سلطات النيابة العامة في الجرائم المعلوماتية
(المعاينة – التفتيش)

د. نديم محمد حسن الترزي

أستاذ القانون الجنائي المساعد
كلية الشرطة


2003
١٤٢٤
جامعة الأندلس
العلوم والتقنية
Alandalus University For Science & Technology

(AUST)

ISSN : 2410-1818

سلطات النيابة العامة في الجرائم المعلوماتية
(المعاينة – التفتيش)

ملخص البحث:

أصبحت الجرائم المعلوماتية (cyber crimes) محط اهتمام الكثير من الباحثين القانونيين، نظراً لاتصالها المباشر بالحياة الخاصة، ولما لهذه الوسائل من تأثير خطير على الأمن القومي للدول، وكذلك على الجوانب الاقتصادية للشركات والأشخاص. لذلك فإن السلطة المختصة بالتحقيق فيها وكشف أسرارها هي النيابة العامة. ولها في سبيل التحقيق فيها العديد من الإجراءات التي نص عليها قانون الإجراءات الجزائية اليمني؛ كالمعاينة والتفتيش والاستجواب والضبط.

وسوف أكتفي في هذا البحث بالحديث عن إجراءات المعاينة والتفتيش لأهميتهما، ولما يترتب عليهما من اتصال مباشر بالحياة الخاصة.

وقد هدفت هذه الدراسة إلى توضيح سلطات النيابة العامة – المعاينة، التفتيش - في الجرائم المعلوماتية، مع بيان النصوص القانونية التي تحكم هذه المسائل، والقصور فيها، والتوصيات المقترحة لمعالجة هذا القصور.

Abstract:

The cyber-crimes became in the center of attention of many legal scholars, because of the direct contact with the private life, and the serious impact on the national states security, as well as on the economic sides of the companies and people.

The public prosecution is the competent authority investigation.

The public prosecution, according to the yemeni Code of criminal procedures has the competence to examine, inspect, interrogate and seize.

In this research I'm going to talk only about the procedures of examination and inspection because of the their direct contact with private life.

This study aimed to clear up the authorities of public prosecution in the cyber-crimes, and to study the legal texts that govern these issues and their shortcomings, to suggest the recommendations for rectifying the shortcomings, as well.

ISSN : 2410-1818

مقدمة:

من الواضح أن الجرائم المعلوماتية (cyber-crime) في تزايد مستمر، وهذا يرجع إلى تطور أدواتها، وسهوله استخدامها، وبسبب الانفتاح العالمي وارتباط أسواق المال ببعضها البعض.

ونتيجة لذلك التطور في تكنولوجيا المعلومات، فقد ازدادت التهديدات والمخاطر التي تصيب الأفراد والدول في جميع المجالات، إذ لم تُعد تقتصر هذه الجرائم على المال فحسب، بل تعدت ذلك لتشمل الحريات الشخصية التي تمس الفكر والأخلاق وغيرها.

ولاكتشاف وضبط هذا النوع من الجرائم فقد خوّل المشرع النيابة العامة سلطة التحقيق في هذه الجرائم - كغيرها من الجرائم - كونها صاحبة الاختصاص الأصيل في التحقيق في الجرائم.

وتتميز إجراءات التحقيق في الجرائم المعلوماتية بالعديد من السمات خاصة التي تميزها عن إجراءات الاستدلال، نظراً للسلطات الواسعة التي منحها المشرع للنيابة العامة أثناء التحقيق؛ كالمعاينة والتفتيش والاستجواب والضبط.

وتجدر الإشارة إلى أن الحماية الجنائية من الجرائم المعلوماتية لا تزال من خلال النصوص الجنائية التقليدية، إذ أن تكنولوجيا المعلومات وما صاحبها من جرائم ألقت بضلالها على القانون الجنائي، بينما لا تزال نصوص هذا القانون تواجه الجرائم التقليدية، مع وجود بعض النصوص التي تواجه بعض الجرائم ذات الصلة بالجانب المعلوماتي.

لذلك فإن النيابة العامة ليس أمامها إلا الاستعانة بما هو موجود من نصوص في القانون الجنائي لمواجهة الجرائم المعلوماتية، والاستعانة بالخبراء، مع اقتراح النصوص الجنائية المراد إضافتها إلى القانون الجنائي أو تعديل بعض نصوصه.

وبالرغم من عدم وجود النصوص القانونية الحديثة التي تواجه الجرائم المعلوماتية، إلا أن ذلك لا يعني أن يظل المحقق الجنائي وأسلوب التحقيق جامداً، بل يجب عليه أن يتطور بما يتناسب لمواجهة هذا النوع من الجرائم.

ISSN : 2410-1818

أولاً: مشكلة الدراسة: تتمثل مشكلة الدراسة في الآتي:

١. تزايد حجم ظاهرة الجرائم المعلوماتية بسرعة فائقة، مما شكّل تحدياً كبيراً لأجهزة العدالة – ومنها النيابة العامة – لمواجهة هذه الجرائم.
٢. ندرة النصوص القانونية الجنائية التي تواجه الجرائم المعلوماتية بنصوص صريحة.
٣. ضعف المهارات في مجال تكنولوجيا المعلومات لدى سلطات التحقيق لمواجهة الجرائم المعلوماتية.

ثانياً: أهمية الدراسة: تظهر أهمية الدراسة من كونها تسلط الضوء على موضوع هام يرتبط بالإجراءات المخولة لسلطات التحقيق في قانون الإجراءات الجزائية لمواجهة الجرائم المعلوماتية، وما يجب أن يتوافر لدى المحققين من مهارات لمواجهة هذا النوع من الجرائم.

ثالثاً: أهداف الدراسة: تهدف هذه الدراسة إلى تحقيق الآتي:

١. بيان الإجراءات الواجب اتباعها من قبل سلطات التحقيق لمواجهة الجرائم المعلوماتية.
٢. الكشف عن مدى كفاية النصوص القانونية لمواجهة الجرائم المعلوماتية.
٣. التعرف على المهارات اللازم توافرها لدى المحققين لمواجهة الجرائم المعلوماتية.
٤. وضع التصورات المناسبة لمعالجة القصور في النصوص القانونية وإجراءات سلطات التحقيق.
٥. إثراء الفكر القانوني الجنائي بالإجراءات الواجب اتباعها لمواجهة الجرائم المعلوماتية.

رابعاً: تساؤلات الدراسة: نأمل في هذه الدراسة أن تجيب على التساؤلات الآتية:

١. ما هي الإجراءات اللازم اتباعها لمواجهة الجرائم المعلوماتية؟
٢. هل النصوص القانونية الحالية كافية لمواجهة الجرائم المعلوماتية؟
٣. ما هي المهارات التي يجب أن تتوافر لدى سلطات التحقيق لمواجهة الجرائم المعلوماتية؟
٤. ما هي التصورات المناسبة لمعالجة القصور في النصوص القانونية وإجراءات سلطات التحقيق؟

ISSN : 2410-1818

خامساً: منهجية الدراسة: سوف اعتمد في هذه الدراسة على المنهج الوصفي، لوصف الإجراءات المستخدمة من قبل سلطة التحقيق – النيابة العامة – للحصول على الدليل في الجريمة المعلوماتية، مع الأخذ بالمنهج التحليلي – كلما تطلب الأمر ذلك – لتحليل بعض المفاهيم والنصوص القانونية ذات العلاقة بالجرائم المعلوماتية، بالإضافة إلى المنهج المقارن – كلما تطلب الأمر ذلك أيضاً – لمعرفة المستوى الذي وصلت إليه بعض الدول في الجرائم المعلوماتية.

سادساً: خطة الدراسة: سأتناول هذه الدراسة – بإذن الله تعالى – من خلال مبحثين يسبقهما مطلب تمهيدي، نتناول في المطلب التمهيدي الإطار النظري للجرائم المعلوماتية، أما المبحث الأول فنتناول فيه إجراءات المعاينة في الجرائم المعلوماتية، بينما نتناول إجراءات التفتيش التي تقوم بها النيابة العامة في الجرائم المعلوماتية في المبحث الثاني، وسوف اختتم هذه الدراسة بخاتمة تتضمن مجموعة من النتائج والتوصيات.

المطلب التمهيدي: الإطار النظري للتحقيق في الجرائم المعلوماتية

لاشك أن الغاية التي يهدف إليها المشرع من التحقيق الجنائي هي الوصول إلى الحقيقة، ولن يتم الوصول إلى هذه الغاية إلا من خلال مراعاة الطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية عن غيرها من الجرائم التقليدية، ونظراً لهذه الطبيعة الخاصة للجرائم المعلوماتية؛ فإن ذلك يستدعي التطرق إلى المبادئ الأساسية للتحقيق في الجرائم المعلوماتية.

وهذه الطبيعة الخاصة والمبادئ الأساسية للتحقيق في الجرائم المعلوماتية تقتضي وجود محقق ذو كفاءة وخبرة عالية في مجال الجرائم المعلوماتية، بالرغم من وجود معوقات قد تعيق عمله في اكتشاف هذا النوع من الجرائم، لذلك سنتناول هذا المطلب في أربعة فروع على النحو الآتي:

الفرع الأول: الطبيعة الخاصة بالتحقيق في الجرائم المعلوماتية

تتميز إجراءات التحقيق في الجرائم المعلوماتية بطابع خاص، وذلك لتعلقها بحرمة الحياة الخاصة، إذ يجب أن تتوفر الضمانات القانونية للمتهم عند الدخول إلى البيانات المخزنة آلياً، كما هو الحال في دخول المنازل، بيد أن الدخول إلى البيانات المخزنة آلياً

ISSN : 2410-1818

يختلف عن الدخول إلى المنازل؛ فالدخول إلى البيانات المخزنة آلياً يتم عن طريق تشغيل الجهاز عن قرب أو عن بعد ، وذلك باستخدام برنامج خاص بذلك [1].

ويظهر الطابع الخاص للتحقيق في الجرائم المعلوماتية في نصوص قانون الإجراءات الجزائية وقانون الجرائم والعقوبات اليمني، إذ أننا نجد فيها نصوصاً خاصةً بالوسائل الالكترونية، ففي قانون الإجراءات الجزائية اليمني نصت المادة (٢/١٢) على أن: " حرية وسرية المراسلات البريدية والسلكية واللاسلكية وكافة وسائل الاتصال مكفولة وفقاً للدستور، لا يجوز مراقبتها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون ".

وعاقب قانون الجرائم والعقوبات اليمني كل من اعتدى على حرمة الحياة الخاصة في المادة (٢٥٦) منه، إذ نصت على أنه: " يعاقب بالحبس مدة لا تزيد على سنة أو بالغرامة كل من اعتدى على حرمة الحياة الخاصة، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضا المجني عليه:

١. استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة – أياً كان نوعه– محادثات جرت في مكان خاص عن طريق الهاتف.
٢. التقط أو نقل بجهاز من الأجهزة – أياً كان نوعه – صورة شخص في مكان خاص.

وتأسيساً على هذه النصوص نجد أن المشرع قد وضع نصوصاً – وإن لم تكن متوسعة – تحافظ على حرمة الحياة الخاصة، وتعاقب كل من اعتدى عليها.

كما أن من الخصوصية التي تتسم بها الجريمة المعلوماتية أن يقوم بالتحقيق فيها محققين لديهم مهارات عالية[2]، وحداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفاء ومحو آثارها[3].

---

(١) د. شيماء عبد الغني عطاء الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، طبعة ٢٠٠٧م، ص ٢٤١.

(٢) عبد الله بن حسين القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤م، ص ٥٩. Repository.nauss.edu.sa/handle تاريخ ٢٠١٦/٥/١م، الساعة ٥:١٥ pm.

(٣) سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة ماجستير في العلوم القانونية، قسم الحقوق، جامعة الحاج خضر، الجزائر، ٢٠١٢م-٢٠١٣م، ص٩٢. http//digitallibrary.univ-batna.dz:8080/ispui/handle، تاريخ ٢٠١٦/٤/٣٠م، الساعة ١١:٣٥ pm.

ISSN : 2410-1818

الفرع الثاني: المبادئ الأساسية للتحقيق في الجرائم المعلوماتية

يتطلب التحقيق في الجرائم المعلوماتية الالتزام بالأصول التي حددها المشرع في قانون الإجراءات الجزائية، إذ أن من شأن هذه الأصول أن تزيد من فاعلية إجراءات التحقيق في هذا النوع من الجرائم، وتؤدي في الأخير إلى الكشف السريع عن الجريمة، دون أن تعطي المجال للقائمين بالتحقيق مباشرة التحقيق بشكل اجتهادي أو وفق رغباتهم [٤].

ويمكن ذكر المبادئ الأساسية التي يجب على المحقق اتباعها من خلال عرض العناصر الأساسية للتحقيق، وكذا القواعد الخاصة بالجرائم المعلوماتية، وذلك على النحو الآتي:

أولاً: العناصر الأساسية للتحقيق في الجرائم المعلوماتية: تتمثل هذه العناصر في الآتي[٥]:

١. **تحديد وقت ومكان ارتكاب الجريمة المعلوماتية**: تثير النتيجة الإجرامية في مجال الجريمة المعلوماتية مشاكل عديدة؛ منها على سبيل المثال مكان وزمان تحقق النتيجة الإجرامية في الجرائم المعلوماتية، فلو ارتكب أحد المتهمين جريمة في دولة ما من خلال اختراق حساب بنكي في دولة أخرى، فهذا يثير مشكلة وقت وقوع الجريمة، هل هو وقت ارتكاب الجريمة في بلد المتهم أم توقيت البنك المسروق، كما يثير مشكلة أخرى تتعلق بمكان وقوع الجريمة.

٢. **إظهار الركن المادي للجريمة المعلوماتية**: إن النشاط أو السلوك المادي في الجرائم المعلوماتية يتطلب معرفة السلوك المادي الذي قام به الجاني لارتكاب الجريمة المعلوماتية، من خلال تجهيز الحاسب الآلي وتحميل البرامج، وبالرغم من أن التجهيز يُعد من الأعمال التحضيرية في الجرائم التقليدية، إلا أن الأمر يختلف في الجرائم المعلوماتية، فشراء برامج الاختراق وبرامج الفيروسات وتحميلها تمثل جريمة في حد ذاتها.

---

(٤)عبد الله بن حسين القحطاني، مرجع سابق، ص٤٣.

(٥) حول هذا الموضوع أنظر: د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية، طبعة ٢٠١٠م، ص٥٢، عبد الله بن حسين القحطاني، مرجع سابق، ص٤٩.

ISSN : 2410-1818

٣. **إظهار الركن المعنوي للجريمة المعلوماتية**: ويقصد به الحالة النفسية وإرادة الجاني، التي تربط بين ماديات الجريمة وشخصية الجاني.

علانية التحقيق: إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولا يقتصر الأمر على تحقق الاطمئنان في قلب المتهم، بل لابد أن تتضمن في ذاتها حماية لأحكام القاضي من أن تكون محلاً للشك أو الخضوع للتأثير، كما أنها تشكل اطمئناناً للجمهور على أن الأمور تسير بشكل طبيعي.

والعلانية في مرحلة التحقيق هي نسبية تقتصر على الخصوم في الدعوى الجزائية، بينما العلانية في مرحلة المحاكمة مطلقة، يجوز لأي فرد من الجمهور حضور المحاكمة.

ثانياً: تطبيق القواعد الخاصة بالجرائم المعلوماتية[٦]: هناك عدة قواعد خاصة بالجرائم المعلوماتية، والتي تحكم النطاق المكاني، وهي مبدأ الإقليمية، ومبدأ العينية، ومبدأ الشخصية، ومبدأ العالمية، ونوضح ذلك فيما يلي:

١. **مبدأ الإقليمية:** ويقصد به تطبيق القانون الوطني على كل جريمة تقع على إقليم الدولة بغض النظر عن جنسية مرتكبها.

وبمطالعة قانون الجرائم والعقوبات اليمني نجد أنه طبق مبدأ الإقليمية على كل الجرائم التي تقع على إقليم الدولة كلها أو بعضها، ونصت على ذلك المادة (٣) منه، إذ جاء فيها: "يسري هذا القانون على كافة الجرائم التي تقع على المقيم في الدولة أياً كانت جنسية مرتكبها، وتُعد الجريمة مقترفة في إقليم الدولة إذا وقع منه الإعمال المكونة لها، ومتى وقعت الجريمة كلها أو بعضها في إقليم الدولة يسري هذا القانون على من ساهم فيها أو وقعت مساهمته في الخارج".

وكذلك الحال في التشريع المصري فقد طبق مبدأ الإقليمية على كل الجرائم التي تقع على إقليم الدولة كلها أو بعضها.

ويستند مبدأ الإقليمية على مبررات، منها: سهولة الوصول إلى الأدلة، وسهولة إجراءات المحاكمة في موقع الجريمة، وتحقيق الردع العام لإرضاء المشاعر الاجتماعية.

---

(٦) د.أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، طبعة ٢٠١٠م، ص ١٨١.

ISSN : 2410-1818

٢. **مبدأ العينية:** ويقصد به تطبيق قانون الجرائم والعقوبات على الجرائم التي تمس مصالح أساسية للدولة، أياً كان مكان وقوعها أو ارتكابها أو جنسية مرتكبها. ولم يُشر قانون الجرائم والعقوبات إلى الجرائم المعلوماتية تطبيقاً لمبدأ العينية، وإنما حصر مبدأ العينية في عدد من الجرائم منها:

أ. الجرائم الماسة بأمن الدولة (الفصل الثاني والثالث)[٧].

ب. الجرائم ذات الخطر العام (الباب الثاني)[٨].

ج. الجرائم الماسة بالاقتصاد القومي (الباب الثالث)[٩].

د. الجرائم الماسة بالوظيفة العامة (الباب الرابع)[١٠].

٣. **مبدأ الشخصية:** ويُعد هذا المبدأ اتساعاً لمبدأ الإقليمية، وذلك للعقاب على الجرائم التي ارتكبت خارج الدولة عند عودة الفاعل إلى وطنه؛ ويمكن تطبيق هذا المبدأ على الجرائم المعلوماتية، عندما يقوم الجاني بإعداد الجريمة في وطنه، وتنفيذها عند مغادرته إلى دولة أخرى، وتثور الصعوبة حول ما إذا كانت الجريمة غير معاقب عليها في القانون الأجنبي.

ولم ينص قانون الجرائم والعقوبات اليمني بشكل صريح على تطبيق هذا المبدأ في الجرائم المعلوماتية، ولكن يمكن إعمال نص المادة (٣) منه على من يرتكب من اليمنيين إحدى صور الجرائم المعلوماتية كلها أو بعضها في إقليم الدولة. ومبدأ الشخصية نصت عليه أيضاً المادة (٢) من القانون ذاته[١١]. وقد أخذ قانون العقوبات المصري بمبدأ الشخصية عند توافر الشروط الآتية:

أ. أن يكون الجاني مصرياً.

ب. أن تكون الجريمة المرتكبة جناية أو جنحة وفقاً للقانون المصري.

ج. أن يكون الفعل المرتكب في الخارج يُعد جريمة وفقاً للقانون الأجنبي.

---

(٧) الباب الأول، القسم الأول، الكتاب الثاني من قانون الجرائم والعقوبات اليمني.

(٨) القسم الأول، الكتاب الثاني من قانون الجرائم والعقوبات اليمني.

(٩) المرجع السابق.

(١٠) المرجع السابق.

(١١) إذ جاء فيها:" المسئولية الجزائية شخصية..".

ISSN : 2410-1818

٤. **مبدأ العالمية:** ويقصد به تطبيق النص الجنائي للدولة التي يتواجد فيها الجاني، دون النظر إلى جنسيته أو جنسية المجني عليه أو مكان ارتكاب الجريمة؛ وبمطالعة قانون الجرائم والعقوبات نجد أنه لم ينص على مبدأ العالمية، كون هذا النوع من الجرائم مقيد بحالة الإنابة القضائية[١٢].

وكذلك الحال بالنسبة للتشريع المصري فلم يأخذ بهذا المبدأ، وإنما يتم النظر في بعض القضايا التي تقع خارج الإقليم المصري وفقاً للاتفاقيات الدولية.

الفرع الثالث: المحقق الجنائي في الجرائم المعلوماتية

تباشر النيابة التحقيق في الجرائم بوصفها صاحبة الاختصاص الأصيل فيها كقاعدة عامة، وقد أولاها المشرع هذا الاختصاص باعتبارها جهة قضائية مكلفة بحماية حقوق وحريات الأفراد. وهذا الاختصاص جاء بنص المادة (٢١) من قانون الإجراءات الجزائية، والتي نصت على أن:" النيابة العامة هي صاحبة الولاية في تحريك الدعوى الجزائية ورفعها ومباشرتها أمام المحاكم..".

ومن المعروف أن النيابة العامة تقوم بالتحقيق من خلال مجموعة من المحققين ذوي الخبرات القانونية، وقد يقوم بالتحقيق النائب العام بنفسه أو بواسطة احد أعضاء النيابة العامة[١٣].

والمحقق الجنائي: هو الشخص القائم بأعمال إجراءات التحقيق، ولا يختلف تعريف المحقق في الجرائم التقليدية عن تعريفه في الجرائم المعلوماتية، فالفرق في نوعية الجريمة وليس في المحقق[١٤].

وبما أن الجرائم المعلوماتية تعتمد على تقنية المعلومات ووسائل التكنولوجيا، فإن التحقيق فيها يجب أن يكون من قبل محققين لديهم المعارف والخبرات الضرورية لمواجهتها[١٥].

---

(١٢) نصت المادة (٢٥٣) منه على أنه:" تقبل النيابة العامة أو المحكمة الإنابة القضائية التي ترد إليها بالطرق الدبلوماسية من إحدى السلطات الأجنبية، ويجري تنفيذها وفقاً للقواعد المقررة في القانون اليمني".

(١٣) حيث نصت المادة (٢٣ أ.ج) على أنه:" يقوم النائب العام بنفسه أو بواسطة أحد أعضاء النيابة العامة بمباشرة الدعوى الجزائية كما هو مقرر بالقانون".

(١٤) د. خالد ممدوح إبراهيم، مرجع سابق، ص٨٦.

(١٥) د.على جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، طبعه ٢٠٠٩م، ص١٢٧ ومابعدها.

ISSN : 2410-1818

لذلك فإن المحققين المكلفين للتحقيق في الجرائم المعلوماتية يجب أن يكون لديهم مهارات تعتمد على التأهيل التكنولوجي، بالإضافة إلى الصفات التي يجب أن يتحلى بها المحقق في جميع الجرائم؛ كالموهبة والسرعة في إجراءات التحقيق وغيرها، وتتمثل هذه المهارات في الآتي[١٦]:

١. الإلمام بالجوانب الفنية والتقنية واستخدامها في التحقيق الجنائي.
٢. مهارة تقييم الجريمة المعلوماتية.
٣. معرفة المكونات المادية للأجهزة الرقمية والتعامل المبدئي معها.
٤. تمييز أنظمة التشغيل والتعامل المبدئي معها.
٥. التعرف على الصيغ المختلفة للملفات، وتطبيقات الحاسب الآلي.
٦. إجادة التعامل مع خدمات الانترنت الرئيسية.
٧. معرفة الأدوات والأساليب المستخدمة في ارتكاب الجريمة المعلوماتية.
٨. معرفة أهم تقنيات الحاسب الآلي والانترنت وأدواتها وطريقة عملها.
٩. معرفة الجرائم المعلوماتية والخصائص التي تتميز بها.
١٠. الإلمام بالتشريعات المتعلقة بالجرائم المعلوماتية.

الفرع الرابع: معوقات التحقيق في الجرائم المعلوماتية

هناك العديد من المعوقات التي قد تواجه القائمين بالتحقيق الجنائي في الجرائم المعلوماتية، وتتمثل هذه المعوقات في الآتي[١٧]:

أولاً: المعوقات التي تتعلق بالجرائم المعلوماتية: تظهر هذه المعوقات فيما يلي:

١. سهولة وسرعة إخفاء ومحو الدليل الرقمي، نظراً للتقنية العالية في ارتكاب الجريمة المعلوماتية.
٢. صعوبة الوصول إلى الدليل الرقمي لإحاطته بوسائل الحماية الفنية.
٣. ضخامة حجم المعلومات والبيانات المتعين فحصها.
٤. إمكانية خروج الجرائم المعلوماتية عن نطاق إقليم الدولة.

---

(١٦) للمزيد أنظر: د.على جبار الحسيناوي، مرجع سابق، ص١٣٢، د. خالد ممدوح إبراهيم، مرجع سابق، ص١٠٠،عبد الله القحطاني، مرجع سابق، ص٥٩٠، سعيداني نعيم، مرجع سابق، ص١١٥.

(١٧) أنظر: د. خالد ممدوح إبراهيم، مرجع سابق، ص٦٤ وما بعدها، سعيداني نعيم، مرجع سابق، ص١٨٦ وما بعدها، عبد الله بن حسين القحطاني، مرجع سابق، ص٦٤ وما بعدها.

ISSN : 2410-1818

٥. ضعف الحماية الأمنية التقنية للمعلومات الرقمية الهائلة.

ثانياً: المعوقات التي تتعلق بالجهات المتضررة

١. عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين على أنظمة المعلومات.
٢. اغفال جانب التوعية لإرشاد المستخدمين لأنظمة المعلومات من خطورة الجرائم المعلوماتية.
٣. التساهل من قبل مستخدمي المعلومات في وضع الحماية الأمنية التقنية، بهدف تبسيط الإجراءات وكسب المزيد من الزبائن.
٤. الإحجام عن الإبلاغ لأسباب كثيرة؛ كمحدودية الجريمة المعلوماتية، أو لصغر سن الجاني، أو بسبب الخوف من الجاني.

ثالثاً: المعوقات التي تتعلق بجهات التحقيق

١. نقص المهارة الفنية المطلوبة للتحقيق في الجرائم المعلوماتية لدى المحققين.
٢. عدم مسايرة التطور المتسارع لتكنولوجيا المعلومات، والتي أصبحت تشمل معظم مناحي الحياة.
٣. قلة البرامج والأدوات التقنية المخصصة للمساعدة في عملية التحقيق، مقارنة بالتسارع الهائل في التقنية.
٤. خوف بعض المحققين من استخدام وسائل تكنولوجيا المعلومات، أو عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

المبحث الأول: المعاينة في الجرائم المعلوماتية

تمهيد وتقسيم: تعتبر المعاينة من الإجراءات الهامة التي تقوم بها النيابة العامة، وتهدف إلى إظهار الحقيقة في جريمة وقعت، عن طريق الانتقال إلى مسرح الجريمة لجمع الأشياء المتعلقة بالجريمة ومعاينة الآثار المترتبة عليها.

والمعاينة قد تكون من إجراءات الاستدلال، وقد تكون من إجراءات التحقيق، فإذا كانت إجراءات المعاينة في مكان عام على المكونات المادية فإنها من إجراءات الاستدلال، إما إذا تطلبت المساس بحرمة خاصة؛ كمعاينة برامج الكمبيوتر فإن ذلك من إجراءات التحقيق.

ISSN : 2410-1818

وتختلف المعاينة في الجرائم المعلوماتية عنها في الجرائم التقليدية، ففي الجرائم المعلوماتية يتطلب الأمر - بالإضافة إلى الإجراءات التقليدية - جمع واستخلاص الدليل الرقمي من التطبيقات والبرامج الرقمية.

والمشرع لم يُجز الحصول على الدليل دون شروط أو ضوابط قانونية، تضمن سلامة الإجراءات من العيوب؛ لذلك، فإننا سنتناول هذا المبحث في ثلاثة مطالب على النحو الآتي:

المطلب الأول: مفهوم المعاينة في الجرائم المعلوماتية.

المطلب الثاني: محل المعاينة في الجرائم المعلوماتية والسلطة المختصة بها.

المطلب الثالث: القواعد الأساسية الواجب اتباعها في معاينة الجرائم المعلوماتية.

المطلب الأول: مفهوم المعاينة في الجرائم المعلوماتية

تهدف المعاينة إلى كشف الغموض عن كل ما له علاقة بالجريمة، وهي إجراء غايته الوصول إلى الحقيقة من خلال صيانة العناصر التي تتعلق بالجريمة، ولمزيد من البيان عن المعاينة، فإننا سوف نتناول في هذا المطلب مفهوم المعاينة في الجريمة المعلوماتية، وطبيعتها وأهميتها، في فرعين على النحو الآتي:

<u>الفرع الأول: تعريف المعاينة في الجرائم المعلوماتية وطبيعتها</u>

أولاً: تعريف المعاينة:

يقصد بها: " ملاحظة وفحص حي مباشر لمكان أو شخص أو شيئ له علاقة بالجريمة، لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة"(١٨).

فالمعاينة إجراء بمقتضاه ينتقل المحقق الجنائي إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها، وكذلك جمع الأشياء الأخرى التي تفيد في كشف الجريمة(١٩)، وهذا ما أشارت إليه المادة (١٣٠ أ.ج) بقولها:"

(١٨) د. أحمد محمود مصطفى، مرجع سابق، ص ١٣٤.

(١٩) د. خالد ممدوح إبراهيم، مرجع سابق، ص ١٤٩ .

ينتقل المحقق إلى محل الحادث أو إلى أي مكان لمعاينته، كلما رأى ذلك مفيداً للتحقيق لإثبات حالة الأماكن والأشياء والأشخاص ووجود الجريمة وأثارها ..".

وبالرغم من أن هذا النص جاء قبل ظهور الجريمة المعلوماتية، إلا أن المشرع قد استعمل عبارات واسعة يمكن إعمالها على الجرائم المعلوماتية، إذ لم يقتصر المشرع في المعاينة على الأماكن والأشخاص فحسب، بل شمل أيضاً الأشياء، وهذه يمكن أن يكون منها الجرائم المعلوماتية.

ثانياً: طبيعة المعاينة في الجرائم المعلوماتية

المعاينة قد تكون من إجراءات التحقيق، وقد تكون من إجراءات الاستدلال، ولا تعتمد طبيعتها على صفة من يجريها، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الإفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال، إما إذا اقتضت دخول منزل أو له حرمة خاصة كانت إجراء تحقيق(٢٠).

وهذه الطبيعة المختلفة للمعاينة - كونها إجراء استدلال أو إجراء تحقيق - أشارت إليها المادتين(٩٢، ١٣٠) من قانون الإجراءات الجزائية اليمني، ففي المادة (٩٢) جعلت اختصاص المعاينة مقصوراً على معاينة مكان وقوع الجريمة والمحافظة على أدلة الجريمة وما يسهل تحقيقها، وهذه من إجراءات الاستدلال، لأن ليس منها أي مساس بما له حرمة خاصة، أما إذا كانت المعاينة تمس الأشياء التي لها حرمة خاصة؛ كالبحث في الكمبيوتر أو المعلومات فإنها من أعمال التحقيق وليس الاستدلال، وهذا ما أشارت إليه المادة (١٣٠) سالفة الذكر.

وتأسيساً على ما سبق، فإن المعاينة في علم التحقيق الجنائي هي مشاهدة المكان الذي ارتكبت فيه الجريمة - ومنها الجرائم المعلوماتية - وعمل وصف شامل له لإثبات حالته بالكيفية التي تركها بها الجاني[٢١].

(٢٠) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط٢ ، ١٩٨٨م، ص٦٤٠.
(٢١) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٤٩.

ISSN : 2410-1818

الفرع الثاني: أهمية المعاينة في الجرائم المعلوماتية

يمكن استخلاص أهمية المعاينة في الجرائم المعلوماتية -كما هو الحال في الجرائم التقليدية -من نص المادة (١٣٠ أ.ج.ي) والتي أشارت إلى أهمية المعاينة للتحقيق، لإثبات حالة الأماكن والأشياء والأشخاص ووجود الجريمة مادياً وآثارها وكل ما يلزم إثبات حالته.

إلا إن الفارق بين الجرائم المعلوماتية والجرائم التقليدية، إن الأخيرة لها مسرحاً جرت عليه الأحداث، وتركت آثارها المادية التي تنبثق منها الأدلة، بينما مسرح الجريمة في الجرائم المعلوماتية يختلف عن مسرح الجريمة التقليدية، والذي يتمثل في المعدات والأنظمة المعلوماتية التي كانت محلاً للجريمة أو أداتها[٢٢].

ولا تتمتع المعاينة في مجال الجرائم المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجرائم التقليدية، ومرد ذلك إلى اعتبارين[٢٣]:

١. إن الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثاراً مادية.
٢. إن عدداً كبيراً من الأشخاص قد يتردد على مكان أو مسرح الجريمة المعلوماتية، خلال الفترة الزمنية التي تتوسط عادةً ارتكاب الجريمة واكتشافها، مما قد يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها، وهو ما قد يثير الشك في الدليل المستمد من المعاينة.

المطلب الثاني: محل المعاينة في الجرائم المعلوماتية والسلطة المختصة بها

سوف نتحدث في هذا المطلب عن محل المعاينة في الجرائم المعلوماتية والسلطة المختصة بها، على النحو الآتي:

الفرع الأول: محل المعاينة في الجرائم المعلوماتية

(٢٢) صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، عام ٢٠١٣م، www.ummto/dzLship?articl. تاريخ ٢٠١٦/٤/٣٠م، الساعة ١١:٣٠ pm

(٢٣) د.أحمد محمود مصطفى، مرجع سابق، ص١٣٤.

ISSN : 2410-1818

أحرز التقدم التكنولوجي وضعاً جعل المعلومات متاحةً في متناول الجميع، وترتب على ذلك ظهور جرائم استخدم فيها الكمبيوتر والانترنت كأداة للجريمة، أو ضحية لهذا النشاط الإجرامي، فالجرائم المعلوماتية تنصب على العناصر التالية(٢٤):

١. **المعلومات**: وتتمثل هذه الجرائم في سرقة أو تغيير أو حذف المعلومات، كالنشاط الإجرامي الذي يستهدف اختراق البريد الالكتروني والعبث بمحتوياته.
٢. **الأجهزة**: وتشمل الجرائم المعلوماتية التي تقع على أجهزة الكمبيوتر بهدف تعطيلها أو تخريبها بإرسال الفيروسات أو البرامج التي تسبب تلف هذه الأجهزة.
٣. **الأشخاص أو الجهات**: وهي الجرائم التي تقع على الأشخاص أو الجهات باستخدام شبكة الانترنت والكمبيوتر، كالتهديد أو الابتزاز أو السرقة أو ممارسة الفاحشة وغيرها.

وتأسيساً على ذلك، فإن محل المعاينة في الجرائم المعلوماتية هو معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية، سواء كانت هذه الآثار على المعلومات أو الأجهزة أو الأشخاص، ويمكن استخلاص ذلك من نص المادة (١٣٠ أ.ج.ي) -سالفة الذكر -والتي أشارت إلى أن المعاينة تكون للأماكن والأشياء والآثار التي تخلفت عن الجريمة.

ولم تهتم معظم التشريعات الجنائية المعاصرة بتحديد مسرح الجريمة - محل المعاينة - بشكل دقيق، كما هو الحال في التفتيش، ويرجع عدم الاهتمام بتحديد مسرح المعاينة إلى اعتبارين[٢٥]:

١. إن معظم القوانين الجنائية لا ترتب آثاراً قانونية بالبطلان أو الانعدام على تجاوز مسرح الجريمة - الحدود المكانية - عند إجراء المعاينة، طالما فيه مصلحة للتحقيق ولا يوجد فيه خروج على قواعد الاختصاص.
٢. لا تثور عادةً بشأن تحديد مسرح الجريمة منازعة بين الخصوم في الدعوى الجزائية أو طلب البطلان تأسيساً على تجاوز النطاق المكاني، كما هو الشأن في التفتيش، لأن المعاينة هي إجراء واجب من إجراءات التحقيق تفرضه القوانين على

(٢٤)عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، ٢٠٠٧م، ص١٨.
(٢٥) د.أحمد محمود مصطفى، مرجع سابق، ص١٣٤.

ISSN : 2410-1818

المختصين بمجرد علمهم بوقوع الجريمة، فلا يجوز لأي طرف الاعتراض على هذا الإجراء.

والجدير بالذكر إن المعاينة في الجرائم التقليدية تكون بالانتقال إلى مكان وقوع الجريمة، أما في الجرائم المعلوماتية، فإن هناك عده طرق يستطيع بها المحقق المعاينة في العالم الافتراضي وهي(٢٦):

١. من مكتبه في النيابة العامة.
٢. من إحدى مقاهي الانترنت.
٣. من مقر مزود الخدمة.
٤. من مكتب الخبير الفني.

الفرع الثاني: السلطة المختصة بمعاينة الجرائم المعلوماتية

المعاينة -كما سبق القول -قد تكون إجراء استدلال، وقد تكون إجراء تحقيق، فإذا جرت في مكان عام فإنها إجراء استدلال، إما إذا اقتضت دخول منزل أو معاينة شيئ له حرمة خاصة فإنها من إجراءات التحقيق(٢٧).

لذلك، فإن تحديد مكان وقوع الجريمة له أهمية بالغة في تعيين السلطة صاحبة الاختصاص لمباشرة إجراءات المعاينة، وفي تحديد أولويات البحث والتنقيب عن الآثار والمخلفات الناشئة عن الجريمة، بهدف توضيح الأسلوب الأمثل لكشف كامل أبعادها دون إغفال جانب منها(٢٨).

وبما أن إجراءات التحقيق -ومنها المعاينة -تطال حقوق وحريات الأفراد الخاصة، فقد حرص المشرع في قانون الإجراءات الجزائية اليمني على إيلائها إلى جهة قضائية وهي النيابة العامة، وهذا ما أشارت إليه المادة (١٣٠) منه.

ولسلطة التحقيق الاستعانة بالخبراء لإجراء المعاينة وتقديم الإيضاحات في أي مسألة من المسائل المتعلقة بالجرائم المعلوماتية التي تخرج عن نطاق اختصاصها، وهذا ما

(٢٦) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٥٦.
(٢٧) محمود نجيب حسني، مرجع سابق، ص٦٤٠.
(٢٨) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٦٩.

ISSN : 2410-1818

أكدته المادة (١٣٠ أ.ج.ي) بقولها: ".. وله استدعاء الخبراء لإجراء المعاينة ويحرر محضراً بالمعاينة يكون صورة كاملة ومطابقة للشيء محل المعاينة..".

وأكدت ذلك أيضاً المادة (٢٠٧) من القانون ذاته، إذ نصت على أنه:" للنيابة العامة أن تطلب من طبيب أو شخص له خبرة فنية في أي مجال إبداء الرأي في أي مسألة متعلقة بالتحقيق..".

وللنيابة العامة سلطة تقديرية في تقدير رأي الخبير، فلها أن تأخذ به، ولها أن ترفضه مع تحديد أسباب الرفض، أو طلب تقرير إضافي من الخبير ذاته أو من خبير آخر، إذا احتوى التقرير الأول على أوجه نقص، كما يجوز طلب تقرير من خبير آخر في حالة وجود شك في صحة التقرير الأول[٢٩].

وتأسيساً على ما سبق، فالنيابة هي صاحبة الاختصاص الأصيل في معاينة الجرائم المعلوماتية - كغيرها من الجرائم الأخرى - عندما تتعلق المعاينة بالحريات الخاصة للأشخاص، بالرغم من أن نصوص قانون الإجراءات الجزائية لا تزال نصوصاً تقليدية، ولم تنص صراحة على الجرائم المعلوماتية، إلا أن الألفاظ الواردة في هذه النصوص تتسع لتشمل الجرائم المعلوماتية.

المطلب الثالث: القواعد الأساسية الواجب اتباعها في معاينة الجرائم المعلوماتية

نظراً للطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية، فإنه يجب مراعاة مجموعة من الخطوات قبل البدء في معاينتها، وكذا الالتزام بالشروط الواجب اتباعها لصحة المعاينة في هذا النوع من الجرائم، لذلك فإننا سنتناول هذا المطلب في فرعين على النحو الآتي:

(٢٩) حيث نصت المادة (٢١٦ أ.ج.ي) على أنه:" لا يكون تقرير الخبير ملزماً للنيابة العامة أو المحكمة، ولكن قرار عدم الموافقة على التقرير يجب أن يكون مسبباً، ويجوز طلب تقرير إضافي من الخبير نفسه أو من خبير آخر، إذا احتوى التقرير الأول على أوجه نقص، كما يجوز طلب تقرير جديد من خبير آخر إذا ثار شك حول صحة التقرير الأول ".

ISSN : 2410-1818

الفرع الأول: الخطوات الواجب مراعاتها قبل البدء في معاينة الجرائم المعلوماتية

نظراً لأن الجرائم المعلوماتية على تماس مباشر مع حقوق الأشخاص وحرياتهم، فإن على المحقق اتباع مجموعة من الخطوات قبل البدء في معاينة الجرائم المعلوماتية، وهي[٣٠]:

١. تحديد فريق المعاينة من المحققين والخبراء الذين تتوافر فيهم الكفاءة العلمية والخبرة الفنية في المجال المعلوماتي.
٢. توفير معلومات مسبقة عن مكان الجريمة، والمالك لهذا المكان، ونوع وعدد اجهزة الكمبيوتر والشبكات المرتبطة بها فنياً.
٣. تجهيز الأدوات والاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في معاينة الجرائم المعلوماتية.
٤. اتخاذ الإجراءات والاحتياطات المسبقة قبل البدء بالمعاينة؛ كقطع التيار الكهربائي عن مكان المعاينة، لمنع الجاني من القيام بأي فعل من شأنه التأثير على أدلة الجريمة أو محو آثارها.
٥. عدم نقل أي مادة معلوماتية من مسرح الجريمة المراد معاينته قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أي مجال لقوى مغناطيسية يمكن أن تسبب في محو البيانات المسجلة.
٦. منع تواجد أي شخص في مسرح الجريمة المعلوماتية حتى لا يؤثر ذلك على الآثار والأدلة.

الفرع الثاني: شروط صحة المعاينة

يشترط لصحة المعاينة توافر عدة شروط، أهمها ما يلي:

١. **سرعة الانتقال إلى مسرح الجريمة المعلوماتية**: على المحقق فور تلقي بلاغ بوقوع جريمة معلوماتية الانتقال إلى مكان وقوع الجريمة المعلوماتية المراد معاينته، وعليه فور وصوله اتخاذ الاحتياطات الآتية[٣١]:

(٣٠) أنظر: د. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ٢٠٠٤م، ص١١١، صغير يوسف، مرجع سابق، ص٨٦ ، د. خالد ممدوح إبراهيم، مرجع سابق، ص١٥٧.
(٣١) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٥٨.

ISSN : 2410-1818

أ. حصر الأشخاص المتواجدين داخل مسرح الجريمة وتدوين بياناتهم.
ب. التأكد من عدم لمس أية آثار إلا من قبل المختصين.
ج. إخطار الخبراء بالبدء بالمعاينة ورفع الآثار.
د. التحفظ على كل ماله ارتباط وعلاقة بالجريمة المعلوماتية.

٢. **توثيق كل إجراءات المعاينة**: على المحقق عند وصوله إلى مسرح الجريمة المعلوماتية توثيق تاريخ ووقت المعاينة ووصف مسرح الجريمة بكامل محتوياته وصفاً دقيقاً، وتوثيق الأدلة الرقمية بدقة، والوضعية التي كانت عليها وتحريزها - متى أمكن ذلك - وتوثيق الشبكات المرتبطة بأجهزة الكمبيوتر - مسرح الجريمة - والبرامج المستخدمة في ارتكاب الجريمة المعلوماتية[٣٢].

٣. **التحفظ على مسرح الجريمة بعد المعاينة**: من الأشياء التي ينبغي على المحقق اتباعها هي التحفظ على مسرح الجريمة بعد الانتهاء من إجراءات المعاينة، وعلة ذلك هي إمكانية العودة إليه كلما أراد المحقق كشف غموض شيء أو التأكد من آثار معينة، فالمعاينة المتكررة لمسرح الجريمة تكشف دائماً أشياء جديدة، قد يكون الجاني قام بإخفائها[٣٣].

٤. **تدوين المعاينة**: تفادياً لضياع الأدلة والحفاظ على مسرح الجريمة ينبغي على المحقق تدوين إجراءات المعاينة لمسرح الجريمة المعلوماتية، وحتى يكون للتدوين أهميته، فإنه ينبغي اتباع الإجراءات التالية[٣٤]:

أ. تصوير الحاسب الآلي والأجهزة الطرفية المتصلة بها، مع تسجيل وقت وتاريخ ومكان التقاط الصور.
ب. تدوين الطريقة التي تم بها إعداد النظام.
ج. إثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، حتى يمكن إجراء عمليات المقارنة والتحليل عند عرض الأمر فيما بعد على المحكمة.

(٣٢) صغير يوسف، مرجع سابق، ص٨٦.
(٣٣) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٦٣.
(٣٤) المرجع السابق، ص١٦٤.

ISSN : 2410-1818

المبحث الثاني: التفتيش في الجرائم المعلوماتية

تمهيد وتقسيم :

يُعد التفتيش من أهم وأخطر إجراءات التحقيق، لمساسه بالحريات الخاصة التي تحميها الدساتير والقوانين. والتفتيش إجراء قانوني يهدف إلى كشف أدلة الجريمة التي وقعت، أو المحتمل وقوعها، وتزداد خطورة التفتيش بشكل كبير في الجرائم المعلوماتية، والسبب في ذلك يرجع إلى أن محل التفتيش فيها هو نظام المعالجة الالكترونية، وهذا النظام ذو طابع غير مادي، إذ أنه مجرد معلومات الكترونية ليس لها مظهر مادي محسوس في العالم الخارجي؛ كما هو الحال في الجرائم التقليدية، كما أنه قد لا يقتصر على المعلومات الموجودة في كمبيوتر معين، بل أنه قد يتجاوز إلى أنظمة ومعلومات أخرى مرتبطة به، ولو اختلف مكان وجودها. لذلك ينبغي على المحقق الجنائي مراعاة الشروط والضمانات القانونية أثناء التفتيش عن الجرائم المعلوماتية، حتى لا توصم إجراءات التفتيش بالبطلان.

ولأهمية موضوع التفتيش في الجرائم المعلوماتية، سنتناوله في ثلاثة مطالب على النحو الآتي:

المطلب الأول: مفهوم التفتيش في الجرائم المعلوماتية.

المطلب الثاني: محل التفتيش في الجرائم المعلوماتية والسلطة المختصة به.

المطلب الثالث: الشروط الواجب مراعاتها أثناء التفتيش في الجرائم المعلوماتية.

المطلب الأول: مفهوم التفتيش في الجرائم المعلوماتية

التفتيش في الجرائم المعلوماتية - كما سبق القول - من أهم وأخطر إجراءات التحقيق، والذي يهدف إلى كشف الغموض عن جريمة وقعت باستخدام إحدى الأنظمة المعلوماتية، وللتفتيش أهمية كبيرة بالنسبة للتحقيق الجنائي، لذلك سنتناول هذا المطلب في فرعين على النحو الآتي:

ISSN : 2410-1818

الفرع الأول: تعريف التفتيش في الجرائم المعلوماتية

عرف البعض التفتيش بشكل عام بأنه:" البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها إلى المتهم"[٣٥].

وعرفه آخر بأنه:" إجراء من إجراءات التحقيق يقوم به موظف مختص طبقاً للإجراءات المقررة قانوناً في محل يتمتع بالحرمة بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم"[٣٦].

وبمطالعة قانون الإجراءات الجزائية نجد أنه لم يضع تعريفاً محدداً للتفتيش، وإنما يستفاد مفهوم التفتيش من نص المادة (١٣٧) منه، والتي نصت على أنه:" لا يجوز التفتيش إلا للبحث عن الأشياء والآثار الخاصة بالجريمة التي يجري التحقيق بشأنها، ولا يجوز أن يتجاوز إلى سواه، إلا إذا ظهرت عرضاً أثناء التفتيش أشياء تُعد حيازتها جريمة أو تفيد في كشف الحقيقة عن جريمة أخرى..".

وتأسيساً على ذلك فإنه يمكن تعريف التفتيش بأنه: " إجراء قانوني من إجراءات التحقيق تقوم به سلطة التحقيق المختصة أو من تندبه لذلك، للبحث عن أدلة وقوع الجريمة ونسبتها إلى المتهم".

وهذه التعريفات وإن كانت عبارات تقليدية، إلا أنها – في رأيي - تدل على التفتيش بشكل عام، سواءً في الجرائم التقليدية أو في الجرائم المعلوماتية، والتفتيش في كليهما يفيد في كشف الحقيقة عن الجريمة وأدلتها والمتهم فيها، وتخضع للضوابط القانونية للتفتيش.

وقد عرف البعض التفتيش في الجرائم المعلوماتية بأنه: " البحث عن طريق التفتيش والضبط عن البيانات المخزنة في النظام المعلوماتي للحاسب الآلي أو في دعامة تخزين المعلومات، سواء كانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات"[٣٧].

---

(٣٥) د. مفتاح بو بكر المطردي، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية، جمهورية السودان، ٢٣-٢٠١٢/٩/٢٥م، ص ٤٢. www.shatharat.net/vb/showthr تاريخ ٢٠١٦/٥/١٤م الساعة ١٠:٠٠ pm.

(٣٦) د.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٦م، ص ١٩٢.

(٣٧) د. مفتاح بو بكر المطردي، مرجع سابق، ص٤٩.

ISSN : 2410-1818

الفرع الثاني: أهمية التفتيش

للتفتيش أهمية كبيرة، إذ يساعد سلطة التحقيق في كشف غموض الجريمة - سواء كانت من الجرائم التقليدية أو من الجرائم المعلوماتية – وتلك الأهمية تتعلق بالواقعة الإجرامية أو بأطرافها، ونبين ذلك فيما يلي[٣٨]:

أولاً: بالنسبة للواقعة الإجرامية: يكشف التفتيش أمور عدة؛ نبينها فيما يلي:

١. **ثبوت وقوع الجريمة**: يؤكد التفتيش صحة البلاغ الوارد من الشاهد أو المجني عليه بوقوع الجريمة من عدمه.
٢. **وقت ومكان وقوع الجريمة**: يساعد التفتيش المحقق في تحديد وقت ومكان ارتكاب الجريمة، بالرغم من أن بعض الجرائم المعلوماتية عابرة الحدود مما يصعب تحديد مكانها.

ثانياً: بالنسبة لأطراف الخصومة الجنائية: يساعد التفتيش المحقق الجنائي في كشف المستور عن الباعث لارتكاب الجريمة، وشخصية الجاني، ودرجة خطورته وأسلوبه الإجرامي، وعلاقته بالمجني عليه، ونبين ذلك على النحو الآتي:

١. **تحديد الباعث على ارتكاب الجريمة**: قد يكشف التحقيق عن مدى كراهية الجاني للمجني عليه، من خلال وجود أدلة تفيد في معرفة رغبة الجاني في الانتقام أو تهديد المجني عليه.
٢. **تحديد شخصية الجاني**: من خلال التفتيش لمسرح الجريمة – التقليدي والمعلوماتي - يمكن التعرف على شخصية الجاني.
٣. **تحديد حرفته وأسلوبه الإجرامي وخطورته**: قد يكشف التفتيش عن وجود اسطوانات أو برامج لفك الشفرات أو برامج فيروسات أو شهادات تدل على أن الجاني متخصص في مجال الكمبيوتر والانترنت، كذلك يوضح التفتيش أسلوب الجاني، من خلال طريقة الدخول إلى شبكة المعلومات، أو المواقع الالكترونية، وطريقة ارتكابه للواقعة الإجرامية، وكذا مدى خطورته.

(٣٨) د. خالد ممدوح إبراهيم، مرجع سابق، ص١٨٤ وما بعدها.

ISSN : 2410-1818

٤. **تحديد عدد الجناة وعلاقتهم بالمجني عليه**: يؤدي تفتيش مسرح الجريمة المعلوماتية إلى الكشف عن عدد الجناة، وعلاقتهم بالمجني عليه.

المطلب الثاني: محل التفتيش في الجرائم المعلوماتية والسلطة المختصة به

ينصب التفتيش في الجرائم المعلوماتية على نظم الكمبيوتر وقواعد البيانات وشبكة المعلومات، ويقوم بهذا التفتيش سلطة التحقيق المختصة أو من يندبونهم من مأموري الضبط القضائي أو الخبراء، وللمزيد من البيان حول هذا الموضوع، سنتناول هذا المطلب في فرعين على النحو الآتي:

الفرع الأول: محل التفتيش في الجرائم المعلوماتية

يقع التفتيش على مكونات الحاسوب والبيانات المرتبطة به، ولا توجد مشكلة في تنفيذ التفتيش للمكونات المادية للكمبيوتر، لإمكانية ذلك وسهولته، ولأنه يقع على أشياء مادية، مع مراعاة الإجراءات والشروط القانونية الخاصة بالتفتيش، نظراً لحساسية البيانات التي تحتويها أجهزة الحاسوب وإمكانية إتلافها أو محوها بسهولة[٣٩]، لكن المشكلة في إمكانية تفتيش وضبط مكونات الحاسوب المعنوية؛ كالبرامج والنظم الخاصة بالتشغيل وقواعد البيانات، والتي يمكن أن تخزن طريقة ارتكاب الجريمة بواسطة الحاسوب[٤٠].

فذهب رأي إلى أن الجرائم التي تقع على الكيانات المعنوية للكمبيوتر يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، إما إذا تحولت إلى مستخرجات أو مستندات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها أو بواسطتها[٤١].

وأتفق مع الرأي الذي يرى إمكانية التفتيش في الكيانات المعنوية، لأن المكونات المعنوية باعتبارها محتوى لمعلومات وبيانات وحوار وكلمات سر يمكن تصنيفها وتحليلها، لاستظهار الدليل المعلوماتي[٤٢].

([٣٩]) د.علي جبار الحسيناوي، مرجع سابق، ص١١٦.

([٤٠]) المرجع السابق، ص١١٦.

([٤١]) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢٠٠.

([٤٢]) د.مفتاح بو بكر المطردي، مرجع سابق، ص٤٤.

ISSN : 2410-1818

الفرع الثاني: السلطة المختصة بالتفتيش في الجرائم المعلوماتية

التفتيش عمل من أعمال التحقيق، لا يجوز أن يقوم به إلا من خوّله القانون الصفة القانونية للقيام بهذا العمل، وهي النيابة العامة كقاعدة عامة، إلا أن المحقق يستطيع أن يندب أحد مأموري الضبط القضائي للقيام بإجراء التفتيش. وهذا ما أشارت إليه المادة(١١٦ ،أ.ج.ي)، والتي نصت على أنه: " يتولى النائب العام سلطة التحقيق وكافة الاختصاصات التي ينص عليها القانون وله أن يباشر سلطة التحقيق بنفسه أو بواسطة أحد أعضاء النيابة العامة أو من يندب لذلك من القضاء أو مأموري الضبط القضائي".

واتساقاً مع الضمانات التي ينبغي توافرها عند ممارسة التفتيش، فإنه لا يكفي توافر صفة قاضي التحقيق أو عضو النيابة العامة لكي يقوم بهذا الإجراء، بل لابد أن يكون مختصاً بالتحقيق في الجريمة، سواء من حيث الاختصاص المكاني أو النوعي[٤٣]. وقد أشارت إلى الاختصاص المادة (١١٥ أ.ج.ي)، والتي نصت على أنه: "يتحدد اختصاص أعضاء النيابة العامة في التحقيق بالجرائم الواقعة في نطاق اختصاص المحاكم التي يعملون في دوائرها".

ويتحدد الاختصاص المكاني إما بمكان وقوع الجريمة، وإما بالمكان الذي يقيم به المتهم، أو المكان الذي ضبط فيه، أما الاختصاص النوعي فيتحدد بالجريمة التي يقوم المحقق بالتفتيش فيها من حيث نوعها[٤٤].

ولما كانت سلطة التحقيق الأصلية غير مطالبة بإجراء التفتيش بنفسها في كل الحالات، إما بسبب عدم اتساع وقت المحقق لذلك، أو بسبب تعدد الأمكنة أو الأشياء المراد تفتيشها، فإنه يجوز للمحقق تفويض بعض سلطاته لمأموري الضبط القضائي عن طريق الندب، وهذا ما أكدته المادة (١١٦ أ.ج.ي) -سالفة الذكر – والمادة (١١٧) والتي نصت على أنه:" لعضو النيابة أن يندب أحد مأموري الضبط القضائي للقيام بإجراء أو أكثر من إعمال التحقيق عدا استجواب المتهم..".

(٤٣) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، لم يحدد الناشر ومكان النشر، الطبعة الثانية، ٢٠٠٨م، ص١٣٦.

(٤٤) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢١٦.

ISSN : 2410-1818

إلا أن اختصاص سلطة التفتيش قد يتجاوز أنظمة الكمبيوتر الموجودة إلى أنظمة أخرى مرتبطة بها، وهذا هو الوضع الغالب في ظل شيوع التشبيك بين أجهزة الكمبيوتر وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، مما خلق تحديات كبيرة، أهمها مدى قانونية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب النظم التي يمتد إليها التفتيش[٤٥].

ولمعرفة الآراء المتعلقة حول هذا الموضوع، سنتناوله من زاويتين هما:

الزاوية الأولى: بالنسبة لامتداد الاختصاص داخل الدولة: يرى فريق أن الاختصاص بالتفتيش يمكن أن يمتد إلى خارج اختصاص سلطة التحقيق داخل الدولة. واستدلوا ببعض التشريعات التي أخذت بذلك، ومنها قانون الإجراءات الجنائية الفيدرالي الأمريكي، إذ أنه في القاعدة (٤١ -أ) مد اختصاص سلطة التحقيق للتفتيش إلى خارج دائرة سلطة التحقيق، نظراً للطابع الخاص للجرائم المعلوماتية، ويكون ذلك لمتابعة الرسائل والاتصالات الالكترونية عبر أكثر من جهاز أين ما وجد داخل الدولة[٤٦].

وكذلك الحال بالنسبة لقانون تحقيق الجنايات البلجيكي في المادة (٨٨) فإن لقاضي التحقيق أن يأمر بامتداد التفتيش إلى نظام معلوماتي آخر غير المكان الأصلي وفقاً لضابطين[٤٧]:

١. إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث.
٢. إذا وجدت مخاطر بضياع بعض الأدلة لسهولة عملية محو أو إتلاف أو تحريف أو نقل البيانات محل البحث.

أما الفريق الآخر فيرى أنه لا يمكن امتداد التفتيش إلى مكان آخر داخل الدولة، وإنما على المحقق الذي وقعت الجريمة في اختصاصه أن يصدر أمر بالتفتيش، ويطلب

([٤٥]) د.محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة ٢٠١٢م، ص٢١١.
([٤٦]) د.غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة ٢٠١٠م، ص١٩٥.
([٤٧]) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢٠٣.

ISSN : 2410-1818

من المحقق الآخر الذي يتواجد في اختصاص الأجهزة المراد تفتيشها أن يقوم بالتفتيش[٤٨].

وهذا هو الاتجاه الذي سار عليه قانون الإجراءات الجزائية اليمني، إذ نصت المادة (١١٧) منه على أنه:" .. ولعضو النيابة العامة إذا دعاه الحال اتخاذ إجراء من الإجراءات خارج دائرة اختصاصه أن يكلف به عضو النيابة المختص".

الزاوية الثانية: بالنسبة لامتداد الاختصاص خارج الدولة: يثير امتداد الاختصاص بالتفتيش للجرائم المعلوماتية خارج الدولة مشاكل كبيرة، نظراً لما تتمتع به الدول من سيادة، إلا أن بعض الدول ومنها هولندا سمحت لسلطة التحقيق تفتيش نظم الحاسوب المرتبطة بها حتى وإن كانت موجودة في دولة أخرى، بشرط أن يكون هذا التدخل مؤقتاً، وأن تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة[٤٩].

ويرى جانب من الفقه أن التفتيش الالكتروني العابر للحدود لابد وأن يتم في إطار الاتفاقيات الدولية التي تجيز الامتداد[٥٠].

وفي رأيي إن امتداد اختصاص سلطة التحقيق داخل الدولة ضرورة تستدعيها طبيعة الجرائم المعلوماتية، بشرط النص عليها في نصوص قانون الإجراءات الجزائية، أما امتداد الاختصاص خارج الدولة فأنا اتفق مع من يرى ضرورة وجود اتفاقيات تعاون ثنائية أو دولية، حتى لا يترتب على إجراءات التفتيش البطلان.

المطلب الثالث: الشروط الواجب مراعاتها أثناء التفتيش في الجرائم المعلوماتية

حرصت القوانين الإجرائية ومن بينها قانون الإجراءات الجزائية اليمني على إحاطة إجراءات التحقيق - ومنها التفتيش - بشروط وضمانات تنظم القواعد الأساسية في جميع إجراءات التحقيق، وتهدف هذه القوانين إلى صيانة الإنسان وحماية حقوقه وخصوصياته، لذلك سنتناول في هذا المطلب شروط التفتيش على النحو الآتي:

<u>الفرع الأول: الشروط الموضوعية الواجب مراعاتها لإجراء التفتيش</u>

تتمثل هذه الشروط في الآتي:

---

(٤٨) د.غنام محمد غنام، مرجع سابق، ص١٩٤.

(٤٩) د.أحمد محمود مصطفى، مرجع سابق، ص١٤١.

(٥٠) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢٠٥.

ISSN : 2410-1818

الشرط الأول: وجود سبب للتفتيش

كقاعدة عامة فإن سبب التفتيش - باعتباره من إجراءات التحقيق - هو وقوع جريمة، واتهام شخص أو عدة أشخاص بارتكابها أو المساهمة فيها، مع توافر أمارات أو قرائن قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو غيره[٥١].

وتأسيساً على ما سبق، وتطبيقاً على الجرائم المعلوماتية، وحتى يكون التفتيش فيها مشروعاً فلابد من تحقق الآتي[٥٢]:

١. وقوع جريمة معلوماتية.
٢. اتهام شخص أو أكثر بارتكاب هذه الجريمة المعلوماتية أو المساهمة في ارتكابها.
٣. توافر إمارات قوية أو قرائن على وجود أدلة معلوماتية في أحد الأجهزة الالكترونية أو الشبكات تفيد في كشف الحقيقة.

الشرط الثاني: تحديد محل التفتيش

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، ومحل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الاتصال. وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجودة فيه، فيما إذا كان من الأماكن العامة أو الأماكن الخاصة، ويمكن توضيح ذلك على النحو الآتي[٥٣]:

١. **حالة وجود الكيانات المعلوماتية في الأماكن الخاصة**: ففي هذه الحالة تكون لها حكم تفتيش المساكن من حيث الضمانات المقررة قانوناً، سيما اشتراط الإذن بالتفتيش من السلطات القضائية عندما يكون التفتيش من قبل مأموري الضبط القضائي في حالة الندب، وهذا ما نصت عليه المادة (١٣٢ أ.ج.ي) بقولها :" لا يجوز تفتيش الأشخاص أو دخول المساكن أو الاطلاع على المراسلات البريدية أو تسجيل

(٥١) سعيداني نعيم، مرجع سابق، ص١٥٤.
(٥٢) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢٠٩.
(٥٣) سعيداني نعيم، مرجع سابق، ص١٥٥.

ISSN : 2410-1818

المحادثات السلكية واللاسلكية أو الشخصية وكذا ضبط الأشياء إلا بأمر من النيابة العامة أثناء التحقيق ومن القاضي أثناء المحاكمة".

٢. **حالة وجود الكيانات المعلوماتية في الأماكن العامة**: تُجيز أغلب التشريعات التفتيش الواقع على مكونات الحاسب أو الشبكات في الأماكن العامة؛ كمقاهي الانترنت، بهدف مراقبتها والتأكد من احترامها للآداب العامة، وتفتيشها عند وجود جريمة مشهودة.

الشرط الثالث: الإذن بالتفتيش

من المستقر عليه أنه لا يجوز دخول المساكن للتفتيش – عندما يكون التفتيش من قبل مأموري الضبط القضائي – بغير سبق الحصول على إذن الدخول إلى المساكن من النيابة العامة في حالة الندب، وكذلك الحال عند الدخول إلى النظام المعلوماتي والذي يتم عن طريق تشغيل الجهاز عن قرب أو عن بعد، فإنه يتطلب الحصول على إذن مسبق.

وتطبيقاً لذلك فقد جاء التعديل الرابع للدستور الأمريكي لحماية البيانات المعالجة آلياً عن بعد، مقيماً التماثل بين الاقتحام المادي للمنازل والاقتحام المعنوي للمعلومات، ومثال على ذلك التنصت وتسجيل المكالمات الالكترونية والهاتفية، فلا يشترط تسجيل المحادثات الالكترونية والهاتفية الدخول إلى أماكن خاصة، بل أنه يمكن أن يتم ذلك عن بعد، لذلك فإنه يشملها الحظر القانوني، ويتطلب التفتيش فيها صدور إذن مسبق[٥٤].

وتجدر الإشارة إلى أن معظم التشريعات الإجرائية ومنها قانون الإجراءات الجزائية اليمني تشترط تحديد مجال التفتيش كشرط لصحة التفتيش، فالتفتيش في البيئة المعلوماتية يجب أن يكون محدداً في بيانات محددة لا يتجاوز سواها، إذ أن البيانات المطلوبة للقائم بالتفتيش قد تختلط بكميات هائلة من البيانات الأخرى، لذلك فإنه لايستقيم الأمر مع مبدأ الخصوصية أن يطلع القائم بالتفتيش على جميع البيانات الموجودة بالحاسوب، وهذا ما أشارت إليه المادة (١٣٧ أ.ج.ي)، إذ نصت على أنه:

(٥٤) د. شيماء عبد الغني محمد عطا الله، مرجع سابق، ص٢٤١.

ISSN : 2410-1818

"لايجوز التفتيش إلا للبحث عن الأشياء والآثار الخاصة بالجريمة التي يجري التحقيق بشأنها، ولا يتجاوز إلى سواه إلا إذا ظهرت عرضاً أثناء التفتيش أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة عن جريمة أخرى فيجوز لمن يقوم بالتفتيش ضبطها وإثباتها في المحضر".

الفرع الثاني: الشروط الشكلية الواجب مراعاتها لإجراء التفتيش

تأتي الضمانات الشكلية – الشروط الشكلية - مكملة للشروط الموضوعية، وتهدف إلى الاطمئنان إلى سلامة إجراءات التفتيش، وصوناً للحريات الشخصية من التعسف، لذلك تتمثل هذه الشروط في الآتي:

الشرط الأول: ضرورة حضور بعض الأشخاص عند إجراء التفتيش لنظم الحاسب الآلي

اشترط قانون الإجراءات الجزائية اليمني في المادة (١٣٤) منه ضرورة حضور شخص أو أشخاص أثناء التفتيش، سواء كان القائم بالتفتيش سلطة التحقيق أو مأموري الضبط القضائي بناءً على الندب من المحقق المختص، فقد نصت هذه المادة على أنه:" يحصل التفتيش بحضور المتهم أو من ينيبه وبحضور شاهدين من أقاربه أو جيرانه.. ولايجوز أن يكون الشاهدان من رجال التحقيق".

وبهذا يتقارب المشرع اليمني مع المشرع الفرنسي الذي اشترط في الفقرة الأولى من المادة (٥٧) من قانون الإجراءات الجنائية أن يتم التفتيش في حضور صاحب المكان الذي يتم فيه التفتيش مع حضور شاهدين، سواء كان القائم به قاضي التحقيق أو مأمور الضبط القضائي، بعكس المشرع المصري الذي لم يشترط حضور شهود أثناء تفتيش المسكن إذا كان القائم بالتفتيش هو قاضي التحقيق، إما إذا كان القائم بالتفتيش هو مأمور الضبط القضائي فقد اشترط حضور شهود أثناء التفتيش، إلا إذا كان منتدباً من قبل قاضي التحقيق، فإنه لا يلتزم باستدعاء شهود، لان المندوب يحل محل النادب تماماً[٥٥].

(٥٥) د.هلالي عبد اللاه أحمد، مرجع سابق، ص١٦٤ وما بعدها.

ISSN : 2410-1818

وتأسيساً على ما سبق، فان النص الذي جاء به المشرع اليمني في المادة (١٣٤ أ.ج) هو نص عام يمكن أن يسري على الجرائم المعلوماتية، كالجرائم التقليدية، خاصة عندما يكون تفتيش الأنظمة المعلوماتية في مكان أو أمكنة خاصة.

الشرط الثاني: الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية

لم يحدد قانون الإجراءات الجزائية اليمني ميعاد إجراء التفتيش في الجرائم المعلوماتية، وإنما حدد مواعيد التفتيش للمساكن[٥٦]. وقد حرص المشرع بهذا النص إلى صون الحرية الفردية وحرمة المساكن، ولم يجز تفتيشها ليلاً إلا في حالات معينة، وهي حالة الجريمة المشهودة أو في حالة مطاردة شخص هارب من وجه العدالة.

وبالرغم من عدم النص على الجرائم المعلوماتية، إلا أنه ليس أمام سلطة التحقيق إلا التوسع في تفسير النصوص القائمة لتطبيقها على الجرائم المعلوماتية حتى لا تبقى هناك جرائم بعيدة عن العقاب. وتطبيقاً لذلك فإن هذا النص يسري على جميع الجرائم، التقليدية منها والمعلوماتية، بالرغم من أنه - من وجه نظري - يمكن إجراء التفتيش في الجرائم المعلوماتية في أي وقت، إذا لم يتطلب الأمر الدخول إلى أماكن مغلقة، إذ يمكن في بعض الحالات تفتيش الأنظمة المعلوماتية عن بعد، مع مراعاة الضوابط القانونية.

الشرط الثالث: تحرير محضر بإجراء التفتيش

أوجبت المادة (١٥٠ أ.ج.ي) ضرورة إعداد محضر بإجراءات التفتيش بقولها: " يجب على عضو النيابة القائم بالتفتيش أن يحرر محضراً بالإجراءات وما أسفرت عنه وما تم ضبطه من أشياء..".

وتأسيساً على ذلك، فإنه ينبغي على القائم بالتفتيش تحرير محضر يثبت فيه ما تم من إجراءات، وما أسفر عن التفتيش من إدانة، وما تم ضبطه من أشياء، ولم يشترط المشرع شكلاً معيناً فيه، مما يعني أنه لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر، وهي أن يكون مكتوباً، والتوقيع عليه، وأن يحتوي على كافة

(٥٦) حيث نصت المادة(١٤٤/أ) منه على أنه: " تفتيش المساكن يجب أن يكون بعد شروق الشمس وقبل غروبها إلا في حالة الجريمة المشهودة أو مطاردة شخص هارباً من وجه العدالة".

ISSN : 2410-1818

الإجراءات المكتوبة في المحضر من قبل محقق مختص بالجرائم المعلوماتية، أو من قبل خبير يتم اصطحابه لهذا الغرض[٥٧].

خاتمة الدراسة :

يُعد ما سبق حصيلة جهد متواضع لدراسة سلطات النيابة العامة في التحقيق في الجرائم المعلوماتية، إذ أن التحقيق بشكل عام من اختصاص النيابة العامة في الجمهورية اليمنية – وإن كانت جديدة في مجال الجرائم المعلوماتية – ولها في سبيل التحقيق في الجرائم المعلوماتية العديد من الاجراءات القانونية، والتي تهدف في الأخير إلى الوصول إلى الحقيقة في كل جريمة.

وقد اكتفيت بالحديث عن أهم هذه الإجراءات، والتي لها مساس مباشر بالحرية الشخصية، وتتمثل هذه الاجراءات في المعاينة والتفتيش.

لذلك تناولت في المطلب التمهيدي من هذا البحث الإطار النظري للتحقيق في الجرائم المعلوماتية، وذلك في أربعة فروع، بينت في الفرع الأول منه الطبيعة الخاصة بالتحقيق في الجرائم المعلوماتية، ووضحت في الفرع الثاني المبادئ الأساسية للتحقيق في الجرائم المعلوماتية، ثم تناولت في الفرع الثالث التعريف بالمحقق الجنائي في الجرائم المعلوماتية، وفي الفرع الرابع والأخير تطرقت إلى معوقات التحقيق في الجرائم المعلوماتية.

أما المبحث الأول من هذا البحث فقد خصصته للحديث عن المعاينة في الجرائم المعلوماتية، وقسمته إلى ثلاثة مطالب، تناولت في المطلب الأول منه مفهوم المعاينة في الجرائم المعلوماتية، وبينت في المطلب الثاني محل المعاينة في الجرائم المعلوماتية والسلطة المختصة بها، ووضحت في المطلب الثالث القواعد الأساسية الواجب اتباعها في معاينة الجرائم المعلوماتية.

وفي المبحث الثاني تطرقت إلى موضوع التفتيش في الجرائم المعلوماتية، والذي تناولته في ثلاثة مطالب، أوضحت في المطلب الأول منه مفهوم التفتيش في الجرائم

(٥٧) د.خالد ممدوح إبراهيم، مرجع سابق، ص٢٢٤.

ISSN : 2410-1818

المعلوماتية، وخصصت المطلب الثاني للحديث عن محل التفتيش في الجرائم المعلوماتية والسلطة المختصة به، وبينت في المطلب الثالث شروط التفتيش في الجرائم المعلوماتية.

وفي الأخير اختتمت هذه الدراسة بمجموعة من النتائج والتوصيات، والتي أرجو من الله تعالى أن تكون ملاءمة، وهي على النحو الآتي:

أولاً: النتائج

يمكن ذكر أهم النتائج المستخلصة من هذا البحث فيما يلي:

١. تتميز إجراءات التحقيق في الجرائم المعلوماتية بطبيعة خاصة، لتعلقها بحرمة الحياة الخاصة، وما تتطلبه من خبرة ومعرفة تامة بهذا النوع من الجرائم. بالرغم من أن غالبية النصوص القانونية لا تزال عامة ولم تتناول الجرائم المعلوماتية بصفة خاصة.

٢. محل المعاينة في الجرائم المعلوماتية أوسع من محل التفتيش فيها، إذ أن المعاينة تشمل الأشخاص والأماكن والمعلومات، وهي إجراء واجب من إجراءات التحقيق تفرضه القوانين على المختصين بمجرد علمهم بوقوع الجريمة، ولا ترتب معظم التشريعات آثاراً بالبطلان لتجاوز مسرح الجريمة؛ كون المعاينة تأتي لمصلحة الأطراف ولمصلحة التحقيق، بينما نجد أن معظم التشريعات الجنائية شددت في تحديد محل التفتيش بشكل دقيق – وإن كانت لا تزال في الجرائم التقليدية – نظراً لما يتطلبه التفتيش من الغوص في خبايا الأنظمة المعلوماتية، وما يترتب على ذلك من كشف أسرار قد تكون أكثر خصوصية للأشخاص المرتبطين بهذه الأنظمة.

٣. بالرغم من الطبيعة الخاصة التي تتميز بها الجرائم المعلوماتية، إلا أن قانون الإجراءات الجزائية اليمني لا يسمح في المادة (١١٧) منه امتداد التفتيش إلى مكان آخر داخل الدولة، وإنما يطلب المحقق المختص من المحقق الآخر الذي يتواجد في مكان وجود الأدلة إجراء التفتيش.

٤. تتميز الجرائم المعلوماتية بأنها من الجرائم عابرة القارات، وهذا قد يؤدي إلى صعوبة الوصول إلى الأدلة وتفتيش الأنظمة المعلوماتية التي تقع خارج الدولة، دون وجود اتفاقيات دولية تسمح بذلك، ودون الإشارة إليها في قانون الإجراءات الجزائية.

ISSN : 2410-1818

٥. لم يُجز قانون الإجراءات الجزائية - في الجرائم التقليدية - التفتيش ليلاً إلا في حالات معينة، حمايةً للحقوق والحريات الخاصة، ولم تكن الجرائم المعلوماتية قد ظهرت وقت وضع التشريع، وما تتميز به من طبيعة خاصة، وإمكانية تفتيشها عن بعد دون المساس بالحريات الخاصة.

٦. حداثة الجرائم المعلوماتية ووسائل تنفيذها أدى إلى صعوبة مسايرة التطور المتسارع في مجال تكنولوجيا المعلومات من قبل سلطة التحقيق، وكذا بسبب نقص المهارة الفنية العملية لديهم في هذا المجال.

ثانياً: التوصيات

لأهمية هذا الموضوع فإنني أوصي بما يلي:

١. ضرورة العمل بما جاء من قواعد عامة في قانون الإجراءات الجزائية في مجال التحقيق في الجرائم المعلوماتية، حتى يتم تعديل نصوصه بما يتوافق مع طبيعة هذا النوع من الجرائم.

٢. ضرورة سد الفراغ التشريعي في قانون الإجراءات الجزائية في مجال التحقيق الجنائي، لتحديد ما هو من إجراءات المعاينة، وما هو من إجراءات التفتيش في الجرائم المعلوماتية بشكل دقيق، لتجنب الشك في الدليل المستخرج من النظم المعلوماتية.

٣. ضرورة تعديل نص المادة (١١٧) من قانون الإجراءات الجزائية، بحيث يتم النص فيها بالسماح لسلطة التحقيق بتفتيش الأنظمة المعلوماتية التي تقع خارج اختصاصها داخل الدولة – عن بعد – ما دام الأمر لا يتطلب الانتقال إلى الأماكن الخارجة عن اختصاصهم.

٤. ضرورة النص في قانون الإجراءات الجزائية على العمل بما جاء في الاتفاقيات الدولية المتعلقة بمد الاختصاص إلى خارج الدولة في مجال الجرائم المعلوماتية، كون الأدلة المعلوماتية سهلة التغيير والإزالة، بهدف تسهيل إجراءات التفتيش وضبط الجاني والحرص على عدم ضياع الأدلة.

٥. ضرورة تعديل نص المادة (١٤٤) من قانون الإجراءات الجزائية اليمني، بحيث تمنح سلطة التحقيق المختصة الحق بالتفتيش في الجرائم المعلوماتية ليلاً، إذا لم يتطلب

ISSN : 2410-1818

الأمر الدخول إلى أماكن مغلقة؛ إذ يمكن في بعض الحالات تفتيش الأنظمة المعلوماتية عن بعد، مع مراعاة الضوابط القانونية للتفتيش.

٦. ضرورة تحديث مناهج المعهد العالي للقضاء، لتضم البرامج التقنية العملية في مجال التحقيق في الجرائم المعلوماتية إلى جانب المناهج النظرية، مع ضرورة تأهيل أعضاء النيابة الحاليين بالدورات التخصصية في مجال التحقيق في الجرائم المعلوماتية، وإصدار دليل ارشادي قانوني من قبل النيابة العامة، يوضح فيه آلية التحقيق في الجرائم المعلوماتية (المعاينة، التفتيش، الاستجواب، الضبط).

قائمة المراجع:

أولاً: المراجع المتخصصة

١. د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، طبعة ٢٠١٠م.

٢. د. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية، طبعة ٢٠١٠م.

٣. د. شيماء عبد الغني عطاء الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الإسكندرية، جمهورية مصر العربية، طبعة ٢٠٠٧م.

٤. د. عبدالفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٦م.

٥. عبدالله عبدالكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، ٢٠٠٧م.

٦. د. على جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، طبعه ٢٠٠٩م.

٧. د. غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة ٢٠١٠م.

٨. د. محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، جامعة نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ٢٠٠٤م.

ISSN : 2410-1818

٩. د. محمود أحمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، طبعة ٢٠١٢م.

١٠.د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ط٢ ، ١٩٨٨م.

١١.د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، لم يحدد الناشر ومكان النشر، الطبعة الثانية، ٢٠٠٨م.

ثانياً: مراجع الانترنت

١. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة ماجستير في العلوم القانونية، قسم الحقوق، جامعة الحاج خضر، الجزائر، ٢٠١٢م -٢٠١٣م. http//digitallibrary.univ-batna.dz:8080/ispui/handele تاريخ ٢٠١٦/٤/٣٠م، الساعة ١١:٣٥ pm.

٢. صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، عام ٢٠١٣م، www.ummto/dzLship?articl. تاريخ ٢٠١٦/٤/٣٠م، الساعة ١١:٣٠ pm.

٣. عبد الله بن حسين القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، رسالة ماجستير في العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤م. Repository.nauss.edu.sa/handle تاريخ ٢٠١٦/٥/١م، الساعة ٥:١٥ pm.

٤. د. مفتاح بو بكر المطردي، ورقة عمل مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية - جمهورية السودان، ٢٣ - ٢٠١٢/٩/٢٥م. www.shatharat.net/vb/showthr تاريخ ٢٠١٦/٥/١٤م الساعة ١٠:٠٠ pm.

ثالثاً: التشريعات

١. قانون الجرائم والعقوبات اليمني رقم (١٢) لسنة ١٩٩٤م.

٢. قانون الإجراءات الجزائية اليمني رقم (١٣) لسنة ١٩٩٤م.