جـــامـــعـــة يـــحـــي فـــــارس بـــالـــمـــديـــة

كـلـيـة الـحـقـوق والـعـلـوم السيـاسـة

إجراءات الضبط والمعاينة في الجريمة الإلكترونية

مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص قانون جنائي وعلوم جنائية

إعداد الطالبتين :

فلة بوقصة

نجوى عواد

تحت إشراف الأستاذة :

د/ يحياوي سمية

أعضاء اللجنة المناقشة :

الاسم واللقب	الجامعة	الصفة
الأستاذة مصباح رشيدة	جامعة المدية	عضوا رئيسا
الأستاذة يحياوي سمية	جامعة المدية	عضوا مشرفا
الأستاذة بن دالي براهم نسيمة	جامعة المدية	عضوا مناقشا

الموسم الجامعي :

2025-2024


بسم الله الرحمن الرحيم

الإهداء

إلى أغلى الناس، إلى من كانت لهم بصمة في حياتي ، وتوجيه في دراستي ، وأمل في مستقبلي .

إلى والدتي ووالدي، اللذين كانا دائما مصدر الإلهام والقوة في كل خطوة أخذتها، شكرا لوقوفكما إلى جانب في كل لحظة من لحظات هذه الرحلة .

إلى أصدقائي الذين كانوا شركاء في كل لحظة من لحظات السعادة والصعوبة ، شكرا لدعمكم اللامحدود .

إلى أساتذتي الكرام ، الذين قدموا لي العلم والإلهام ، فكانوا سببا في وصولي إلى هذا الإنجاز .

وأخيرا ، أهدي هذا النجاح إلى نفسي ، التي واجهت التحديات ولم تستسلم ، التي عملت بجد لتحقق الحلم.

عواد نجوى.

الإهداء

إلى نبع الحنان التي غمرتني بحبها وعطفها وكانت نعم العون لي أمي العزيزة، وكذا وسندي الذي دعمني وزرع في حب العلم والدراسة أبي العزيز، شكرا لكم لدعمي المستمر للوصول إلى هنا فاهدي هذا العمل لكما .

ولكل أخواتي وعائلتي الصغيرة وعائلتي الكبيرة ولأساتذتي الكرام الذين لم يبخلوا بتوجهاتهم وإلى صديقاتي وأصدقائي الأعزاء الذين كانوا لي خير عون وسند، أهدي لكل هؤلاء هذا العمل المتواضع.

بوقصة فلة .

شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات ، وبفضله تحقق النجاح .

أتقدم بخالص الشكر وعظيم الامتنان إلى كل من كان له دور في مساعدتي خلال إعداد هذه المذكرة .

أخص بالشكر والامتنان أستاذتي المشرفة يحياوي سمية ، لما قدمها لنا من توجيه

ودعم علمي ونفسي وشكر الأستاذ طبال إحسان على تقديمه لنا عنوان المذكرة، فلهما منا كل التقدير والعرفان .

كما لا يفوتني أن أشكر أساتذة الكلية على ما بذلوه من جهد في سبيل تعليمنا وتكويننا خلال سنوات الدراسة.

وإلى عائلتي الكريمة ، التي كانت السند والداعم الأول ، أبعث أسمى آيات الحب والتقدير ، لما قدموه لي من دعم متواصل ، وتحفيز دائم .

ولا أنسى زملائي وأصدقائي الذين شاركوني هذه الرحلة العلمية، فلكم كل الحب والتقدير.

مقدمة

مقدمة:

شهد العالم في العقود الأخيرة تطورا تكنولوجيا متسارعا عبر مختلف جوانب الحياة ، وفتح أفاقا واسعة أمام التواصل والمعرفة وتبادل المعلومات ، إلا أن هذا التطور على الرغم من مزاياه الكبيرة ، أفرز في المقابل تحديات جديدة تمثلت في بروز أنماط جديدة مستحدثة من الجرائم ، أطلق عليها الجرائم الإلكترونية وهي أفعال إجرامية ترتكب عبر الوسائط التكنولوجية الحديثة ، مثل شبكات الإنترنيت والهواتف الذكية والحواسب ، ومنصات التواصل الاجتماعي المختلفة ، وتتسم هذه الجرائم بالتعقيد والتطور المستمر ،إذ أنها غالبا ما تنفذ من خلال أدوات رقمية يصعب تعقبها ، ويستغل فيها إخفاء الهوية والحدود الجغرافية المفتوحة للفضاء السبيراني ، وقد استهدفت هذه الأفعال الإجرامية الأفراد، من خلال سرقة بياناتهم الشخصية أو ابتزازهم إلكترونيا ، كما استهدفت المؤسسات الاقتصادية عبر الاختراقات المعلوماتية ، حتى أنها استهدفت أمن الدول عبر الهجومات التي تستهدف البنية التحتية الرقمية الحيوية .

وتكمن أهمية هذا الموضوع في كونه يتناول أحد أبرز الإشكاليات العلمية التي تواجه أجهزة العدالة في العصر الرقمي حيث تختلف طبيعة الجريمة الإلكترونية عن الجرائم التقليدية من حيث أدوات ارتكابها وآثارها وطريقة تتبعها لذلك أصبحت الحاجة ملحة لتطوير أساليب الضبط والمعاينة بما يواكب هذا التحول التكنولوجي ، وقد ترتكب الجريمة الإلكترونية في ظل التشريع الجزائري عن بعد وبهوية مجهولة ومن خلال تقنيات معقدة تصعب عملية الكشف والتعقب ، كم أ مسرح الجريمة في هذا السياق ليس ماديا بل افتراضيا، مما يثير إشكاليات قانونية وتقنية دقيقة تتعلق بإثبات الجريمة وضبط الأدلة .

وهدف الأساسي من دراسة هذا الموضوع التعريف الدقيق بإجراءات الضبط والمعاينة في الجريمة الإلكترونية ، باعتبارها أدوات قانونية وتقنية جوهرية في التصدي لهذا النوع المستحدث من الجرائم ، فالتحولات الرقمية التي يشهدها العالم اليوم ، جعلت من الفضاء السبيراني ساحة جديدة لارتكاب أفعال إجرامية تتسم بالسرعة واللامادية والتعقيد ، مما يفرض تحديات كبيرة على أجهزة الأمن والعدالة الجنائية ومواجهة الخطر المتنامي للجريمة الإلكترونية في ظل التشريع الجزائري على الفرد والمجتمع ومحاسبة مرتكبي هذه الجريمة وفقا للقانون ، دون المساس بالحقوق والأفراد وحرياتهم .

وتم اختيار الموضوع لعدة أسباب نظرا لتزايد معدلات الجريمة الإلكترونية في المجتمعات الحديثة ولقلة الدراسات العربية المتخصصة التي تعالج الجانب الإجرائي منها لاسيما في ما يتعلق بالضبط والمعاينة التي تعتبر حجر الأساس في إثبات الجريمة الإلكترونية وكشف مرتكبيها. ومن الأسباب التي دفعتنا لدراسة هذا الموضوع هناك أسباب ذاتية وأخرى موضوعية، من الأسباب الذاتية كون الموضوع يدور حول جريمة مستحدثة تتطلب إجراءات خاصة وحتى طريقة مكافحتها تختلف عن الجرائم التقليدية لكونها تقع في عالم افتراضي عابر للحدود يصعب تحديد مرتكبيها لكونها تقع على أشياء غير مادية أما الأسباب الموضوعية فتتمثل في كون الجريمة الإلكترونية تمس مختلف القطاعات والدولة تحاول جاهدة في إنشاء إدارة إلكترونية ولمكافحتها يجب إتباع عدة إجراءات منها ما هو تقليدي وأخر حديث.

هناك مجموعة من الدراسات السابقة المختصة بإجراءات الضبط والمعاينة في الجريمة الإلكترونية المتمثلة في رسائل ماجستر منها دراسة بعنوان إجراءات التحقيق في الجريمة الإلكترونية لبخي فاطمة الزهراء ، كذلك مباركة رابح إجراءات التحري والتحقيق في الجريمة الإلكترونية ، عزالدين عثمان مقال إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية .

أما الإشكالية التي تطرح في هذا الصدد هي : **ما مدى فعالية إجراءات الضبط والمعاينة في الجريمة الإلكترونية في ظل التشريع الجزائري؟**

على ضوء هذه الإشكالية سنطرح جملة من التساؤلات الفرعية :

- ما المقصود بالضبط والمعاينة ؟

- ماهي شروط الضبط والمعاينة في الجريمة الإلكترونية ؟

- ماهي الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية والهيئات المختصة بها ؟

ويقتصر موضوعنا على إجراءين تقليديين هما الضبط والمعاينة في الجريمة الإلكترونية وقد اعتمدنا في ذلك على بعض المناهج الملائمة لطبيعة الموضوع منها المنهج الوصفي لوصف وبيان الإطار المفاهيمي للضبط والمعاينة في الجريمة الإلكترونية وكذا المنهج التحليلي من أجل تحليل مختلف القوانين الخاصة بتنظيم إجراءات لضبط والمعاينة في الجريمة الإلكترونية .

وقد مررنا بصعوبات وعراقيل كثيرة لإنجاز موضوعنا ومن بين الصعوبات قلة المصادر والمراجع التي تتحدث عن عملية الضبط وإن وجدت المراجع فالمعلومات قليلة وذلك راجع لقلة مراجع الكتاب الجزائريين حيث ما جمعناه من كتب لمشارقة كمصر والأردن .

وقد اتبعنا في ذلك خطة منهجية ثنائية الفصول حيث خصصنا الفصل الأول للضبط والمعاينة كوسائل لجمع الأدلة الرقمية في الجريمة الإلكترونية أما الفصل الثاني قد خصصناه للأساليب لفنية للضبط والمعاينة في الجريمة الإلكترونية.

الفصل الأول:الضبط والمعاينة كوسائل لجمع الأدلة الرقمية في الجريمة الإلكترونية

الفصل الأول:

الضبط والمعاينة كوسائل لجمع الأدلة الرقمية في الجريمة الإلكترونية

التقدم التكنولوجي الذي يشهده العصر الحديث يحتم ضرورة وجود قانون حديث يسايره ويتصدى للتطورات الإجرامية التي تصاحبه ، محاولا حماية هذه التقنية الحديثة من الانتهاكات الخطيرة التي تهدد سلامة الأفراد ، سواء في أموالهم ، أعراضهم ،حرياتهم الشخصية ، وغيرها من الحقوق التي أصبحت مهددة مع انتشار استخدام الكمبيوتر والإنترنيت من مختلف فئات المجتمع ، مما أدى إلى انتشار الجرائم الإلكترونية بمختلف أنواعها مثل النصب والسب والقذف...وغيرها، ونظرا لحداثتها واعتبارها جرائم عابرة للحدود ،وصعوبة تحديدها ، وذلك لأنها تقع في عالم افتراضي غير ملموس ، وللكشف عنها يقوم المحققون والجهات المختصة لمكافحتها ، بإتباع إجراءات قانونية وخاصة في البحث والتحري والتحقيق للكشف عنها ، ومن بين هذه الإجراءات الضبط والمعاينة واللذان يكونان نتيجة للتفتيش لولا التفتيش لا يكون هناك ضبط ومعاينة في الجريمة الإلكترونية.

وأصبحت الجرائم الإلكترونية في عصر الرقمنة تشكل تهديدا متزايدا مما يستدعي تطوير آليات فعالة لجمع الأدلة الرقمية وتقديمها للمحاكم .

ويعتبر الضبط والمعاينة من أهم الوسائل المستخدمة في هذا المجال، حيث يهدفان إلى الحفاظ على الأدلة الرقمية وتوثيقها بشكل صحيح لضمان قبولها في الإجراءات القانونية .

أما موضوع دراستنا فيقتصر على هذين الإجراءين الضبط والمعاينة ، وسنحاول في هذا الفصل التطرق إلى تحديد مفهوم الضبط في الجريمة الإلكترونية في المبحث الأول ، وسنتطرق إلى مفهوم المعاينة في الجريمة الإلكترونية في المبحث الثاني .

المبحث الأول :تحديد مفهوم الضبط في الجريمة الإلكترونية

يعتبر الضبط من أهم الإجراءات التي يقوم بها ضباط الشرطة القضائية في مرحلة التحقيق في الجرائم الإلكترونية، لأن الأدلة الرقمية يصعب التعامل معها، ومن خلال هذا المبحث سنتطرق إلى مفهوم الضبط في الجريمة الإلكترونية تعريفه وأهميته ونطاقه وذلك في المطلب الأول، تم تحديد شروط الضبط والصعوبات المرتبطة به في المطلب الثاني .

المطلب الأول: مفهوم الضبط في الجريمة الإلكترونية

الضبط هو إحدى الإجراءات التي يقوم بها ضباط الشرطة القضائية ، وهو من الإجراءات التقليدية التي تتم بعد التفتيش، ويختلف الضبط في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل، وهو يعتبر الغاية أو الهدف من التفتيش، وذلك بهدف ضبط الأدلة المادية والمعنوية المرتبطة بالجريمة التي تفيد في الكشف عن الحقيقة و إزالة اللثام عن الغموض الذي يدور حول الجريمة الإلكترونية ، من أجل تحقيق العدالة ومحاسبة مرتكبيها .

وقد ارتأينا في هذا المطلب لتعريف موجز للجريمة الإلكترونية قبل تعريف الضبط .

الفرع الأول: تعريف الضبط في الجريمة الإلكترونية

عرف بعض الفقه الجريمة الإلكترونية على أنها :" فعل غير مشروع الذي يتورط في ارتكابه الحاسب أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية "[1].

سنتطرق في هذا الفرع إلى تعريف الضبط في الجريمة الإلكترونية، لغة واصطلاحا و قانونا.

أولا : التعريف اللغوي للضبط

الضبط في اللغة له عدة معاني منها :

اللزوم والحبس، يقال: "ضبط عليه الشيء، أي لزمه وحبسه ". كما يقال: ضبط الشيء أي حفظه بالحزم[2].وتعني "ضبط الشيء ضبطا"[3]. كما يعني "ضبط الشيء: حفظه بالحزم، والرجل ضابط ، أي

---

[1] نهلا عبد القادر مومني ، **الجرائم المعلوماتية** ، الطبعة الأولى ، دار الثقافة للتوزيع والنشر ، عمان ،أردن ، 2008 ، ص 48

[2] أبي الفصل جمال الدين محمد بن مكرم ابن منظور الإفريقي المصري، **لسان العرب**، الجزء السابع، طبعة جديدة، دار المعارف، القاهرة، مصر، ص 340.

[3] ابن فارس، **معجم مقاييس اللغة**، الجزء الأول، دار الفكر للطباعة والنشر والتوزيع ،1979،ص386.

حازم"[1].

ثانيا : التعريف الاصطلاحي للضبط

الضبط يعني: " وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها "[2].

كما يعرف على أنه :"هو العثور على الأدلة في الجريمة التي يباشر التحقيق بشأنها والبحث عليها وهو الغاية من التفتيش ونتيجته المباشرة المستهدفة، ولذلك يتعين لإجرائه أن تتوفر فيه نفس القواعد التي تنطبق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط "[3].

الضبط هو:"الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأن الجريمة الإلكترونية، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها، أو غير ذلك مما يفيد في كشف الحقيقة و نظرا لكون الضبط في مجال الجرائم الإلكترونية هو ضبط بيانات المعالجة إلكترونيا "[4] .

كما يقصد بضبط الأدلة إجراءات جمعها، وهو : "الخلاصة النهائية لآلية التفتيش والذي يقصد به وضع اليد على الجريمة المتعلقة به كالأقراص الصلبة، الأشرطة، برامج، طباعة، بطاقات الائتمان "[5].

كما عرف على أنه:"وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة الإلكترونية التي وقعت، تفيد في كشف الحقيقة عنها وعن مرتكبيها "[6].

ويمكن تعريف الضبط بأنه :" وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها سواء كان هذا الشيء عقارا أو منقولا وقد يرد الضبط على الأشخاص وهو ما

---

(1) إسماعيل بن حماد الجوهري ، **الصحاح تاج اللغة وصحاح العربية** ، الجزء الثالث ، الطبعة الرابعة ، دار العلم للملايين ، بيروت ، لبنان ، 1990 ،ص279 .

(2) خالد عياد الحلبي ، **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت** ، الطبعة الاولى ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2011 ،ص168 .

(3) مصطفى محمد موسى ، **التحقيق الجنائي في الجرائم الإلكترونية** ، الطبعة الأولى ، مطابع الشرطة ، القاهرة ، مصر ، 2008 ،ص 208 .

(4) عادل لبيض ،نزلي بشرى، **إثبات الجريمة الإلكترونية** مذكرة ماستر تخصص قانون جنائي وعلوم جنائية ،كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، الجزائر،2017-2018 ، ص45 .

(5) عبد القادر فلاح ، نادية آيت عبد المالك ،**التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري** ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، المجلد 04 ، العدد 02 ، 2019 ،ص 1697 .

(6) لامية وعلي ،كاهنة سعودي ،**إجراءات مكافحة الجريمة الإلكترونية** ،كلية الحقوق والعلوم السياسية ،جامعة عبد الرحمان ميرة ، بجاية ، الجزائر ،2018-2019،ص83.

يصطلح على تسميته بالقبض "[1].

ثالثا :التعريف القانوني للضبط

نظم المشرع الجزائري الضبط في المادة 06 من القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي تتمكن من خلالها السلطة التي تباشر التفتيش من الضبط أو حجز المعطيات تكون مفيدة في كشف الجرائم أو مرتكبها [2] .

حيث نصت المادة 06 من القانون09-04 على مايلي :" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها، وأنه ليس من الضروري حجز المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة التخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية. يجب على كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة ..." *.

ومن كل هذه التعريفات السابقة يمكن أن نعرفه وهو وضع اليد على الأشياء المضبوطة المتعلقة بالجريمة الإلكترونية من أجل كشف عن الحقيقة وعن مرتكبيها ،سواء كانت تلك الأشياء مادية كالحاسوب أو الأقراص الصلبة أو معنوية كمعلومات وبرامج .

الفرع الثاني :الطبيعة القانونية للضبط في الجريمة الإلكترونية

الطبيعة القانونية للضبط قد تكون من إجراءات الاستدلال والتحقيق ،وتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص ولاقتضى الأمر تجريده من حيازته يكون الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال[3] .

---

[1] عبد الفتاح بيومي حجازي ، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت** ، الطبعة الأولى ، دار الفكر الجامعي الإسكندرية ، مصر ، 2006 ، ص207-208 .

[2] انظر المواد06-07-08 من قانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها ، الجريدة الرسمية ، العدد 47 ، المؤرخ في 16 أوت 2009 .

*وضع المشرع الجزائري إجراءات خاصة بضبط البيانات المعلوماتية تحت عنوان حجز المعطيات المعلوماتية وذلك من خلال المواد 06-07-08 من القانون 09-04 .

[3] بوحزمة نصيرة ، **التحقيق الجنائي في الجرائم الإلكترونية** ، دراسة مقارنة تخصص قانون جنائي ،رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية ، القانون الخاص ، كلية العلوم السياسية ، جامعة جيلالي إلياس ، سيدي بلعباس ، الجزائر ، 2021-2022 ، ص329.

تتسم طبيعة الضبط في الجريمة الإلكترونية بطابع فني وتقني، إذ يعتمد بشكل أساسي على تقنيات الحاسوب ونظم المعلومات في جمع الأدلة الرقمية وحفظها ، بما يضمن قبولها قانونا أمام المحاكم .

كما يجب أن يتم هذا الضبط وفقا لإجراءات تراعي فيها حماية الخصوصية الفردية والحريات العامة ، وتجنب انتهاك حقوق الأفراد [1] .

الفرع الثالث : محل أو نطاق الضبط في الجريمة الإلكترونية

يختلف محل الضبط في الجريمة الإلكترونية عن محل الضبط في الجريمة التقليدية، ومحل أو نطاق الضبط في الجريمة الإلكترونية يتمثل في ضبط الكيانات المادية وضبط الكيانات المعنوية، فالجرائم الإلكترونية ترد على أشياء ذات طبيعة معنوية وهي البيانات والمراسلات والاتصالات الإلكترونية أما الجرائم التقليدية فيرد على الأشياء مادية منقولة أو عقارات[2] .

أولا : ضبط الكيانات المادية

تطرق المشرع الجزائري للقواعد الخاصة بالضبط من خلال نص المادة 84 ق.إ.ج [3]، التي ورد فيها أنه يجب جرد الوثائق أو الأشياء المضبوطة ووضعا في أحراز مختومة يجوز للجهة القضائية المختصة الإطلاع عليها بعد تحرير محضر بذلك، وبحضور المتهم مصحوبا محاميه، ويمكن إصدار نسخ للوثائق التي تبقى مضبوطة، إذا تم تسليم النسخ يقوم الكاتب بالتأشير عليها بمطابقتها بالأصل ،أما إذا اشتمل الضبط على النقود أو سبائك أو أوراق تجارية أو أوراق ذات قيمة مالية، ولم يكن من الضرورة لإظهار الحقيقة للاحتفاظ بها عينا فإنه يتم إيداعها بالخزينة[4] .

ومن بين الأدلة المتحصل عليها هي الورق وجهاز الكمبيوتر وملحقاته، الورق وهو يعتبر من الأدلة التي ينبغي الاهتمام بها في البحث والتفتيش لمسرح الجريمة ، وينقسم إلى أوراق تحضيرية وأوراق تالفة وأوراق أصلية. الأوراق التحضيرية ويتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها

---

(1) عادل حماد عثمان ، **ضبط الأدلة في مجال الجريمة المعلوماتية** ، المجلد 109 ، العدد 532 ، كلية الحقوق ، جامعة دار العلوم ، الرياض ،السعودية ، ص 165

(2) أشرف عبد القادر قنديل ، **الإثبات الجنائي في الجريمة الإلكترونية** ، بدون طبعة ، دار الجامعة الجديدة للنشر ، الإسكندرية ، مصر ، 2015 ، ص 154-155.

(3) انظر المادة 84 من قانون الإجراءات الجزئية .، رقم 155/66 المؤرخ في 08-06-1966 ، المعدل والمتمم بقانون رقم 10/19 المؤرخ في 19-12-2019،الجريدة الرسمية ، العدد 84 ، صادر بتاريخ 14-12-2022 التي تضم التعديلات .

(4) فاطمة الزهراء بخي ،**إجراءات التحقيق في الجريمة الإلكترونية** ، مذكرة الماستر تخصص قانون جنائي علوم جنائية ، كلية الحقوق والعلوم السياسية جامعة المسيلة ،الجزائر 2013-2014 ،ص79.

أما الأوراق التالفة فتتم طباعتها للتأكد، ومن ثم إلقائها في سلة المهملات، والأوراق الأصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة[1] .

يتألف جهاز الكمبيوتر وملحقاته من مجموعة من الوحدات الأساسية التي تعمل يتناغم لأداء مختلف المهام وتشمل هذه الوحدات:- وحدة الإدخال وهي التي تستعمل لإدخال المعلومات أو المعطيات أو البرامج المراد معالجتها من الوسط الموجود عليه إلى ذاكرة الحاسوب، وهي تتكون من عدة أنواع وهي وسائل تسمح بالاتصال المباشر بين الوسط الخارجي وبين وحدة المعالجة المركزية، وكذلك مشغل الأقراص الممغنطة ، والفأرة والماسح الضوئي ومشغل الأقراص [2] .

-وحدات المعالجة المركزية تعتبر بمثابة العقل المفكر والمسيطر على عمل باقي الوحدات ، وتقوم بمعالجة البيانات حسب التعليمات الواردة في البرنامج وهي تتكون من وحدة التحكم والمسيطرة ، ووحدة الحساب والمنطق .

-وحدة الذاكرة وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية وهي تنقسم إلى ثلاثة وحدات وهي ،وحدة الذاكرة الرئيسية ووحدة و الذاكرة المساعدة ووحدات الإخراج .

وحدة الذاكرة الرئيسية هي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت ، وتشمل ذاكرة القراءة وذاكرة عشوائية [3]. كما وحدة الذاكرة المساعدة تستخدم لتخزين البيانات بصورة دائمة ،ومن أهم وسائط التخزين المستخدمة الأقراص المرنة الصلبة والأشرطة الممغنطة ، والأقراص المضغوطة. و وحدات الإخراج وهي الوحدات التي يمكن من خلال تحويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة أو مرئية ، وهي وسائل استخراج نتائج الاتصال بين الأفراد والحاسب الآلي ، وتشمل الشاشات بأنواعها، الطابعات على مختلف أنواعها ، وحدات رسم المنحيات البيانات ، الوحدات الظرفية [4].

---

[1] محمد الأمين البشري ،**التحقيق في الجرائم المستحدثة** ،الطبعة الأولى ،جامعة نايف العربية للعلوم الأمنية ،الرياض ،السعودية ،2004 ،ص117.

[2] فاطمة الزهراء بخي ، المرجع السابق ، ص 80-81 .

[3] نهلا عبد القادر المومني ، المرجع السابق ، ص 26-27 .

[4] علي جبار الحسناوي ،**جرائم الحاسوب والأنترنيت** ، الطبعة الأولى ، دار اليازوري ،عمان ،الأردن، 2009 ،ص24-25.

ثانيا :ضبط الكيانات المعنوية

انقسمت التشريعات الإجرائية حول إمكانية ضبط الأشياء المعنوية ، فظهر اتجاهين الأول يرى عدم إمكانية تصور إجراء الضبط على الكيان المعنوي كونه ينصب على بيانات الحاسوب التي تختلف عن الأشياء المادية المحسوسة القابلة للضبط .

ومن التشريعات التي أخذت بهذا الاتجاه قانون الإجراءات الجنائية الألماني ،حيث حصرت المادة 94 منه محل الضبط على الأشياء المادية المحسوسة أو الملموسة، واتبعت اليابان نفس المنهج ، ويقترح إتباع هذا الاتجاه إضافة عبارة المواد المعالجة عن طريق الحاسوب أو بيانات الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط ليشمل التطور التكنولوجي لبيئة المعلومات .

أما الاتجاه الثاني فيرى بأنه لا مانع من ضبط البيانات الإلكترونية مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة المادية المفيدة في كشف الحقيقة ، وبالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها ومن أخذ بهذا الاتجاه القانون الكندي وكذلك الشأن بالنسبة لفرنسا وأمريكا[1].

ومن بين المكونات المنطقية لجهاز الحاسوب التي يمكن ضبطها هي المعلومات والبيانات وبرمجيات الحاسوب التي تشمل الوثائق ،المستندات والمواد التي يطلق عليها المواد المساندة ، وهي مواد مكتوبة في صورة كتيبات أو منشورات تطبع حاليا على الوسائط الإلكترونية مثل الأقراص المرنة أو المدمجة، وتنقسم إلى برمجيات النظم والبرمجيات التطبيقية[2].

المطلب الثاني : شروط الضبط في الجريمة الإلكترونية والصعوبات المرتبطة بها

قبل الشروع في عملية الضبط في الجريمة الإلكترونية يتعين على ضباط الشرطة القضائية استيفاء مجموعة من الشروط الموضوعية والشكلية ، وذلك على رغم من الصعوبات العديدة التي تعترضهم أثناء تنفيذ هذه العملية .

وعليه سنتطرق في هذا المطلب إلى شروط الضبط في الجريمة الإلكترونية في الفرع الأول، والصعوبات المرتبطة بها في الفرع الأول .

---

[1] نور الهدى زيبحة ، **الإثبات الجنائي في الجرائم الإلكترونية** ، مذكرة الماستر تخصص قانون الأعمال ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي ، أم البواقي ، الجزائر ، 2015-2016 ،ص 82 .

[2] فاطمة الزهراء بخي ، المرجع السابق ، ص 82-83 .

الفرع الأول :شروط الضبط في الجريمة الإلكترونية

تتلخص هذه الشروط في إجراء الإذن، وإجراء التفتيش والحجز بحضور أشخاص معينين قانونا،ومواعيد التفتيش والحجز، ورضا المشتبه فيه بالتفتيش، وتحرير محاضر التفتيش والحجز .

أولا :إجراء الإذن

لم يشترط المشرع الجزائري كقاعدة عامة الإذن في التفتيش في المنظومة المعلوماتية لكن طبق عليها القواعد العامة في حالة ما إذا تعلق بالانتقال إلى منزل المشتبه فيه من اجل تفتيش منظومة معلوماتية فتطبق في هذه الحالة القواعد الخاصة بتفتيش المنازل والأماكن الخاصة ، إذا ألزم المشرع الجزائري إذن مكتوب من وكيل الجمهورية المختص من اجل القيام بجراء التفتيش وإلا اعتبر التفتيش تعسف[1]، ويمكن التفرقة بين حالتين، الحالة الأولى الانتقال لتفتيش منظومة معلوماتية* في الأماكن الخاصة ويطبق على إجراء تفتيش الأماكن الخاصة كالمنازل بإذن مكتوب. الحالة الثانية الانتقال لتفتيش منظومة في مكان عام كمقهى أو ساحة عامة تطبق عليها نفس القواعد التي تطبق على تفتيش الأماكن العامة ولا يوجد إذن ،ولقد نص المشرع الجزائري على الإذن في الدخول إلى الأماكن الخاصة في نص المادة 44 من قانون الإجراءات الجزائية [2].

حيث يجب أن يتضمن الإذن المذكور أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي ستتم زيارتها وتفتيشها وإجراء الحجز فيها ،وذلك تحت طائلة البطلان[3] .

ثانيا :إجراء التفتيش والحجز بحضور أشخاص معينين قانونا

يتم القيام بإجراء التفتيش والحجز بحضور كل من المشتبه فيه، القائم بالتفتيش، والشاهدين، فالأصل في التفتيش، وكما عرفته القواعد الخاصة بالتفتيش يتم بحضور المتهم أو من يجوز أن يمثله، وضابط الشرطة القضائية القائم بالتفتيش، وإذا تعذر حضور المتهم أو من يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين للسلطة، إلا أن المشرع الجزائري استثنى على هذه القواعد في نص المادة 45

---

[1] عبد القادر عدو ، **الجريمة الإلكترونية إجرائيا** ، الطبعة الثانية ، دار هومة ، الجزائر ، 2016 ، ص 86

* تفتيش المنظومة المعلوماتية مرتبط بالحجز حيث يطبق نفس قواعد التفتيش على الحجز ،كما أنه إذا بطلان التفتيش يبطل الحجز .

[2] انظر المادة 44 من قانون الإجراءات الجزائية من الأمر 66-155.

[3] محمد رزيق ، **إجراءات المعاينة ، التفتيش والحجز داخل المنظومة المعلوماتية** ، مذكرة الماستر ، كلية الحقوق والعلوم السياسية ، جامعة أكلي محند أولحاج ، بويرة ، الجزائر ، 2018-2019 ص20 .

من قانون الإجراءات الجزائية [1]على انه لا تطبق هذه الأحكام إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذ يمكن تفتيش لمنظومة المعلوماتية بدون حضور المتهم أو الشاهدين [2].

ثالثا :مواعيد التفتيش والحجز

كقاعدة عامة في الجرائم التقليدية التفتيش في الأماكن الخاصة لا يكون قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا، غير أن تفتيش المنظومة المعلوماتية لا يخضع لهذه القواعد إذ نص المشرع الجزائري انه يجوز إجراء التفتيش والحجز في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في أي ساعة من ساعات النهار أو الليل، بناءا على إذن مسبق من وكيل الجمهورية المختص، وهذا ما نصت عليه المادة 47 الفقرة 3 من قانون الإجراءات الجزائية ،كونها حالة من الحالات الاستثنائية التي اقر بها القانون[3] .

رابعا : رضا المشتبه فيه بالتفتيش والحجز

لا يجوز تفتيش المساكن أو حجز الأشياء المثبتة للمتهم إلا برضا صريح من الشخص الذي ستنفذ هذه الإجراءات، ويجب أن يكون هذا الرضا مكتوب بخط يده أو من استعان به أو اختاره في حالة عدم قدرته على الكتابة شريطة أن يختار بنفسه هذا الشخص ويذكر ذلك في المحضر مع الإشارة إلى ذلك في محضر التفتيش والحجز[4] ، غير انه في جريمة ماسة بالأنظمة المعلوماتية فتطبق الأحكام المنصوص عليها في نص المادة 47 مكرر من قانون الإجراءات الجزائية [5].

وحسب نص المادة 45 من قانون الإجراءات الجزائية فتتم عمليات التفتيش التي تجرى طبقاللمادة44 أعلاه على الوجه الأتي:

-إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية فانه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فان ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له ، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته [6].

---

[1] انظر المادة 54 من قانون الإجراءات الجزائية .

[2] ناصر جوادي ، **إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية** ، الطبعة 3 ، الجزائر ، 2011 ، ص47 .

[3]انظر المادة 47 من قانون الإجراءات الجزائية المعدل والمتمم بقانون 06-22 المؤرخ في 20-12-2006 الصادر بالجريدة الرسمية ،العدد 84 الصادر في ديسمبر 2006 .

[4]محمد رزيق ، المرجع السابق ،ص 22 .

[5]انظر المادة 47 مكرر من قانون الإجراءات الجزائية.

[6]انظر المادة 44 ،45 من القانون الإجراءات الجزائية .

-وإذا جرى التفتيش في مسكن شخص أخر يشتبه بأنه يحوز أوراقا وأشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش وإن تعذر ذلك أتبع الإجراء المنصوص عليه في الفقرة السابقة ولضباط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى أعلاه الحق في الإطلاع على الأوراق أو المستندات قبل حجزها .

خامسا : تحرير محاضر التفتيش والحجز

المحاضر هي عبارة عن ملخص عن الواقعة، ويتضمن إثبات جميع ما قام به المحقق من إجراءات قانونية وفنية من أجل كشف الغموض على الواقعة وضبط الأدلة [1] ، ويكون بتكليف القائم بالتفتيش باصطحاب كاتب من أعوان الضبط القضائي يحرره محضر خاص بالتفتيش سواء كان ايجابيا أو سلبي ويتم تسجيل فيه جميع وقائع التحقيق والتفاصيل ، وذكر البيانات والأشياء والوثائق التي تتم ضبطها بكل دقة وأمانة.

وأوجب القانون على المحقق أن يوقع على المحاضر وكذلك الحال بالنسبة للكاتب، ويجب أن يتم التوقيع على كل صفحة من صفحات المحاضر وهذا فضلا عن نهاية المحضر، وذلك لإبعاد أية شبهة كالتزوير على أنه بالنسبة للكاتب يكفي توقيعه مع المحقق في نهاية محضر التحقيق، لأن الوثائق القائمة بالمحضر مستبعدة من توقيع عضو النيابة العامة[2].

أما بالنسبة للحجز فبالرجوع إلى نصوص المواد 44،45،47 وما يليها من قانون الإجراءات الجزائية[3] نجد أن المشرع لم يحدد قواعد خاصة بالحجز داخل المنظومة المعلوماتية بل اشترط نفس القواعد المطبقة على التفتيش داخل هذه المنظومة ، أي أنه لم يحدد طبيعة الحجز إما على بيانات المنطقية أو المعنوية من جهة أو على الوسائل المادية كجهاز الكمبيوتر ولواحقه إلا أنه من الجانب الميداني تطبق القواعد المنصوص عليها في قانون الإجراءات الجزائية أي لا يزال تطبق إجراءات الحجز التقليدي على الجرائم الإلكترونية وهو الحجز على الوسائل المادية[4].

---

[1] محمد رزيق ، المرجع السابق ،ص23 .

[2] ابتسام بغو ،**إجراءات المتابعة الجزائية المعلوماتية** ، مذكرة ماستر في القانون الجنائي للأعمال ، كلية الحقوق ، جامعة العربي بن مهيدي ، أم البواقي ، الجزائر ، 2015 ، ص 47

[3] انظر المواد 44 ، 45 ،47 ، من قانون الإجراءات الجزائية .

[4] محمد رزيق ، المرجع السابق ،ص24 .

الفرع الثاني :الصعوبات المرتبطة بالضبط في الجريمة الإلكترونية

الضبط بحسب الأصل لا يرد إلا على أشياء مادية ، فلا صعوبة بالتالي بضبط أدلة الجريمة الواقع على المكونات المادية للكمبيوتر كرفع البصمات مثلا عنها ، ولذلك فلا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في النسخة غير المشروع أو إتلافها بوسائل تقليدية كالكسر أو الحرق، ولكن تكمن أهمية الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل :الفيروس وفي ضبط بيانات الكمبيوتر DATA بعدم وجود أي دليل مرئي في هذه الحالات والسهولة تدمير الدليل في ثواني معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات ، ومن الصعوبات التي تواجه إجراء الضبط وعملية استخلاص الدليل في الجريمة الإلكترونية كذلك نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن، كذلك لدى أجهزة العدالة الجنائية الممثلة في سلطة الاتهام والتحقيق، وذلك فيما يتعلق بشفافية الحاسب الآلي، والإلمام بعناصر المعلوماتية وكيفية التعامل معها، لذلك كخطوة أولى يتعين منح الضبطية القضائية لأولئك العاملين في مجال المعلومات الأمنية سواء كانوا من أفراد الأمن أو في القطاعات ذات العلاقة بجهاز الحاسب الآلي سواء كانوا فنين أو خبراء [1] .

المبحث الثاني : المقصود بالمعاينة في الجريمة الإلكترونية

تعتبر المعاينة من أهم إجراءات التحقيق، وتهدف إلى كشف الغموض عن كل ماله علاقة بالجريمة وهي إجراء غايته الوصول إلى كشف الحقيقة .

وسنتطرق في هذا المبحث لمفهوم المعاينة في الجريمة الإلكترونية في المطلب الأول، وشروطها والصعوبات المرتبطة بها في المطلب الثاني .

المطلب الأول: مفهوم المعاينة في الجريمة الإلكترونية

تعد المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة، ومن أهم المراحل الإطلاع و نظرا لما يمكن أن توفره من أدلة إثبات للجريمة، وتزداد أهميتها في الجرائم الإلكترونية.

وسنتطرق في هذا المطلب إلى تعريف المعاينة في الجريمة الإلكترونية في الفرع الأول وأهميتها في الفرع الثاني ومحل أو نطاق المعاينة في الجريمة الإلكترونية في الفرع الثالث .

[1] نور الهدى زيبحة ، المرجع السابق ، ص52 .

الفرع الأول :تعريف المعاينة في الجريمة الإلكترونية

لم يعرف المشرع الجزائري المعاينة ولكن سنتطرق في هذا الفرع إلى تعريف المعاينة في الجريمة الإلكترونية من الناحية اللغوية والاصطلاحية والفقهية فقط .

أولا : التعريف اللغوي للمعاينة

تعني المعاينة لغة :"عاينه معاينة،وعيانا:رأه بعينه، ولقيته عيانا ،ومعاينة لم أشك في رؤيتي إياه"[1].
وتعني المعاينة أيضا: "العين المعاينة: النظر، وقد عاينه معاينة وعيانا ،...لقبه عيانا أي معاينة و رأه عيانا: لم يشك في رؤيته إياه، رأيت فلانا عيانا أي مواجهة، عين كل شيء، شاهده وحاضره "[2] .

ثانيا :التعريف الاصطلاحي للمعاينة

وردت عدة تعريفات للمعاينة فهناك من يعرفها بأنها: "إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما يفيد من الآثار في الكشف عن الحقيقة، فهي بذلك تعد من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما رأت فيذلك ضرورة لإجلاء الحقيقة أو بناء على طلب من الخصوم والأصل أن تجرى المعاينة بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة "[3].

كما تعرف على أنها: "فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو ثقوب "[4].

وعرفت أيضا أنها: "إجراء يتطلب إثبات حالة الأمكنة والأشياء والأشخاص، ووجود الجريمة إجراء لا يتضمن إكراه أو الاعتداء على حرمة الأشياء والأشخاص "[5] .

كما عرفت أيضا، هي: " إثبات حالة الأماكن و الأشخاص وكل ما يفيد في كشف الحقيقة، وهي تتطلب أن ينتقل ضابط الشرطة القضائية إلى عين مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه

---

(1) إبراهيم أنيس ، عبد الحليم منتصر ، وآخرون ، **المعجم الوسيط** ، الطبعة الرابعة ، مكتبة الشروق الدولية ،2004 ، ص 461 .

(2) أبي الفضل جمال الدين محمد بن مكرم ابن المنظور الإفريقي المصري ، **لسان العرب** ، المجلد 13 ، دون طبعة ، دار صادر ، بيروت ، لبنان ، دون سنة ، ص309-302 .

(3) محمد رزيق ، مرجع السابق ، ص 09 .

(4) أمير فرج يوسف ، **الجرائم المعلوماتية على شبكة الانترنيت** ، بدون طبعة ، دار المطبوعات الجامعية ، الإسكندرية ، مصر ،2009 ، ص219 .

(5) محمد حماد مرهج الهيتي ، **جرائم الحاسوب** ، الطبعة الأولى ، دار المناهج ، عمان ،الأردن ،2006 ، ص255 .

من الأشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء "[1]. وتعرف أيضا: "هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة "[2] .

ثالثا : التعريف الفقهي للمعاينة

المشرع الجزائري لم يعرف المعاينة في قانون الإجراءات الجزائية ،وإنما نظم إجراءات القيام بها حيث ترك مجال تعريفها للفقه. وقد تعددت التعريفات الفقهية للمعاينة: فهناك من عرفها على أنها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وهي إجراء يتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها "[3] .

كما عرفها بعض الباحثين على أنها: "ملاحظة وفحص حي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة، لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة "[4] .

كما عرفها البعض الأخر من الفقهاء على أنها: "عرض حال عن المكان والأشياء التي تلتقطها العين واليد ..."[5] .

ونستنتج من خلال كل هذه التعريفات أن المعاينة هي قيام ضابط الشرطة القضائية برؤية وفحص مكان الجريمة بعينه وكل ما يتعلق بالجريمة، مع التحفظ على مختلف الأشياء الموجودة في مسرح الجريمة من أجل كشف الحقيقة .

الفرع الثاني :أهمية المعاينة في الجريمة الإلكترونية

للمعاينة أهمية بارزة في مجال التحقيق الجنائي لكونها مصدرا أصيلا من مصادر الأدلة المادية والفنية الراسخة والثابتة التي تكون دائما محل ثقة سلطات التحقيق والقضاء، ومرآة صادقة تعكس بأمانة

---

(1) عمار حشمان ، **الجريمة المعلوماتية في التشريع الجزائري** ، مذكرة ماستر المهني ، كلية الحقوق والعلوم الاقتصادية والعلوم التجارية وعلم التسيير ، جامعة قاصدي مرباح ، ورقلة ، الجزائر ، 2019-2018 ،ص48 .

(2) سحنون نادية ، **التنظير لقانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية** ، المؤسسة المركز الجامعي ، سوق أهراس ، الجزائر ،ص50 .

(3) أشرف عبد القادر قنديل ، المرجع السابق ، ص153 .

(4) لطيفة خلفي ، سارة اليزيد ، وآخرون ، **المعاينة في الجرائم الإلكترونية**، مذكرة الماستر ، كلية العلوم القانونية والاقتصادية والاجتماعية ، جامعة محمد الخامس ، الرباط ، المغرب ، 2019-2018 ، ص04 .

(5) سومية قلات ، عبد العالي حاجة ، **مقتضيات المعاينة المعلوماتية في التشريع الجزائري** ، مجلة الحقوق والحريات المجلد 11 ، العدد 01 ، كلية الحقوق والعلوم السياسية ، جامعة بسكرة ، الجزائر ، 2023 ، ص 523 .

وقائع وملابسات الجريمة، فهي ناطقة بما أتاه شاهد على ما فعله الجاني دون انحياز أو تعديل أو نقصان[1].

فالهدف من المعاينة يكمن في جمع الأدلة الناتجة عن الجريمة، وكذا إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها ولا غموض عن كيفية وقوع الجريمة [2] .

وتتجلى أهمية المعاينة أيضا في كونها إجراء أولية حاسما يهدف إلى جمع الأدلة المادية قبل أن تطالها يد العبث أو التشويه، مما يمكن من الحفاظ على القيمة الإثباتية لتلك الأدلة، كما تتيح المعاينة اتخاذ إجراءات فورية على نحو يساهم في توثيق الوقائع، من ذلك سماع الشهود الذين قد يكونون حاضرين بمسرح الجريمة[3] .

الفرع الثالث :محل أو نطاق المعاينة في الجريمة الإلكترونية

عند علم ضابط الشرطة القضائية بوقوع جريمة إلكترونية، فإن أول إجراء يتخذه هو الانتقال إلى مسرح الجريمة الإلكترونية بهدف مباشرة التحقيق. ويلاحظ أن مسرح الجريمة في الجرائم الإلكترونية يختلف بطبيعته عن مسرح الجريمة التقليدية، سواء من حيث المكان أو الأدوات المستخدمة، كما أن محل المعاينة يختلف بدوره بين البيئة المادية في الجرائم التقليدية والبيئة الافتراضية في الجرائم الإلكترونية.

أولا :البيئة التقليدي

يقع هذا النوع من الأدلة خارج بيئة الحاسوب والانترنيت، ويشمل المكونات المادية المحسوسة في مكان وقوع الجريمة ، مثل شاشة الحاسوب ، لوحة المفاتيح ، الأقراص ، وغيرها. يشبه إلى حد كبير مسرح الجريمة التقليدي ، حيث يمكن لضابط الشرطة القضائية معاينة هذه الأدلة التي قد تحمل بصمات أو وسائط تخزين أو متعلقات شخصية تساعد في كشف الجريمة [4].

---

[1] بن نعوم خالد أمين ، **إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري** ، مذكرة ماستر ، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم ، الجزائر ،2018-2019 ،ص74 .

[2] فاطمة الزهراء بخي ، المرجع السابق ،ص85 .

[3] مصطفى السلمي ، **محاضرالضبطية ودورها في إثبات الجرائم المعلوماتية** ،مذكرة ماستر في لقانون الخاص ، كلية العلوم القانونية والاقتصادية والاجتماعية ، جامعة سيدي محمد بن عبد الله ، فاس ، المغرب ، 2021-2022 ، ص28 .

[4] محمد رزيق ، المرجع السابق ،ص10 .

وتجدر الإشارة أن الجرائم الواقعة على المكونات المادية للحاسوب تدخل ضمن نطاق الجرائم التقليدية لأنها تستهدف المال ، لأن مكونات الحاسوب المادية تدخل ضمن حيز الأموال المنقولة التي هي محل للاعتداء عليها بالجرائم الموصوفة بوقوعها على المال، وجرائم الإتلاف والتخريب[1] .

والجرائم الإلكترونية تنصب عل العناصر التالية :

1- المعلومات وتتمثل هذه الجريمة في سرقة أو تغير أو حذف المعلومات، كالنشاط الإجرامي الذي يستهدف اختراق البريد الإلكتروني والعبث بمحتوياته .

2- الأجهزة وتشمل الجرائم الإلكترونية التي تقع على أجهزة الكمبيوتر بهدف تعطيلها أو تخريبها بإرسال الفيروسات أو البرامج التي تسبب تلف هذه الأجهزة .

3- الأشخاص أو الجهات وهي الجرائم التي تقع على الأشخاص أو الجهات باستخدام شبكة الانترنيت والكمبيوتر كالتهديد أو السرقة...وغيرها [2] .

ثانيا : البيئة الافتراضي

تكون هنا المعاينة للجرائم الواقعة على المكونات غير المادية وهي برامج الجهاز وبياناته، وهذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينات أو فائدتها وتستخلص في نقص وقلة الآثار المادية التي تقع على المكونات غير المادية للجهاز، وتردد عدد كبير من الأشخاص على مسرح الجريمة خلال فترة زمنية قصيرة، والتي غالبا ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها[3].

ويقع داخل البيئة الالكترونية ، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنيت ،في ذاكرة الأقراص الصلبة الموجودة بداخله [4].

وتتم معاينة مكونات الحاسب الذي يعتبر مصدرا غنيا بالأدلة الإلكترونية خاصة الحواسيب الشخصية ،الحاسب الآلي يقوم في تركيبته على ثلاثة عناصر أساسية هي :القطع الصلبة ، والقطع المرنة أو البرمجيات، وكذا المعطيات أو المعلومات أو البيانات، فمعاينة الحاسب تستلزم الفحص المادي والمعنوي لكل هذه العناصر نظرا للارتباط الطبيعي بين بعضها البعض .

---

[1] لطيفة الخلفي ، سارة اليزيد ،وآخرون ، المرجع السابق ،ص 10 ، انظر الملحق الأول ، إحصائيات الجرائم الإلكترونية 2024 ،ص57.

[2] المرجع نفسه ، ص 11 .

[3] محمد رزيق ، المرجع السابق ، ص 10 .

[4] أشر ف عبد القادر قنديل ، المرجع السابق ، ص 138 .

كما تتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي ، للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله، وفحص القرص الصلب تساعد المحقق عادة على جمع البيانات والمعطيات المخزنة فيه بشكل آلي أو إرادي التي كان يستخدمها الجاني ، من معلومات أو صفحات وعناوين الانترنيت أو وسائل البريد الإلكتروني المرسلة والمتلقاة ، وكذا البرامج الجاهزة المتخصصة التي استعملها المشتبه فيه للتواصل مع أصدقائه[1].

المطلب الثاني :شروط المعاينة في الجريمة الإلكترونية والصعوبات المرتبطة بها

تخضع إجراءات المعاينة الإلكترونية لجملة من الشروط ،كما تواجه عدة معوقات وهذا ما يجعلهالا ترق لنفس الدرجة من الأهمية مقارنة مع المعاينة في الجرائم التقليدية وسنتطرق في هذا المطلب إلى شروط المعاينة في الجريمة الإلكترونية في الفرع الأول والصعوبات المرتبطة بها في الفرع الثاني .

الفرع الأول : شروط المعاينة في الجريمة الإلكترونية

يشترط لصحة المعاينة في الجريمة الإلكترونية توافر عدة شروط هي:

أولا : إذن أو أمر المعاينة الإلكترونية

لا يجوز إجراء المعاينة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات حسب المادة 64 من قانون الإجراءات الجزائية من القانون 90-24 والقانون 06-22 [2]،حتى بالنسبة لمعاينة المساكن فيكون ذلك برضا صاحب المسكن، في حال عدم وجود إذن مسبق، لكن مع وجود الإذن تتم المعاينة سواء في الميعاد المحدد أو خارجه، إلا في حالة رضا الشخص الذي يكون إجراء المعاينة بعدده[3].

ثانيا : وقت إجراء المعاينة الإلكترونية

يكون إجرائها في كل ساعة من ساعات النهار أو الليل ، بناءا على إذن مسبق من وكيل الجمهورية حسب نص المادة 44 الفقرة 3 من القانون 06-22 قانون الإجراءات الجزائية [4] ، على عكس الجرائم التقليدية التي لها وقت محدد من الساعة الخامسة صباحا إلى غاية الثامنة مساءا .

ثالثا : مكان إجراء المعاينة الإلكترونية

تجرى في أي مكان ارتكبت فيه الجريمة، مراعاة لمبدأ الشخصية والعينة من خلال نصوص المواد

---

[1] بن نعوم خالد أمين ، المرجع السابق ،ص 77 .
[2] انظر المادة 64 من قانون الإجراءات الجزائية الجزائري .
[3] سومية قلات ، عبد العالي حاجة ، المرجع السابق ، ص 528 .
[4] المادة 47 من قانون الإجراءات الجزائية الجزائري .

من 582 إلى 591 من قانون الإجراءات الجزائية [1] والمادة 15 من قانون 09-04 [2] على غرار مبدأ الإقليمية ما عدا السفارات فلا يجوز معاينتها إلا بوجود اتفاقية ترفع الحصانة، وبحضور السفير شخصيا وأيضا الثكنات العسكرية لا يجوز معاينتها إلا بواسطة وكيل الجمهورية لدى القضاء العسكري[3].

رابعا : الأشخاص الذين يحق لهم حضور المعاينة الإلكترونية

يحق لكل من المتهم، الضحية، ومحاميهم، بالإضافة إلى وكيل الجمهورية وقاضي التحقيق وضابط الشرطة القضائية، أن يطلبوا إجراء المعاينة في أي مرحلة من مراحل التحقيق بهدف الكشف عن الحقيقة. كما يجوز لأطراف القضية تقديم هذا الطلب مباشرة إلى قاضي التحقيق للقيام بهذا الإجراء وإذا ارتأى قاضي التحقيق عدم جدوى إجراء المعاينة ، يتعين عليه إصدار أمر مسبب بالرفض خلال أجل لا يتجاوز عشرين20 يوما من تاريخ تقديم الطلب من قبل الأطراف أو محاميهم. وفي حال لم يبت قاضي التحقيق في الطلب خلال الأجل المحدد، يجوز للطرف المدني أو المتهم أو وكيل الجهورية الطعن أمام غرفة الاتهام، وذلك وفقا لأحكام المادتين 69 مكرر و172 من قانون الإجراءات الجزائية الجزائري [4].

كما يستعين ضباط الشرطة القضائية أو قاضي التحقيق بأشخاص مؤهلين، أي ضباط متخصصين في المجال المعلوماتية ، وهذا ما نصت عليه المادة 49 من قانون الإجراءات الجزائية الجزائري [5].

ولقاضي التحقيق أن يخطر وكيل الجمهورية عند رغبته في إجراء المعاينة، كما انه يستعين بكاتب التحقيق ويحرر محضر بما يقوم به من إجراءات المادة 79 من قانون الإجراءات الجزائية [6]، ويقوم قاضي التحقيق أيضا بجمع الآثار التي يعثر عليها في مكان الجريمة ويقوم بجردها وحفظها في أحراز ويمكن رسم مكان الجريمة وأخذ صور شمسية والاستماع إلى أقوال الأشخاص الحاضرين بعين المكان وهذا ما يقوم به ضباط الشرطة القضائية عندما يتم القيام بإجراء المعاينة

---

[1] انظر المواد من 582 إلى591 من قانون الإجراءات الجزائية الجزائري .
[2] انظر المادة 15 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .
[3] سومية قلات ، عبد العالي حاجة ، المرجع السابق ، ص 529 .
[4] انظر المادتين 69 مكرر و 172 من قانون الإجراءات الجزائية الجزائري .
[5] انظر المادة 49 من قانون الإجراءات الجزائية الجزائري .
[6] انظر المادة 79 من قانون الإجراءات الجزائية الجزائري .

خامسا : محضر المعاينة الالكترونية

هو ثمرة مجهود ما قامت به الهيئات المكلفة بها ، حيث اوجب قانون إجراءات الجزائية على ضباط الشرطة القضائية تحرير محاضر عن أعمالهم التي يقومون بها و يضمنها مجموع ما قام به من إجراءات هذا ما نصت عليه المادتين 18 و 54 من قانون إجراءات الجزائية الجزائري[1] ، كما أن ضابط الشرطة القضائية ليس ملزما قانونا طبقا للمادة 20 من قانون إجراءات الجزائية [2] ، أن يصطحب معه كاتبا وأن كان له الحق في الاستعانة بأعوانه في تحرير محضر المعاينة ، و يتضمن محضر المعاينة مجموعة من البيانات تتعلق بالجريمة و المشتبه فيه و محرر المحضر و وظيفته و رتبته و توقيعه و ختمه و تاريخ المحضر ، وتدوين أقوال الحاضرين و أي شخص له معلومات عن الجريمة مع التوقيع عن المحضر و أن امتنعوا يصرح بذلك في المحضر [3].

الفرع الثاني : الصعوبات المرتبطة بالمعاينة في الجريمة الإلكترونية

تواجه المعاينة عدة صعوبات وهذا ما يجعلها لا ترق لنفس درجة من الأهمية مقارنة مع المعاينة في الجرائم التقليدية وذلك راجع إلى ما يلي :

أولا : ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على أدوات المعلومات .

ثانيا :الأعداد الهائلة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية ، وحتى يكمن للمحقق القيام بالمعاينة في العالم الافتراضي، لابد عليه أن ينتقل إلى العالم الافتراضي للمعاينة من مكتبه أو اللجوء إلى مقهى الانترنيت أو إلى الخبراء وغيرها من الأماكن التي تساعد في إظهار الحقيقة [4].

ثالثا : إمكانية تلاعب الجاني في البيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية .

رابعا : تخلف تقريبا كلي للآثار في الجرائم الإلكترونية [5].

---

[1] انظر المادتين 18و54 من قانون الإجراءات الجزائية .

[2] انظر المادة 20 من قانون الإجراءات الجزائية .

[3] سومية قلات ، عبد العالي حاجة ن المرجع السابق ،ص 530 .

[4] ابتسام بوميلة ، مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية مذكرة ماستر ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، الجزائر ، 2020-2021 ، ص45 .

[5] عائشة بن قارة مصطفى ، حجية الدليل الالكتروني في القانون الجزائري والقانون المقارن ، بدون رقم طبعة ، دار الجامعة الجديدة ، مصر ، 2010 ، ص 81 .

خلاصة الفصل الأول :

نستنتج من خلال هذا الفصل الأول الذي تطرقنا فيه إلى مفهوم كل من الضبط والمعاينة في الجريمة الالكترونية ، فالضبط في الجريمة الالكترونية يتم من خلال اتخاذ عدة إجراءات لازمة للحفاظ على الأدلة الرقمية ومنع إتلافها والعبث بها ، ويشمل تحديد مختلف الأجهزة والأنظمة المعلوماتية المتورطة في الجريمة مثل الحواسيب ، الهواتف الذكية ، الخوادم ، وشبكات الانترنت، مع نسخ البيانات لضمان عدم ضياع الأدلة الأصلية ، وتتمثل المعاينة في فحص وتحليل الأدلة الرقمية للكشف عن تفاصيل الجريمة وتحديد هوية مرتكبيها ، وهي تشمل فحص الأجهزة والأنظمة المعلوماتية للاستخراج البيانات المخزنة فيها مثل: الملفات ، الرسائل ، السجلات التصفح بها ، وتحليل البيانات لتحديد الأنشطة غير القانونية التي تم القيام بها مثل: القرصنة ، الاحتيال ، نشر المحتوى غير القانوني ، مع استخدام الأدوات والبرامج المتخصصة لتحليل الأدلة الرقمية واستخراج المعلومات المطلوبة .

وللضبط والمعاينة في الجريمة الإلكترونية أهمية كبيرة ، حيث تعتبر من أهم الإجراءات المتبعة في مكافحة الجريمة الإلكترونية ، حيث تضمن الحصول على الأدلة المعلوماتية سواء من البيئة الرقمية أو التقليدية ، كما تساعد في تحديد هوية مرتكبي الجرائم الإلكترونية ، وتقديمهم للعدالة ، كما تساهم في حماية الأفراد والمؤسسات من الأضرار الناجمة عن الجريمة الإلكترونية .

وهناك عدة تحديات للقيام بعملية الضبط والمعاينة في الجريمة الإلكترونية من بينها : صعوبة تتبع الأدلة الرقمية ، حيث يمكن للمجرمين إخفاء آثارهم بسهولة . سرعة تطور التكنولوجيا، مما يتطلب تحديثا مستمرا للأدوات والتقنيات المستخدمة في الضبط والمعاينة في الجريمة الإلكترونية . الحاجة إلى خبرات فنية متخصصة في مجال الأدلة الرقمية، بحيث يجب على الجهات المختصة في مكافحة الجرائم الإلكترونية مواكبة التطورات التكنولوجية ، وتطور قدراتها في مجال مكافحة الجرائم الإلكترونية للقضاء عليها .

الفصل الثاني : الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية والهيئات المختصة بها

الفصل الثاني :

الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية والهيئات المختصة بها

تختلف إجراءات الضبط والمعاينة في الجرائم الإلكترونية عن الجرائم التقليدية ، بسبب طبيعة الأدلة الرقمي التي تتسم بسهولة التغيير أو الحذف، حيث يمكن تغيير الأدلة الرقمية أو حذفها بسهولة، مما يستوجب الحذر الشديد عند التعامل معها، كما أن الأدلة الرقمية تتواجد في عدة أماكن، مثل أجهزة الكمبيوتر والهواتف الذكية ، ويمكن للأدلة الرقمية أن يكون حجمها كبيرا جدا ، مما يتطلب استخدام أدوات وتقنيات متخصصة لتحليلها، لذلك وجب إتباع قواعد محددة عند القيام بالضبط والمعاينة في الجرائم الالكترونية .

ويتم تحديد الجهة المختصة بالضبط والمعاينة في الجرائم الالكترونية وفقا للتشريعات الوطنية والإجراءات القانونية المعمول بها في كل دولة ، ومع ذلك يمكن بشكل عام تحديد بعض الجهات الرئيسية التي تضطلع بهذا الدور، مثل الجهات القانونية المختصة، والسلطات القضائية، وخبراء التقنية المعتمدين.

سنتطرق في هذا الفصل للأساليب الفنية المعتمدة في الضبط والمعاينة في الجريمة الإلكترونية بالإضافة إلى الجهات المختصة بذلك، سنخصص المبحث الأول لدراسة الأساليب الفنية المستخدمة في الضبط والمعاينة، والمبحث الثاني لدراسة الهيئات المختصة بالضبط والمعاينة في الجريمة الإلكترونية .

المبحث الأول : الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية

يهدف هذا المبحث إلى تسليط الضوء على الأساليب الأساسية الفنية التي تحكم عملية الضبط والمعاينة في الجريمة الإلكترونية وفحص الآثار بكل دقة وعناية من اجل الحصول على الدليل الإلكتروني من قبل ضباط الشرطة القضائية ، ونتطرق في المطلب الأول إلى الخطوات الفنية للضبط في الجريمة الإلكترونية ، وفي المطلب الثاني للخطوات الفنية للمعاينة في الجريمة الإلكترونية .

المطلب الأول: الخطوات الفنية للضبط في الجريمة الإلكترونية

الضبط في الجريمة الإلكترونية يتطلب مجموعة من الخطوات الدقيقة، كما يتطلب أيضا استخدام مجموعة من الأدوات والتقنيات المتطورة والحديثة التي تساهم في تحديد الجريمة ، وتهدف إلى ضمان جمع الأدلة الرقمية وتحليلها بشكل قانوني ودقيق لضمان تقديم معلومات موثوقة في التحقيقات ، وتقديم المتهمين إلى العدالة .

الفرع الأول : الخطوات المتبعة لإجراء الضبط في الجريمة الإلكترونية

يكون وصول الجريمة التقليدية إلى علم سلطات الضبط عن طريق الشكوى أو البلاغ، أو في حالة ضبط الجريمة المتلبس بوقوعها ن بينما في الجريمة الإلكترونية، تصل أخبارها إلى سلطات الضبط بإحدى الطرق التالية :

أولا: تلقي سلطات الضبط أو أجهزة التحقيق معلومات مفادها أن أشخاصا معروفين أو غير معروفين يمارسون أنشطة تندرج تحت تعريف الجريمة الإلكترونية، وذلك في مكان معروف وعلى أجهزة محددة ،وفق لغة برمجية معلومة [1].

ثانيا: ضبط شخص معين بحوزته أموال مشبوهة أو بطاقات مزورة ، أو بطاقات تعريف مشبوهة .

ثالثا: بلاغ على سلطات الضبط أو التحقيق من المجني عليه يفيد بتلاعب أو ممارسات خاطئة في حقه أو حقوق الآخرين ، سواء تمثل ذلك في صورة عجز مالي في حسابات المؤسسة مالية أو أوضاع حقوق أو تغيرات في الودائع.

رابعا : توفر المعلومات عن نشر فيروسات تخريبية عبر شبكة الانترنيت ، لاسيما وأن تطبيق القانون في مجال مكافحة الفيروسات المعلوماتية يواجه صعوبات ، وموانع كثيرة [2] .

---

[1] نور الهدى زيبحة ، المرجع السابق ، ص 51.

[2] المرجع نفسه والصفحة .

الفرع الثاني : قواعد تحريز وتأمين المضبوطات الإلكترونية

الدليل الإلكتروني يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية، إلا أنه نظرا إلى الطبيعة الخاصة له ، فإن عملية ضبطه وتحريره، والتأمين عليه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا وصيانته من إمكانية العبث به وبالتالي المحافظة على سلامة هذه المضبوطات الإلكترونية، ومن هذه الإجراءات ما يلي:[1]

أولا : تحديد المادة الإلكترونية المراد ضبطها

نظرا لسهولة التلاعب في بيانات الأنظمة المعلوماتية وشبكاتها ، وبدون ترك أي أثار ، فإنه يتعين على المحقق عند تحديد البيانات المراد ضبطها ، وضع علامة مادية خاصة عليها ، ويثقلها إلى أقراص أو أشرطة ممغنطة ، ثم يقوم المحقق ومشغل النظام بتسجيل بياناته على هذه الأشرطة ، ثم يتم وضعها في علب مخصصة لحفظها والتوقيع عليها وختمها ، على أن تنظم هذه الإجراءات بمحضر ، يوقع عليه حسب ما تقتضيه الأحكام القانونية الخاصة بضبط الأشياء وحفظها [2].

ثانيا : تأمين البرامج المضبوطة قبل تشغيلها

على المحقق في حالة ضبط البرامج الإلكترونية أن يعمل على تأمين هذه البرامج فنيا، يعمل نسخة كاملة وسليمة منها ، قبل البدء بتشغيلها من قبل الخبراء وبواسطة أنظمة معلوماتية مأمونة من جانبه، وإذا تم تشغيل هذه البرامج بغير الطريقة التي صممت فيها ، قد تتحول إلى برنامج تدمير ، وبالتالي يفقد الدليل[3].

ثالثا : الالتزام بإتباع القواعد الفنية الخاصة بكيفية نقل الأحراز*الإلكترونية وحملها

تحتاج البيانات الإلكترونية المضبوطة والمفرغة على الأقراص إلى عناية خاصة من التلف أو الضياع ، لذا لا بد عند ثقلها مراعاة عدم تعريضها للأتربة ، والأشعة كهرومغناطسية حتى لا يتم إتلاف

---

[1] غازي عبد الرحمان ، هيان الرشيد ، **الحماية القانونية من الجرائم المعلوماتية** ، أطروحة أعدت لنيل شهادة الدكتوراه في القانون ، كلية الحقوق ، الجامعة الإسلامية ، لبنان ،2004 ، ص 566 -567 .

[2] بوحزمة نصيرة ، **التحقيق الجنائي في الجرائم الالكترونية** ، دراسة مقارنة ، رسالة لنيل شهادة الدكتوراه في العلوم القانونية القانون الخاص ، كلية الحقوق والعلوم السياسية ، جامعة الجيلالي اليابس ، سيدي بلعباس ن الجزائر ، 2021-2022 ، ص 333 .

[3] رشيدة كابوية ، **حجية الدليل الرقمي في الإثبات الجنائي** ، مداخلة للمشاركة في فعاليات الملتقى الدولي حول أدلة الإثبات الجنائية في التشريعات المقارنة ، المتعقد ليومي 25-26 أفريل 2018 ، كلية الحقوق والعلوم السياسية ، جامعة طاهري محمد ، بشار ، الجزائر ، 2018 ص 2221 .

* أحراز هي الأشياء أو المواد التي يتم ضبطها إثناء التحقيق أو التفتيش لصلتها بالجريمة ، ويتم تحريرها أي حفظها وتأمينها بطريقة تضمن عدم العبث بها أو تغيير حالتها ، لتستخدم كأدلة في القضية ، وهي تشمل أجهزة الحاسوب والهواتف المحمولة ، الأقراص الصلبة ووسائط التخزين ، رسائل البريد لالكتروني ، ملفات الرقمية ، بيانات المخزنة على الشبكة .

محتوياتها [1].

رابعا : مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز الإلكترونية

عند التخزين الأقراص والأشرطة الممغنطة التي تم ضبطها يجب مراعاة ظروف التخزين من حيث درجة الحرارة والرطوبة المناسبة لحفظها، والتي يجب أن تتراوح درجة الحرارة فيها بين 4-32 درجة وتكون درجة الرطوبة فيها مابين 20-80 درجة، مع تفادي تعريضها للأضواء أو لأي سائل من السوائل ،مع العلم أنه يمكن أن تصل مدة صلاحية تخزين هذه الأقراص إلى ثلاث سنوات دون يصيبها تلف أو تعديل أو تحويل [2] .

خامسا : منع الأشخاص غير المرخص لهم من الوصول إلى المعطيات

منع الأشخاص غير المرخص لهم من الوصول إلى المعطيات والبيانات التي تم ضبطها داخل دعامة مادية للتخزين ،من خلال إحاطتها بتدابير الحماية الفنية كالترميز والتشفير أو أية وسيلة إلكترونية أخرى تمنع الدخول إليها ، وصيانتها ببرامج منها التحريف والتغيير في البيانات مثل برامج منع الكتابة[3].

الفرع الثالث : طرق الضبط الإلكتروني

أصبحت أنظمة الضبط الإلكتروني تلعب دورا حيويا في مختلف مجالات الحياة ، لاسيما في القطاعات الأمنية ، والإدارية ، والتعليمية ، والإنتاجية ، وهو يقوم على استخدام تقنيات رقمية وأنظمة المعلومات لمراقبة ، وتوجيه ، وتحسين الأداء البشري ، وتتنوع طرق الضبط الإلكتروني بحسب الفرض منها ، حيث يتم ضبط البيانات والمعلومات بطرق التالية :

أولا : يمكن طباعة البيانات ومصادرتها ، كطباعة الرسائل والبريد الإلكتروني على الورق .

ثانيا : الاستيلاء على الوسط الملموس الذي يتم تخزين البيانات عليه .

ثالثا : استنساخ البيانات على النموذج الملموس الذي يتم حفظ نسخة عليه مثل ذاكرة فلاش USB.

---

[1] بوحزمة نصيرة ، المرجع السابق ، ص 333.

[2] حسام محمد الشنراقي ، **الجرائم المعلوماتية** ، دراسة تطبيقية مقارنة على جرائم الاعتداء على التوقيع الالكتروني ، بدون رقم طبعة ، دار شتات للنشر والبرمجيات ، مصر ، 2013 ،ص525.

[3] عدلي دحمان سعد الدين ثامر البشير ، **التحقيق الجنائي في الجرائم الإلكترونية** ،مذكرة ماستر في الحقوق تخصص قانون الجنائي والعلوم الجنائية ،كلية الحقوق والعلوم السياسية ،جامعة زيان عاشور ، الجلفة ، الجزائر 2020-2021، ص 55.

رابعا : إنشاء نسخ أصلية من البيانات الإلكترونية المخزنة على الأجهزة الرقمية ذات صلة بالجريمة [1] .

خامسا: استخدام برامج الكمبيوتر اللازمة للنفاذ والوصول إلى البيانات والأدلة المحتملة بالجريمة ذات صلة.

سادسا : ضبط الأجهزة الرقمية التي سجلت عليها البيانات والمعلومات والتحفظ عليها [2].

المطلب الثاني : الأساليب الفنية للمعاينة في الجريمة الإلكترونية

تعد المعاينة في مسرح الجريمة الإلكترونية مرحلة حاسمة في عملية التحقيق الجنائي الرقمي ،تختلف بشكل جوهري عن معاينة مسارح الجرائم التقليدية ، نظرا لطبيعة الأدلة الرقمية غير المادية وسهولة تلفها والعبث بها ، وتقتضي المعاينة في الجريمة الإلكترونية الالتزام بإجراءات تقنية منظمة ودقيقة ،تهدف إلى صون الأدلة الرقمية من أي تلف أو تلاعب، بما يضمن إمكانية استخدامها بفعالية في الإجراءات القضائية .

وسنتطرق في هذا المطلب إلى الخطوات الفنية المتبعة قبل الانتقال للمعاينة في الجريمة الإلكترونية في الفرع الأول ،والخطوات الفنية المتبعة عند الانتقال لمعاينة في الجريمة الإلكترونية في الفرع الثاني .

الفرع الأول : الخطوات الفنية المتبعة قبل الانتقال لمعاينة في الجريمة الإلكترونية

قبل الشروع في المعاينة في الجريمة الإلكترونية ، هناك مجموعة من الخطوات الفنية الأساسية يجب على المحققين إتباعها وتتمثل فيما يلي :

أولا :وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها [3].

ثانيا : وجود خريطة توضح الموقع الذي ستتم معاينته ، تفاصيل المبنى أو الطابق موضوع البلاغ،وعدد الأجهزة والخزائن والملفات ،ويحدد ذلك من خلال مصادر سرية لجهات الأمن [4].

ثالثا : تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية ، حتى يتم تحديد كيفية التعامل معها فنيا

---

[1] حورية خليصة ، حمزة فيروز ، **خصوصية التحقيق في الجريمة المعلوماتية** ، مذكرة الماستر في الحقوق تخصص قانون جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي ، أم البواقي ، الجزائر ، 2023-2024 ، ص 53 .

[2] خالد ممدوح إبراهيم ، **سلطات النيابة العامة في الجرائم الالكترونية** ، الطبعة الأولى ، دار الفكر الجامعي ، الإسكندرية ، مصر ، 2021 ، ص 268-269 .

[3] حسام محمد الشنراقي ، المرجع السابق ، ص 353 .

[4] خيرت علي محرز ، **التحقيق في الجرائم الحاسب الآلي** ، بدون طبعة ، دار الكتاب الحديث ، القاهرة ، مصر ، 2012 ، ص61 .

قبل المعاينة سواء من حيث الضبط أو التأمين أو حفظ الأوراق المستندات المتداولة [1].

رابعا :تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج[2].

خامسا : إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن[3].

سادسا : تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في الفريق المعاينة على حدة، وذلك حتى لا تتداخل الاختصاصات [4].

سابعا : إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتى يستعد من الناحية الفنية والعلمية ، وذلك لكي يضع الخطة المناسبة ضبط أدلة الجريمة حال معاينتها [5].

ثامنا: إعداد خطة للمعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل [6].

تاسعا : أن تتم كل هذه الإجراءات وفق مبدأ المشروعية ، وفي إطار ما تنصت عليه القوانين الجنائية [7].

عاشرا : الاحتفاظ بسرية المعاينة حتى نهاية المأمورية بأن تتم التحرك لإجرائها في سرية تامة ،ويراعي كذلك عدم الإفصاح عن المعلومات التي تم التحصيل عليها لكون المعلومات التي يتم البحث عنها إتلافها بسهولة من قبل المتهمين أو المتورطين في الجريمة [8].

حادي عشر : تحدد مصدر التيار الكهربائي حتى لا يستطيع الجاني أو شركاؤه إتلاف الأدلة بقطع التيار الكهربائي عن مكان المعاينة ، فيتم تأمينه بمجرد الوصول لمكان المعاينة [9].

الفرع الثاني : الخطوات الفنية المتبعة عند الانتقال للمعاينة في الجريمة الإلكترونية

هناك عدة خطوات يجب على المحقق إتباعها عند الانتقال للمعاينة في الجريمة الإلكترونية ، وهذه الخطوات تتمثل فيما يلي :

---

[1] سحتوت نادية ، المرجع السابق ، ص 50

[2] مصطفى السالمي ، المرجع السابق ، ص 30 .

[3] نور الهدى زيبحة ، المرجع السابق ،ص 40 .

[4] سعيدة بعرة ، **الجريمة الإلكترونيية في التشريع الجزائري** ، مذكرة الماستر في الحقوق قانون جنائي ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، الجزائر ، 2015-2016 ،ص 77 .

[5]بوديسة بحاد عبد الرؤوف ، **آليات التحري عن الجريمة الالكترونية في القانون الجزائري** ، مذكرة الماستر تخصص قانون الإعلام الآلي والانترنيت ، كلية الحقوق والعلوم السياسية ، جامعة محمد بشير الإبراهيمي ، برج بوعريريج ، الجزائر ، ص 58 .

[6]سعيدة بعرة ، المرجع السابق ،ص 77.

[7] خيرت علي محرز ، المرجع السابق ، ص 62.

[8]حسام محمد نبيل الشنراقي ، المرجع السابق ، 354 .

[9] المرجع نفسه ، ص 355 .

أولا : تحديد الأجهزة الحاسب الآلي الموجودة في مكان المعاينة ، وتحديد مواقعها بأسرع فرصة ممكنة ،وفي حالة وجود شبكة اتصالات يجري البحث عن خادم الملف file server ، وذلك لتعطيل الاتصالات لمنع تخريب الأدلة الموجودة أو محوها ، يراعي تصوير الأجهزة الموجودة خاصة الأجزاء الخلفية منها[1].

ثانيا : ضرورة وضع حراسة كافية على مكان المعاينة ، مراقبة التحركات داخل مسرح الجريمة، مع رصد الاتصالات الهاتفية من وإلى مسرح الجريمة، مع إبطال مفعول الهواتف النقالة التي تساعد عن طريق تقنية الجيل الثالث في تدمير الأدلة من خلال اتصالها بالأجهزة محل المعاينة [2] .

ثالثا : عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة ، وذلك قبل إجراء الاختبارات اللازمة ، للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي ، حتى لا يحدث أي إتلاف للبيانات المخزنة ، ومحو البيانات المسجلة [3].

رابعا : التحفظ على سلة ا لمهملات وما فيها من أوراق ممزقة وشرائط والأقراص الممغنطة وغير السلمية أو المحطمة ، وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة [4].

خامسا : القيام بحفظ المستندات الخاصة بالإدخال ، وكذا مخرجات الحاسوب الورقية ذات الصلة بالجريمة ورفع ما قد يوجد عليها من بصمات أو يثار مادية [5].

سادسا :حصر عملية المعاينة في فئة المختصين والمحققين الذين يتوفرون على الكفاءة العلمية والخبرة الفنية في مجال النظم المعلوماتية ، والذين تلقوا تدريبا فنيا كافيا على التعامل مع الأدلة الإلكترونية ، ففي فرنسا مثلا: يقوم فريق التحقيق المكون من 13 شرطيا بالإشراف على تنفيذ المهام التي يأمر بها وكيل الجمهورية أو قاضي التحقيق ، فيرافقون المحققون أثناء عملية المعاينة ، و يعملون على فحص الأجهزة ،ونسخ محتوياتها والتحقيق ، وإعداد تقارير فنية ترسل إلى قاضي [6].

سابعا : وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي على المسؤولين بها، ودور كل واحد منهم [7].

---

[1] خيرت علي محرز ، المرجع السابق ،ص 63 .

[2] مباركة رابح ، **إجراءات التحري والتحقيق في الجريمة الإلكترونية** ،مذكرة ماستر في قانون الإعلام الآلي والإنترنيت ، كلية الحقوق والعلوم السياسية ، جامعة البشير الإبراهيمي ، الجزائر ،2021-2022 ، ص37 .

[3] عمار حشمان ، المرجع السابق ، ص 48 .

[4] أمير فرج يوسف ، المرجع السابق ، ص 24 .

[5] أشرف عبد القادر قنديل ، المرجع السابق ، ص 139 .

[6] مباركة رابح ، المرجع السابق ، ص38 .

[7] رزيق محمد ، المرجع السابق ، ص 13 .

ثامنا : ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها ، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغيير[1] .

تاسعا: ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء [2] .

المطلب الثالث :نموذج تطبيقي لإجراء الضبط والمعاينة في جريمة اختراق حساب فيسبوك وسرقة البيانات الشخصية في الجزائر

مثال تطبيقي بعنوان جريمة اختراق حساب فيسبوك وسرقة بيانات شخصية في الجزائر

الفرع الأول :الوقائع

في جانفي 2024 تقدمت المواطنة س.ب بشكوى إلى فرقة مكافحة الجرائم السيبرانية لدى الشرطة القضائية ، تفيد بتعرض حسابها على موقع فيسبوك للاختراق ، واستخدامه من قبل مجهول لإرسال رسائل مسيئة لأقاربها ونشر صورها الخاصة .

الفرع الثاني :الإجراءات الضبط والمعاينة في القضية

أولا : تحرير محضر* رسمي : استمعت الشرطة لأقوال الضحية وتم تحرير محضر يصف الواقعة ويبين طبيعة الأضرار المادية والمعنوية .

ثانيا : المعاينة الإلكترونية : قامت الفرقة المتخصصة في مكافحة الجرائم الالكترونية بمعاينة هاتف الضحية والحاسوب الشخصي ، وتم تفريغ محتويات الرسائل ، والولوج إلى الحساب المخترق بعد استرجاعه . وتم تتبع ال ip الذي تم من خلاله تنفيذ الاختراق .

طلب إذن قضائي ومراسلة فيسبوك : بناءا على المادة 66 من قانون الإجراءات الجزائية الجزائري [3]أصدر إذن من وكيل الجمهورية بمراسلة شركة فيسبوك لطلب تفاصيل الولوج ل ip.

ثالثا : تحديد الفاعل والضبط : توصلت التحريات إلى أن المتهم أ .ك طالب جامعي ، وهو من اخترق الحساب ، تم توقيفه بعد إذن بتفتيش مسكنه وضبط حاسوبه المحمول وهاتفه الذكي . وأظهرت المعاينة وجود برامج اختراق حسابات وتسجيل نشاطات رقمية تربط الجهاز بعملية الاختراق .

---

[1] نايري عائشة ، المرجع السابق ، ص 47 .
[2]بن دالي رانيا ، المرجع السابق ، ص 73 .
[3]انظر المادة 66 من قانون الإجراءات الجزائية الجزائري .
*انظر الملحق الثاني والثالث ،ص58-59 .

المبحث الثاني : الهيئات المختصة بالضبط والمعاينة في الجريمة الإلكترونية

أصبحت الجريمة الالكترونية تشكل تهديدا متزايدا للأفراد والمؤسسات والدول على حد سواء ،تتسم هذه الجرائم بطبيعتها العابرة للحدود وصعوبة تتبعها ، فإن ذلك يستدعي وجود هيئات متخصصة ومؤهلة للتعامل معها بفعالية ، ويرتكز مكافحة هذا النوع من الجرائم على إجراءين أساسيين هما الضبط والمعاينة واللذان يتطلبان خبرات فنية وقانونية دقيقة لضمان جمع الأدلة الرقمية بشكل سليم و قانوني ، وقد تتعدد الهيئات المختصة بالقيام بهذه المهام، وهي تتمثل في مختلف جهات القانون من شرطة وأجهزة أمنية متخصصة في مكافحة الجريمة الإلكترونية، بالإضافة إلى وحدات التحقيق الرقمي داخل النيابة العامة ،كما يتم الاستعانة بخبراء متخصصين في الأدلة الرقمية وعلم الحاسوب للمساعدة في عمليتي الضبط والمعاينة .

وسنتطرق في هذا المبحث للهيئات القضائية في المطلب الأول ، والهيئات الأمنية في المطلب الثاني ، والهيئات المتخصصة في المطلب الثالث .

المطلب الأول : الهيئات القضائية

تعد عملية الضبط والمعاينة في الجريمة الإلكترونية من أهم المراحل الإجرائية التي تتطلب مهارات خاصة وأدوات تقنية متقدمة ، نظرا لما تعرضه هذه الجرائم من طابع تقني وسرعة في التنفيذ والإخفاء ، لذا كان من الضروري أن تناط هذه المهمة بهيئات قضائية قادرة على جمع الأدلة الرقمية بشكل قانوني ومحترف ، لضمان صحة الإجراءات وعدالة المحاكمة.

الفرع الأول : النيابة العامة

تعد النيابة العامة من أهم الهيئات القضائية في منظومة العدالة الجنائية ، حيث تضطلع بدور محوري في مكافحة الجريمة ، لاسيما في ظل التطورات التقنية المتسارعة التي أفرزت أنماطا جديدة من الجرائم وعلى رأسها الجرائم الإلكترونية ، وما تنطوي عليه من تعقيد تقني وتجاوز لحدود الجغرافية ، مما فرضت تحديات جديدة أمام الجهات القضائية ، تستدعي تكييفا وظيفيا وإجرائيا من قبل النيابة العامة، التي اكتسبت اختصاصا خاصا في الضبط والمعاينة في الجريمة الإلكترونية .

هذا الاختصاص يتطلب مهارات تقنية عالية ، وفهما دقيقا لآليات ارتكاب هذه الجرائم ،سواء تعلق الأمر بانتهاك المعطيات الشخصية أو باختراق الأنظمة المعلوماتية ، في الدور الذي تقوم به النيابة العامة في هذا الإطار لا يقتصر على تحريك الدعوى العمومية ، بل يشمل أيضا الإشراف على أعمال الضبط القضائي ،وتوجيه الأبحاث ، واتخاذ الإجراءات المستعجلة لحفظ الأدلة الرقمية قبل ضياعها أو تغييرها .

للنيابة العامة عدة اختصاصات في مجال الضبط والمعاينة في الجرائم الإلكترونية ضمن إطار قانون الإجراءات الجزائية الجزائري، خاصة بعد التعديلات التي ادخلها القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 [1].

أولا : الانتقال إلى مكان الجريمة وإجراء المعاينة

بموجب المادة 36 من قانون الإجراءات الجزائية[2] ، يجوز لوكيل الجمهورية أن ينتقل بنفسه إلى مكان وقوع الجريمة لإجراء المعاينة ، وذلك في الجرائم المتلبس بها ، أو الجنح الهامة ، ويهدف ذلك إلى جمع الأدلة المادية والفنية ، مثل الأجهزة الإلكترونية ، والبيانات المخزنة ، والبرمجيات المستخدمة في ارتكاب الجريمة ، كما يجوز لوكيل الجمهورية مرافقة قاضي التحقيق للقيام بالمعاينة في الجريمة الإلكترونية حسب نص المادة 79 من قانون الإجراءات الجزائية [3].

ثانيا : التفتيش وضبط الأدلة الإلكترونية

وفقا للمادة 45 من قانون الإجراءات الجزائية [4] يمكن لوكيل الجمهورية أن بأذن بالتفتيش في الجرائم الإلكترونية ، وتشمل ذلك تفتيش الأجهزة الإلكترونية مثل : الحاسوب ، الهواتف الذكية ، البحث عن الأدلة المتعلقة بالجريمة، ويجب أن يتم التفتيش وفقا للشروط القانونية، بما في ذلك الحصول على إذن مسبق ، من السلطة القضائية المتخصصة .

بموجب المادة 37 من قانون الإجراءات الجزائية الجزائري[5] ، يتم توسيع نطاق اختصاص النيابة العامة ليشمل الجرائم الإلكترونية ، مما يتيح لوكيل الجمهورية اتخاذ الإجراءات اللازمة في أي دائرة اختصاص ، حتى وإن كانت خارج نطاق محكمته الأصلية ، وذلك في الجرائم الماسة بأنظمة المعالجة الآلية المعطيات .

---

[1] قانون الإجراءات الجزائية الجزائري المعدل والمتمم بالقانون رقم 06-222 المؤرخ في 20 ديسمبر 2006 ، صدر في العدد 23 من الجريدة الرسمية الجزائرية ، الصادر بتاريخ 06 أفريل 2022 .

[2] انظر المادة 36 من قانون الإجراءات الجزائية الجزائري .

[3] انظر المادة 79 من قانون الإجراءات الجزائية الجزائري .

[4] انظر المادة 45 من قانون الإجراءات الجزائية الجزائري .

[5] انظر المادة 37 من قانون الإجراءات الجزائية الجزائري .

ثالثا : تفتيش المنظومة المعلوماتية

يسمح لوكيل الجمهورية بتفتيش المنظومة المعلوماتية ، وهو إجراء يختلف عن التفتيش التقليدي ، من حيث الشروط الشكلية والموضوعية ، حسب نص المادة 05 من لقانون 09-04 [1]، والتي يجيز للسلطات القضائية .المختصة وكذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية ، الدخول وتفتيش المنظومة المعلوماتية جزء منها أو كلها، وكذا المعطيات المعلوماتية المخزنة فيها ولو عن بعد[2].

الفرع الثاني :قاضي التحقيق

يلعب قاضي التحقيق دورا محوريا في ضبط الأدلة الرقمية وإجراء المعاينات التقنية اللازمة ،من خلال الإشراف المباشر على إجراءات التحقيق ، كإصدار أوامر التفتيش الإلكتروني ، وحجز الأجهزة والبيانات ،وتكليف الخبراء في المجال المعلوماتي لتحليل الأدلة الرقمية ، كما يتمتع بصلاحيات مهمة في إطار القانون الجزائري ، وفقا لما نص عليه قانون الإجراءات الجزائية الجزائري ، مما يضمن التوازن بين فعالية التحقيق واحترام ضمانات المتهم وحقوقه الأساسية .

أولا : الإجراءات التي يباشرها قاضي التحقيق *في الجريمة الإلكترونية

لقد خص المشرع الجزائري قاضي التحقيق بسلطات واختصاصات واسعة في سبيل تحقيق الهدف من إسناد مهمة التحقيق إلى قاضي تحقيق مستقل عن جهة المتابعة وجهة الحكم ، وقد خولته المادة 68 قانون الإجراءات الجزائية الجزائري سلطة اتخاذ أي إجراء يراه ضروريا للكشف عن الحقيقة ، كاستجواب المتهمين ، وسماع الشهود ، والتفتيش وإجراء الخبرات والمعاينات .... وغيرها من الاختصاصات [3].

إن أعمال قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من آثار و سماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم والمتهم أو من أطراف أخرى، وهو ما قرره المشرع الجزائري في المادة 79 قانون الإجراءات الجزائية الجزائري[4] ، ويتم المعاينة في الجريمة الالكترونية المرتكبة عبر الانترنيت ، كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة

---

[1] انظر المادة 05 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

[2] انظر المادة 05 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

*قاضي التحقيق هو قاضي مكلف بإجراء تحقيقات أولية في القضايا الجنائية ، وله صلاحيات واسعة في جمع الأدلة واستجواب المتهمين واتخاذ بعض القرارات القضائية المتعلقة بالتحقيق

[3] انظر المادة 68 ، من قانون الإجراءات الجزائية الجزائري .

[4] انظر المادة 79 ، من قانون الإجراءات الجزائية الجزائري .

الإجرامية ، إلا أن الانتقال هناك لا يكون إلى العالم المادي ، وإنما إلى العالم الافتراضي أو الفضاء الإلكتروني [1] .

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة ، وحتى يستطيع قاضي التحقيق أن ينتقل إلى عالم الفضاء الالكتروني لمعاينته ، يتبع عدة طرق تتمثل في : الانتقال إلى عالم

الافتراضي من المكتب بالمحكمة من خلال الكمبيوتر الخاص به. وكذلك اللجوء إلى مقهى الانترنيت [2]. ويجوز له اللجوء أيضا إلى مقر عمل مزود خدمة الانترنيت *الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة . وكما يستطيع قاضي التحقيق أيضا الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص[3].

1-الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة الالكترونية

يجب على قاضي التحقيق قبل الانتقال إلى المعاينة مسرح الجريمة الالكترونية إتباع الخطوات التالية :

- توفير معلومات مسبقة عن مكان الجريمة ، ومالك المكان ، ونوع وعدد أجهزة الكمبيوتر.

- الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل [4].

- قطع التيار الكهربائي عن مواقع المعاينة لشل فعالية الجاني من القيام بأي فعل من شانه التأثير على أو محو آثار الجريمة .

-إعداد فريق بحث من المختصين والفنيين [5].

2- شروط صحة معاينة مسرح الجريمة

حتى تعطي المعاينة ثمارها للكشف عن الغموض ولتوصل إلى الجاني لابد أن يراعي قاضي التحقيق مايلي:

أ-سرعة الانتقال إلى مكان الجريمة

---

[1] عبد الغالي الديري ، الجرائم الالكترونية ، المركز القومي للإصدارات القانونية ، القاهرة ، مصر ، 2012 ، ص264 .
[2] خالد ممدوح إبراهيم ، المرجع السابق ، ص 156.
*مزود خدمة الانترنيت : هي شركة التي توفر لعملائها إمكانية الوصول إلى الإنترنيت
[3] خالد ممدوح ، المرجع السابق ، ص158 .
[4] العمري سلسبيل ، الحديدي هدى ، المرجع السابق ، ص 49 .
[5] نبيلة هروال ، المرجع السابق ، ص 45 .

فور تلقي قاضي التحقيق البلاغ عن وقوع الجريمة من الجرائم الالكترونية ، والتأكد من صحة الواقعة ، عليه أن ينتقل إلى مكانها ، وذلك ضمانا لعدم التغيير شكل مسرح الجريمة عن الوضع والحالة التي تركها الجاني عليه ، والحصول على شهادة الشهود [1].

ب- السيطرة على مكان وقوع الجريمة

بمجرد وصول قاضي التحقيق البلاغ عن مكان وقوع الجريمة من اجل معاينتها لابد من أن يتبع مجموعة من الإجراءات التالية :

-منع تواجد احد بتداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة التي تم العثور عليها في المسرح الجريمة الالكترونية .

- التأكد من عدم لمس أية أثار أو أدوات داخل مسرح الجريمة الالكترونية .

- التحفظ على كل ماله علاقة بالحادث من أشياء وأشخاص .

- إخطار الخبراء لرفع الآثار والبصمات [2].

ثانيا : التفتيش في الجريمة الالكترونية

خولت المواد من 79 إلى 81 من قانون الإجراءات الجزائية الجزائري [3] لقاضي التحقيق الانتقال إلى منازل المتهمين أو المشتبه فيهم أو الذين بحوزتهم أشياء لها علاقة بالجريمة لتفتيشها والحصول على الأدوات المستعملة في الجريمة [4].

وحتى يكون التفتيش الذي يقوم به قاضي التحقيق سواء بنفسه أو بواسطة إنابة ضابط الشرطة القضائية ، لابد من احترام مجموعة من القيود والشروط الآتية :

-وقوع الجريمة فعلا وان يتحصل على فائدة من وراء التفتيش من اجل كشف الحقيقة .

- أن يكون هناك اهتمام قائم ضد شخص معين من اجل القيام بعملية التفتيش .

- أن تكون الواقعة المرتكبة جناية أو جنحة .

---

[1] العمري سلسبيل ، الحديدي هدى ، المرجع السابق ،ص 50 .
[2] خالد ممدوح إبراهيم، المرجع السابق ، ص 159 .
[3] انظر المواد 79 إلى 81 من قانون الإجراءات الجزائية الجزائري.
[4] العمري سلسبيل ، المرجع السابق ، ص 51 .

- أن يكون المنزل أو المحل المراد تفتيشه معروفا ومحددا . لابد أن يتم التفتيش من قبل قاضي التحقيق ، وذلك بعد إخطار وكيل الجمهورية ، الذي يمكن مرافقته ، حيث يكون مصحوبا بكاتب التحقيق . فإذا حصل التفتيش في منزل المتهم أو مسكنه أو مسكن شخص أخر يشتبه أن يحوز أشياء لها علاقة بالجريمة ، فعلى قاضي التحقيق أن يقوم بهذه العملية بحضور المتهم أو صاحب المسكن، فان تعذر حضوره أو كان هاربا يتعين على قاضي التحقيق إحضار شاهدين لايمتان بصلة للمتهم ، وذلك طبقا لنص المادتين 80و 82 من قانون الإجراءات الجزائية الجزائري [1]من الساعة الخامسة صباحا إلى الساعة الثامنة ليلا ، وغير أن لقاضي التحقيق يجوز له في الجرائم الإلكترونية التفتيش ليلا ونهارا ن لنص المادة 47 الفقرة 04 من قانون الإجراءات الجزائية الجزائري [2].

لقد وضع المشرع الجزائري تعريفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية الجزائري [3]، حيث جاء في نصها ما يلي :" يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي ."

ويجب على المحقق إتباع الإجراءات الصحيحة والمشروعة من اجل سرعة المحافظة على أدلة الالكترونية، التي تدل على وقوع الجريمة الالكترونية كما يجب عليه :

-معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنيت والتي تتعلق بالجريمة المرتكبة .

- وصول الشكاوي والبلاغات عن الجرائم الواقعة على الحاسوب والانترنيت من الفنيين الذين يعملون على هذه الأجهزة .

-تشكيل فريق التحقيق فني ، وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش على مسرح الجريمة .

-إتباع الإجراءات الصحيحة والمشروعة من اجل سرعة المحافظة على الأدلة الالكترونية التي تدل على وقوع الجريمة ، وتخزينها في الأقراص المعدة لذلك ومنع حذفها [4] .

-البحث عن الأدوات المستخدمة في ارتكاب الجريمة ، وطرق الدخول على البرامج المخزنة ، وكيفية الحصول على الأرقام السرية والشفرات الفنية التي تمكنهم من الدخول إلى الحاسوب .

---

[1] انظر المادتين 80و82 من قانون الإجراءات الجزائية الجزائري .
[2] انظر المادة 47 الفقرة 04 من قانون الإجراءات الجزائية الجزائري .
[3] انظر المادة 68 ن من قانون الإجراءات الجزائية الجزائري .
[4] العمري سلسبيل ، المرجع السابق ، ص44 .

-وضع خطة عمل مع جميع أعضاء فريق التحقيق ، والتشاور معهم للمعرفة .

ثالثا :ضبط الدليل في مجال الجريمة الالكترونية

الضبط كقاعدة عامة لا يرد إلا على أشياء مادية ، فلا صعوبة في ذلك ، وبالتالي يضبط الدليل في الجريمة الإلكترونية على المكونات المادية للكمبيوتر ، فترفع البصمات مثلا وغيرها ، فلا صعوبة في ذلك ، وتكون الصعوبة في ضبط الوسائل لفنية أو المعنوية المستخدمة في إتلاف البرامج [1].

وقد حذا المشرع الجزائري في المادة 47 الفقرة 04 من قانون الإجراءات الجزائية الجزائري حذو التشريعات الأخرى إمكانية التفتيش والضبط على المكونات المعنوية للحاسوب بنصه على انه : " إذا تعلق الأمر بجريمة ماسة لأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو الحجز ليلا أو نهارا و في أي مكان على امتداد التراب الوطني أو بأمر ضباط الشرطة القضائية للقيام بذلك"[2].

كما نصت المادة 06 من القانون 09-04 [3]على أن حجز المعطيات المعلوماتية ، عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة مفيدة في الكشف عن الجرائم أو مرتكبيها ، وانه ليس من الضروري حجز كل المنظومة ، كما يمكن نسخ المعطيات محل البحث ، وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية ، تكون قابلة للحجز والوضع في أحراز ، وفقا للقواعد المقررة في قانون الإجراءات الجزائري ، كما يجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية .

غير انه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات ،قصد جعلها قابلة للاستغلال لأغراض التحقيق ن شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات[4].كما نصت المادة 07 من نفس القانون 09-04 على الحجز عن طريق منع الوصول إلى المعطيات ، وذلك في حالة استحالة إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه من نفس القانون ، لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي

---

[1] العمري سلسبيل ، المرجع السابق ، ص 52 .

[2] عمار حشمان ، المرجع السابق ، ص 50 .

[3] انظر المادة 06 من قانون 09- 04المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

[4] انظر المادة 06من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

تحتويها المنظومة المعلوماتية ، أو إلى نسخها ووضعها تحت تصرف الأشخاص المرخص لهم قانونا باستعمال هذه المنظومة [1].

الفرع الثالث : ضباط الشرطة القضائية

يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة ، حسب نص المادة 16 الفقرة 01 من قانون الإجراءات الجزائية الجزائري في كافة دائرة اختصاص المجلس القضائي الملحقين به في حالة الاستعجال ، وعليهم أخبار وكيل الجمهورية مسبقا [2].

أولا : القيام بالمعاينة في مسرح جرائم المساس بأنظمة المعالجة آلية للمعطيات

إذا تعلق الأمر ببحث ومعاينة جرائم محددة على سبيل الحصر بما في ذلك جرائم المساس بأنظمة

المعالجة الآلية للمعطيات نصت عليها المادة 16 الفقرة 07 من قانون الإجراءات الجزائية الجزائري [3]، ويعملون تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات المنصوص عليها في المادة 16 الفقرة 08 من قانون الإجراءات الجزائية الجزائري.

تعتبر المعاينة إجراء جائز في كافة الجرائم إلا أن غالبية التشريعات بما فيها التشريع الجزائري الذي نص في المادة 61 من قانون الإجراءات الجزائية الجزائري [4]، تقتصر على الجنايات والجنح الهامة ، حيث يعد إجراء وجوبي في الجنايات وجوازي في الجنح ، وهي قد تتم في مكان عام أو خاص ، ففي الأماكن العامة على مأمور الضبط القضائي لا يحتاج إلى إذن أو ندب صلة التحقيق بإجرائها ، أما في المكان الخاص فتكون بإذن مسبق من سلطة التحقيق ورضا صاحب المكان[5] .

1-معاينة الجرائم الواقعة على المكونات المادية للحاسوب

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي

---

[1] انظر المادة 07 الفقرة 03 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

[2] انظر المادة 16 الفقرة 01 من قانون الإجراءات الجزائية الجزائري .

[3] انظر المادة 16 الفقرة 07 من قانون الإجراءات الجزائية الجزائري .

[4] انظر المادة 61 من قانون الإجراءات الجزائية الجزائري .

[5] أمحمدي بوزينة أمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية ، مركز جيل البحث العلمي ، مؤسسة علمية خاصة ومستقلة ، كتاب ملتقى أليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، المتعقد أعمال يوم 29 مارس 2017 ، الجزائر ، ص 02 .

المحسوس ، فهي لا تثير أية مشكلة بحيث يمكن للمأمور الضبط لقضائي معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة .

2-معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطة softuare

كتلك الواقعة على برامج الحاسوب وبياناته ، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدتها .أما عن المعدات والبرامج ، فهم يستخدمون برامج تستطيع استعادة المعلومات من على الأسطونة الصلبة ، كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة ، كم يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة ومن المهم أن بتم توثيق مسرح الجريمة ، ووصفه بكامل محتوياته بشكل جيد ، مع توثيق كل دليل على حدى بما فيها الأدلة الرقمية [1]، ووضع الأختام في الأماكن التي تمت المعاينة فيها ، وضبط كل الأدوات والوسائل التي استخدمت في ارتكاب الجريمة مع وجوب إخطار النيابة العامة بذلك [2].

تقوم الشرطة القضائية بتلقي الشكاوي والبلاغات وجمع الاستدلالات ، وإجراء التحقيقات الابتدائية ، وتنفيذ الإنابات القضائية حسب نص المادة 07 من قانون الإجراءات الجزائية الجزائري[3] .

فرجال الشرطة القضائية عند سماع بوقوع الجريمة ينتقل بسرعة إلى مكان الحادث بعد التأكد من صحة المعلومة ، وذلك بعد إخطار وكيل الجمهورية من اجل اتخاذ التدابير اللازمة التي تكفل الحفاظ عليه من أن ينتدب إليه يد أي شخص ، وذلك طبقا لنص المادة 43 من قانون الإجراءات الجزائية الجزائري [4]. ليأتي بعد ذلك دور الشرطة التقنية والعلمية في معاينة ، وفحص المكان لرفع الآثار التي خلفها المجرم وفق خطة ومنهاج معين ، وتهيئة لنقلها إلى المخبر الجنائي لإجراء عليها مختلف الفحوصات من اجل الوصول والكشف عن الجريمة [5].

ثانيا : حجز معطيات المعلوماتية

أكدت المادة 06 من القانون 09-04 أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ومرتكبيها ، وأنه ليس من ضروري حجز المنظومة ،ويتم نسخ المعطيات محل البحث ، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية

---

[1] أمحمدي بوزينة أمنة ، المرجع السبق ، ص06 .

[2] شليق موسى ، نوي سمير ، **دور الشرطة العلمية في مواجهة جرائم الأنظمة المعلوماتية** ، مذكرة ماستر مهني في الحقوق تخصص قانون الإعلام الآلي ، كلية الحقوق والعلوم السياسية ، جامعة محمد البشير الإبراهيمي ، برج بوعريريج ، الجزائر ، 2022-2023 ، ص 57 .

[3] انظر المادة 07 من القانون الإجراءات الجزائية الجزائري .

[4] انظر المادة 43 من قانون الإجراءات الجزائية الجزائري .

[5] شليق موسى ، المرجع السابق ، ص 10 .

تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية الجزائري [1].

ويجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية ، التي تجري بها العملية ، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات ، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه أحكام المادة 06من نفس القانون [2] .

المطلب الثاني : الهيئات الأمنية

تعد الجريمة الالكترونية من ابرز التحديات الأمنية في العصر الرقمي ، وقد دفعت خطورتها وتشعب أساليبها الدول إلى إنشاء هيئات أمنية متخصصة تتولى مهام الضبط والمعاينة والتحقيق ، وهذه

الهيئات تمتلك كفاءات تقنية وقانونية عالية ، وتعمل بالتنسيق مع أجهزة الشرطة القضائية ، والنيابة العامة ،مؤسسات الأمن السبيراني.

وهذه الهيئات تمتلك القدرة في التعامل مع الأدلة الرقمية تختلف عن الأدلة التقليدية ، إذ تحتاج إلى أدوات وتقنيات متقدمة لحفظها ، وتحليلها واستخدامها قانونيا دون الإخلال بسريتها أو المساس بمصداقيتها ، كما تلعب دورا هاما ورئيسيا في كشف هوية الجناة ، وتتبع أنشطتهم عبر الشبكة المعلوماتية ، وتقديمهم للعدالة .

ومن بين هذه الهيئات فرق مكافحة الجرائم الإلكترونية التابعة للشرطة ، ووحدات التحريات الرقمية ، والمراكز الوطنية للأمن السبيراني، والتي تتعاون على المستوى الدولي مع منظمات مثل الأنتربول، وذلك نظرا للطابع العابر للحدود النى تتسم به الجرائم الإلكترونية ، وكذا الدرك الوطني .

الفرع الأول : وحدات الأمن الوطني

تضع المديرية العامة للأمن الوطني في إطار تجسيد سياسية أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستخدمة منها كالجرائم الالكترونية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات

[1] أمحمدي بوزينة أمنة ، المرجع السابق ،ص07 .

[2] انظر المادة 06 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة، وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[1] .

تعتبر مديرية الأمن الوطني صاحبة الاختصاص الأصلي للوقاية ، ويقودها جهاز الشرطة في الجزائر العاصمة ، تحت إشراف وزارة الداخلية ، من مهامها حفظ لأمن والنظام العام ، وحماية الأشخاص والممتلكات والتحقيق في الجرائم والقبض على الجناة ، ومراقبة الحدود ، وتقوم بإنابة مهامها لشرطة العملية والتقنية [2].

كما يكمن دور مديرية الأمن الوطني من الجانب الوقائي من خلال عقد دورات افتراضية على مستوى شبكة المعلومات عموما ، ومواقع التواصل الاجتماعي خصوصا ، كما تقوم من الجانب التحسيسي بتنظيم دروس توعوية في مختلف الأطوار الدراسية والمشاركة في الملتقيات والندوات الوطنية ...الخ [3]. أما من الناحية الردعية يكون في حالة الإخلال بالنظام العام أو في حالة منشورات تمس النظام العام كعرض أجهزة ممنوعة للبيع في مواقع الانترنيت ، فيتم اتخاذ الإجراءات القانونية المناسبة بعد تحديد هوية صاحب الحساب ، مع إعداد ملف قضائي ضده ، فالدور الردعي للمديرية الأمنية يكون متصلا بدورها الوقائي .

كما تكمن جهود الأمن الوطني في محاربة الجريمة الالكترونية وذلك بتكوين محققين مختصين فيمجال محاربة الجرائم الالكترونية ، وتكوين متداخلين أوليين في مجال الجرائم الالكترونية والتكوين القاعدي على مستوى مدارس الشرطة ، وكذا تكوين متخصصين في مجال تحليل واستغلال الأدلة الرقمية ، وخلق علاقة في مجال التكوين الخاص مع الجامعات والمؤسسات البحث لعلمي في ميدان الأمن المعلوماتي والتحقيق الجنائي الرقمي ، والمشاركة في الملتقيات والبحوث الدولية في مجال مكافحة الجريمة الالكترونية[4].

الفرع الثاني : جهاز الدرك الوطني

يعتبر جهاز الدرك الوطني قوة عمومية ذات طابع عسكري ، ويتعلق بأجهزة الأمن والأجهزة الوطنية الأخرى ، وتتمثل مهمته الأساسية في الدفاع عن الوطن وفقا للخطط المقرر من طرف وزير الدفاع

---

[1] بوديسة بجاد عبد الرؤوف ، المرجع السابق ، ص29 .
[2] حورية خليصة ، حمزة فيروز ، المرجع السابق ، ص 13 .
[3] حورية خليفة ، حزمة فيروز المرجع السابق ، ص 15 .
[4] المرجع نفسه ، ص 16 .

الوطني ، وقد حدد المرسوم الرئاسي رقم 23-313 المتضمن مهام الدرك الوطني وتنظيمه للقائمين بهذا الجهاز[1].

حيث نص جاء في المادتين 07 و08 من نفس المرسوم أن جهاز الدرك الوطني يقوم بممارسة مهام الشرطة القضائية والإدارية والشرطة العسكرية[2] .

كما يتضمن الدرك الوطني وفقا للمادة 13 من المرسوم 23-313 على أجهزة منها قيادة الدرك الوطني ، الوحدات الإقليمية ، الوحدات المتخصصة وهياكل التكوين [3].

جهاز الدرك الوطني يلعب دورا كبيرا في مكافحة الجرائم الإلكترونية ، عن طريق وضع مصالح الشرطة التابعة للدرك الوطني لمحاربة الجرائم التي ترتكب بواسطة الحاسب الآلي ، من خلال تسهيل مهمة البحث والمعاينة والتفتيش في أنظمة المعلوماتية ومراقبة شبكات الحاسب الآلي ، حسب الاختصاص ونوع الجريمة.

ويمكن تقسيمها إلى ثلاث مستويات وهي: مستوى مركزي فتحمل المؤسسة الدرك الوطني على مواجهة والتصدي للجرائم الإلكترونية بإنشاء هيئات خاصة تعمل على ذلك .

أما المستوى الجهوي تقوم المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بتنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية ، ودعمها بالوسائل اللازمة والخاصة بالتحريات والأبحاث المعقدة .

أما مستوى المحلي تقوم المصالح المكلفة بمكافحة الجرائم الخطيرة ومنها الجرائم الالكترونية بتحقيقات تتطلب تحريات معقدة ، فهي تقوم بتدعيم نشاط الأبحاث والتحريات التي تقوم بها فرق الدرك الوطني [4].

---

[1] المرسوم الرئاسي رقم 23-313 الصادر في 03 سبتمبر 2023 معدل والمتمم بالمرسوم الرئاسي رقم 09-143 المؤرخ في 27 أفريل 2009 المتعلق بمهم وتنظيم الدرك الوطني الجزائري ، العدد 59 ، من الجريدة الرسمية الصادرة 10 سبتمبر 2023 .

[2] انظر المادتين 07 و08 من المرسوم 23-313 .

[3] انظر المادة 13 من المرسوم 23-313 .

[4] حسن ربيعة ، رحاب شادية ، **آليات البحث والتحري في الجرائم المعلوماتية** ، أطروحة شهادة الدكتوراه ، تخصص قانون العقوبات والعلوم الجنائي ، كلية الحقوق والعلوم السياسية ، جامعة باتنة ، الجزائر ، 2015-2016 ، ص183-184-185-186 .

المطلب الثالث : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مقدم الخدمات

مع التطور المتسارع لتكنولوجيا الإعلام والاتصال ، برزت أنواع جديدة من الجرائم التي تستغل الفضاء الرقمي لارتكاب أفعال تمس بالأمن والمصالح العامة والخاصة ، والتي أصبحت تعرف بالجرائم الالكترونية ، ومواجهة هذا التحدي ، أنشأت العديد من الدول هيئات متخصصة تعني مكافحة هذا النوع من الجرائم من بينها الهيئة الوطنية الوقاية من الجرائم العامة بتكنولوجيا الإعلام والاتصال .

وتعد هذه الهيئة جهازا وطنيا مختصا يهدف إلى التصدي لظاهرة الجريمة الإلكترونية من خلال الوقاية ، والرصد والتحليل ، والمساهمة في التحقيق والمعاينة التقنية للجرائم المرتكبة عبر الوسائل الرقمية ، وتكمن أهميتها في قدرتها على مواكبة التطورات التكنولوجية ،مما يجعلها فاعلة في تقديم الدعم الفني والتقني للجهات القضائية والأمنية المختصة.

تلعب الهيئة الوطنية دورا محوريا في الضبط والمعاينة من خلال استخدام أدوات رقمية وتقنيات متطورة ، تمكنها من تتبع اثر الجريمة الالكترونية ، جمع لأدلة الرقمية ، وتحليل محتوى الوسائط الالكترونية وفقا لمعايير دقيقة تضمن سلامة الإجراءات القضائية .

كما تساهم في إعداد التقارير الفنية اللازمة لتوثيق الجرائم الرقمية ، والتعاون مع الهيئات الدولية المختصة ، ما يعزز من فاعلية منظومة العدالة في هذا المجال .

وتتجلى أهمية الهيئة في تعزيز الأمن السيبراني الوطني ، ورفع مستوى الوعي بمخاطر الجريمة الالكترونية ، والمساهمة في تطوير الإطار القانوني و التنظيمي المتعلق بهذا النوع من الجرائم .

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال

نصت المادة 14 من قانون09-04 على تولي الهيئة المذكورة في المادة 13 من نفس القانون بالمهام الآتية :

أولا : تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

ثانيا : مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك ، تجميع المعلومات ، وانجاز الخبرات القضائية .

ثالثا : تبادل المعلومات مع نظيراتها ف الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، وتحديد مكان تواجدهم [1].

رابعا : ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة [2].

خامسا : تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية ، وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية[3] .

سادسا : السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية ، وتطوير تبادل المعلومات والتعاون عل المستوى الدولي في مجال اختصاصها .

سابعا : تطوير التعاون مع المؤسسات والهيئات الوطنية المعينة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال .

ثامنا : المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال .

تاسعا: المساهمة في تعين المعايير القانونية في مجال اختصاص الهيئة [4].

الفرع الثاني : مقدم خدمات الانترنيت

عرف لمشرع الجزائري مقدم الخدمات في القانون رقم 09-04 بأنه أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات ، كما عرفه بأنه أي كيان يقوم بمعالجة أو تخزين معطيات معلوماتية لقائدة خدمات الاتصال ومستعمليها . ألقى المشرع الجزائري على عاتق مزودي خدمات الانترنيت عدة التزامات ، وذلك بموجب المرسوم التنفيذي رقم 98-257 والمتعلق بضبط شروط وكيفيات إقامة خدمات الانترنيت واستغلالها[5]، وكذا القانون رقم 09-04

---

[1] انظر المادة 14 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

[2] العمري سلسبيل ، الحديدي هدى ، المرجع السابق ، ص 17 .

[3] المرجع نفسه ، ص 17 .

[4] انظر المواد 02 و03 من المرسوم الرئاسي رقم 15-216 المؤرخ في 08 أكتوبر 2015 ، يحدد تشيكلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، الجريدة الرسمية الجمهورية الجزائرية ، العدد 53 ، 08 أكتوبر 2015 ، ص 16-17 .

[5] المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 المتضمن ضبط شروط وكيفيات إقامة خدمات الانترنيت واستغلالها ، الجريدة الرسمية ، العدد 63 ، المؤرخة في 26 أوت 1998 ص 05 .

أولا:الالتزام بمساعدة السلطات العامة

يتعين على مقدم الخدمات كتمان سرية العمليات التي يتجوزها بطلب من المحققين ، وكذلك المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق .

ثانيا:الالتزام بحفظ المعطيات المتعلقة بحركة السير

اوجب القانون على مقدمي الخدمات التزامات خاصة منصوص عليها في المادة 12 من القانون09-04 وهي واجب التداخل فورا لحسب المعطيات أو المحتويات المخالفة للقانون و تخزينها أو منع الدخول إليها باستعمال وسائل تقنية تحول دون الدخول إليها .

وضع الترتيبات التقنية التي بموجبها يتم حصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وان يخبروا المشتركين لديهم بوجودها [1].

ثالثا:الالتزام بالسرية والشفافية

ألزم المشرع مقدمي الانترنيت وحفاظا على الحياة الخاصة لمشتركيه ، بالمحافظة على سرية كل المعلومات المتعلقة بمشتركي خدمات الانترنيت وعدم الإدلاء بها إلا في الحالات المنصوص عليها قانونا ،إذا يلتزم مقدم الخدمة بالحفاظ على معطيات مشتركيه تحت طائلة العقوبات المتعلقة بإفشاء الأسرار المنصوص عليها في قانون العقوبات [2] .

كما فرض عليهم التزام أخلاقي متمثل في احترام قاعد حسن السيرة بالامتناع خاصة عن استعمال أي طريقة غير مشروعة سواء اتجاه المستعملين أو اتجاه مقدمي خدمات الإنترنيت .

---

[1] عبد الفتاح محمود الكيلاني ، **مدى المسؤولية القانونية لمقدمي خدمات الانترنيت** ،مقال منشورة على شبكة الإنترنيت على الرابط التالي :www.flaw.bu.edu.eg/flaw/images/pat2.pdf,22 ماي 2025 ، 16:54 .

[2] انظر المادة 14 من المرسوم التنفيذي رقم 98-257 ، المرجع السابق ، ص 08 .

خلاصة الفصل الثاني :

من خلال هذا الفصل الذي تطرقنا فيه إلى الأساليب الفنية لضبط والمعاينة في الجريمة الالكترونية ، والتي تتطلب إجراءات خاصة تختلف عن الجريمة التقليدية ، نظرا لطبيعة الأدلة الرقمية ، ومن أهم الأساليب الفنية المستخدمة جمع الأدلة الرقمية من ملفات ورسائل وما تحتويه الأجهزة من معلومات وبيانات قبل تحللها ، ونسخ البيانات وذلك أجل حمايتها من التلف أثناء التحقيق ، ومن ثم تحليل الأدلة الرقمية وذلك باستخدام برامج متخصصة للاسترجاع وتحليل الملفات المحذوفة أو المشفرة .

وكذا تتبع الشبكات والاتصالات أي تتبع عناوين البريد الالكتروني ونشاط الانترنيت، وتحليل سجلات والمحادثات عبر التطبيقات، وكذلك تامين مسرح الجريمة الرقمية من خلال فصل الأجهزة عن الانترنيت، وتجميد أي نشاط الكتروني قد يغير أو يمسح الأدلة، واستخدام أدوات وتقنيات جنائية متقدمة من اجل فحص الأجهزة المحمولة ومختلف الحواسيب .

أما في ما يخص الهيئات المختصة بالضبط والمعاينة في الجريمة الالكترونية فيها تتمثل في وحدات مكافحة الجريمة الالكترونية الشرطة والدرك الوطني ، وهي الجهة الأساسية لجمع وتحليل الأدلة الرقمية ، وكذا خبراء في امن المعلومات والتحقيق الجنائي الرقمي ، والنيابة العامة التي تقوم بإصدار الأوامر القضائية بالضبط والتفتيش الرقمي ، والهيئات القضائية التي تقوم بالمعاينة المتمثلة في قاضي التحقيق والهيئة الوطنية للأمن السيبراني التي تضع السياسات العامة لحماية القضاء السبيراني ، والتعاون مع الأجهزة الأمنية لضبط الجرائم الالكترونية ، بالإضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومقدم الخدمات المذكورين في القانون 09-04([1]) .

([1]) انظر المادة 12 والمادة 14 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها .

.

الخاتمة

الخاتمة :

في الأخير عالجنا الموضوع من خلال فصلين تطرقنا في الفصل الأول إلى الضبط والمعاينة كوسائل لجمع الأدلة الرقمية في الجريمة الإلكترونية ،أما في الفصل الثاني تطرقنا إلى الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية وكذا الهيئات المختصة بالضبط والمعاينة في الجريمة الإلكترونية.

نستنتج أن إجراءات الضبط والمعاينة في الجريمة الإلكترونية تواجه تحديات جوهرية تتعلق بطبيعة هذه الجريمة نفسها ، التي تتسم بالسرعة والديناميكية، وامتدادها العابر للحدود، فعلى الرغم من الجهود التشريعية والإجرائية المبذولة لتكييف آليات الضبط والمعاينة التقليدية مع البيئة الرقمية ،إلا أن فعالية هذه الإجراءات مازالت رهينة لعدة عوامل من أبرزها التطور التقني المتسارع وافتقار بعض الأنظمة القانونية إلى نصوص واضحة تواكب هذا التطور بالإضافة إلى ضعف التنسيق الدولي ، وفعاليتها تظل نسبية تستدعي مراجعة مستمرة ودقيقة توازن بين حماية الحقوق والحريات من جهة وضمان فعالية العدالة الجنائية من جهة أخرى ، من الضروري العمل على تطوير أدوات رقمية حديثة للضبط والمعاينة وتوفير التكوين المتخصص لرجال الضبط القضائي وتعزيز التعاون القضائي والأمني الدولي في مجال مكافحة الجريمة الإلكترونية.

من خلال هذه الدراسة توصلنا للنتائج التالية :

1-خصوصية الجريمة الإلكترونية التي تختلف عن الجرائم التقليدية من حيث الوسائل والمكان والزمان ما يجعل إجراءات الضبط والمعاينة أكثر تعقيدا وصعوبة .

2-أهمية ضبط الأدلة الرقمية في الجريمة الإلكترونية ، والتي غالبا ما تكون بيانات ، ملفات ، سجلات إلكترونية ، وهي سهلة التلاعب أو الإتلاف إن لم يتم التعامل معها بشكل تقني دقيق وسريع .

3- عدم مواكبة التشريعات التقليدية والتي لا تزال غير محدثة ، بشكل كاف لمواكبة تطورات الجريمة الإلكترونية ، مما يخلق نظرات قانونية قد تعيق فعالية الضبط والمعاينة .

4-أهمية التكوين والتخصص لأعوان الضبط القضائي الذين يواجهون تحديات تقنية كبيرة أثناء التعامل مع الجرائم الإلكترونية ، ما يستدعي تأهيلهم وتدريبهم على أحدث الوسائل والبرمجيات المتعلقة بالتحقيق الرقمي .

5- الحاجة إلى تعاون الدولي نظرا للطبيعة العابرة للحدود للجريمة الإلكترونية ، فإن التعاون الدولي بين الدول أصبح ضروريا لتبادل المعلومات والمساعدة القانونية المتبادلة .

6- يجب أن تتم إجراءات الضبط والمعاينة وفقا لضوابط قانونية تحترم حقوق الأفراد ، خصوصا الحق في الخصوصية وعدم التعسف في استعمال السلطة .

7- أهمية السرعة في المعاينة ،أي أن كل تأخير في إجراءات المعاينة والضبط قد يؤدي إلى فقدان الأدلة وهو ما يتطلب تفعيل آليات التدخل العاجل عند وقوع الجرائم الإلكترونية .

8- عدم تطرق المشرع الجزائري لتعريف المعاينة .

من خلال هذه النتائج توصلنا إلى الاقتراحات الآتية :

1- تكوين أعوان الضبط القضائي من خلال توفير برامج تدريبية متخصصة لأعوان الضبط القضائي والقضاة في مجال الجرائم الإلكترونية والتحقيقات الرقمية ، لضمان التعامل المهني والسليم مع الأدلة الإلكترونية .

2- إنشاء وحدات متخصصة ، لتعزيز و توسيع نطاق الفرق والوحدات المختصة بمكافحة الجريمة الإلكترونية ضمن أجهزة الأمن ، وتجهيزها بأحدث الوسائل التقنية .

3- وضع آلية قانونية لضبط الأدلة الرقمية ، وذلك باعتماد بروتوكلات تقنية وقانونية دقيقة لضبط الأدلة الرقمية ومعاينتها ، بما يضمن الحفاظ على سلامتها القانونية وقابليتها للاستخدام القضائي .

4- تعزيز التعاون الدولي والقضائي والأمني من خلال الاتفاقيات الثنائية والمتعددة الأطراف ، لتسهيل تبادل المعلومات وملاحقة مرتكبي الجرائم الإلكترونية عبر الحدود .

5- تنظيم حملات التحسيس والتوعية للمواطنين حول مخاطر الجريمة الإلكترونية وطرق الوقاية منها, بما يساهم في تقليل نسبة وقوعها وتسهيل التبليغ عنها .

6- ضمان التوازن بين الفعالية والحقوق وذلك من خلال الحرص على أن تكون إجراءات الضبط والمعاينة في إطار احترام الحريات والحقوق الدستورية ، وخاصة الحق في الخصوصية الرقمية وسرية الاتصالات .

قائمة الملاحق

قائمة الملاحق :

الملحق الأول :إحصائيات الجرائم الإلكترونية لسنة 2024

أنواع الجرائم	عدد القضايا
جريمة الدخول والبقاء عن طريق الغش	22 قضية
جريمة القذف	46 قضية
جريمة مخالفة السب	11 قضية
جريمة مخالفة التهديد	04قضايا
جريمة التهديد والابتزاز	07قضايا
جريمة انتحال صفة	02قضايا
جريمة المساس بالحياة الخاصة	15 قضية
جريمة نشر صور مخلة بالحياء	قضية واحدة
جريمة تحريض القصر على الفسق والدعارة	قضية واحدة
جريمة إعادة نشر مناشير تحريضية تشير بالإرهاب	قضية واحدة
جريمة النصب	87 قضية
جريمة تحريض على الكراهية بين المواطنين والسكان	05 قضايا
جريمة نشر محتوى عبر النظام العام	08قضايا
حالات أخرى	30قضية
مجموع القضايا	**241 قضية**

الملحق الثاني : محضر تفتيش تقني حول قضية المساس بحرمة الحياة الخاصة عن طريق منظومة معلوماتية

محضر تفتيش وحجز إلكتروني

-/ **انه في يوم**: الإثنين الموافق للثاني عشر من شهر جانفي----------

قضية : -/ **من سنة**: ألفين وخمسة عشر(2015).-------/**الساعة**: الثامنة صباحا. ----------
-/ **نحن**: ملازم أول للشرطة ----------، بمديرية الشرطة القضائية. ----------
-/ **ضابط الشرطة القضائية** بدائرة الاختصاص بمساعدة..... بفرقة مكافحة الجرائم المعلوماتية ----------
-/في إطار التحقيق المفتوح في قضية المساس بحرمة الحياة الخاصة التي راحت ضحيتها المدعوة/ .....
-/بناءا على نص المادة 05 من قانون رقم 04/09/ المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال، وبناءا على الأمر بتمديد الاختصاص والإذن بالتفتيش المنظومة المعلوماتية الحاملين للرقم 14/000615 بتاريخ 2015/01/05 الصادرين عن السيد/ وكيل الجمهورية لدى محكمة الحراش، الناص على تمديد الاختصاص إلى محكمة عين تموشنت، المؤشر عليه من طرف السيد/ وكيل الجمهورية لدى نفس المحكمة بتاريخ 2015/01/07، و الإذن بالتفتيش الناص على تفتيش مسكن المدعوة/ ف ق، نقول أننا بتاريخ 2015/01/07 انتقلنا إلى مقر السكن موضوع الإذن بالتفتيش الكائن..... العملية التي كانت إيجابية و تم من خلالها حجز الوحدة المركزية لجهاز الإعلام الآلي التي تحمل علامة Emachines، ملك المشتبه فيه المدعو/ .....----------

الموضوع:

-/ أنه بتاريخ اليوم و الساعة المشار إليهما أعلاه إجراء عملية معاينة و تفتيش إلكتروني.
-/ يتبين من خلال فحص الجهاز أن المشتبه به قام بحذف نظام التشغيل السابق وتثبيت نضام WINDOWS 7 جديد بتاريخ 2014/11/18 (صورة01)----------

صورة خاصة بالضحية

صورة01

-/في الوهلة الأولى قمنا بمعاينة متصفح الأنترنات « Google Chrome » المثبت على جهاز الكمبيوتر الخاص بالمشتبه فيه، أين عثرنا على عنوان البريد الإلكتروني «----------» (صورة02)، المستعمل في إنشاء حساب الفيسبوك « -----Ka » الذي قام من خلاله بالاتصال بالضحية بعد قرصنة جهازها، مع العلم أنه قام بتغيير إسم حسابه من إسم « ----- إلى « o----- »
-/عملية تفتيش الأقراص الصلبة بينت أن عملية الولوج إليها محمية بكلمة سر ----------
/ تفتيش القرص الصلب C لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق، كما أنه لا يوجد أي برنامج يستعمل في القرصنة مثبت على الجهاز بعد تاريخ حذف نظام تشغيل الجهاز المذكور أعلاه----------
-/ تفتيش القرص الصلب D لم يسفر عن أي نتيجة تتعلق بالقضية محل التحقيق مع وجود بعض البرامج التي قد تستعمل في عمليات القرصنة----------
-/تفتيش القرص الصلب الأخير E بين مايلي:----------
-/ وجود ملف باسم Nouveau document texte(2).txt يحوي ثلاثة (3) روابط على موقع www.golfup.com حيث قام المشتبه فيه بوضع الفيروس يقوم الضحايا بتحميله على أساس أنه ملف أخر (صورة03) ----------

الملحق الثالث: محضر معاينة إلكترونية

الملحق رقم 03

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة الداخلية، الجماعات المحلية
والتهيئة العمرانية
المديرية العامة للأمن الوطني
أمـــن ولايـــة غرداييـــــة.
رقم: .....

محضـــر معايـنة إلـكترونية

قضية ضد :

--/ إنه في : يوم الجمعة الموافق للحادي عشر من شهر جوان ----------
---/ **سنة :** الفين و سبعة عشر ----------
--------/**الساعة:** العاشرة صباحا. ----------
-----/ **نحن :** ..... ملازم أول للشرطة ، ضابط الشرطة القضائية ، رئيس فرقة مكافحة الجرائم المعلوماتية ، بالمصلحة الولائية للشرطة القضائية بامن ولاية غرداية ----------/ضابط الشرطة القضائية بدائرة :الاختصاص و المقيم بها----------
--/ استمرارا في التحقيق المفتوح في شكوى ..... بخصوص قضية السب و الشتم عبر وسائط إلكترونية و المساس بحرمة الحياة الخاصة للأشخاص و قرصنة حسابها عبر مواقع التواصل الاجتماعي – فيس بوك ،و بعد تقدم الشاكية لمصالحنا .----------
--/ لما سبق ذكره قمنا بمكتبنا وباستعمال وسائل المصلحة وبحضور و موافقة صاحبة الحساب / ..... بالولوج إلى حسابها بموقع الفايسبوك الحامل للرقم IP.....

الموضوع: محضر معاينة إلكترونية

--/ المعاينة جـــــــاءت نتائجها إيجابية مثلما هو مبين في الصور أسفل هذا:----------
----

--/ دامت المعاينة حوالي نصف الساعة، وأغلق المحضر في حدود الساعة 09:30 صباحا من نفس اليوم .----------
--/ حرر هذا المحضر إثباتا للعملية والذي نمضيه في اليوم والساعة المذكورين أعلاه.----------

التكييف:

ضابط الشرطة القضائية

قائمة المصادر والمراجع

قائمة المصادر والمراجع :

أولا : المصادر

- القوانين

1-المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 ، المتضمن ضبط شروط وكيفية إقامة خدمات الإنترنيت واستغلالها ، الجريدة الرسمية ،العدد 63 ، المؤرخ في 26 أوت 1998 .

2- قانون الإجراءات الجزائية الصادر بموجب الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 ، المعدل والمتمم .

3- القانون 09-04 المؤرخ في5أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلامم والاتصال ومكافحتها ، الجريدة الرسمية ، العدد 47 ، المؤرخ في 16 أوت 2009 .

4- المرسوم رقم 15-215 المؤرخ في 8 أكتوبر 2015 ، يحدد تشكيل وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، الجريدة الرسمية ، العدد 53 ، الصادر في 8أكتوبر 2015 .

5- المرسوم الرئاسي رقم 23-313 الصادر في 3 سبتمبر 2023 المعدل والمتمم بالمرسوم الرئاسي رقم 09- 143 المؤرخ في 27 أبريل 2009 المتعلق بمهام وتنظيم الدرك الوطني ، الجريدة الرسمية ، عدد 59 الصادر في 10 سبتمبر 2023 .

ثانيا : المراجع

أ- المعاجم

1-أحمد بن فارس بن زكريا بن محمد بن حبيب الرازي ، معجم مقاييس اللغة ، الجزء الأول ، دار الفكر للطباعة والنشر والتوزيع ،1997 .

2-إسماعيل بن حماد الجوهري الفراني ،تاج اللغة وصحاح العربية ، الجزء الثالث ، الطبعة الرابعة ، دار العلم للملايين ، بيروت ن لبنان ،1990 .

3-إبراهيم أنيس , عبد الحليم منصور ، عطية الصولحي ، محمد خلف الله أحمد ، معجم الوسيط ، الطبعة الرابعة ، مكتبة الشروق الدولية ، دون بلد النشر ، 2004 .

4- أبو الفضل جمال الدين محمد بن محمد بن مكرم بن منصور ، لسان العرب ن الجزء السابع ، طبعة جديدة ، دار المعارف ، القاهرة ، مصر ، بدون سنة .

5- أبو الفضل جمال الدين محمد بن مكرم بن منصور , لسان العرب ،المجلد 13 ، بدون رقم الطبعة ،دار الصادر ، بيروت ، لبنان ، دون سنة .

ب- الكتب

1-محمد الأمين البشري ، التحقيق في الجرائم المستحدثة ، الطبعة الأولى ،أكاديمية نايف للعلوم لأمنية ، الرياض ، السعودية ، 2004 .

2- عبد الفتاح بيومي الحجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت ، الطبعة الأولى ن دار الفكر الجامعي ، الإسكندرية ، مصر ،2006 .

3- محمد حماد مرهج الهيتي ، جرائم الحاسوب ، الطبعة الأولى دار المناهج ، عمان ، الأردن ،2006 .

4- نهلة عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2008 .

5- مصطفى محمد موسى ، التحقيق في الجرائم الإلكترونية ، الطبعة الأولى مطابع الشرطة ، القاهرة ، مصر ، 2008.

6- علي جبار الحسناوي ، جرائم الحاسوب والإنترنيت ، الطبعة الأولى ، دار اليازوري االعلمية للنشر والتوزيع ، عمان ، الأردن,2009 .

7- أمير فرج ، الجرائم المعلوماتية على شبكة الإنترنيت ، بدون رقم طبعة ، دار المطبوعات الجامعية، الإسكندرية , مصر, 2009 .

8- خالد عباد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنيت ، الطبعة الاولى ، دار الثقافة للنشر والتوزيع ، عمان , الأردن ،2011 .

9- خيرت علي محرز, التحقيق في جرائم الحاسوب الآلي ، بدون رقم طبعة ، دار الكتاب الحديث , القاهرة ,مصر ، 2012 .

10- عبد الغالي الديربي ، الجرائم الإلكترونية ، بدون رقم طبعة ، المركز القومي للإصدارات القانونية ، مصر ، 2012 .

11- حسام نبيل الشنراقي ، الجرائم المعلوماتية ، دارسة تطبيقية على جرائم الإعتداء على التوقيع الإلكتروني ، بدون رقم طبعة ، دار الشتات للنشر والبرمجيات ، مصر , 2013 .

12- أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الإلكترونية ، بدون رقم طبعة ، دار الجامعة الجديدة للنشر ، الإسكندرية ، مصر ن 2015 .

13- خالد ممدوح إبراهيم ، سلطات النيابة العامة في الجرائم الإلكترونية ,دار الفكر الجامعي ، الإسكندرية ، مصر , 2021 .

ت-الرسائل الجامعية

1-غاري عبد الرحمان ، هيان الرشيد ، الحماية القانونية من الجرائم المعلوماتية , أطروحة لنيل شهادة دكتوراه في القانون ، كلية الحقوق ، الجامعة الإسلامية ، لبنان ، 2004 .

2- ابتسام بغو ، إجراءات المتابعة الجزائية في الجريمة المعلوماتية ، مذكرة ماستر ، تخصص قانون جنائي للأعمال ، كلية الحقوق ، جامعة العربي بن مهيدي ، أم البواقي , الجزائر ، 2005 .

3- نبيلة هبة هروال , الجوانب الإجرائية لجرائم الإنترنيت ، مذكرة الماستر ، كلية الحقوق , جامعة الإسكندرية ، مصر, 2006 .

4- فاطمة الزهراء بخي ، إجراءات التحقيق في الجريمة الإلكترونية ، مذكرة ماستر ، تخصص جنائي ، كلية الحقوق ، جامعة محمد بوضياف ، المسيلة , الجزائر , 2013-2014 .

5- حسن ربيعة ، رحاب شادية ، آليات البحث والتحري في الجرائم المعلوماتية ، أطروحة دكتوراه ، تخصص قانون العقوبات والعلوم الجنائية ، كلية الحقوق والعلوم السياسية ، جامعة باتنة ،الجزائر ، 2015-2016 .

6- نور الهدى زيبحة ، الإثبات الجنائي في الجرائم الإلكترونية ، مذكرة ماستر ، تخصص قانون الأعمال ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن المهيدي ، أم البواقي ، الجزائر ، 2015-2016 .

7- سعيدة بعرة ، الجريمة الإلكترونية في التشريع الجزائري ، مذكرة الماستر في الحقوق ، تخصص القانون الجنائي ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، الجزائر ، 2015-2016 .

8- نايري عائشة ، الجريمة الإلكترونية في التشريع الجزائري ، مذكرة ماستر في القانون الإداري ، كلية الحقوق والعلوم والسياسية ، جامعة أحمد دارية ، أدرار ، الجزائر ، 2016-2017 .

9- عادل حماد عثمان ، ضبط الأدلة في مجال الجريمة المعلوماتية ، كلية الحقوق ، جامعة دار العلوم ،الرياض ،السعودية ، 2018 .

10- لامية وعلي ، كهينة سعودي ، إجراءات مكافحة الجريمة الإلكترونية ، مذكرة ماستر ، تخصص قانون جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية ، جامعة عبد الرحمان ميرة ، بجاية ،الجزائر ، 2018-2019 .

11- محمد رزيق ، إجراءات المعاينة ن التفتيش والحجز داخل المنظومة المعلوماتية ، مذكرة ماستر قانون عام ، تخصص قانون جنائي وعلوم جنائية ، كلية الحقوق والعلوم السياسية ، جامعة أكلي محند ، البويرة ، الجزائر ، 2018-2019 .

12- عمار حشمان ، الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر مهني ، كلية الحقوق والعلوم لإقتصادية والتجارية وعلم التسيير , جامعة قاصدي مرباح ، ورقلة, الجزائر ، 2018-2019 .

13- لطيفة خلفي ، سارة اليزيد ,سناء لمخوص , عثمان سفياني , المعاينة في الجرائم الإلكترونية , مذكرة ماستر كلية العلوم القانونية والاقتصادية والاجتماعية ، جامعة محمد الخامس ن الرباط ، المغرب ، 2018-2019 .

14- خالد أمين بن نعوم ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، تخصص القانون القضائي ، كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم، الجزائر ، 2018-2019 .

15- ابتسام بومايلة ، مناهج التحقيق الجنائي في الالجرائم الإلكترونية ، مذكرة ماستر في الحقوق , تخصص القانون الجنائي والعلوم الجنائية ، كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، ورقلة ، الجزائر ، 2020-2021 .

16- عدلي دحمان ن سعد الدين ثامر ن التحقيق الجنائي في الجرائم الإلكترونية ن مذكرة ماستر في القانون الخاص ، كلية العلوم القانونية والإقتصادية والإجتماعية , جامعة زيان عاشور ، الجزائر ، 2021-2022.

17- مصطفى السالمي ، محاضر الضبطية ودورها في إثبات الجرائم المعلوماتية ، مذكرة ماستر في القانون الخاص ، كلية العلوم القانونية والاقتصادية والاجتماعية ، جامعة سيدي محمد بن عبد الله ، فاس , المغرب ، 2021-2022.

18- بوديسة بجاد عبد الرؤوف ، آليات التحري عن الجريمة الإلكترونية في الجزائري ، مذكرة ماستر ، تخصص قانون الإعلام الآلي والإنترنيت ، كلية الحقوق والعلوم السياسية ، جامعة محمد البشير الإبراهيمي ، برج بوعريريج ، الجزائر ، 2021-2022 .

19- مباركة رابح ، إجراءات التحري والتحقيق في الجريمة الإلكترونية ، مذكرة ماستر في قانون لإعلام الآلي والإنترنيت ، كلية الحقوق والعلوم السياسية ،جامعة محمد البشير الإبراهيمي ، الجزائر ،2021-2022 .

20- العمري سلسبيل ، الحديدي هدى ، خصوصية التحقيق الجنائي في الجرائم الإلكترونية ، مذكرة ماستر في قانون الأعمال ، كلية الحقوق والعلوم السياسية ، جامعة محمد البشير الإبراهيمي , الجزائر ، 2021-2022 .

21- شليق موسى ، نوى سمير ، دور الشرطة في مواجهة جرائم الأنظمة المعلوماتية ، مذكرة ماستر مهني في الحقوق ، تخصص قانون الإعلام اللي ، كلية الحقوق والعلوم السياسية , جامعة البشير الإبراهيمي ، برج بوعريريج ، الجزائر ، 2022-2023 .

22- بن داني رانيا , الجريمة الإلكترونية في التشريع الجزائري ، مذكرة ماستر في القانون العام ن كلية الحقوق والعلوم السياسية ، جامعة عبد الحميد بن باديس، مستغانم ،الجزائر ، 2022-2023 .

23- حورية خليصة ، حمزة فيروز ، خصوصية التحقيق في الجريمة المعلوماتية ، مذكرة ماستر في الحقوق ، تخصص قانون جنائي وعلوم جنائية , كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي ، أم البواقي ، الجزائر ، 2023-2024 .

ث- المجلات

1-سحنون نادية ، التنظيم القانوني للجريمة المعلوماتية وأدلة الإثبات ، المجلد 1 ، العدد 1 ، المجلة الجزائرية للحقوق والعلوم السياسية ، سوق أهراس ، الجزائر ، 2009 .

2- عبد القادر فلاح , نادية عبد المالك , التحقيق الجنائي في الجرائم الإلكترونية وإثباتها في التشريع الجزائري ، المجلد 4 ، العدد 2 ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، 2019 .

3- سمية قلات ، عبد العالي حاحة ، مقتضيات المعاينة المعلوماتية في التشريع الجزائري ، المجلد 11 ، العدد 1 ، مجلة الحقوق والحريات , جامعة عبد الحميد بن باديس ، مستغانم ، الجزائر ، 2023 .

ج- الدراسات القانونية والأبحاث

1-عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن ، دار الجامعة الجديدة ، الإسكندرية ، مصر ،2010.

2- ناصر جوادي ، إجراءات التحري الخاصة في ظل قانون الإجراءات الجزائية ، الجزائر ، 2011 .

3- عبد القادر عدو ، الجريمة الإلكترونية إجرائيا ، دار هومة، الجزائر ، 2016 .

4- أمحمدي بوزينة أمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية ، ملتقى أعمال آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد يوم 29 مارس 2017 ، الجزائر ،2017.

5- رشيدة كابوية ، حجية الدليل الرقمي في الإثبات الجنائي ، مداخلة للمشاركة في فعاليات الملتقى الدولي حول أدلة الإثبات الجنائية في التشريعات المقارنة المنعقد ليومي 25-26 ابريل 2018 ، كلية الحقوق والعلوم السياسية ، جامعة طاهري محمد ، بشار ، الجزائر ، 2018 .

6- عبد الفتاح محمود الكيلاني ، مدى المسؤولية القانوية لمقدمي خدمة الإنترنيت ،الموقع www.flaw-bu-edu.eg

فهرس المحتويات

فهرس المحتويات:

الإهداء ..... ت
شكر وعرفان ..... ج
مقدمة.....1

الفصل الأول:

الضبط والمعاينة كوسائل لجمع الأدلة الرقمية في الجريمة الإلكترونية.....5
المبحث الأول :تحديد مفهوم الضبط في الجريمة الإلكترونية 6
المطلب الأول: مفهوم الضبط في الجريمة الإلكترونية 6
الفرع الأول: تعريف الضبط في الجريمة الإلكترونية.....6
أولا : التعريف اللغوي للضبط.....6
ثانيا : التعرف الاصطلاحي لضبط.....7
ثالثا :التعريف القانوني للضبط 8
الفرع الثاني :الطبيعة القانونية للضبط في الجريمة الإلكترونية 8
الفرع الثالث : محل أو نطاق الضبط في الجريمة الإلكترونية.....9
أولا : ضبط الكيانات المادية 9
ثانيا :ضبط الكيانات المعنوية.....11
المطلب الثاني : شروط الضبط في الجريمة الإلكترونية والصعوبات المرتبطة بها.....11
الفرع الأول :شروط الضبط في الجريمة الإلكترونية 12
أولا :إجراء الإذن.....12
ثانيا :إجراء التفتيش والحجز بحضور أشخاص معينين قانونا.....12
ثالثا :مواعيد التفتيش والحجز.....13
رابعا : رضا المشتبه فيه بالتفتيش والحجز 13
خامسا : تحرير محاضر التفتيش والحجز 14
الفرع الثاني :الصعوبات المرتبطة بالضبط في الجريمة الإلكترونية 15
المبحث الثاني : المقصود بالمعاينة في الجريمة الإلكترونية 15
المطلب الأول: مفهوم المعاينة في الجريمة الإلكترونية 15
الفرع الأول :تعريف المعاينة في الجريمة الإلكترونية 16
أولا : التعريف اللغوي للمعاينة 16
ثانيا :التعريف الاصطلاحي للمعاينة.....16

ثالثا : التعريف الفقهي للمعاينة 17
الفرع الثاني :أهمية المعاينة في الجريمة الإلكترونية 17
الفرع الثالث :محل أو نطاق المعاينة في الجريمة الإلكترونية 18
أولا :البيئة التقليدي 18
ثانيا : البيئة الافتراضي.....19
المطلب الثاني :شروط المعاينة في الجريمة الإلكترونية والصعوبات المرتبطة بها 20
الفرع الأول : شروط المعاينة في الجريمة الإلكترونية.....20
أولا : إذن أو أمر المعاينة الإلكترونية 20
ثانيا : وقت إجراء المعاينة الإلكترونية.....20
ثالثا : مكان إجراء المعاينة الإلكترونية 20
رابعا : الأشخاص الذين يحق لهم حضور المعاينة الإلكترونية 21
خامسا : محضر المعاينة الالكترونية.....22
الفرع الثاني : الصعوبات المرتبطة بالمعاينة في الجريمة الإلكترونية 22
خلاصة الفصل الأول : 23

الفصل الثاني :

الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية والهيئات المختصة بها.....25
المبحث الأول : الأساليب الفنية للضبط والمعاينة في الجريمة الإلكترونية.....26
المطلب الأول: الخطوات الفنية للضبط في الجريمة الإلكترونية 26
الفرع الأول : الخطوات المتبعة لإجراء الضبط في الجريمة الإلكترونية 26
الفرع الثاني : قواعد تحريز وتأمين المضبوطات الإلكترونية.....27
أولا : تحديد المادة الإلكترونية المراد ضبطها.....27
ثانيا : تأمين البرامج المضبوطة قبل تشغيلها.....27
ثالثا : الالتزام بإتباع القواعد الفنية الخاصة بكيفية نقل الأحرازالإلكترونية وحملها 27
رابعا : مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز الإلكترونية 28
خامسا : منع الأشخاص غير المرخص لهم من الوصول إلى المعطيات.....28
الفرع الثالث : طرق الضبط الإلكتروني 28
المطلب الثاني : الأساليب الفنية للمعاينة في الجريمة الإلكترونية 29
الفرع الأول : الخطوات الفنية المتبعة قبل الانتقال لمعاينة في الجريمة الإلكترونية 29
الفرع الثاني : الخطوات الفنية المتبعة عند الانتقال للمعاينة في الجريمة الإلكترونية 30

المطلب الثالث :نموذج تطبيقي لإجراء الضبط والمعاينة في جريمة اختراق حساب فيسبوك وسرقة البيانات الشخصية في الجزائر 32
الفرع الأول : الوقائع 32
الفرع الثاني :الإجراءات الضبط والمعاينة في القضية 32
المبحث الثاني : الهيئات المختصة بالضبط والمعاينة في الجريمة الإلكترونية.....33
المطلب الأول : الهيئات القضائية.....33
الفرع الأول : النيابة العامة.....33
أولا : الانتقال إلى مكان الجريمة وإجراء المعاينة 34
ثانيا : التفتيش وضبط الأدلة الإلكترونية 34
ثالثا : تفتيش المنظومة المعلوماتية.....35
الفرع الثاني :قاضي التحقيق.....35
أولا : الإجراءات التي يباشرها قاضي التحقيق في الجريمة الإلكترونية 35
1-الخطوات الواجب إتباعها قبل الانتقال إلى مسرح الجريمة الالكترونية 36
2- شروط صحة معاينة مسرح الجريمة 36
أ-سرعة الانتقال لى مكان الجريمة 36
ب- السيطرة على مكان وقوع الجريمة 37
ثانيا : التفتيش في الجريمة الالكترونية.....37
ثالثا :ضبط الدليل في مجال الجريمة الالكترونية 39
الفرع الثالث : ضباط الشرطة القضائية.....40
أولا : القيام بالمعاينة في مسرح جرائم المساس بأنظمة المعالجة آلية للمعطيات 40
1-معاينة الجرائم الواقعة على المكونات المادية للحاسوب 40
2-معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطة softuare 41
ثانيا : حجز معطيات المعلوماتية.....41
المطلب الثاني : الهيئات الأمنية 42
الفرع الأول : وحدات الأمن الوطني.....42
الفرع الثاني : جهاز الدرك الوطني 43
المطلب الثالث : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مقدم الخدمات 45
الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال.....45
الفرع الثاني : مقدم خدمات الانترنيت.....46

أولا:الالتزام بمساعدة السلطات العامة 47
ثانيا:الالتزام بحفظ المعطيات المتعلقة بحركة السير.....47
ثالثا:الالتزام بالسرية والشفافية.....47
خلاصة الفصل الثاني.....48
الخاتمة 50
قائمة الملاحق 53
قائمة المصادر والمراجع 57
الفهرس 63

الملخص

الملخص :

تعدد إجراءات الضبط والمعاينة في الجريمة في الجريمة الإلكترونية من الوسائل الأساسية لجمع الأدلة الرقمية ، نظرا لطبيعة هذه الجرائم غير المادية وسرعة زوال آثارها ، وتشمل المعاينة فحص الأجهزة والشبكات وتوثيق البيانات المرتبطة بالجريمة ، بينما يركز الضبط على حفظ الأدلة الرقمية بطريقة قانونية تضمن عدم تغييرها ، وتتطلب هذا النوع من التحقيق الاستعانة بخبراء تقنيين لضمان سلامة الإجراءات وتنفيذ المعاينة والضبط بإذن قضائي من جهة مختصة ، وتحت رقابة مشددة لحماية الخصوصية وضمان مشروعية الدليل أمام القضاء .

الكلمات المفتاحية :

الجريمة الإلكترونية ، الضبط ، المعاينة ، الإجراءات الجزائية ،الأدلة الرقمية .

Résumé:

En matiére de cy berciminalite les procedures de saise et dinspection sontessentielles pour recueillir des preuves numeriques compte tenu de la nature immaterielle de ces crimes et de la disparition rapide de leurs effets linspection comprendlexamen des appareills et des reseaux ainsi que la documentation des donnees relatives a linfra ction tandisque la saisie repose sur la preservation legale des preuves numeriques afin de garantir leur inalteration ،ce type denquete necessite lassistance dexperts juridiques pour garantir linspection et de la saisie avec lartorisation judiciaire dune autorite competente dous une supervision stricte afin de proteger la vie pricee et de garantis la legitimite des preunesdevant la justice elle est effectuee par une autorite judiciare et de decuritecompetente

Mots clés :

Criminal ،procedures ، preuve، numeriques، linspection

Abstract :

In cybercrime seizure and inspection procisedures are essential means of collecting digital evidence given the non material nature of these crimes and the rapid disapprarance of their effects includes examininig devices and networks and documenting date related to the crime while seizure is based on legally preserving digital evidence to ensure it is not altered this type of inestigation requires the assistance of technical expets to ensure the integrity of procedures and the implementation of inspection and seizure with judicial permission from a competent authority under strict superrvision to protect privacy and ensure the legitimacy of evidence before the judiciary and is carried out by a competent judicial and security authority

Keywords :

Cybercrime، procedures، digital ،evidence ،inspection judicial