى معاينة مكونات الحاسب الآلي (الفرع الأول) بالإضافة إلى معاينة أنظمة الاتصال بشبكة الانترنت (الفرع الثاني).

الفرع الأول: معاينة مكونات الحاسب الآلي

تعتبر الحواسيب مصدرا غنيا بالأدلة الالكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم، لذلك فإن عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها،

[1] بن فردية، محمد. مرجع سابق، ص125.

أو محل وقوعها، والمعروف أن الحاسب الآلي يقوم في تركيبته على ثلاث عناصر أساسية هي:

القطع الصلبة(Hardware)، القطع المرنة (Software) وكذا المعلومات والبيانات(données informatique) وهو العنصر الذي يتوزع بين القطع الصلبة والبرمجيات[1].

لذلك فمعاينة هذا الحاسب تستلزم "**الفحص المادي والمعنوي** " لكل هذه العناصر نظرا للارتباط الطبيعي بين بعضها البعض، وقد تعتمد عملية الفحص هنا على طريقتين، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كاملإلى طالب الفحص أما الطريقة الثانية فهي الفحص بواسطة حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية أو جزئيات عبر الحاسب،[2] وتشمل عملية فحص مكونات الحاسب العناصر التالية:

الفقرة الأولى: معاينة القرص الصلب

القرص الصلب هو تلك الوحدة المختومة الموجودة داخل جهاز الحاسوب، والتي تقوم بوظيفة التخزين الدائم، بحيث لا يزول ما تم تخزينه بانقطاع التيار الكهربائي ويحتوي القرص الصلب على صفائح معدنية لا يمكن إزالتها[3].

يتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله، والتي تتميز بعدم التشابه فيما بينها رغم وحدة الرقم الثنائي (0-1) الذي يتكون منه تفصيل هذه البيانات[4]، ولتحقيق ذلك يقوم المحقق بنزع القرص من الحاسب المراد فحصه بكل عناية وحذر من أي ارتجاج أو اصطدام بأي

---

[1] براهيمي، جمال. *التحقيق الجنائي في الجرائم الالكترونية*.أطروحة دكتوراه، جامعة تيزي وزو،2018، ص59.

[2] قلات، سومية، حاحة، عبد العالي. المرجع السابق، ص 538.

[3] نفس المرجع والصفحة.

[4] براهيمي، جمال. المرجع السابق، ص 60.

شـــخص تفاديا لإتلافه أو تعطيله، أو فقد أي بيانات، ثم يقوم بفحص وتحليل النســـخ التي تصدر من القرص نفسه أو بواسطة الخبير المختص.[1]

فعملية فحص القرص الصلب تساعد المحقق عادة على جمع البيانات والمعطيات المخزنة فيه بشـــكل آلي أو إرادي التي كان يستخدمها الجاني، من معلومات أو صفحات وعناوين الأنترنت، أو رســـائل البريد الالكتروني المرسلة والملتقاة وكذا مجموعة البرامج الجاهزة المتخصـــصة التي استعملها (المشتبه فيه)، للتواصل مع أصدقائه (شركاء المشتبه فيه في الجريمـــة)، ثم تحليلها وتحديد تاريخها، ومن ثم مقارنتها مع وقائع الجريمة لاســـتخلاص الدليل[2].

الفترة الثانية: معاينة البرمجيات

يقصـــد بالبرنامج (program) مجموعة التعليمات المتسلسلة التي تخبر الحاسوب مع ماذا يفعل، أما البرمجيات(Software) فهي عبارة عن مصطلح يطلق على أي برنامج منفرد أو مجموعة البرامج والبيانات والمعلومات المخزنة[3]، التي يتم من خلالها تشـــغيل الحاسوب، ومن دون البرمجيات يتعذر على المستخدم التعامل مع الحاسوب[4].

ولمعـــاينـــة البرمجيـــات يتتبع المحقق طريقتين همـــا الفحص الداخلي للبرمجيات والفحص الخارجي لها؛ فالفحص الداخلي يتم من خلال البحث عن البناء المنطقي للبرمجية

---

[1] ممدوح، خالد إبراهيم. *الجرائم المعلوماتية*. الإسكندرية: دار الفكر الجامعي، 2009، ص 215.

[2] براهيمي، جمال. المرجع السابق، ص 61.

[3] عمر شامل أحمد. *تطبيقات في الحاسوب* .محاضرات منشورة على الرابط-https://uomosul.edu.iq/agriculture/wp-content/uploads/sites/11/2023/09/%D8%AA%D8%B7%D8%A8%D9%8A%D9%82%D8%A7%D8%AA-%D9%81%D9%8A-%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D9%88%D8%A8-1_2_compressed.pdf، آخر إطلاع بتاريخ 2025/02/24 على الساعة 16:33 .

[4] زبون، خالد حمدي. *الحاسوب المرحلة الأولى* .كلية شط العرب الجامعة، 2021-2022، ص 15. محاضرات على الرابط :https://sa-uc.edu.iq/uploads/curriculum/1656848217.pdf آخر إطلاع بتاريخ 2025/02/24 على الساعة 17:49

بما يكشف عن وجود مجهود تجديدي في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي للوصول لمصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة المعلوماتية، والتعرف على الكيفية التي تم الإعداد لها ،علما أن النسخ عبر الأنترنت يختلف من النسخ باستخدام برمجيات المعالجة (Word processing)[1]،أما الفحص الخارجي يتم بواسطة البحث عن البناء المنطقي للبرمجية للتأكد ما إذا كانت منسوخة أولا، ثم مقارنة النسخة الأصلية مع النسخة محل الاشتباه للدلالة على ثبوت ارتكاب الجريمة المعلوماتية[2].

والجدير بالذكر هنا، أنه ينبغي عدم التعويل كثيرا على الدليل المتحصل عليه من معاينة برمجيات الحاسب الآلي المستمد من هاتين الطريقتين، لأن برمجيات الحاسب ليست ذات نظرة مثالية، غالبا ما يشوبها عيب، أو قصور ولو جزئي في أداء وظيفتها، وهذا القصور من شأنه أن يؤثر في الحاسب فيجعله محل شك تهتز معه قيمة الدليل[3].

الفقرة الثالثة: معاينة النظام المعلوماتي

يقصد بالنظام المعلوماتي حسب ما ورد في الفقرة الخامسة من المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أنه:" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"،[4] فالنظام المعلوماتي للحاسب لا يحتوي على معلومات مكتوبة كما يعتقد معظم الناس، إنما يتكون من بيانات ثنائية رقمية يتم إيداعها في الحاسب الآلي في شكل تخزين، ثم يقوم الحاسب بمعالجتها آليا و إبرازها على هيئة معلومة موحدة كلما تم

---

[1] براهيمي، جمال. المرجع السابق، ص 62.

[2] قلات، سومية، حاحة، عبد العالي. المرجع السابق، ص 540.

[3] براهيمي، جمال. المرجع السابق، ص62.

[4] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21 ديسمبر سنة 2010، المصادق عليها بموجب مرسوم رئاسي رقم 14-252 المؤرخ في 8 سبتمبر سنة 2014، ج رج ج،ع 57، الصادرة في 28 ديسمبر سنة 2014، ص 04.

استدعاؤها من قبل مستخدم الحاسب، أما إذا لم يتم استدعاء معلومة محددة فان بياناتها تضل مخزنة على حالتها الأصلية داخل الحاسب [1].

وعليه، فإن معاينة النظام المعلوماتي للحاسب هو قيام المحقق بفحص وضبط كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات والتي يمكن استردادها عبره بأية حركة استردا دية ممكنة، ما دام موضوعها يشكل جريمة[2].

وقد أكد المختصون في مجال تكنولوجيات الإعلام والاتصال بأن نظام التخزين في ذاكرة الحاسب يعد مصدرا مهما للدليل الالكتروني، لأنه يسمح للحاسب الآلي بالاحتفاظ آليا بنسخة كاملة مما اطلع عليه المشتبه فيه من مواقع وصفحات الانترنت أثناء إبحاره عبر العالم الافتراضي، كما أن هناك أنظمة وبرمجيات جديدة فور ربطها بذاكرة التخزين يمكن لها تتبع كل خطوات المشتبه فيه ومساره عبر شبكة الانترنت واسترجاع ما تم تصفحه لفترات طويلة من الزمن قد تصل إلى ستة أشهر كاملة، ولو قام المشتبه به بإغلاق الاتصال بشبكة الانترنت وحذف كل ما قام نظام التشغيل بتخزينه[3].

الفرع الثاني: معاينة أنظمة الاتصال بشبكة الأنترنت

أحيانا لا يكفي معاينة مكونات الحاسب الآلي وحدها لاستخلاص الدليل الرقمي، وإنما يتطلب من المحقق فحص أنظمة الاتصال بشبكة الانترنت كذلك، ويقصد بهذه الأخيرة –بالمفهوم الإجرائي – تلك الإجراءات والتطبيقات المتبعة حال استخدام وسيلة الاتصال بشبكة الانترنت، لذلك فعملية معاينة هذه الأنظمة يشمل بالأساس فحص مسار الانترنت أو ما يعرف ببروتوكول الانترنت، والنظام الأمني للشبكات وفحص الخادم[4].

---

[1] الغافري، حسين بن سعيد بن يوسف. *السياسة الجنائية في مواجهة جرائم الأنترنت*. أطروحة دكتوراه، جامعة عين الشمس، القاهرة، 2005 ص 430.

[2] ممدوح، خالد إبراهيم. *الجرائم المعلوماتية*. المرجع السابق، ص 219.

[3] براهيمي، جمال. المرجع السابق، ص 63.

[4] المرجع نفسه، ص64.

الفقرة الأولى: معاينة مسار الأنترنت

تتم هذه العملية من خلال تتبع الحركة التراســـلية للنشـــاط الممارس عبر الأنترنت باســـتخدام نظام فحص الكتروني يســـمى علم البصمات المعاصر، وينتج عن هذه العملية بروتوكولات وهما IPوTCP وهما اختصاري (transmission Contrd protocole) (Internet Protocol adresse) حيث يعتبرIPعنوان رقمي[1] المكون من أربع بيتات، يتكون هذا العنوان من قســـمين رئيسيين، يختص الأول بتحديد عنوان الشبكة(Net Id أو Subne Id) تبعا للحالة، في حين يختص الثاني بدقة عنوان المضـــيف داخل الشـــبكة (Host Id)، وتتباين النسبة المخصصة لكل قسم وفقا للفئة المعتمدة [2].

وبالنســـبة للبرتوكول TCP فهو يعمل بين الموزع والزبون حيث يقوم بإنشاء حوار بينهما حول تحويل وإيصـــال المعطيات، أين يكون هناك بطاقات إرسال وبطاقات استقبال، وهو بروتوكول قوي جدا ويوفر شروط ممتازة لإيصال المعطيات.[3]

حيث يعمل البروتوكولان معا TCP/IP على تقنية التبديل المعلوماتي بواســـطة الحزم المعلوماتية (Packet) بين مختلف الوصـــلات السلكية واللاسلكية المتخصصة التي تربط الشـــبكات المختلفة الموصـــولة فيما بينها، وحزمة المعلومات جزء أو قســـم من ملف معلوماتي، ذات حجم مصـــغر ثابت حمل رقما خاصا ومعلومات تعريفية بكل من المرسل والمرســـل إليه، وعند كل اتصـــال تتم قراءة جهة المقصـــد أو المرسل إليه، ثم تتم إعادة الحزمة المارة عبرها إلى الوصلات التالية الأقرب إلى جهة المقصد النهائية .[4]

---

[1] سومية قلات، حاحة، عبد العالي .المرجع السابق ،ص524.

[2] CALECA, CHRISTIA.TCP/*IP*. Article publié sur internet, le site:https://csricted.univ-setif.dz/Documents/cours-informatique/TCP-IP.pdf Dernière visite le 25/02/2025 ،à 10:00, p 10.

[3] قلات، سومية ، حاحة، عبد العالي. المرجع السابق ،ص 543.

[4] ممدوح، عبد الحميد عبد المطلب. "استخدام بروتوكولTCP/IP في بحث وتحقيق الجرائم على الكمبيوتر. مقال منشور على الرابطhttp://3dpolice.blogspot.com/2008/01/tcpip.html?m=1 ،آخر اطلاع بتـــاريخ 2025/02/25 على الساعة 21:58.

أهميـــة الاســـتعانة بالمعلومات والمصـــادر التي يمكن أن يحتويها نظام البروتوكول (TCP/IP) للتحقيق من الجريمة المعلوماتية، في كونها تدل بصـــفة جازمة عن مصـــدر الجهاز المســـتخدم في ارتكاب الجريمة، وتحدد الأجهزة التي أصابها الضرر جراء الفعل الإجرامي، ونوعيـــة النشـــاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة، كما أنها تســـاعد على الإطلاع على جميع المراســـلات والمحادثات، وكل ما تم نقله أو تبادله أو معالجته من بيانات عبر شـــبكة الأنترنت، وكذا الكشـــف عن مصدرها وتتبع مسارها إلى غاية نقطة وصـــولها ،ومن ثم تحديد هوية المرسل والمرسل إليه اللذان قد يمثلان المشتبه فيهم [1].

من خلال ما تقدم، نصـــل إلى القول أن هذين البروتوكولين مهمين في التحري والتحقيق عن الجرائم الواقعة داخل المنظومة المعلوماتية من خلال إجراء المعاينة.

غير أنه هناك تحديات تواجه الســـلطة المختصـــة بالمعاينة المعلوماتية عند اســـتخدام بروتوكول TCP/IPوالتي نوجزها كما يلي:

1- بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاســـوب وليس عن الأشـــخاص ولذلك فمن الصـــعوبة إثبات أن شـــخصـــا محددا أحدث الفعل غير المشروع.

2- الجاني يعمد إلى اســـتخدام عناوين ومعلومات غير صحيحة، باستخدام حاسوبها في ملف خدمات عامة لتجنب التعرف عليه، ويســـتخدم عنوان IP ذي مستخدمين كثر ويمكنهم إســـتخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الاتصال وبعد فترة يعيد الاتصـــال مما يجعل النشـــاط الإجرامي غالبا موزعا على عدة عناوين IP[2].

---

[1] براهيمي، جمال. المرجع السابق، ص ص(65-66).

[2] الحلبي، خالد عياد إجراءات *التحري والتحقيق في جرائم الحاسوب والأنترنت*. الأردن: دار الثقافة للنشر والتوزيع، 2011، ص 226.

ثانيا: فحص الخادم (Server)

يتضـــمن نظام فحص الاتصال بالأنترنت لزوم فحص الخادم، وهو حاسوب ضخم مهمته تحقيق حركة الاتصـــال بالمواقع وصفحات الأنترنت، ثم استقبالها وتخزينها فيه على هيئة رقميـــة. ومن هنا للخادم وظيفة مزدوجة؛ إذ يتولى من جهة ربط مســـتخدمي الأنترنت بالمواقع والصـــفحات التي يريدون الاطلاع عليها، ويقوم من جهة ثانية باســـتضافة هذه المواقع والصفحات وتخزينها على شكل بيانات رقمية[1].

وللقيام بعملية فحص الخادم ينبغي على المحقق الالتزام بالضوابط المقررة لإجراء المعاينة وفقا للقانون المطبق في النطاق الإقليمي الذي يوجد فيه، واتخاذ كافة التدابير التقنية والفنية اللازمة للمحافظة على مسرح الجريمة من أي تلاعب.[2]

تجدر الإشـــارة إلى أن المؤسس الدستوري كفل حرمة الحياة الخاصة وهو ما نصت عليه المادة 47 من التعديل الدســـتوري لسنة 2020على أنه" لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مســـاس بـــالحقوق المذكورة في الفترتين الأولى والثانية إلا بأمر معلل من الســـلطة القضائية حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق"[3].

يستشف من خلال نص المادة السابق أن المشرع الجزائري أولى أهمية بالغة لحق حرمة الحياة الخاصة إذ يتعين على ضابط الشرطة القضائية وكل من له الحق بإجراء المعاينة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التقيد بحدودها وعدم الاطلاع على كل

---

[1] ممدوح، خالد إبراهيم. الجرائم *المعلوماتية*، المرجع السابق، ص212.

[2] براهيمي، جمال. المرجع السابق، ص 67.

[3] مرسوم رئاسي رقم 20 –442. المؤرخ في01 نوفمبر 2020، المتضمن التعديل الدستوري، ج ر ج ج،ع 82،الصادرة في30 ديسمبر سنة2020.

ما يدخل في إطار الحياة الخاصـــة، وهو ما يتضـــح لنا جليا من خلال الفقرتين الأولى والثانية من المادة آنفة الذكر، كما يضمن المؤسس الدستوري هذا الحق لجميع الأشخاص ولا يمكن بأي حال من الأحوال المساس به إلا بأمر مسبب من السلطة القضائية، وأن كل انتهـــاك للحقوق الواردة في المادة تترتب عنه قيام المســـؤولية الجزائية وهو ما جاء في المادة 303مكرر في الفقرة الأولى من القانون06-22[1]، حيث نصت على "يعاقب بالحبس من سنة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من50.000 دج إلى300.000 كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت..."[2]

تقابلها المادة 164 من القانون رقم 18-04[3]، والتي نصت على أنه " يعاقب بالحبس من ســـنة (1) إلى خمس (5) ســـنوات وبغرامة من 500.000 دج إلى 1.000.000 دج كل شـــخص ينتهك ســـرية المراســـلات عن طريق البريد والاتصالات الإلكترونية أو يفشي مضـــمونها أو ينشـــره أو يســـتعمله دون ترخيص من المرسل إلى المرسل إليه أو يخبر بوجودها".

[1] الأمر رقم 66 -156.المؤرّخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات، المعدل والمتمم بالقانون رقم 06 - 23 المؤرخ في 20 ديسمبر سنة006 2، ج ر ج ج، ع 84، الصادرة في 24ديسمبر سنة 2006، ص 11.

[2] راجع المادة 303 مكرر من ق ع، المصدر نفسه، ص 23.

[3] قانون رقم 18-04 مؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر ج ج،ع 27، الصادرة في 13 مايو سنة 2018، ص 03.

خلاصة الفصل الأول:

بعد أن فرغنا من دراســـة الفصـــل الأول تحت عنوان" الإطار القانوني للمعاينة المعلوماتية"، فلا ريب أن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أصبحت تشكل نمطـــا خطيرا في وقتنا الحالي، ومن هنا فإن للمعاينة أهمية بالغة في اســـتجلاء الحقيقة والكشف عن مرتكبيها.

وحتى تأتي المعاينة المعلوماتية بثمارها لابد من مراعاة جملة من الشروط والقواعد القانونية من قبل الســـلطة المختصـــة بإجرائها، ويمكن القول هنا أن المشـــرع الجزائري وبالرغم من اســـتحداثه لقانون مســـتقل وخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصـــال إلا أنه لم ينص على هذا الإجراء، وبالتالي فإن غياب النصـــوص القانونية التي تنظم إجراء المعاينة المعلوماتية في التحري والكشـــف عن الجرائم الواقعة داخل المنظومة المعلوماتية يثير العديد من الصـــعوبات، لذا كان لازما على المشـــرع الجزائري تدارك هذه المسألة وذلك من خلال وضع ترسانة قانونية تنظم هذه العملية بشكل دقيق يتوافق والطبيعة المحضة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفصل الثاني

الإطار القانوني للتفتيش والحجز داخل المنظومة المعلوماتية

تمهيد وتقسيم

إلى جانب إجراء المعاينة المعلوماتية الذي سبق دراسته في الفصل الأول كأحد أهم الإجراءات فعالية في الكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، نجد أن المشرع الجزائري استحدث ضمن القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إجراءات تفتيش المنظومات المعلوماتية وحجز المعطيات التي من شأنها الكشف عن هذه الجرائم والقبض على مرتكبيها.

وحتى تتحقق الغاية المرجوة، لا بد من التكامل بين هذه الإجراءات ومنه لا يمكن القيام بإجراء دون آخر.

وعليه، سنقسم دراستنا في هذا الفصل وفقا لمبحثين، نتناول ضمن الأول " التفتيش داخل المنظومة المعلوماتية "، في حين نخصص الثاني لتطرق إلى "الحجز داخل المنظومة المعلوماتية"

المبحث الأول: التفتيش داخل المنظومة المعلوماتية

يعد التفتيش من أخطر إجراءات التحقيق المقررة في الجرائم التقليدية بصفة عامة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة، كونه يمس بالحق في حرمة الحياة الخاصة المكفول دستوريا، إلا أنه في الوقت نفسه يشكل آلية هامة في الكشف من ملابسات الجريمة، والوصول إلى الحقيقة.

وبناء على ما سبق، فإن دراستنا لهذا المبحث تقتضي منا التطرق "لمفهوم تفتيش المنظومة المعلوماتية" في مطلب أول، ثم "القواعد الإجرائية لتفتيش المنظومة المعلوماتية" في مطلب ثان.

المطلب الأول: مفهوم تفتيش المنظومة المعلوماتية

لقد نظم المشرع الجزائري أحكام التفتيش الالكتروني التي لا تتوافق والتفتيش التقليدي في القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مكافحتها، في الفصل الثالث تحت عنوان "القواعد الإجرائية لتفتيش المنظومات المعلوماتية".

من خلال هذا المطلب ستتناول " تعريف التفتيش الالكتروني" ضمن الفرع الأول، كما سنبرز "خصائص التفتيش الالكتروني" في الفرع الثاني، في حين سنتطرق في الفرع الثالث إلى "الطبيعة القانونية للتفتيش الالكتروني"، أما الفرع الرابع نبين من خلاله صور التفتيش الالكتروني".

الفرع الأول: تعريف التفتيش الالكتروني

بالرجوع إلى التشريع الجزائري نجد أن المشرع الجزائري لم يتناول تعريف التفتيش الإلكتروني بل اكتفى بالنص على أحكامه، ضمن القانون 09-04-تاركا المجال للفقه، حيث تباينت التعاريف بخصوص هذا الإجراء ويقصد به" البحث في مستودع سر المتهم

عن أشـــياء تفيد في كشـــف الحقيقة[1]، وهناك من عرفه على أنه" البحث أو لإطلاع على محل منحه القانون حماية خاصة سواء كان مسكنا أو جهاز حاسوب أو أنظمة أنترنت"[2].

الفرع الثاني: خصائص التفتيش الالكتروني

للتفتيش الإلكتروني جملة من الخصائص، تم استنتاجها من التعاريف السابقة، تتمثل في:

– التفتيش في المنظومات المعلوماتية فيه تعرض قانوني لحرية المتهم الشـــخصـــية أو لحرمة مســـكنه رغما عنه، فهو إعتداء على أســـراره الموجودة على مســـتوى نظامه المعلوماتي أو حاسوبه الآلي وحتى بريده الإلكتروني.

–لا يتطلـــب التفتيش في الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات في كثير من الأحيان الانتقال إلى مساكن الأشخاص، وإنما قد يتم عن بعد perquisition en ligne، كمـــا يتطلـــب فيمن يباشـــره أن يكون مختصـــاً في التحقيق الجنائي ومعالجة البيانات والحسابات.

–تفتيش المنظومات المعلوماتية فيه مساس خطير بالحياة الخاصة[3].

– التفتيش إجراء من إجراءات التحقيق وهو ما نصت عليه المادة 05 /ف01 من القانون 09–04" يجوز للســـلطات القضائية المختصة وكذا ضابط الشرطة القضائية ... الدخول بغرض التفتيش ولو عن بعـــد إلى منظومـــة معلومـــاتيـــة أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين معلوماتية"[4].

---

[1] خضرة شنتير، مرجع سابق، ص71 .

[2] ســـرور، أحمد فتحي. *نظرية بطلان الإجراءات الجنائية*. أطروحة دكتوراه، جامعة القاهرة، نقلا عن: طرشي، نورة. *مكافحة الجريمة المعلوماتية*. رسالة ماجستير، جامعة الجزائر 1 ،2011–2012، ص 115.

[3] همیسي، رضا. "*تفتيش المنظومات المعلوماتية في التشريع الجزائري*". *مجلة العلوم القانونية والسياسية*، جامعة الوادي، م11، ع05، جوان 2012، ص ص (161–162). مقال منشور على الرابط https://asjp.cerist.dz/en/article/5740، آخر اطلاع بتاريخ2025/03/06 على الساعة 17:40

[4] راجع الفقرة الأولى من المادة 05 من القانون 04-09، مصدر سابق، ص 06.

- التفتيش في الجرائم المعلوماتية تقوم به أجهزة معينة مثل المعهد الوطني للأدلة الجنائية وعلم الإجرام التابع للقيادة العامة للدرك الوطني، قسم الإعلام والإلكترونيك الذي يختص بالجرائم المعلوماتية والذي تم استحداثه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004، وكذا مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحته[1].

الفرع الثالث: الطبيعة القانونية للتفتيش الإلكتروني

أجمع معظم الفقه بشأن تحديد الطبيعة القانونية للتفتيش الالكتروني إلى القول إنه إجراء من إجراءات التحقيق الذي يمس بحقوق وحريات الأفراد[2]، ولهذا يجيز المشرع الجزائري أمر القيام به إلى سلطة التحقيق "أي قاضي لتحقيق" صاحب الاختصاص الأصيل، حيث يجوز له أن ينتقل إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته[3].

ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة[4]، وإذا تعذر عليه القيام بنفسه بجميع إجراءات التحقيق جاز له أن يندب ضابط الشرطة القضائية للقيام بجميع أعمال التحقيق اللازمة ضمن الشروط المحددة قانونا.

---

[1] خليفي، فتيحة، مهداوي، محمد صالح ."خصوصية التفتيش في البيئة الرقمية". *المجلة الجزائرية للقانون*، جامعة تلمسان، م 05، عدد 09، جويلية 2022، ص 06.مقال منشور على الرابط:
https://asjp.cerist.dz/en/article/197938، آخر إطلاع بتاريخ 2025/03/06 على الساعة 19:04

[2] محمودي، سماح ."مشكلات التفتيش الجنائي من المعلومات فيم الكمبيوتر والانترنت". *مجلة الحقوق والعلوم السياسية*، جامعة ع خنشلة، ع 08، جوان2017، ص 331. مقال منشور على
الرابط:https://asjp.cerist.dz/en/article/42459 ،آخر إطلاع بتاريخ 2025/03/07 على الساعة: 12:08.

[3] راجع المادة 79 من الأمر رقم 66 -155المتضمن ق إ ج، المصدر السابق، ص 630، المعدل والمتمم بالقانون رقم 21-11. المؤرخ في 25 غشت سنة 2021، ج رج ج،ع 65، الصادرة في 26 غشت سنة 2021.

[4] المادة81 ق إ ج، نفس المرجع والصفحة.

بناء على ما تقدم، فإن التفتيش سـواء كان في الجرائم العادية أو الجرائم الالكترونية يعد إجراء من إجراءات التحقيق، حيث يجوز لسـلطة التحقيق مباشرته بنفسها أو عن طريق الإذن أو الإنابة[1]، كما يمكن الاستعانة بخبير له دراية بعمل المنظومات المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي. تتضـمنها قصـد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها[2].

الفرع الرابع: صور التفتيش الالكتروني

إن عمليـة تفتيش المنظومة المعلوماتية تنصـب على المكونات المادية بأوعيتها المختلفة بغرض البحث عن شـيء يتصل بجريمة معلوماتية والكشف عنها، ويدخل هذا الأمر في نطاق التفتيش التقليدي وفقا للإجراءات المعمول بها[3]، حيث يشمل التفتيش كل ما يخص الوسـائط الإلكترونيـة المسـاعدة على إرتكاب الجريمة المعلوماتية كالهواتف النقالة، الحواسيب، وتعد هذه الأخيرة محور دراستنا باعتبارها الوسيلة الأكثر شيوعاً.

الفقرة الأولى: تفتيش المكونات المادية للحاسب الآلي

يقصـد بـالمكونـات المادية للنظام المعلوماتي تلك الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالكابلات، الشاشات،...[4].

---

[1] بن خليفة، إلهام. "التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصـلة بتكنولوجيا الإعلام والاتصال . *المجلة الدولية للبحوث القانونية والسـياسية*، جامعة الوادي، م02 ، ع01 ، ماي 2018، ص 36. مقال منشور على الرابط: https://asjp.cerist.dz/en/article/66489 آخر إطلاع بتاريخ 2025/03/07 على الساعة 12:23.

[2] راجع الفقرة الأخيرة من المادة 05 من القانون 09-04 المصدر السابق، ص 06.

[3] بن طالب، ليندا. "التفتيش في الجرائم المعلوماتية". *مجلة العلوم القانونية والسـياسـية*، جامعة الوادي، م11، ع 06، جوان 2017، ص ص (459-490). مقال منشـور على الرابط https://asjp.cerist.dz/en/article/46702آخر إطلاع بتاريخ 2025/03/08 على الساعة 21:37.

[4] سوير، سفيان. *الجرائم المعلوماتية*. رسالة ماجستير. جامعة تلمسان، 2010 -2011، ص 40 .

وهناك حالات خاصة لتفتيش هذه المكونات، ومن ذلك:

- إذ كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم، فإنها تخضع لنفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا.
- في حال كانت هذه المكونات منعزلة عن غيرها من أجهزة الكمبيوتر أو متصلة بجهاز في مكان آخر كمسكن غير المتهم، وحتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود التي يوجبها المشرع لتفتيش هذه الأماكن.
- إذا وجدت مكونات الحاسوب المادية في الأماكن العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات[1].

وبخصوص هذه الصورة –تفتيش المكونات المادية للحاسب الآلي–فإن التفتيش الواقع على هذه المكونات لا توجد بخصوصه أي مشكلة، لأنه يرد على أشياء مادية مع ضرورة مراعاة الجانب الفني لضبط الأجهزة من أجل ضمان عدم إتلافها[2].

---

[1] حمـــداش، شـــمس الدين. بن مبروك، البشـــير. "القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري". *مجلة صـــوت القانون*، جامعة خميس مليانة، م09 ،ع 02، ماي 2003، ص ص (101–102). مقال منشـــور على الرابط https://asjp.cerist.dz/en/article/221449 آخر إطلاع بتاريخ2025/03/09، على الساعة 22:15.

[2] خلف الله، فاروق." الآليات القانونية لمكافحة الجريمة"*مجلة الحقوق والحريات*، جامعة بسكرة، ع 02 ، ديسمبر 2015 ،ص 09، مقال منشور على الرابط :https://asjp.cerist.dz/en/article/139256 ، آخر اطلاع بتاريخ 2025/03/05 على الساعة 18:36، أنظر كذلك : مانع، سلمى. "التفتيش كإجراء للتحقيق في الجرائم المعلوماتية"**.***مجلة العلوم الإنسانية* ، جامعة بسكرة ،ع 21 ، جوان 2011 ، ص 234 . مقال منشور على الرابط https://asjp.cerist.dz/en/article/49479آخر اطلاع بتاريخ 2025/03/09 على الساعة 19:00

الفقرة الثانية: تفتيش المكونات المعنوية للحاسب الآلي

يطلق كذلك على المكونات المعنوية للحاسوب بالبرمجيات، فهي بمثابة عصب الكمبيوتر إذ توفر إمكانات وسرعة فائقة في انجاز المهام المطلوبة[1]، وعليه فقد أثار تفتيش المكونات المعنوية للحاسب الآلي خلافا كبيرا في الفقه بشأن جواز تفتيشها من عدمه، وهذه المسألة – قابلية المكونات المعنوية للتفتيش – هي محل جدل، وانقسم الفقه بشأنها إلى رأيين، فالرأي الأول يذهب إلى أنه اذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة ، فإن هذا المفهوم لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة، ويقترح هذا الرأي لمواجهة هذا القصور ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة "المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني هو البحث عن الأدلة المادية بواسطة الحاسب[2].

أما الرأي الثاني فهو على نقيض الرأي الأول، حيث يرى أنه يسمح بتفتيش بيانات الحاسب غير المحسوسة، ويستند هذا الرأي على القوانين الاجرائية عندما تنص على إصدار الاذن بتفتيش أي شيء وبذلك يمكن تفسيره أنه يشمل بيانات الحاسب الآلي المحسوسة وغير المحسوسة، لأن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة وعليه فإن هذا المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها[3].

---

[1] بوحليط، يزيد. "تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري". *مجلة التواصل في الاقتصاد* والإدارة والقانون، جامعة عنابة، ع48، ديسمبر 2016، ص 85. مقال منشور على الرابط:https://asjp.cerist.dz/en/article/19945آخر إطلاع بتاريخ 2025/03/09 على الساعة 20:35

[2] رابحي، عزيزة. *الأسرار المعلوماتية وحمايتها الجزائية*. أطروحة دكتوراه، جامعة تلمسان، 2017–2018، ص ص (280–281).

[3] رابحي، عزيزة. التفتيش في نظم المعالجة الآلية للمعطيات". *مجلة القانون والعلوم السياسية*، المركز الجامعي النعامة، م 02، ع01، جانفي 2016، ص397. مقال منشور على الرابط https://asjp.cerist.dz/en/article/86813آخر إطلاع بتاريخ 2025/03/09 على الساعة 22:15.

أما المشرع الجزائري فقد أجاز صراحة تفتيش النظم المعلوماتية، بموجب المادة 05 من القانون 09-04، حيث جاء فيها" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضـــائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول، بغرض التفتيش، ولو عن بعد، إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ...[1]

الفقرة الثالثة: تفتيش شبكات الحاسب الآلي

إن ارتباط الحاسبات الآلية فيما بينها عبر الشبكات الافتراضية، طرح عدة إشكالات قانونية فيما يخص إجراء التفتيش عبر هذه الأخيرة، فإذا كان التفتيش عبر الشـــبكات الافتراضية الموجودة داخل الاقليم الوطني لا يطرح اشـــكالا بحده فإن امتداد التفتيش خارج الحدود الوطنية يطرح عدة إشكالات قانونية وإجرائية[2]، وهو ما سنوضحه في الحالات التالية:

أولا: حالة ارتباط حاسب المتهم بمنظومة معلوماتية داخل الاقليم الوطني

عند انتقال الجهة المختصة بالتفتيش إلى مكان تواجد الحاسب الآلي، قد تتفاجأ كونه متصل مع حاســـب أو حواســـيب أخرى، داخل الدولة، في هذه الحالة يثور التســـاؤل حول مدى امكـــانيـــة تمديد الجهة المختصـــــة للتفتيش خارج الحيز المكاني المحدد في إذن التفتيش، وبعبارة أخرى هل تملك الجهة المختصـــة بالتفتيش سلطة الولوج إلى الحواسيب الأخرى المرتبطة بالحاسب الآلي بحثا عن الأدلة الإجرامية[3].

---

[1] راجع المادة 01/05 من القانون 09-04، المرجع السابق، ص 06

[2] صغير، يوسف. "التفتيش كآلية لإثبات جرائم نظم المعلوماتية". *المجلة النقدية للقانون والعلوم السياسية*، جامعة تيزي وزو، م 16، ع04، ديسمبر 2021، ص 59. مقال منشور على الرابط https://asjp.cerist.dz/en/article/176255اخر إطلاع بتاريخ 2025/03/10، على الساعة 12:00

[3] المناعسة، أسامة أحمد وآخرون.*جرائم الحاسب الآلي –دراسة تحليلية مقارنة*، ط12، عمان: دار وائل للطباعة والنشر، 2001، ص 280 .

وقد أجاب المشـــرع الجزائري على هذا التســـاؤل بموجب الفقرة "02" من المادة "5" من القانون 04/09"...وإذا كانت هناك أســـباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة

في منظومـــة معلومـــاتيـــة أخرى، وأن هـــذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بســـرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ..."[1]

ثانيا: حالة ارتباط حاسب المتهم بمنظومة معلوماتية خارج الإقليم الوطني

من المتصـــور حسب هذه الحالة أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شـــبكات الإتصال البعيدة، بهدف عرقلة عملية التفتيش وجمع الأدلة الرقمية،[2] حيث تواجه ســـلطات التحقيق في هذه الحالة مشـــكلة الإلكترونية تتمثـــل في "مدى جواز تمديدها لإجراءات التفتيش الالكتروني إلى خارج الإقليم الجغرافي للدولة"، وهو ما يسمى "بالتفتيش العابر للحدود"، وقد إتفق الفقه على أنه لا يجوز لسلطات التحقيق اللجوء إلى التفتيش الالكتروني العـــابر للحدود إلا في إطار اتفاقيات تعاون تجيز وتنظم هذا التمديد، أو في إطار الانابات القضـــائية المتبادلة على الأقل بعد الحصول على الإذن الصريح من الدولة الأجنبية، وفي حالة غياب هذه الاتفاقيات يعد اتخاذ هذا الإجراء انتهـــاكا فعليا لمبدأ الســـيادة،[3] حيث جاء في المادة 5 في فقرتها الثالثة من القانون رقم 09- 04 أنـــه "إذا تبين مســـبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني، فإن

---

[1] راجع أحكام المادة 05/ف 02 من القانون 09-04، ص 06

[2] رابحي، عزيزة. "التفتيش في نظم المعالجة الآلية للمعطيات". المرجع السابق، ص 400.

[3] نطيحي، نسمة . *الوقاية من الجرائم الالكترونية*. محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص إدارة الكترونية وخدمات رقمية، كلية الحقوق والعلوم السـياسية، جامعة سطيف، 2021-2022، ص ص (35-36). منشورة على الرابط: http://en.univ-setif2.dz/mod/folder/view.php?id=3291 ،آخر إطلاع بتاريخ 2025/03/19، على الساعة 09:04.

الحصـــول عليها يكون بمســـاعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[1].

من خلال هذه المادة، يتبين أن المشـــرع الجزائري أقر صراحة تمديد التفتيش الالكتروني من قبل الســـلطات المختصة ليشمل معطيات مخزنة في منظومة معلوماتية خارج التراب الوطني لا يكون إلا في إطار المســـاعدة القضائية طبقا للاتفاقيات المبرمة في هذا المجال وكذا وفقا لمبدأ المعاملة بالمثل.

وبـــالرجوع للفقرة الرابعـــة من ذات المادة من القانون 09-04، يتضـــح لنا أنه يمكن للســـلطـــات المكلفـــة بالتفتيش تســـخير أهل الخبرة الذين لديهم دراية بعمل المنظومة المعلوماتية[2].

المطلب الثاني: القواعد الإجرائية لتفتيش المنظومة المعلوماتية

نظرا لخطورة التفتيش الالكتروني ومســـاســـه بالحرية الشخصية للفرد، فقد حرصت جل التشريعات الإجرائية بما فيها المشرع الجزائري على ضرورة إحاطته بجملة من الضوابط التي من شـــأنها إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة من جهة أخرى، وبين تحقيق الفاعلية المطلوبة في الكشف عن الجريمة وعن مرتكبيها من جهة أخرى.

وعلى هذا الأســـاس فإن دراستنا لهذا المطلب تقتضي منا تسليط الضوء على الإجراءات الواجب مراعاتها من قبل السلطة المخول لها القيام بعملية التفتيش الكتروني.

الفرع الأول: إجراء الإذن بالتفتيش الإلكتروني

بالرجوع لقانون الإجراءات الجزائية، نجد أن المشـــرع الجزائري نص على هذا الإجراء وتحديدا في المادة 44 من ذات القانون، والتي أكدت على ضرورة أن يكون التفتيش بناء

---

[1] المادة 03/05 من القانون رقم 09-04 المرجع السابق، ص 06

[2] ورد في الفترة الرابعة من المادة 05 من القانون 09-04:"يمكن للســـلطات المكلفة بالتفتيش تســـخير كل شخص له دراية بعمل المنظومات المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية الي تتضـــمنها، قصد مساعدتها وتزويدها بكل المعلومة الضرورية لإنجاز مهمتها ".

على إذن مكتوب صـــادر من وكيل الجمهورية أو قاضـــي التحقيق مع وجوب اســـتظهار الاذن قبل الشـــروع في التفتيش، ويكون الأمر كذلك إذ ما تعلق الأمر بالجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات[1].

كما نص المؤســـس الدستوري على هذا الإجراء في الباب الثاني، الفصل الأول "الحقوق والحريات الأساسية" وضمن المادة 03/48 من التعديل الدستوري لسنة 2020.[2]

بناء على ما ســـبق، فإنه يشرط وجود اذن مكتوب من وكيل الجمهورية أو قاضي التحقيق متى تعلق الأمر بالتفتيش الالكتروني، باعتبار أن التفتيش يمس بخصـــوصـــية الأفراد، ومراعاة للطبيعة المستمرة للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، إضافة لكون أدلة الإثبات فيها سهلة وسريعة التلف[3].

وجدير بالملاحظة أن المشـــرع الجزائري نص على هذا الإجراء في المراقبة الإلكترونية دون التفتيش الالكتروني ضمن القانون 09-04، وهذا الأمر غاية في الخطورة ما يتطلب تدخل المشـــرع لتدارك هذا الاغفال، كون أن عدم وجود الاذن لمباشرة إجراءات التفتيش داخل المنظومة المعلوماتية يشكل انتهاكا صارخا لحق الخصوصية المكفولة دستوريا.

الفرع الثاني: إجراء التفتيش الإلكتروني بحضور أشخاص معينين قانونا

ســـبق الإشـــارة إلى أن التفتيش بوجه عام يشكل إعتداء على حرمة أو حرية الأشخاص والاطلاع على أســـرارهم، وعليه اشترطت بعض التشريعات حضور المشتبه فيه أو من ينوبه عنه، أو الشهود في عملية التفتيش وذلك لضمان سلامة هذا الإجراء والحيلولة دون

---

[1] راجع الفقرتين 1 و2 من المادة 44 من القانون 06 -22، المصدر السابق ص6.

[2] تنص المادة 48 من التعديل الدستوري لسنة 2020 على:" تضمن الدولة عدم انتهاك حرمة المسكن "لا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، لا تعيش إلا بأمر مكتوب صادر من السلطة القضائية المختصة ".

[3] مجدوب، نوال. "الآليات الإجرائية للكشف من الجريمة المعلوماتية". *مجلة البحوث القانونية* السياسية، المركز الجامعي آفلو، م 06، ع01، جانفي 2023، ص 197. مقال منشور على الرابط https://asjp.cerist.dz/en/article/213392،آخر إطلاع بتاريخ 2025/03/12 على الساعة 10:36.

تعســـف الجهة القضائية بالتفتيش[1]، وهو ما ذهب إليه المشرع الجزائري في نص المادة 45/ف1، من ق إ ج ،"... يجب أن يحصل التفتيش بحضوره ، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضـــابط الشـــرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا اســـتدعي ضـــابط الشـــرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته[2].

غير أنه ونظرا لخصـــوصية الجرائم الماسة بأنظمة المعالجة الآلية المعطيات وما يتطلبه بشـــأنها من بسط نوع من السرية أثناء جمع الدليل الالكتروني بالإضافة إلى الاسراع في استخلاصه قبل فقدانه[3]، فقد أورد المشرع الجزائري إستثناء في الفقرة الأخيرة من ذات المادة المذكورة ســـابقا أين اســـتبعد من خلالها تطبيق هذا الإجراء عند تفتيش المنظومة المعلوماتية، ومنه يمكن للجهات المخول لها قانونا مباشـــرة عمليات التفتيش في الجرائم الماســـة بأنظمة المعالجة الآلية دون التقيد بضرورة حضور المشتبه فيه أو من ينوب عنه حتى الشهود[4].

ما يمكن قوله بخصوص هذا الإجراء وحسب وجهة نظرنا فإن استبعاد المشرع الجزائري لتطبيق أحكام المادة 45 ق إج، على التفتيش الالكتروني يعد خطوة إيجابية، وهذا بالنظر للطبيعة التقنية المحصنة التي تتميز بها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

---

[1] عربوز، فاطمة الزهراء. "التفتيش الالكتروني كإجراءات حقيق في الجرائم المعلوماتية". *مجلة جيل الأبحاث القانونية* المعم قة، جـــامعـــة ســـيـــدي بلعبـــاس، ع 34، أكتوبر 2019، ص 103. مقـــال منشـــور على الرابط: https://jilrc.com/archives/11227 ، آخر اطلاع بتاريخ 2025/03/12، على الساعة 16:05.

[2] المادة 45 /ف01 من القانون 06- 22-، المصدر السابق، ص 06.

[3] براهيمي، جمال. المرجع السابق، ص 44.

[4] تنص الفقرة الأخيرة من المـــادة 44 من القـــانون 06 -22 على: " لا تطبق هـــذه الأحكام إذا تعلق الأمر بجرائم المخـــدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والارهاب والجرائم المتعلقة بالتشـــريع الخاص بالصـــرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني المذكورة أعلاه".

الفرع الثالث: رضا المشتبه فيه بالتفتيش الالكتروني

إن الفرض هنا يتعلق بمدى قبول الشـــخص إراديا الخضـــوع لإجراء التفتيش، وتلك في الحقيقة مشـــكلة اعتراضية يعالجها الفقه تحت تسمية" رضا الشخص بالتفتيش أو التفتيش الإرادي"، إلا أنه في غالب الأحيان يعرض ضـــابط الشـــرطة القضائية على شخص أن يفتشه أو يفتش مسكنه ويقبل ذلك الشخص لهذا الإجراء بشكل عادي[1].

وقد نصت المادة 64 ق إج على هذا الإجراء، حيث تؤكد المادة عدم جواز تفتيش المساكن إلا برضـــا صـــريح من الشخص الذي ستتخذ لديه هذه الإجراءات، على أن يكون الرضا مكتوب بخط صـــاحب الشـــأن، وإذا تعذر ذلك وكان لا يعرف الكتابة جاز له أن يستعين بشخص يختاره بنفسه مع ضرورة التنويه في المحضر والاشارة إلى رضاه[2].

كمـــا جاء في الفقرة الثالثة من المادة أعلاه، أنه "عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المـــذكورة في المادة 47 (الفقرة 3) من هذا القانون، تطبيق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر"[3].

---

[1] مرنيز، فاطمة. "التفتيش الافتراضي كإجراء استدلالي في ضوء القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها – دراسة مقارنة–". *مجلة الاجتهاد للدراسات القانونية والاقتصادي*، جامعة تامنغست، م 01، ع02، 2جوان2021 ، مقال منشور على الرابط:
https://asjp.cerist.dz/en/article/152366 أخر إطلاع بتاريخ 12/03/ 2025 على الساعة 22:07

[2] تنص المادة 64 من القانون 06 –42 على: " لا يجوز تفتيش المســـاكن ومعاينتها وضـــبط الأشياء المثبتة للتهمة إلا برضـــا صـــريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره لنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاة".

[3] راجع المادة 03/64 من القانون 06 –22، المصدر السابق، ص07.

كما نص المشـــرع الجزائري على قيام المســـؤولية الجزائية في حق كل من له ســـلطة التفتيش، دخول منزل أحد المواطنين بغير رضـــاه وهو ما نصت عليه المادة 135[1] من القانون 82-04[2].

ما يلاحظ في المادة 64 ق إ ج، أن تفتيش المساكن سواء في الجرائم التقليدية والمستحدثة قائم على رضـــا الشـــخص وهذا يعتبر شرط موقف لمباشرة إجراء التفتيش الإلكتروني، وعليه كان لابد على المشرع أن ينوه كذلك لحالة رفض الشخص لهذا الاجراء

الفرع الرابع: مواعيد التقشيش الإلكتروني

يقصـــد بالميقات في التفتيش أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن[3].

وبهذا الخصوص فقد اشترط المشرع الجزائري وقت معين لتفتيش المنازل من قبل السلطة المختصة، وهو ما يعد ضمانة للمحافظة على خصوصيات الآخرين[4]، حيث نصت المادة 47 ق إج في الفقرة الأولى "لا يجوز البدء في تفتيش المساكن قبل الساعة الخامسة صباحا ولا بعد الســـاعة الثامنة مســـاء، إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا".

---

[1] جاء في نص المادة 135 من ق ع " كل موظف في الســـلك الإداري أو القضائي وكل ضابط شرطة وكل قائد أو أحد رجال القوة العمومية دخل بصـــفته المذكورة منزل أحد المواطنين بغير رضاه، وفي غير الحالات المقررة في القانون وبغير الإجراءات المنصوص عليها فيه يعاقب بالحبس من شهرين إلى سنة وبغرامة من20.000 إلى 100.000 دج دون الإخلال بأحكام المادة 107".

[2] الأمر رقم 66-156

[3] بن قارة مصطفى، عائشة. مرجع سابق، ص110.

[4] غلاب، فـــايز محمـــد راجح. *الجرائم المعلومـــاتيـــة في القـــانون الجزائري واليمني*. أطروحـــة دكتوراه، جـــامعة الجزائر،2009-2010، ص 329.

غير أن هذا الشرط لم يؤخذ به على إطلاقه، وإنما خضع لبعض الاستثناءات ومن ذلك ما ورد في المادة أعلاه[1]، وما يهمنا من استثناءات ما جاءت به الفقرة الثالثة من المادة 47 إذ نصت على أنه: "وعندما يتعلق الأمر بجرائم المخدرات، والجريمة المنظمة عبر الحدود الوطنيـــة أو الجرائم المـــاســـة بأنظمة المعالجة الآلية للمعطيات وجرائم تبيض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشـــريع الخاص بالصـــرف، فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل ســـكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

كما نصـــت كذلك الفقرة الرابعة من ذات المادة وفي حالة الجرائم المشار اليها في الفقرة الثالثة من المادة 47 السابق بيانها أنه يمكن لقاضي التحقيق القيام بأية عملية تفتيش ليلا أو نهارا وحتى في أي مكان على امتداد التراب الوطني أو يأمر ضـــباط الشـــرطة القضائية بذلك.

وباستقراء المادة 05 لاسيما الفقرتين الثانية والثالثة من القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصـــلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نجد أن المشرع أجاز تمديد تفتيش المنظومة المعلوماتية أو جزء منها، وذلك بعد إعلام الســـلطة القضائية المختصة[2]وإذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومـــة الأولى مخزنـــة في منظومـــة معلومـــاتية تقع خارج الإقليم الوطني، فإن الحصـــول عليها يكون بمســـاعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل[3].

---

[1] جبار، فطيمة. الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، رسالة ماجستير، جامعة البليدة، 2013، ص75.

[2] تنص الفقرة الثانية من المادة 5 من القانون 09-04" إذا كانت هناك أســـباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعلومات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة الى هذه المنظومة، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك"

[3] أنظر الفقرة 03 من المادة 05 من القانون 09-04، المصدر السابق، ص 06.

ما يمكن قوله بخصـــوص "ميعاد التفتيش الالكتروني"، أن المشرع الجزائري وفق نوعا ما في اســـتبعاد تطبيق الميقات الزمني على النظم المعلوماتية، ذلك أنه لو علم الجاني مسبقا بالوقت الذي ســـيتم فيه تفتيش أنظمته المعلوماتية سيأخذ كافة احتياطاته، ويقوم بمحو أدلته بســـرعة، لكن كان لا بد من النص على هذا الإجراء من قبل المشرع طالما أنه استحدث قانونا خاصا بالوقاية من تكنولوجيات الإعلام والاتصال ومكافحته.

الفرع الخامس: تحرير محضر بالتفتيش الالكتروني

إضافة إلى الإجراءات السابقة الذكر، ولما كان التفتيش عمل من أعمال التحقيق فإنه يجب تحرير محضـــر يثبت فيه كل ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة[1]، وهو ما نصت عليه المادة 18 ق إج، إضافة إلى ما ورد في الفقرة الثانية من المادة 68 ق إ ج " تحرر نســـخة عن هذه الإجراءات وكذلك عن جميع الأوراق ويؤشر أمين ضبط التحقيق أو ضابط الشرطة المنتدب على كل نسخة بمطابقتها للأصل...[2].

بحيث لا يلزم القانون وجود شكلا أو شروطا خاصة في محضر التفتيش، وانما يكفي أن يتوافر فيه ما تتطلبه القواعد العامة في المحاضـــر عموما، كالكتابة باللغة الرسمية، تاريخ تحريره وأن يتضـــمن كافة البيانات المتعلقة بالتفتيش[3]، وفي ذات الســـياق، فإن الأمر يختلف عما إذا كان التفتيش من طرف ضـــابط الشـــرطة القضـــائية الذي يخضع للقواعد العامة، عنه إذا كان قد أجري من طرف قاضـــي التحقيق الذي يشترط ان يكون مصحوبا بكاتب يتولى تحرير المحضـــر وتدوين ما تم من إجراءات والتأشـــير عليه تحت طائلة البطلان[4].

---

[1]بحرية، هارون. *وسائل الاثبات في الجريمة المعلوماتية*. رسالة ماجستير، جامعة خنشلة، 2013 –2014، ص 133.

[2]المادة 68 /ف2 من الأمر رقم 66–155، المتضمن ق إ ج، المصدر السابق، المعدل والمتمم بالقانون رقم 01–08 مؤرخ في 26 يونيو 2001، ج ر ج ج، ع34، الصادرة في 27 يونيو سنة 2001، ص07.

[3]القهيري، عمر محمود حمدان. إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الالكترونية. رسالة ماجستير، جامعة الشرق الأوسط، 2023، ص 45.

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

أما بالنسبة لمحضر التفتيش الالكتروني، فإنه يستلزم بالإضافة إلى الشكليات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة العامة بتقنية المعلومات، ثم ينبغي بعد ذلك أن يكون هناك شخص متخصص في الحاسب يرافقه للاستعانة به في مجال الخبرة الفنية الضرورية، فلا شك أن وجود خبير لمعالجة البيانات سوف يساعد في صياغة مسودة محضر التفتيش، بحيث تتم تغطية كل الجوانب في عملية التفتيش [1].

[1] هروال، نبيلة هبة. الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، – دراسة مقارنة–.الإسكندرية: دار الفكر الجامعي، 2013، ص 263.

المبحث الثاني: الحجز داخل المنظومة المعلوماتية

تنتهي عملية تفتيش المنظومة المعلوماتية بحجز المعطيات التي من شأنها الكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ونظرا للتطور الذي اقتحم الفضاء المعلوماتي، استحدث المشرع الجزائري القانون 09-04 والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1] ومكافحتها، أين نص بموجبه على هذا الإجراء وضمن الفصل الثالث من ذات القانون تحت عنوان "حجز المعطيات المعلوماتية ".

ومن أجل التفصيل أكثر في هذا الإجراء كان لا بد لنا من تقسيم هذا المبحث إلى مطلبين، نتطرق في الأول إلى "مفهوم الحجز الالكتروني"، أما الثاني سنبين" القواعد الإجرائية للحجز داخل المنظومة المعلوماتية".

المطلب الأول: مفهوم الحجز الالكتروني

تدخل المشرع الجزائري ضمن القانون 09-04 لتنظيم إجراء حجز المعطيات داخل المنظومة المعلوماتية كما سبق وأن أشرنا، والذي له علاقة وطيدة بإجراء تفتيش المنظومة المعلوماتية، ومن هنا سنحاول تعريف الحجز الإلكتروني في الفرع الأول" ونتناول في "الفرع الثاني " وظائف الحجز الالكتروني

[1] يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، راجع المادة 02/ف "أ" من القانون 09-01، المرجع السابق، ص.05.

الفرع الأول: تعريف الحجز الالكتروني

لم يتطرق المشرع الجزائري لتعريف الحجز الالكتروني بالرغم من تنظيم إجراءاته ضمن المادة 06 من القانون 09 -04، تاركا المجال للفقه، حيث يقصد به "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في الكشف عنها وعن مرتكبيها "[1].

ويمكن أيضا تعريفه على أنه:" العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة، والحجز هو الغاية من التفتيش ونتيجته المباشرة، ولذلك يتعين عند إجرائه أن تتوافر فيه نفس القواعد الي تطبيق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الحجز[2].

ما يلاحظ في هذين التعريفين أنهما ينطبقان على الحجز في الجرائم العادية وعليه فإن الحجز داخل المنظومة المعلوماتية مختلف من حيث محله على الحجز في الجرائم التقليدية، ذلك أن محل الحجز في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أثار جدلا بين فقهاء القانون وانقسموا بشأنه إلى اتجاهين: الاتجاه الأول يرى أنصاره عدم ضبط المعلومات المعالجة في المجال الافتراضي إلا بعد نقلها إلى كيان مادي ملموس إما تصويريا أو بواسطة دعائم التخزين الالكتروني، أما الاتجاه الثاني يرى أن المعطيات المعالجة الكترونيا ما هي إلا ذبذبات الكترونية، أو موجات كهرومغناطيسية قابلة للتسجيل والحفظ والتخزين، يمكن نقلها واستقبالها وبذلك لا يمكن إنكار وجودها المادي[3].

---

[1] بلقاسم، سمية، بوشوشة، حميد. "الجريمة الالكترونية بُعدٌ جديد للإجرام في الجزائر...واقعها وآليات مجابهتها "،*مجلة العلوم الانسانية*، جامعة أم البواقي، م10، ع 01، جوان2023،ص544. مقال منشور على الرابط: https://asjp.cerist.dz/en/article/226117 ، آخر إطلاع بتاريخ 2025/03/15 على الساعة 10:15.

[2] مسعود، مريم أحمد. *آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09*. رسالة ماجيستير، جامعة ورقلة،2012-2013، ص 94 .

[3] توفيق، مجاهد، عباسة، طاهر. "جريمة الإرهاب الالكتروني في ضوء أحكام الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات لعام 2010". *مجلة العلوم القانونية و السياسية*، جامعة الوادي، م 09، ع03، ديسمبر 2018، ص91. مقال منشور على الرابط https://asjp.cerist.dz/en/article/72222 ،آخر إطلاع بتاريخ 2025/03/15 على الساعة 17:40.

الفرع الثاني: وظائف الحجز الإلكتروني

للحجز داخل المنظومة المعلوماتية وظيفتان أساسيتان، هما:

الفقرة الأولى: جمع أدلة الاثبات وفحص البيانات الرقمية

هي الخطوة الأولى في عملية التحقيق الجنائي، وهي تحديد مصـــدر الدليل الرقمي المتوقع حتى يتم الحصـــول عليه بصورة رقمية تمهيدا لفحصه وتحليله، فمصادر البيانات تختلف فقد تكون أقراصا صلبة، أقراصا خارجية،...[1].

الفقرة الثانية: مصادرة المعطيات

وهي العملية الموالية لجمع أدلة الإثبات التي تفيد في الوصـــول إلى الحقيقة قد تشمل هذه المعطيات الصـــور، مقاطع الفيديو، سجلات المكالمات،... كما يجب التنويه أن الحجز لا يؤدي بالضرورة إلى حذف المعطيات بصفة نهائية[2].

المطلب الثاني: القواعد الإجرائية للحجز داخل المنظومة المعلوماتية

حتى تباشـــر السلطة المختصة حجز المعطيات داخل المنظومة المعلوماتية –التي تفيد في الكشـــف عن ملابسات الجريمة والحصول على الدليل الرقمي، لابد لها من مراعاة جملة من الخطوات الجوهرية ومرية التي نظمها المشـــرع الجزائري في القانون المتضـــمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

وعليه فإننا ســـتتناول هذا المطلب وفقا لفرعين، تخصص الأول لا براز إجراءات الحجز الالكتروني، أما الثاني نبين من خلاله "طرق الحصـــول والتعامل مع الدليل الرقمي أثناء الحجز الإلكتروني".

---

[1] فلاح، عبد القادر. "حجز وحفظ المعطيات في الجريمة الالكترونية". *مجلة صوت القانون*، جامعة خميس مليانة، م 08، ع 01، نوفمبر 2021، ص180. مقال منشـــور على الرابط: https://asjp.cerist.dz/en/article/169811 ، آخر إطلاع بتاريخ 2025/03/15 على الساعة 21:40

[2] مناصـــرة، يوسف. *الإثبات الالكتروني في القانون الجنائي. أطروحة* دكتوراه، جامعة الجزائر 2016 –2017، ص 344.

الفرع الأول: إجراءات الحجز الالكتروني

إن الهدف من تفتيش المنظومة المعلوماتية هو ضبط وحجز الأدلة التي تفيد في كشف الحقيقة، فالحجز هو غاية التفتيش، أي الأثر المباشر الذي يسفر عنه الإجراء، وباعتباره أحد إجراءات التحقيق فتطبق عليه القواعد التي تطبق على التفتيش فإذا بطل التفتيش بطل الحجز[1].

وعليه سيم دراسة حملة من الإجراءات المنصوص عليها قانونا، ضمن هذا الفرع

الفقرة الأولى: الحجز عن طريق نسخ المعطيات والبيانات

فتح المشرع الجزائري المجال للسلطة الى تباشر التفتيش لنسخ المعطيات والبيانات على دعامة الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة قانونا، التي من شأنها الكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو مرتكبها[2].

وهو ما ورد في الفقرة الأولى من نص المادة 06 من القانون 09 -04" 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 المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية".

وقد قصد المشرع الجزائري إدراج عبارة "دعامة تخزين الكترونية "، وهي عبارة واسعة من شأنها احتواء ما قد يظهر ويستجد من تقنيات تخزين جديدة بناء على التطورات التقنية المذهلة في مجال صناعة الحواسيب وملحقاتها[3].

---

[1] الطوالبة، علي حسن محمد. *التفتيش الجنائي على نظم الحاسوب والأنترنت –دراسة مقارنة–*". د ب ن:دار عالم الكتب الحديثة ،2004،ص 135.

[2] بهلول، سمية ، ذبيح، عماد دمان. "الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري". *مجلة الحقوق والعلوم السياسية*، جامعة خشلة، ع13، جانفي 2020، ص 153، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/107549 ، آخر إطلاع بتاريخ 2025/03/15، على الساعة 15:00

[3] تمام، شوقي يعيش. *الجريمة المعلوماتية .دراسة تأصيلية*، الجزائر: مطبعة الرمال،2019، ص 69.

الفقرة الثانية: الحجز عن طريق منع الوصول إلى المعطيات

للقيام بالحجز عن طريق منع الوصول إلى المعطيات يتوجب توافر شرط استحالة الحجز، الذي مراده أسباب تقنية؛ ففي هذه الحالة يتعين على السلطات التي تقوم بإجراء التفتيش استعمال كل التقنيات لمنع الوصول إلى كل من المعطيات التي ينظمها نظام المعالجة الآلية، يعتبر هذا الإجراء وقائي واحترازي، الهدف المرجو منه هو الحفاظ على الأدلة الرقمية في بيئتها الأصلية، وهذا يتلاءم مع طبيعتها الخاصة التي تتميز بسرعة الاتلاف[1]. وقد نص المشرع الجزائري على هذا الإجراء في المادة 07 من القانون 09-04، وقد جاء فيها " 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 الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة"[2].

الفقرة الثالثة: حجز المعطيات ذات المحتوى المجرم

نصت المادة 08 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على أنه " يمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك"[3].

يتضح من خلال هذه المادة أن المشرع الجزائري أجاز للسلطة المخول لها مباشرة هذا الإجراء اتخاذ أي إجراء ضروري لمنع الإطلاع على المعطيات، كما أن تكليف شخص

---

[1] زراري، نسرين. *السياسة الجنائية لمكافحة الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات*. أطروحة دكتوراه، جامعة خنشلة،2023-2024، ص 327.

[2] أنظر المادة 7 من القانون 09-04، المصدر السابق، ص 7

[3] المادة 8 من القانون 09-04، المصدر نفسه.

مؤهل ورد على سبيل المثال لا على سبيل الحصر وهذا من خلال عبارة "لا سيما" الواردة في المادة الأخيرة.

الفقرة الرابعة: حدود استعمال المعطيات المتحصل عليها

جاء في المادة 09 من القانون 09-04 "لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحريات القضائية "[1]، من خلال هذه المادة يتبين أن المشرع الجزائري لم يترك استعمال هذه المعطيات المحصلة مطلقا وإنما أورد قيودا على استعمالها لأن الحجز أحيانا يشكل مساسا بالحقوق لاسيما الحق في الخصوصية، وضمان الاحترام هذا الحق أقر المشرع ضمانات من خلال فرضه لحدود استعمال المعطيات المحجوزة إلا بما يسمح به القانون ، واستخدامها بالقدر الضروري الذي تتطلبه التحريات أو التحقيقات القضائية[2] .

الفرع الثاني: طرق الحصول والتعامل مع الدليل الرقمي أثناء الحجز الالكتروني

بعد انتهاء عملية التفتيش الالكتروني تأتي عملية التحقق من الأدلة الرقمية المراد حجزها وذلك من خلال جمع هذه الأدلة والحصول عليها لكي يتم اعتمادها في الاثبات، إلا أنه وفي الوقت نفسه نجد جملة من الصعوبات التي تواجه السلطة المختصة أثناء عملية حجز الدليل الرقمي.

وبناء عليه، فان دراستنا لهذا الفرع تتطلب منا التطرق، أولا لتعريف الدليل الرقمي ومن ثم بيان طرق جمع الدليل الرقمي والحصول عليه، كما سنبرز العوائق التي تواجه حجز الدليل الرقمي.

---

[1] المادة 09 من القانون 09-04، المصدر السابق، ص 07.

[2] زراري، نسرين. المرجع السابق، ص 326.

الفقرة الأولى: تعريف الدليل الرقمي

تعددت التعاريف التي قيلت بشـــأن الدليل الرقمي، فقد عرفه البعض على أنه "تذبذبات أو نبضـــات إلكترونية يمكن تجميعها وتحليلها باســـتخدام برامج وتطبيقات خاصة من أجهزة الحاســـب الآلي وملحقاته أو من شبكات الأنترنت أو أي جهاز آخر له خاصية معالجة، أو تخزين المعلومات وتشـــكل هذه المعلومات والبيانات دليلا جنائيا يمكن الاعتماد عليه في مرحلة التحقيق والمحاكمة.[1] كما يمكن تعريفه على أنه ذلك الدليل الذي ينشـــأ في العالم الرقمي، والذي يكون على شكل مستخرج مادي يتم قبوله في جلسة المحاكمة.[2]

وللدليل الرقمي جملة من الخصائص تميزه عن غيره من الأدلة التقليدية، ومن ذلك:

أولا: أنه دليل علمي

إن الـــدليل الرقمي يحتاج إلى بيئته التقنية التي يكون فيها من بيانات ومعلومات ذات هيئة إلكترونية غير ملموســـة لا تترك بالحواسب العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاســـبات الآلية واســـتخدام نظم برامجية حاسوبية، فهو يحتاج إلى بيئة التقنيـــة إلى يتكون فيهـــا، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي[3].

ثانيا: الدليل الرقمي ذو طبيعة تقنية متطورة

تسمى هذه الطبيعة بالطبيعة الثنائية للدليل المعلوماتي، ومفاد ذلك أن هذا الدليل يتكون من تعداد غير محدود الأرقام ثنائية في هيئة (1-0)، والتي تتميز بعدم التشابه فيما بينها رغم

---

[1] بن مالك، أحمد، الخال، إبراهيم. "دور الأدلة الرقمية في الاثبات الجنائي". *مجلة العلوم الإنسانية*، المركز الجامعي، تندوف،م05، ع 01، أفريل2021، ص108. مقال منشور على الرابط https://asjp.cerist.dz/en/article/148870آخر إطلاع بتاريخ 2025/03/19، على الساعة 21:30.

[2] بن فردية، محمد. "الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائري –دراسة مقارنة–"*.المجلة الأكاديمية للبحث*، جامعة بجاية،م09، ع01، جوان 2014، ص 278.مقال منشور على الرابط : https://asjp.cerist.dz/en/article/55437آخر إطلاع بتاريخ 2025/03/19 على الساعة 18:35.

[3] بن طالب، ليندا. مرجع سابق، ص ص (41-42).

وحدة الرقم الثنائي الذي تتشكل منه، فمثلا البيانات المخزنة في الحاسوب سواء كانت في شـــكل نصوص حروف أو صور ليس لها وجود مادي وهذا الذي عرف في شكل ورقي، وإنما هي مجموعة أرقام ترجع إلى أصـــل واحد، وهو الذي يجعل الدليل المعلوماتي ذو طبيعة تقنية غير ملموسة.[1]

الأدلة الرقمية ذات طبيعة ديناميكية فائقة الســـرعة تتنقل من مكان لآخر عبر شـــبكات الإتصـــال متعدية لحدود الزمان والمكان، ويعتمد الدليل الرقمي على التطور التلقائي وهذا راجع لبيئته التقنية المتطورة بطبيعتها[2].

الفقرة الثانية: برامج جمع الدليل الرقمي والحصول عليه

هناك عدة وسائل وأدوات تساهم في جمع الأدلة الرقمية منها:

أولا –برنامج إذن التفتيش: وهو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات العامة المطلوبة لترقيم الأدلة وتسجيل البيانات، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضـــبوطة لتحديد مكان دليل معين أو تحديد ظروف هذا الدليل.

ثانيا–قرص بدء تشـــغيل الكمبيوتر: وهو قرص يمكن المحقق من تشـــغيل الكمبيوتر، إذا كـــان نظـــام التشـــغيل فيه محميا بكلمة المرور، ويجب أن يكون القرص مزود ببرنامج مضـــاعفة المســـاحة فربما قام المتهم باســـتخدام هذا البرنامج لمضاعفة مساحة القرص الصلب[3].

---

[1] لهوى، رابح. *الشرعية الإجرائية للأدلة المستمدة من التفتيش*. أطروحة دكتوراه، جامعة باتنة1، 2020–2022، ص 34.

[2] محمودي، نور الهدى. "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية". *مجلة الباحث للدراسات الأكاديمية*، جامعة باتنة1، ع11، جوان2017، ص 912، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/24925 آخر إطلاع بتاريخ 2025/03/19 على الساعة 21:36

[3] محمودي، نور الهدى. مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي –دراسة تحليلية–. أطروحة دكتوراه في الحقوق، جامعة باتنة 1 ،2017–2018، ص 186.

ثـــالثـــا–برنـــامج معالجة الملفات كبرنامج (xtree Gold): وهو برنامج معالجة آلية للملفات في أي مكان على الشـــبكة أو القرص الصلب، ويستخدم لتقسيم محتويات القرص الصلب الخاص بالمتهم، والأقراص المرنة المضبوطة كما يستخدم لقراءة البرامج والملفات في صورتها الأصلية.

رابعا–برنامج نسخ البيانات كبرنامج (LAP Link): هو برنامج يمكن المحقق من النسخ على البيانات من حاســـوب المتهم إلى قرص آخر، من خلال تقنية المنفذ المثالي أو المنفذ الموازي، وهو برنامج مفيد جدا يســـمح بنســـخ المعطيات بكل أمان ودقة قبل أي محاولة لتدميرها[1].

خامســـا–**برنامج كشـــف الديســـك:** يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كانت أســـاليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد، ونسخة خاصة بالشرطة.

سادسا –برامج الاتصالات كبرنامج Lan tastic، يستطيع هذا البرنامج ربط جهاز حاسب المحقق بجهاز حاســـب المتهم لنقل ما به من معلومات وحفظها في جهان نسخ المعلومات تم إلى القرص الصلب[2].

ســـابعا–برنامج فحص الشبكة: هي أدوات تستخدم في فحص برتوكول TCP/IP وذلك لمعرفة المشـــكلات المتعلقة بالشبكة وكذا العمليات التي تعرضت لها، وترجع فعاليتها إلى قدرتها على دخول الشـــبكات وتحديد نوع البرامج والفيروسات التي استعملت في عمليات الاختراق وتحديد مصدرها بدقة[3] ومن بين هذه الأدوات نذكر:

أداة (ARP): وظيفتها تحديد مكان الحاسوب على الشبكة .

أداة (TRACER): هي أداة تعمل على رسم مسار بين حاسوب الجاني والعناوين

---

[1] ربيعي، حسين. مرجع سابق، ص 249.

[2] ممدوح، خالد إبراهيم. *الجرائم المعلوماتية*. مرجع سابق، ص ص (204–205).

[3] ربيعي حسين، نفس المرجع والصفحة.

التي زارها والفترات التي قضاها هناك.

أداة (NAT SAT): هي أداة لفحص حالة الإتصال الحالي للبروتوكول TCP/IP ولها عدد من المهام، ومن أهمها عرض جميع الاتصـــالات الحالية ومنافذ التنصت إضافة إلى عرض المنافذ والعناوين بصورة رقمية[1].

هذه أهم التقنيات العلمية المعتمدة في جمع الأدلة الرقمية، والتي يجب أن يقوم بها الخبراء في هـــذا المجـــال نظرا لعملية ودقة هذه الأدلة، ومن وجهة نظر جهات التحقيق فإن جمع الأدلة الالكترونية يمكن أن يشكل صعوبة نسبية.

فبالرغم من أن ملفات الولوج log File تبدو مشابهة للملفات العادية، إلا أنه يمكن جمعها مثـــل اي ملف آخر، فهي تحتوي على كميـــة هائلة من المعلومات الى قد تفيد في البحث والتحقيق الجنائي[2].

كما أنه لا يجب الحصـــول على الدليل الرقمي بطرق غير مشروعة، مثل الإكراه وإفشاء الســـــر المهني في غير الأحوال المقررة قانونا أو خيانة الأمانة وغيرها من الطرق غير المشروعة، ولا بد أن يكون الدليل صحيحا لا يشوبه بطلان يتقرر بمخالفة الإجراءات لأن مشروعية الأدلة تعتبر حدا لا يمكن للقاضي تجاوزه[3].

---

[1] الحلبي، خالد عياد. مرجع سابق، ص ص (211-212).

[2] محمودي، نور الهدى. *مشروعية الوسائل العلمية الحديثة في الأثبات الجنائي*. المرجع السابق، ص ص (186-187).

[3] رابحي، عزيزة. *الأسرار المعلوماتية وحمايتها الجزائية*. المرجع السابق، ص 269

الفقرة الثالثة: طرق الحصول والتعامل مع الدليل الرقمي أثناء الحجز الالكتروني

بعـــد عمليـــة التفتيش الإلكتروني تتم عملية التحقق من الأدلة الرقمية، بحيث يجب أن يمر الدليل الرقمي المراد حجزه بمراحل.

أولا: جمع الدليل الرقمي والحصول عليه

إن الخطوة الأولى في عملية التحقيق الجنائي هي تحديد مصدر الدليل الرقمي وذلك تمهيدا لفحصـــه، وتختلف مصـــادر البيانات فقد تكون أقراص صـــلبة، ذاكرة عشوائية ... إلخ، وللحصـــول على البيانات يجب تحديد مسبقا الطريقة التي سيتم اتباعها وكذا الأدوات التي يســـتلزم استخدامها، مع الحرص على عدم المساس بالدليل الرقمي بأي شكل من الأشكال أثناء عمليه تحويل أو نسخ جزء من المنظومة أو البيانات[1].

ثانيا: فحص البيانات الرقمية

يقوم المحقق في هذه المرحلة بفحص الأدلة المتعلقة بالقضـــية واستخراج البيانات التي تم الحصـــول عليها في الخطوة السابقة، ويجب على المحقق هنا مراعاة استخدام نوع الأداة المناسبة لاستخراج الدليل الرقمي[2].

ثالثا: تحليل ومراجعة الأدلة

تتم عملية تحليل البيانات التي تم اســـتخراجها في عملية الفحص، حيث يقوم المحقق خلال هذه المرحلة بتدوين عملية التحقيق منذ البداية إلى غاية نهايتها ضـــمن محاضـــر وتقارير ترفق كملف مجمـــل وذلك لإثبات الدليل الذي تم نقله من مســـرح الجريمة المعلوماتية، ويستحسن أن يقوم بعملية التحليل أكثر من محقق، ذلك أنه لكل محقق طريقته الخاصة في البحث والتحليل وبالتالي الحصول على أكبر عدد من الأدلة لدعم ملف القضية[3]

---

[1] رزيق، محمد. *إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية*. مذكرة لنيل شـــهادة الماســـتر، جامعة البويرة، 2018 -2019، ص49 .

[2] جباري، عمار. *التفتيش الإلكتروني*. مذكرة لنيل شهادة الماستر، جامعة تبسة، 2022 -2023، ص 75.

[3] رزيق، محمد. المرجع نفسه، ص 52 .

الفقرة الرابعة: العوائق التي تواجه الدليل الرقمي أثناء الحجز الالكتروني

تعترض عملية حجز الدليل الرقمي جملة من الصعوبات والي نوجزها فيما يلي:

أولا: الطبيعة غير المرئية للدليل الرقمي

دائما ما يكون الدليل الجنائي في الجريمة التقليدية مرئيا، لكن في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تكون فيها الأدلة عبارة عن نبضات أو مجالات مغناطيسية مشكلة معلومات وبيانات رقمية، ومنه فإن عدم رؤية الدليل الرقمي يثير العديد من الصعوبات أثناء جمعه مما يتوجب توافر لدى المحققين الفنيين دراية كافية ومهارة كبيرة للتعامل مع هذا النوع من الأدلة[1].

ثانيا: سهولة محو وتدمير الدليل الرقمي

تتم جرائم الاعتداء على نظم المعالجة الآلية في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والأنترنت ويطلق عليها "البيئة التقنية" هذه الأخيرة تنعكس على طبيعة الدليل الذي تنتجه مما تجعله غير مرئي، وهو ما يجعل أمر طمسه ومحوه كليا من قبل الفاعل أمر غاية في السهولة وفي زمن قصير جدا[2].

ثالثا: ضخامة البيانات المتعين فحصها

يشكل الكم الهائل للبيانات التي يتم تداولها من خلال الأنظمة المعلوماتية أحد أهم الصعوبات الى تعيق التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والدليل

---

[1] خطوي، مسعود، عكوش، حنان. "خصوصية الدليل الالكتروني ". *مجلة الفكر القانوني والسياسي*، جامعة الأغواط، م 07، ع1، ماي 2023، ص1066. مقال منشور على الرابط https://asjp.cerist.dz/en/article/220981 ، آخر اطلاع بتاريخ 2025/04/02 على الساعة 18:15.

[2] ملياني، عبد الوهاب. *أمن المعلومات في بيئة الأعمال الإلكترونية*. أطروحة دكتوراه، جامعة تلمسان، 2016-2017، ص 253.

على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة بمركز حاسب متوسط الأهمية يتطلب مئات آلاف من الصفحات والتي قد لا تثبت كلها نقل تقريبا شيئا على الإطلاق[1].

رابعا: إعاقة الوصول إلى الدليل الرقمي

إن مرتكبي الجرائم الماسة بأنظمة المعلوماتية غالبا ما يقومون بحماية أنفسهم وإضافة أجهزة البحث والتحري للوصول إلى الأدلة التي تدينهم، وذلك عن طريق استخدام تقنيات التشفير والكلمات السرية، كما يقومون في بعض الأحيان، بإخفاء هوياتهم الحقيقية وانتحال شخصية أخرى، حيث توجد الكثير من البرامج التي يستخدمها الجاني لإخفاء هويته سواء أثناء إرسال البريد أو تصفح المواقع، الأمر الذي يجعل استعادة الأدلة عملية معقدة تحتاج إلى خبرة وأدوات دقيقة قد لا تكون في بعض الأحيان متاحة لدى سلطات البحث والتحري[2].

خامسا: نقص المعرفة التقنية

إن الطبيعة الخاصة بالدليل الرقمي على عمل الجهات المكلفة بالتحقيق والمحاكمة ، حيث يتطلب الكشف عن هذه الجرائم وإثباتها إتباع استراتيجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، فكثيرا ما تفشل جهات التحقيق في جمع الأدلة الرقمية بل أن المحقق نفسه قد يدمر الدليل بخطأ منه أو بإهمال، كقيام ضباط الشرطة القضائية بوضع حقيبة كاملة تحتوي على أسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال فتكون النتيجة أن الإشارات الكهربائية القوية تتسبب في تدميرها جميعا[3].

---

[1] الطبي، البركة، سودي، محمد حاج."إشكالية الإثبات في الجرائم الإلكترونية". *مجلة آفاق علمية*، المركز الجامعي تامنغست، م11، ع01، أكتوبر 2018، ص 276. مقال منشور على الرابط https://asjp.cerist.dz/en/article/84468 ، آخر إطلاع بتاريخ 2025/04/02 على الساعة، 19:00

[2] عميمر، عبد القادر. مرجع سابق، ص ص(148-149).

[3] بن قارة مصطفى، عائشة. *حجية الدليل الالكتروني في مجال الاثبات الجنائي-دراسة مقارنة-*". رسالة ماجستير، جامعة الاسكندرية، 2009، ص 165.

رغم أن المشـــرع الجزائري قد وضـــع نصوصا خاصة تنظم إجراءات التفتيش والحجز داخل المنظومة المعلوماتية، إلا أن هذه الإجراءات لا تزال غير كافية نظرا لتطور أساليب ووســـائل ارتكاب الجريمة، كما أن هذه النصـــوص لم توفر آليه تشـــريعية قادرة على الاضـــطلاع بالآثار الخطيرة التي رتبتها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ولهذا يتطلب الأمر ضرورة مراجعة شاملة للإطار القانوني مع ضرورة تطوير النصوص القانونية لتكون أكثر توافقا مع التحديات الحديثة.

خلاصة الفصل الثاني

خلاصـــة لما سبق، فإنه يمكن القول أن المشرع الجزائري حاول كغيره من التشريعات الأخرى مواكبة التطورات الحاصـــلة في مجال التكنولوجيا ، من خلال سنه لقوانين تنظم إجراءات تفتيش المنظومة المعلوماتية وعملية حجز الدليل الرقمي، وذلك من خلال قانون الإجراءات الجزائيـــة الـــذي تضـــمن الإجراءات المألوفة ، علاوة على ذلك تنظيم هذه الإجراءات في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، غير أن التشريع الجزائري أصبح يميزه الجمود مقارنة بما آلت عليه الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات ، الأمر الذي يستوجب تعديل النصـــوص القانونية على وجه الاستعجال والغاية من ذلك ردع المجرمين ومحاولة الحد من النشاط الإجرامي الماسة بالأنظمة المعلوماتية.

خاتمة

خاتمة

بعد دراستنا لموضوع "إجراءات المعاينة والتفتيش والحجز داخل المنظومة المعلوماتية "، فلا شـــك أنه في خضـــم التحديات التي فرضـــتها التكنولوجيا، وما صاحبها من سلوكيات ســـلبية والتي أثرت بشكل مباشر على الحياة اليومية، أدت إلى ظهور جرائم أكثر خطورة وتعقيدا، على غرار الجرائم الماســـة بأنظمة المعالجة الآلية للمعطيات والتي تعد أحد أشكالها.

وفي إطار التصـــدي للجرائم الواقعة داخل المنظومة المعلوماتية، تبنى المشرع الجزائري ســـياسة مزدوجة لمكافحتها حيث اهتدى إلى تعديل القانون رقم 04-15 المتضمن قانون العقوبات إضافة إلى تعديل قانون الإجراءات الجزائية، وكخطوة جديدة تم استحداث قانون للوقاية من الجرائم المتصـــلة بتكنولوجيات الاعلام والاتصـــال سنة 2009، والذي يمكن اعتباره أكثر تجاوبا نظرا لخصـــوصية الجرائم الواقعة داخل المنظومة المعلوماتية، وهذا التنوع التشـــريعي-إن صـــح التعبير -من شأنه التقليل نوعا ما من تفاقم الاعتداءات على الأنظمة المعلوماتية.

وفي الســـياق ذاته هدف المشـــرع الجزائري من خلال القانون 09-04 إلى وضع قواعد خاصـــة لحماية المنظومة المعلوماتية، على غرار إجراء تفتيش المنظومة المعلوماتية، وحجز المعطيات التي من شـــأنها الكشـــف عن الجرائم الناشئة في الوسط الرقمي وعدم إفلات مرتكبيها من العقاب، رغم النقائص التي يحتويها.

من خلال ما ســـبق نستعرض النتائج التي خلصت إليها دراستنا لهذا الموضوع، ومن ثم الاقتراحات التي نأمل الأخذ بها وذلك على النحو التالي:

أولا: النتائج

- لم يحدد المشرع الجزائري الإجراءات اللازمة لمعاينة مسرح الجريمة المعلوماتية، مما يترك فراغا قانونيا في كيفية التعامل معه.

- رغم الجهود الجبارة التي يبذلها المشـــرع الجزائري في ســـبيل التصـــدي لظاهرة الاجرام الالكتروني والكشـــف عن مرتكبيها، إلا أنها غير كافية لبلوغ الهدف الذي يتطلع إليه، نظرا للتطورات السريعة والمستمرة التي تعرفها هذه الظاهرة من جهة، والطابع العالمي والعابر للحدود الذي يتميز به الإجرام المعلوماتي من جهة ثانية.
- قصـــور القواعد الإجرائية عن مواكبة التغيرات المتسارعة ما قد يقف حاجزا أمام الحصـــول على الدليل الرقمي أو اتلافه وعدم الكشـــف عن خبايا الجرائم الماســـة بالمنظومة المعلوماتية.
- الصعوبة في إستخلاص الدليل الرقمي الذي يشترط في إستخلاصه الاعتماد على أخصـــائيين في مجال تكنولوجيا الإعلام والاتصـــال وذلك لطبيعته التقنية وسرعة محوه واتلافه.

ثانيا: الاقتراحات

- ضـــرورة إدراج إجراء المعاينة المعلوماتية ضمن القانون رقم 09-04، ذلك أن المشـــرع الجزائري تغافل عن ســـن نصـــوص قانونية تنظم كيفية معاينة مسرح الجريمة المعلوماتية، أضـــف إلى ذلك أن الســـلطة المخولة لها مباشـــرة المعاينة المعلوماتية لا يمكنها اتخاذ أي إجراء دون الرجوع إلى القواعد المقررة قانونا إعمالا بمبدأ الشرعية الإجرائية.
- بالرغم من أن المشرع الجزائري نص على إجراءات التفتيش والحجز الالكتروني في القـــانون رقم 09-04 إلا أن هذه الإجراءات غير كافية ولا تحقق الفعالية المطلوبة في حماية المنظومة المعلوماتية وعليه لابد من إعادة النظر في بعض أحكام المواد الخاصـــة بهذه الإجراءات، كمراجعة أحكام المادة 64 ق إ ج التي نصـــت في مضـــمونها على أن عملية التفتيش معلقة على شرط واقف وهو "رضا صاحب المسكن بذلك"، الذي من شأنه عرقلة مهمة الحصول على الدليل الرقمي ،

إضـــافـــة إلى تعديل أحكام المادة 05 من القانون رقم 09-04 والتي تعد المادة الوحيدة التي خصها المشرع الجزائري بإجراء التفتيش الالكتروني.

- كإقتراح عام وجب على المشرع الجزائري إعادة النظر في القانون رقم 09-04 برمته؛ ذلك أنه لم يطرأ عليه أي تعديل ليومنا هذا، فمجرم الأمس ليس بمجرم اليوم خاصـــة أن هذا النوع من الجرائم ينشـــأ في بيئة غير ملموسة، وعلى المشرع أن يكون السباق في سن قوانين تواكب التطور الحاصل.
- التركيز على تأهيل ورفع مســـتوى أداء ومهارات العناصـــر المخول لها إجراء المعاينات والتفتيش والحجز... في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، كعقد دورات تكوينية لأخذ فكرة عن كيفية انجازها تقنيا، الاســـتفادة من تجارب الدول الأخرى من أجل خلق أخصائيين تقنيين في هذا المجال.
- لابد من التفكير في التوجه إلى التعاون التشـــريعي والقضـــائي والأمني مع الدول العربية ولما لا مع الدول الغربية الأكثر دراية بالجرائم الإلكترونية والاســـتفادة من خبراتها في مجال مكافحة هذه الجرائم، إضافة إلى إبرام مختلف الاتفاقيات في هذا الشأن.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: المصادر

❖ القواميس والمعاجم

1- .إبن منظور، محمد بن مُكَرَّم بن علي. لسان العرب، م1، بيروت: دار صادر، د س ن، منشور على الرابط https://waqfeya.net/books/%D9%84%D8%B3%D8%A7%D9%86-%D8%A7%D9%84%D8%B9%D8%B1%D8%A8-%D8%B7-%D8%B5%D8%A7%D8%AF%D8%B1-95f4323034d049229a15f5df1f2fb8ae آخر اطلاع بتاريخ 2025/02/01 على الساعة 14:32

2- أنيس، إبراهيم وآخرون. *المعجم الوسيط*. د ب ن: مكتبة الشروق الدولية، 2004، منشور على الرابط https://waqfeya.com/books/%D8%A7%D9%84%D9%85%D8%B9%D8%AC%D9%85-%D8%A7%D9%84%D9%88%D8%B3%D9%8A%D8%B7-3385fa57ca9e415d96a9a25cf012e664 آخر إطلاع بتاريخ 2025/02/01 على الساعة 16:00.

3- بن هادية، علي وآخرون .القاموس الجديد للطلاب –معجم عربي مدرسي ألفبائي - .ط7، الجزائر : المؤسسة الوطنية .للكتاب،1991.

4- جبران، مسعود. الرائد –معجم اللغوي عصري رتبت مفرداته وفقا لحروفها الأولى–. ط7، بيروت: دار العلم للملايين، 1992،

5- حموي، صبحي. المنجد في اللغة العربية المعاصرة. تح، الحموي، مأمون وآخرون. بيروت: دار المشرق، 2000.

❖ الاتفاقيات الدولية

01. باللغة العربية

- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة في 21 ديسمبر سنة 2010، المصادق عليها بموجب مرسوم رئاسي رقم 14-252 .المؤرخ في 8 سبتمبر سنة 2014، ج رج ج،ع 57، الصادرة في 28 ديسمبر سنة 2014.

02.باللغة الإنجليزية

-The Convention on Cybercrime., dated November 23, 2001, in Budapest.

❖ القوانين

01.قانون رقم 09-04. المؤرخ في 05 غشت سنه 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر ج ج، الصادرة في 16 غشت سنة2009،

02. قانون رقم 18-04. المؤرخ في 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر ج ج، ع 27، الصادرة في 13 مايو سنة 2018 .

❖ الأوامر

01. الأمر رقم 66-155. المتضمن قانون الإجراءات الجزائية، المؤرخ في 8 يونيو1996، ج رج ج، ع48، الصادرة في 10 يونيو 1966 المعدل والمتمم بالقانون رقم 21-11. المؤرخ في25 غشت سنة 2021، ج رج ج، ع 65، الصادرة في 26 غشت سنة 2021.

02.الأمر رقم 66-156.المتضمن قانون العقوبات، المؤرخ في 8 يونيو سنة 1966، ج ر ج ج، ع 49، الصادرة في 11يونيو سنة1966. المعدل والمتمم بالقانون رقم 24-06.المؤرخ في28 أبريل سنة 2024. ج ر ج ج، ع 30، الصادرة في 30 أبريل سنة 2024.

❖ المراسيم

أولا :المراسيم الرئاسية

1-مرسوم رئاسي رقم .261-15 المؤرخ في 8 أكتوبر سنة .2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج ،ع 53 ، الصادرة في8 أكتوبر سنة2015 ،

2- المرسوم الرئاسي رقم 20 -442 . المؤرخ في01 نوفمبر 2020، المتضمن التعديل الدستوري، ج ر ج ج، ع 82،الصادرة في30 ديسمبر سنة2020.

ثانيا : المراسيم التنفيذية

-المرسوم التنفيذي رقم .348-06 المؤرخ في 5أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر ج ج ، ع 63، الصادرة في 8 أكتوبر سنة 2006

ثانيا: المراجع

❖ الكتب

1. البشيري، محمد الأمين. *التحقيق في الجرائم المستحدثة*. دار الأكاديميون للنشر والتوزيع، 2014.
2. الطوالبة، علي حسن محمد، التفتيش الجنائي على نظر الحاسوب والأنترنت –دراسة مقارنة–. د ب ن: دار عالم الكتب الحديثة، 2004.
3. العزيزي، فؤاد حسن. *الجرائم المعلوماتية – دراسة مقارنة–*. الإسكندرية: دار الفكر الجامعي، 2015.
4. المناعسة، أسامة أحمد وآخرون. جرائم الحاسب الآلي –دراسة تحليلية مقارنة، ط12، عمان: دار وائل للطباعة والنشر، 2001.
5. المومني، نهلا عبد القادر. *الجرائم المعلوماتية*. ط2، عمان: دار الثقافة للنشر والتوزيع، 2010.
6. بن قارة مصطفى، عائشة .حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون . الجزائري والقانون المقارن .الإسكندرية :دار الجامعة الجديدة،2016
7. تمام، شوقي يعيش. الجريمة المعلوماتية. دراسة تأصيلية. الجزائر: مطبعة الرمال، 2019.
8. حجازي، عبد الفتاح بيومي. مبادئ الإجراءات الجنائية في جرائم الكمبيوتر. مصر: دار الكتب القانونية، 2007.
9. شملال، علي. الجديد في شرح قانون الإجراءات الجزائية–الاستدلال والإلهام–. ج 1، ط3، الجزائر: دار هومة، 2017.
10. ممدوح، خالد إبراهيم .الجرائم المعلوماتية. الإسكندرية :دار الفكر الجامعي، .2009 ص215
11. ممدوح، خالد إبراهيم. فن التحقيق الجنائي في الجرائم الإلكترونية. الإسكندرية: دار الفكر الجامعي،2009.
12. نجم، محمد صبحي. الوجيز في قانون أصول المحاكمات الجزائية. م01، الأردن: دار الثقافة للنشر والتوزيع،2006.
13. هروال، نبيلة هبة. *الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، –دراسة مقارنة–*. الإسكندرية: دار الفكر الجامعي، 2013.
14. يوسف، أمير فرج. *الجرائم المعلوماتية على شبكة الأنترنت*. الإسكندرية: دار المطبوعات الجامعية، 2010.

❖ **أطروحات الدكتوراه والرسائل والمذكرات الجامعية**

❖ **أطروحات الدكتوراه**

1. الغافري، حسين بن سعيد بن يوسف. *السياسة الجنائية في مواجهة جرائم الأنترنت*. أطروحة دكتوراه، جامعة عين الشمس، القاهرة، 2005.

2. غلاب، فايز محمد راجح. *الجرائم المعلوماتية في القانون الجزائري واليمني*. أطروحة دكتوراه، جامعة الجزائر،2009-2010.

3. بن فردية، محمد. *الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية*. أطروحة دكتوراه، جامعة الجزائر1، 2015.

4. ربيعي، حسين. *آليات البحث والتحري في الجرائم المعلوماتية*.أطروحة دكتوراه، جامعة باتنة 1، 2015 -2016.

5. ملياني، عبد الوهاب. *أمن المعلومات في بيئة الأعمال الإلكترونية*. أطروحة دكتوراه، جامعة تلمسان، 2016-2017.

6. مناصرة، يوسف. *الإثبات الالكتروني في القانون الجنائي*. أطروحة دكتوراه، جامعة الجزائر 2016 -2017.

7. رابحي، عزيزة. *الأسرار المعلوماتية وحمايتها الجزائية*. أطروحة دكتوراه، جامعة تلمسان، 2017-2018.

8. محمودي، نور الهدى. مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي –دراسة تحليلية-. أطروحة دكتوراه، جامعة باتنة 1 ،2017-2018.

9. ملياني، دلال مولاي. *إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري* .أطروحة دكتوراه، جامعة تلمسان، 2017-2018.

10. براهيمي، جمال. *التحقيق الجنائي في الجرائم الالكترونية*.أطروحة دكتوراه، جامعة تيزي وزو،2018.

11. بن طالب، ليندا. *الدليل الإلكتروني ودوره في الإثبات الجنائي –دراسة مقارنة-*. أطروحة دكتوراه، جامعة تيزيوزو،2019.

12. عميم، عبد القادر. *آليات إثبات الجريمة المعلوماتية في التشريع الجزائري –دراسة مقارنة* .أطروحة دكتوراه، جامعة الجزائر،2019-2020.

13. شنتير، خضرة. *الآليات القانونية لمكافحة الجريمة الإلكترونية –دراسة مقارنة-*. أطروحة دكتوراه، جامعة أحمد دراية، أدرار، 2020 -2021.

14. لهوى، رابح. *الشرعية الإجرائية للأدلة المستمدة من التفتيش*. أطروحة دكتوراه، جامعة باتنة1، 2020-2022،

15. زراري، نسرين. *السياسة الجنائية لمكافحة الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات*. أطروحة دكتوراه، جامعة خنشلة،2023-2024.

❖ **رسائل الماجستير**

1. السرحاني، محمد بن نصير. *مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض،2004.

2. المسعد، عبد الله عبد العزيز. *إجراءات المعاينة الفنية لمسرح الأحداث الإرهابي*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.

3. بن قارة مصطفى، عائشة. *حجية الدليل الالكتروني في مجال الاثبات الجنائي –دراسة مقارنة–*. رسالة ماجستير، جامعة الاسكندرية، 2009.

4. سوير، سفيان. *الجرائم المعلوماتية*. رسالة ماجستير، جامعة تلمسان، 2010 -2011.

5. طرشي، نورة. *مكافحة الجريمة المعلوماتية*. رسالة ماجستير، جامعة الجزائر1،2011-2012،

6. بوخبزة، عائشة. *الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري*.رسالة ماجستير، جامعة وهران، 2012 -2013.

7. سعيداني، نعيم. *آليات البحث والتحري عن الجريمة المعلوماتية في التشريع الجزائري*. مذكرة ماجستير جامعة باتنة، 2012-2013.

8. مسعود، مريم أحمد. *آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09*. رسالة ماجيستير، جامعة ورقلة، 2012-2013.

9. الصغير، يوسف. *الجريمة المرتكبة عبر الأنترنت*. رسالة ماجستير، جامعة تيزيوزو، 2013

10. بحرية، هارون. *وسائل الاثبات في الجريمة المعلوماتية*. رسالة ماجستير، جامعة خنشلة، 2013 -2014.

11. جبار، فطيمة. *الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري*. رسالة ماجستير، جامعة البليدة، 2013.

12. جرار، محمد باسل صالح. *معاينة مسرح الجريمة الالكتروني ودوره في الإثبات الجنائي وفق التشريع الفلسطيني*.رسالة ماجستير في القانون العام، جامعة النجاح الوطنية، فلسطين، 2022.

13. حسين، أحمد رمضان. *مسرح الجريمة وأدلته من منظور البحث الجنائي –دراسة تحليلية مقارنة* –. رسالة ماجستير، جامعة الشرق الأدنى، نيقوسيا، 2022.

14. القهيري، عمر محمود حمدان. *إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الالكترونية*. رسالة ماجستير، جامعة الشرق الأوسط، 2023.

❖ **مذكرات ماستر**

01.رزيق، محمد. *إجراءات المعاينة، التفتيش والحجز داخل المنظومة المعلوماتية*. مذكرة لنيل شهادة الماستر، جامعة البويرة، 2018 –2019.

02.جباري، عمار. *التفتيش الإلكتروني*. مذكرة لنيل شهادة الماستر، جامعة تبسة، 2022 –2023.

03.قادة، عبد الهادي. *دور المعاينة الجنائية في الإثبات الجنائي*. مذكرة مكملة لنيل شهادة الماستر، جامعة مستغانم، 2023 – 2024.

❖ **المقالات العلمية المنشورة الكترونيا**

أولا :باللغة العربية

1. الطبي، البركة، سودي، محمد حاج. "إشكالية الإثبات في الجرائم الإلكترونية". *مجلة آفاق علمية*، المركز الجامعي تامنغست، م11، ع01، أكتوبر 2018، مقال منشور على الرابط https://asjp.cerist.dz/en/article/84468، آخر إطلاع بتاريخ 2025/04/02 على الساعة، 19:00.
2. النعيمي، محمد يوسف. "صعوبات التعامل مع مسرح الجريمة الالكترونية –دراسة مقارنة–". *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة، م01، ع72، يونيو 2020، مقال منشور على الرابط: https://mjle.journals.ekb.eg/article_259606_e8106720214fd9fa0fb7bc6872deedcb.pdf ،آخر إطلاع بتاريخ 2025/02/22، على الساعة 17:02.
3. بلقاسم، سمية، بوشوشة، حميد." الجريمة الالكترونية بعد جديد للإجرام في الجزائر...واقعها وآليات مجابهتها". *مجلة العلوم الانسانية*، جامعة أم البواقي، م 10، ع 01، جوان2023، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/226117، آخر إطلاع بتاريخ 2025/03/15 على الساعة 10:15.
4. بن خليفة، إلهام."التفتيش كإجراء تحقيق تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" .*المجلة الدولية للبحوث القانونية والسياسية*، جامعة الوادي، م02 ، ع01 ، ماي 2018. مقال منشور على الرابط: https://asjp.cerist.dz/en/article/66489 ،آخر إطلاع بتاريخ 2025/03/07 على الساعة 12:23.
5. بن طالب، ليندا. "التفتيش في الجرائم المعلوماتية". *مجلة العلوم القانونية والسياسية*، جامعة الوادي، م11، ع 06، جوان 2017.مقال منشور على الرابط https://asjp.cerist.dz/en/article/46702 آخرا إطلاع بتاريخ 2025/03/08 على الساعة 21:37

6. بن فردية، محمد. "الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائري –دراسة مقارنة–". *المجلة الأكاديمية للبحث*، جامعة بجاية، م 09، ع01، جوان 2014، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/55437 ،آخر إطلاع بتاريخ 2025/03/19 على الساعة 18:35.
7. بن لاغة، عقيلة. "الطبيعة القانونية للمعاينة". بحث منشور على الرابط : https://mail.almerja.com/reading.php?idm=92644 ،آخر إطلاع بتاريخ2025/02/04 على الساعة 17:05.
8. بن مالك، أحمد، الخال، إبراهيم. "دور الأدلة الرقمية في الاثبات الجنائي". *مجلة العلوم الإنسانية*، المركز الجامعي، تندوف، م 05، ع 01، أفريل2021. مقال منشور على الرابط https://asjp.cerist.dz/en/article/148870 ،آخر إطلاع بتاريخ 2025/03/19، على الساعة 21:30.
9. بهلول، سمية، ذبيح، عماد دمان. "الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري". *مجلة الحقوق والعلوم السياسية*، جامعة خشلة، ع13، جانفي 2020.مقال منشور على الرابط:https://asjp.cerist.dz/en/article/107549 ،آخر اطلاع بتاريخ 2025/03/15، على الساعة 15:00
10. بوحليط، يزيد. "تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري". *مجلة التواصل في الاقتصاد والإدارة والقانون*، جامعة عنابة، ع48 ، ديسمبر 2016، مقال منشور على الرابط:https://asjp.cerist.dz/en/article/19945 ،آخر إطلاع بتاريخ 2025/03/09 على الساعة 20:35
11. حمداش، شمس الدين. بن مبروك، البشير. "القواعد الإجرائية المقررة لتفتيش المنظومة المعلوماتية في القانون الجزائري". *مجل صوت القانون*، جامعة خميس مليانة، م 09 ،ع 02، ماي 2003،. مقال منشور على الرابط: https://asjp.cerist.dz/en/article/221449 ،آخر إطلاع بتاريخ 2025/03/09، على الساعة 22:15.
12. خطوي، مسعود، عكوش، حنان. "خصوصية الدليل الالكتروني ". *مجلة الفكر القانوني والسياسي*، جامعة الأغواط، م 07، ع1، ماي 2023، مقال منشور على الرابط https://asjp.cerist.dz/en/article/220981، آخر اطلاع بتاريخ 2025/04/02 على الساعة 18:15.

13. خلف الله، فاروق. الآليات القانونية لمكافحة الجريمة المعلوماتية. *مجلة الحقوق والحريات*، جامعة بسكرة، ع 02 ، ديسمبر 2015 . مقال منشور على الرابط: https://asjp.cerist.dz/en/article/139256، آخر اطلاع بتاريخ 2025/03/05 على الساعة 18:36.

14. خليفي، فتيحة، مهداوي، محمد صالح." خصوصية التفتيش في البيئة الرقمية". *المجلة الجزائرية للقانون*، جامعة تلمسان، م 05، ع 09، جويلية 2022.مقال منشور على الرابط https://asjp.cerist.dz/en/article/197938، آخر إطلاع بتاريخ 2025/03/06 على الساعة 19:04

15. رابحي، عزيزة. التفتيش في نظم المعالجة الآلية للمعطيات". *مجلة القانون والعلوم السياسية*، المركز الجامعي النعامة، م 02، ع 01، جانفي 2016.مقال منشور على الرابط https://asjp.cerist.dz/en/article/86813، آخر إطلاع بتاريخ 2025/03/09 على الساعة 22:15.

16. سحتوت، نادية. "التنظيم القانوني للجريمة المعلوماتية –أدلة إثبات الجريمة المعلوماتية". *مجلة دراسات وأبحاث*، جامعة الجلفة، ع01، سبتمبر2009. مقال منشور على الرابط https://asjp.cerist.dz/en/article/4417، آخر إطلاع بتاريخ 2025/02/20 على الساعة 13:50.

17. صغير، يوسف. "التفتيش كآلية لإثبات جرائم نظم المعلوماتية". *المجلة النقدية للقانون والعلوم السياسية*، جامعة تيزي وزو، م 16، ع 04، ديسمبر 2021، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/176255، اطلاع بتاريخ 2025/03/10، على الساعة 12:00

18. عربوز، فاطمة الزهراء."التفتيش الالكتروني كإجراء للتحقيق في الجرائم المعلوماتية ". *مجلة جيل الأبحاث القانونية المعمقة* ، جامعة سيدي بلعباس ، ع 34 ، مقال منشور على الرابط: https://jilrc.com/archives/11227، أخر إطلاع بتاريخ 03/11/ 2025 على الساعة 15:21

19. فلاح، عبد القادر. "حجز وحفظ المعطيات في الجريمة الالكترونية". *مجلة صوت القانون*، جامعة خميس مليانة، م 08، ع 01، نوفمبر2021، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/169811، آخر إطلاع بتاريخ 2025/03/15 على الساعة 21:40

20.قلات، سومية، حاحة، عبد العالي. "مقتضيات المعاينة المعلوماتية". *مجلة الحقوق والحريات*، جامعة بسكرة، م 10، ع1، أفريل 2022، مقال منشور على الرابط https://asjp.cerist.dz/en/article/219038، آخر إطلاع بتاريخ 2025/02/04، على الساعة 14:58 .

21. مانع، سلمى. "التفتيش كإجراء للتحقيق في الجرائم المعلوماتية". مجلة *العلوم الإنسانية*، جامعة بسكرة ،ع 21 ، جوان 2011 ، مقال منشور على الرابط https://asjp.cerist.dz/en/article/49479، آخر اطلاع بتاريخ 2025/03/09 على الساعة 19:00

22. توفيق ، مجاهد، عباسة، طاهر. "جريمة الإرهاب الالكتروني في ضوء أحكام الاتفاقيات العربية لمكافحة جرائم تقنية المعلومات لعام 2010". *مجلة العلوم القانونية والسياسية*، جامعة الوادي، م 09، ع03، ديسمبر 2018، مقال منشور على الرابط https://asjp.cerist.dz/en/article/72222، آخر إطلاع بتاريخ12 /2025/03 على الساعة 17:40.

23. مجدوب، نوال." الآليات الإجرائية للكشف من الجريمة المعلوماتية". *مجلة البحوث القانونية السياسية*، المركز الجامعي آفلو، م 06، ع01، جانفي 2023، مقال منشور على الرابط https://asjp.cerist.dz/en/article/213392، آخر إطلاع بتاريخ 2025/03/15_على الساعة 10:36.

24. محمودي، سماح ." مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت". *مجلة الحقوق والعلوم السياسية*، جامعة خنشلة، ع08،جوان2017.مقال منشور على الرابط:https://asjp.cerist.dz/en/article/42459، آخر إطلاع بتاريخ 2025/03/07 على الساعة: 12:08.

25.محمودي، نور الهدى. "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية". *مجلة الباحث للدراسات الأكاديمية*، جامعة باتنة1،ع11، جوان2017. مقال منشور على الرابط: https://asjp.cerist.dz/en/article/24925، آخر إطلاع بتاريخ 2025/03/19 على الساعة 21:36

26. مرنيز، فاطمة. التفتيش الافتراضي كإجراء استدلالي في ضوء القانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها – دراسة مقارنة -" *مجلة الاجتهاد للدراسات القانونية والاقتصادي*، جامعة تامنغست، م01 ، ع02، 2 جوان 2021، مقال منشور على الرابط: https://asjp.cerist.dz/en/article/152366 ، آخر إطلاع بتاريخ 2025/03/12 على الساعة 22:07.

27.ممدوح، خالد ابراهيم. *معاينة مسرح الجريمة الإلكترونية*. مقال منشور على الرابط: http://kenanaonline.com/users/KhaledMamdouh/posts/81659،آخر اطلاع بتاريخ 10/02/2024، على الساعة 10:35.آخر إطلاع بتاريخ 2025/03/12 على الساعة 10:36.

28 .ممدوح، عبد الحميد عبد المطلب." استخدام بروتوكولTCP/IPفي بحث وتحقيق الجرائم على الكمبيوتر". مقال منشور على الرابط http://3dpolice.blogspot.com/2008/01/tcpip.html?m=1، آخر اطلاع بتاريخ 2025/02/25 على الساعة 21:58

29.همیسي، رضا." تفتيش المنظومات المعلوماتية في التشريع الجزائري". *مجلة العلوم القانونية والسياسية*، جامعة الوادي، م11، ع05، جوان 2012 . مقال منشور الرابط: https://asjp.cerist.dz/en/article/5740، آخر اطلاع بتاريخ 2025/03/06 على الساعة 17:40.

ثانيا : باللغة الأجنبية

1-CALECA, CHRISTIA.TCP/IP. Article publié sur internet, le site : https://csricted.univ-setif.dz/Documents/cours-informatique/TCP-IP.pdf Dernière visite le 25/02/2025، à 10 :00.

❖ **المحاضرات:**

1.أحمد، عمر شامل. *تطبيقات في الحاسوب*. محاضرات منشورة على الرابط https://uomosul.edu.iq/agriculture/wp-content/uploads/sites/11/2023/09/%D8%AA%D8%B7%D8%A8%D9%8A%D9%82%D8%A7%D8%AA-%D9%81%D9%8A-%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D9%88%D8%A8-1_2_compressed.pdf، آخر إطلاع بتاريخ 2025/02/24 على الساعة 16:33.

2.بواط، محمد. *محاضرات في قانون الإجراءات الجزائية*. دروس ألقيت على طلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، 2021 –2022. محاضرات منشورة على الرابط https://www.univ-chlef.dz/fdsp/wp-content/uploads/2023/05/Droit_Procedure_Penal_BOUAT.pdf، آخر إطلاع بتاريخ 2025/02/03 على الساعة 15:12.

3. زبون، خالد حمدي. *الحاسوب المرحلة الأولى*. كلية شط العرب الجامعة، 2021–2022. محاضرات على الرابط: https://sa-uc.edu.iq/uploads/curriculum/1656848217.pdf ،آخر إطلاع بتاريخ 2025/02/24 على الساعة 17:49.

4. شنة، محمد. *إجراءات البحث والتحري*. محاضرات ألقيت على طلبة السنة أولى ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، 2023 -2024. محاضرات منشورة على الرابط: http://dspace.univ-khenchela.dz:4000/items/794bad18-521b-4574-aa4d-993a88f600b9/full، آخر إطلاع بتاريخ 15/02/2025 من الساعة 10:46

5. نطيحي، نسمة .*الوقاية من الجرائم الالكترونية*. محاضرات مقدمة لطلبة السنة الثانية ماستر تخصص إدارة الكترونية وخدمات رقمية، كلية الحقوق والعلوم السياسية، جامعة سطيف، 2021-2022. منشورة على الرابط : http://en.univ-setif2.dz/mod/folder/view.php?id=3291، آخر إطلاع بتاريخ 2025/03/19، على الساعة 09:04.

فهرس المحتويات

العنوان	الصفحة
شكر وعرفان	
إهـــــــــداء	
مقدمة	أ-هـ
الفصل الأول: الإطار القانوني للمعاينة المعلوماتية	**7**
المبحث الأول: مفهوم المعاينة المعلوماتية	**8**
المطلب الأول: تعريف المعاينة المعلوماتية	**8**
الفرع الأول: التعريف اللغوي للمعاينة المعلوماتية	**8**
الفرع الثاني: التعريف الإصطلاحي للمعاينة المعلوماتية	**9**
المطلب الثاني: الطبيعة القانونية للمعاينة المعلوماتية وأهميتها	**11**
الفرع الأول: الطبيعة القانونية للمعاينة المعلوماتية	**11**
الفرع الثاني: أهمية المعاينة المعلوماتية	**14**
المبحث الثاني: القواعد الإجرائية للمعاينة داخل المنظومة المعلوماتية	**17**
المطلب الأول: معاينة مسرح الجريمة المعلوماتية.	**17**
الفرع الأول: مفهوم مسرح الجريمة المعلوماتية	**17**
الفقرة الأولى: المسرح التقليدي	**17**
الفقرة الثانية: المسرح السيبراني	**18**
الفرع الثاني: الخطوات المتبعة قبل وعند الانتقال للمعاينة المعلوماتية	**19**
الفقرة الأولى: الشروط القانونية لصحة المعاينة المعلوماتية	**19**
أولا: إخطار وإذن وكيل الجمهورية	**19**
ثانيا: أوقات المعاينة المعلوماتية	**20**
ثالثا: رضا الشخص بالمعاينة المعلوماتية	**20**
رابعا: محضر المعاينة المعلوماتية	**21**
الفقرة الثانية: الخطوات المتبعة قبل المعاينة المعلوماتية	**22**
الفقرة الثالثة: الخطوات المتبعة عند معاينة مسرح الجريمة المعلوماتية	**23**

المطلب الثاني: نطاق إجراء المعاينة المعلوماتية	**25**
الفرع الأول: معاينة مكونات الحاسب الآلي	**25**
الفقرة الأولى: معاينة القرص الصلب	**26**
الفترة الثانية معاينة البرمجيات	**27**
الفقرة الثالثة: معاينة النظام المعلوماتي	**28**
الفرع الثاني: معاينة أنظمة الاتصال بشبكة الأنترنت	**29**
الفقرة الأولى: معاينة مسار الأنترنت	**30**
ثانيا: فحص الخادم (Server)	**32**
خلاصة الفصل الأول	**34**
الفصل الثاني: الإطار القانوني للتفتيش والحجز داخل المنظومة المعلوماتية	**36**
المبحث الأول: التفتيش داخل المنظومة المعلوماتية	**37**
المطلب الأول: مفهوم تفتيش المنظومة المعلوماتية	**37**
الفرع الأول: تعريف التفتيش الالكتروني	**37**
الفرع الثاني: خصائص التفتيش الالكتروني	**38**
الفرع الثالث: الطبيعة القانونية للتفتيش الالكتروني	**39**
الفرع الرابع: صور التفتيش الالكتروني	**40**
الفقرة الأولى :تفتيش المكونات المادية للحاسب الآلي	**40**
الفقرة الثانية: تفتيش المكونات المعنوية للحاسب الآلي	**42**
الفقرة الثالثة: تفتيش شبكات الحاسب الآلي	**43**
أولا: حالة ارتباط حاسب المتهم بمنظومة معلوماتية داخل الاقليم الوطني	**43**
ثانيا: حالة ارتباط حاسب المتهم بمنظومة معلوماتية خارج الإقليم الوطني	**44**
المطلب الثاني: القواعد الإجرائية لتفتيش المنظومة المعلوماتية	**45**
الفرع الأول: إجراء الإذن بالتفتيش الإلكتروني	**45**
الفرع الثاني: إجراء التفتيش الإلكتروني بحضور أشخاص معينين قانونا	**46**
الفرع الثالث: رضا المشتبه فيه بالتفتيش الالكتروني	**48**

الفرع الرابع: مواعيد التفتيش الإلكتروني	**49**
الفرع الخامس: تحرير محضر بالتفتيش الالكتروني	**51**
المبحث الثاني: الحجز داخل المنظومة المعلوماتية	**53**
المطلب الأول: مفهوم الحجز الالكتروني	**53**
الفرع الأول: تعريف الحجز الالكتروني	**54**
الفرع الثاني: وظائف الحجز الإلكتروني	**55**
الفقرة الأولى: جمع أدلة الاثبات وفحص البيانات الرقمية	**55**
الفقرة الثانية: مصادرة المعطيات	**55**
المطلب الثاني: القواعد الإجرائية للحجز داخل المنظومة المعلوماتية	**55**
الفرع الأول: إجراءات الحجز الالكتروني	**56**
الفقرة الأولى: الحجز عن طريق نسخ المعطيات والبيانات	**56**
الفقرة الثانية: الحجز عن طريق منع الوصول إلى المعطيات	**57**
الفقرة الثالثة: حجز المعطيات ذات المحتوى المجرم	**57**
الفقرة الرابعة: حدود استعمال المعطيات المتحصل عليها	**58**
الفرع الثاني: طرق الحصول والتعامل مع الدليل الرقمي أثناء الحجز الالكتروني	**58**
الفقرة الأولى: تعريف الدليل الرقمي	**59**
أولا: أنه دليل علمي	**59**
ثانيا: الدليل الرقمي ذو طبيعة تقنية متطورة	**59**
الفقرة الثانية: برامج جمع الدليل الرقمي والحصول عليه	**60**
أولا: برنامج إذن التفتيش	**60**
ثانيا: قرص بدء تشغيل الكمبيوتر	**60**
ثالثا: برنامج معالجة الملفات كبرنامج(xtree Gold)	**61**
رابعا: برنامج نسح البيانات كبرنامج(LAP Link)	**61**
خامسا: برنامج كشف الديسك	**61**

سادسا: برامج الاتصالات كبرنامج Lan tastic	**61**
سابعا: برنامج فحص الشبكة	**61**
الفقرة الثالثة: طرق الحصول والتعامل مع الدليل الرقمي أثناء الحجز الالكتروني	**63**
أولا: جمع الدليل الرقمي والحصول عليه	**63**
ثانيا: فحص البيانات الرقمية	**63**
ثالثا: تحليل ومراجعة الأدلة	**63**
الفقرة الرابعة: العوائق التي تواجه الدليل الرقمي أثناء الحجز الالكتروني	**64**
أولا: الطبيعة غير المرئية للدليل الرقمي	**64**
ثانيا: سهولة محو وتدمير الدليل الرقمي	**64**
ثالثا: ضخامة البيانات المتعين فحصها	**64**
رابعا: إعاقة الوصول إلى الدليل الرقمي	**65**
خامسا: نقص المعرفة التقنية	**65**
خلاصة الفصل الثاني	**67**
خاتمة	**69**
قائمة المصادر والمراجع	
ملخص	

ملخص

تعد الجرائم الواقعة داخل المنظومة المعلوماتية من الأنماط الإجرامية المستحدثة التي أفرزتها تكنولوجيا الإعلام والاتصال.

ونظرا لتفاقم الاعتداءات على الأنظمة المعلوماتية وظهور" الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"، نجد أن المشرع الجزائري سطر سياسية جنائية خاصة في الجانب الإجرائي لإستجلاء الحقيقة وحماية المنظومة المعلوماتية من الجرائم الماسة بها، كإجراء المعاينة المعلوماتية، تفتيش المنظومة المعلوماتية إضافة إلى إجراء الحجز الإلكتروني .

وعليه، يمكن القول أن هذه الإجراءات والتي كانت محور دراستنا، لها فعالية نوعا ما في الكشف عن الجرائم الواقعة داخل المنظومة المعلوماتية.

الكلمات المفتاحية: المنظومة المعلوماتية، المعاينة المعلوماتية، التفتيش والحجز الالكتروني، الجرائم الماسة بأنظمة المعالجة الآلية المعطيات.

Summary

Crimes occurring within the information system are a newly emerging category of offenses resulting from information and communication technology.

In light of the rising attacks on information systems and the emergence of « crimes affecting automated data processing systems, » the Algerian legislator has established a specific criminal policy regarding procedural aspects to uncover the truth and protect the information system from related crimes. This includes measures such as digital examination, inspection of information systems, and electronic seizure. Thus, it can be said that these procedures, which were the focus of our study, have a certain effectiveness in detecting crimes occurring within the information system.

Keywords : information system, digital examination, inspection and electronic seizure, crimes affecting automated data processing systems.