إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية

Procedures for inference and preliminary investigation of electronic crimes

إعداد:

عمر محمود حمدان القهيوي

إشراف

الأستاذ الدكتور: أحمد محمد اللوزي

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون

العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

2023

تفويض

أنا عمر محمود حمدان القهيوي أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقيا وإلكترونيا للمكتبات، أو المنظمات، أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: عمر محمود حمدان القهيوي

التاريخ: ٢٠٢٢/١/٢٥م

التوقيع: .....

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها : **إجراءات الإستدلال والتحقيق الإبتدائي في الجرائم الإلكترونية**

وأجيزت بتاريخ :٢٥/ ١ /٢٠٢٢م

للباحث : **عمر محمود حمدان القهيوي**

اعضاء لجنة المناقشة :

الإسم	الصفة	جهة العمل	التوقيع
أ.د. أحمد محمد اللوزي	مشرفاً	جامعة الشرق الاوسط	.....
د. محمد طه الفليح	مناقشاً داخلياً ورئيساً	جامعة الشرق الاوسط	.....
د. إسماعيل محمد الحلالمة	مناقشا داخليا	جامعة الشرق الاوسط	.....
أ.د. سيف ابراهيم المصاروة	مناقشاً خارجياً	جامعة مؤتة	.....

الشكر التقدير

بسم الله الرحمن الرحيم والحمدلله رب العالمين الذي وفقني وأعانني على إنهاء هذه الرسالة والخروج بها بهذه الصورة المتكاملة ، فبالأمس القريب بدأنا مسيرتنا التعليمية ونحن نتحسس الطريق برهبة وإرتباك ، فرأينا أن القانون هدفا ساميا وحبا وغاية تستحق السير لأجلها ، وأن بحثنا يحمل في طياته طموح شباب يحلمون أن تكون أمتهم العربية كالشامة بين الأمم.

وانطلاقا من مبدأ أنه من لا يشكر الله لا يشكر الناس ، فإنني أتوجه بالشكر **الجزيل للأستاذ الدكتور** أحمد اللوزي الذي رافقني في مسيرتي لإنجاز هذه الرسالة وكانت له بصمات واضحة من خلال توجيهاته وإنتقاداته البناءة والدعم الأكاديمي فله مني كل الاحترام والتقدير...

الإهداء

إلى من شجعني على المثابرة طوال عمري ، إلى الرجل الأبرز في حياتي
(والدي العزيز)

إلى من بها أعلو وعليها أرتكز إلى القلب المعطاء
(والدتي الحبيبة)

إلى من بذلوا جهدا في مساعدتي وكانوا خير سند
(إخواني وأخواتي)

إلى أصدقائي وزملائي ...
إلى كل من ساهم في مساندتي إلى كل هؤلاء أهدي هذا العمل ، الذي أسال الله تعالى أن يتقبله خالصا...

قائمة المحتويات

الموضوع **الصفحة**

إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية

إعداد الباحث

عمر محمود حمدان القهيوي

إشراف

الأستاذ الدكتور أحمد محمد اللوزي

الملخص

إن الثورة المعلوماتية التي لامست جميع مجالات الحياة أدت إلى ظهور نوع جديد من الجرائم عرفت باسم الجرائم الإلكترونية التي أصبح لها العديد من الآثار السلبية والملموسة في العصر الحديث ، لذلك جاءت هذه الدراسة للحديث عن إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، وتوصلت إلى نتائج عدة كان أبرزها أن القانون الأردني – بالرغم من خصوصية هذه الجرائم – لم يقرر نصوص خاصة تتعلق بإجراءات الاستدلال والتحقيق الابتدائي فيها ، وترك أمر ذلك للقواعد العامة المقررة في قانون أصول المحاكمات الجزائية الأردني لسنة 1961م ، والتي يتم إتباعها عند القيام بعملية الاستدلال والتحقيق الابتدائي في الجرائم كافة ، كما توصلت إلى أن أعضاء النيابة العامة في الأردن يواجهون العديد من الصعوبات أثناء قيامهم بالتعامل مع هذه النوعية من الجرائم ، وعليه فإن هذه الدراسة توصي المشرع الأردني بضرورة وضع قواعد خاصة تتعلق بإجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، بالإضافة إلى ضرورة إنشاء نيابة مختصة بالنظر في مثل هذا النوع من الجرائم المستحدثة بحيث يتميز أعضاؤها – علاوة على الخبرة القانونية – بالخبرة الفنية والقدرة على البحث والتحري والتحقيق في هذه الجرائم.

الكلمات المفتاحية : إجراءات – الاستدلال – التحقيق الابتدائي – الجرائم الإلكترونية

Procedures for inference and preliminary investigation of electronic crimes

Researcher preparation

Omar Mahmoud Hamdan Al-qhaiwi

Supervision

Professor Dr. Ahmad Mohammed Al-Louzi

Abstract

The information revolution that touched all areas of life led to the emergence of a new type of crime known as electronic crimes, which has many negative and tangible effects in the modern era, so this study came to talk about the procedures of inference and preliminary investigation of electronic crimes , and reached several results, the most prominent of which was that the Jordanian law-despite the - He has not decided on special texts related to the procedures of inference and preliminary investigation in them, and left this matter to the general rules established in the Jordanian code of Criminal Procedure for the year 1961, which are followed when carrying out the process of inference and preliminary investigation of all crimes, and it also concluded that the members of the public prosecution in Jordan face many difficulties while dealing with this type of crimes, and therefore this study recommends to the Jordanian legislator the need to develop special rules related to the procedures of

inference and preliminary investigation of electronic crimes, in addition to the need to establish a specialized prosecution to consider such the type of crime created so that it is characterized Its members-in addition to legal experience – have technical expertise and the ability to search, investigate and investigate these crimes.

Keywords: procedures – inference – preliminary investigation – cybercrime

الفصل الأول
خلفية الدراسة وأهميتها

المقدمة

شهد العالم تطورا هائلا وسريعا في مجال تكنولوجيا المعلومات ، حيث أدى ظهور شبكات الإنترنت والحاسب الآلي إلى جعل العالم متصلا ببعضه البعض ، وأصبح بالإمكان التواصل مع الآخرين في أي مكان بالعالم خلال لحظات معدودة ، كما ساهم هذا التطور في اعتماد كافة القطاعات والمؤسسات عليه ، حيث أصبحت تكنولوجيا المعلومات جزءا رئيسا من أجزاء المؤسسة أو المنظومة التي لا تقوم إلا بوجودها.

ولقد صاحب هذا التطور ظهور نمط جديد من الجرائم عرف باسم الجرائم الإلكترونية والتي ظهرت نتيجة للإستخدام غير المشروع لوسائل التكنولوجيا الحديثة والتي يتم إرتكابها عن طريق الإنترنت والمواقع الالكترونية ، فأصبح المجرم الإلكتروني يتواصل مع الآخرين خلف شاشة إلكترونية وبدون الإفصاح عن شخصيته الحقيقية ويقوم بابتزازهم أو النصب والاحتيال عليهم باسم وهمي وبالتالي ينتج العديد من الضحايا لمثل هذه الجرائم.

وتتميز الجرائم الإلكترونية بخصائص عديدة كسرعة وسهولة ارتكابها ، إذ أصبح المجرم الإلكتروني يحتاج إلى دقائق معدودة لارتكاب جريمته ، كما تمتاز هذه الجرائم بصعوبة إثباتها وسرعة محو الدليل الالكتروني فيها ، إذ يواجه المحقق في الجريمة الإلكترونية العديد من الصعوبات للحصول على الأدلة ويحتاج أحيانا للوقت والجهد الهائل لفحص الآلاف من الصفحات التي تحتوي على البيانات والمعلومات التي تحتوي على الدليل الإلكتروني اللازم لإدانة الجاني في الجريمة.

ولا تقتصر الصعوبات التي يواجهها رجال التحقيق على ذلك فحسب ، وإنما يعاني المحقق من صعوبات خاصة بإجراءات الاستدلال والتحقيق الابتدائي خاصة فيما يتعلق بإجراءات التفتيش للكيانات المادية والمعنوية للحاسب الآلي ، وسوف نتناول في دراستنا هذه مفهوم الجريمة الإلكترونية ، وخصائصها ، والطبيعة القانونية لها ، بالإضافة إلى إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، والصعوبات التي تواجه المحققين في هذا المجال.

مشكلة الدراسة

تكمن مشكلة الدراسة في مرحلة جمع الأدلة حول الجريمة الإلكترونية ، إذ توجد صعوبات عديدة تواجه السلطات المختصة عند القيام بإجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وخاصة في إجراء التفتيش ، وذلك عند قيامهم بتفتيش مكونات الحاسب الآلي ، فلا توجد صعوبة عند القيام بتفتيش المكونات المادية لجهاز الحاسب الآلي ، ولكن تثور المشكلة عند الحاجة لامتداد التفتيش لمكونات الحاسب المعنوية كالبيانات والمعلومات المخزنة فيه لإيجاد الدليل الإلكتروني الذي يختلف بطبيعته عن الدليل المادي الذي يتم ضبطه في الجرائم التقليدية.

كما تظهر مشكلة الدراسة بوضوح في أن المشرع الأردني لم ينص على إجراءات خاصة للاستدلال والتحقيق الابتدائي في الجرائم الالكترونية ، وترك ذلك للقواعد العامة في قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م.

أهداف الدراسة

تهدف هذه الدراسة إلى التعرف على إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، والصعوبات التي تواجه السلطات المختصة أثناء قيامها بهذه الإجراءات ، كما وتهدف هذه الدراسة إلى ما يلي:

- بيان مدى جواز تفتيش المكونات المعنوية للحاسب الآلي لضبط الأدلة منها.

- التعرف على مدى قدرة النصوص الجزائية على مسايرة التطور الحديث.
- بيان مدى خضوع الأجهزة المتصلة بجهاز المتهم للتفتيش وذلك فيما إذا كان جهاز المتهم متصلا بجهاز آخر داخل إقليم الدولة أو خارجها.
- بيان مفهوم الشاهد الإلكتروني والالتزامات المترتبة عليه.
- بيان مفهوم الخبير والخبرة الفنية في الجرائم الإلكترونية وأهم شروطها.

أهمية الدراسة

وتظهر أهمية هذه الدراسة في تناول نوع جديد من الجرائم ألا وهو الجرائم الإلكترونية والتي تختلف عن الجرائم التقليدية من حيث اكتشافها ، والتحقيق بها ، وكيفية إثباتها ؛ نظرا لما لها من طبيعة خاصة تميزها عن الجرائم التقليدية ، إذ لم تعد وسائل التحقيق التقليدية تتناسب مع هذا النوع من الجرائم ، وأصبحت الحاجة لاتباع إجراءات حديثة لمواجهة هذه الجرائم المستحدثة ، كما تبرز أهمية هذه الدراسة من الأهمية التي يوليها العالم لهذا النوع من الجرائم من خلال عقد المؤتمرات والإتفاقيات الدولية التي تصب جل اهتمامها على كيفية مواجهة الجريمة الإلكترونية والحد منها.

ويمكن أن تتمثل أهمية هذه الدراسة في النقاط التالية:

- الاهتمام بالجريمة الإلكترونية التي تشكل خطرا على حقوق الانسان والتي نصت كافة الدول في أنظمتها على صيانتها ، واحترامها ، والاهتمام بها.
- البحث في الإجراءات المتبعة للاستدلال والتحقيق في الجرائم الإلكترونية ، ومعرفة الصعوبات التي تواجه رجال التحقيق أثناء قيامهم بتلك الإجراءات ، والسعي لإيجاد الحلول اللازمة لتجاوز تلك العقبات.

أسئلة الدراسة

هناك عددا من التساؤلات التي تثيرها هذه الدراسة منها :

- ما مدى جواز تفتيش المكونات المعنوية للحاسب الآلي لضبط الأدلة منها ؟
- هل النصوص الجزائية التقليدية قادرة على مسايرة التطور الحديث ؟
- هل يجوز إجبار المتهم على الإفصاح عن كلمة السر ليتمكن المحقق من الوصول إلى الأدلة المحتملة على الجهاز ؟
- في حالة اتصال جهاز المتهم بجهاز آخر داخل إقليم الدولة فهل يمتد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم ؟
- من هو الشاهد الإلكتروني وما هي الالتزامات المترتبة عليه ؟

مصطلحات الدراسة

- **شبكة الانترنت**

طريقة يتم من خلالها توصيل جهاز الحاسوب الخاص بالفرد بأي جهاز حاسوب آخر من جميع أنحاء العالم عبر أجهزة الراوتر والخوادم المخصصة[1].

- **الحاسب الآلي**

جهاز إلكتروني حديث ، قادر على تخزين البيانات ضمن وحدات التخزين المتعددة ، أو مجموعة من الوحدات الإلكترونية لتقديم العديد من الخدمات في شتى المجالات الطبية والعلمية والهندسية والتكنولوجية ، بالإضافة لتلبية الاحتياجات الشخصية ، مثل كتابة وتحرير المستندات

[1] Internet " www.businessdictionary.com "

وتصفح الانترنت وعرض الصور ومقاطع الفيديو وغيرها ، وجميع هذه العمليات التي يقوم بها الحاسب مبنية على نظام التشغيل (Operating system) الذي يشكل أساس عمل الحاسوب[1].

- **مرحلة الاستدلال**

هي مجموعة من الإجراءات التمهيدية السابقة على تحريك الدعوى الجنائية تهدف إلى جمع المعلومات في شأن جريمة ارتكبت كي تتخذ سلطات التحقيق بناء عليها القرار فيما إذا كان من الجائز – أو من الملائم – تحريك الدعوى الجنائية[2].

- **الإجراءات**

سلسلة الأعمال والخطوات والمراحل التي يجب إتباعها لتنفيذ عمل ما[3].

- **التحقيق الابتدائي**

هو مجموعة من الإجراءات التي تجري بمعرفة سلطة معينة ، وتستهدف التنقيب عن الأدلة بشأن جريمة قد ارتكبت ، ثم تقدير مدى كفاية هذه الأدلة لإحالة المتهم إلى المحاكمة[4].

---

[1] Computer من موقع : www.techopedia.com

[2] https://lawyeregypt.net

[3] https://portal.arid.my

[4] حسني ، محمود نجيب (1988) . **شرح قانون الإجراءات الجنائية** . القاهرة : دار النهضة العربية ، ص6.

الدراسات السابقة

1. التحقيق في الجريمة المعلوماتية لنور الهدى السوفي :

وهذه الدراسة عبارة عن رسالة مقدمة لنيل درجة الماجستير في القانون من كلية الحقوق والعلوم السياسية في جامعة قاصدي مرباح بالجزائر عام 2017م ، تحت إشراف الدكتور رضا هميسي.

قسمت هذه الدراسة إلى فصلين مستقلين ، بحيث تناولت الباحثة في الأول منهما ماهية التحقيق في الجريمة المعلوماتية من حيث مفهوم التحقيق في الجريمة المعلوماتية ، والجهة القائمة بالتحقيق فيها ، أما الفصل الثاني فخصص للحديث عن آليات التحقيق في الجريمة المعلوماتية ، وذلك من خلال بيان القواعد الاجرائية العامة والخاصة للتحقيق في الجريمة المعلوماتية.

وما استفاده الباحث من هذه الدراسة هو الاطلاع على القواعد الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية ، وعليه فإن ما سيضيفه الباحث هو دراسة تحليلية بخصوص الإجراءات المتعلقة بمرحلتي الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية.

2. الإجراءات الجزائية الخاصة بالجرائم الإلكترونية في التشريعين الوطني والدولي لتمام محمد أحمد بني فواز:

وهذه الدراسة عبارة عن رسالة مقدمة لنيل درجة الماجستير في القانون من كلية الحقوق في جامعة اليرموك بالأردن عام 2022م ، تحت إشراف الدكتورة ديالا علي الطعاني.

وقسمت هذه الدراسة إلى فصلين مستقلين ، بحيث تناولت الباحثة في الأول منهما إجراءات التحقيق في الجرائم الالكترونية ، وذلك من خلال بيان إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، أما الفصل الثاني فخصص للحديث عن المعوقات التي تواجه إجراءات التحقيق في الجرائم الإلكترونية ، والجهود الدولية المبذولة لمكافحة تلك الجريمة.

وما استفاده الباحث من هذه الدراسة هو التعرف على الإجراءات المتبعة للاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، والمعوقات التي تواجه تلك الإجراءات ، وما سيضيفه الباحث هو دراسة تحليلية بخصوص الإجراءات المتعلقة بمرحلتي الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية.

3. التحقيق الجنائي في الجرائم الإلكترونية لجمال إبراهيمي:

وهذه الدراسة عبارة عن أطروحة لنيل درجة الدكتوراة في العلوم (تخصص القانون) من كلية الحقوق والعلوم السياسية قسم الحقوق في جامعة مولود معمري (الجزائر) عام 2018م ، تحت إشراف الدكتور إقلولي محمد.

وقسمت هذه الدراسة إلى بابين ، بحيث تناول الباحث في الباب الأول منهما الحديث عن آليات التحقيق في الجرائم الالكترونية ، وذلك من خلال فصلين مستقلين تحدث في الأول منهما عن إجراءات التحقيق في الجرائم الإلكترونية من حيث محدودية سريان إجراءات التحقيق المألوفة على الجرائم الإلكترونية والإجراءات المستحدثة للتحقيق فيها ، أما الفصل الثاني فخصصه للحديث عن القيمة الثبوتية للدليل الالكتروني وأثرها على تكوين قناعة القاضي الجزائي ، وذلك من خلال الحديث عن الطبيعة القانونية للدليل الإلكتروني ومدى قبوله من قبل القاضي الجزائي.

وتناول الباحث في الباب الثاني من هذه الدراسة الحديث عن عقبات التحقيق الجنائي في الجرائم الإلكترونية ، والنتائج المترتبة عليها ، والحلول المقترحة لتجاوز تلك العقبات.

وقد استفاد الباحث من هذه الدراسة الاطلاع على الصعوبات والعقبات التي تثيرها الجريمة الإلكترونية ، والحلول المقترحة لتجاوزها ، والتي تناولها الباحث في بحثه ، وما سيضيفه الباحث في هذا البحث ، هو دراسة تحليلية بخصوص الإجراءات المتعلقة بمرحلتي الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية.

منهج الدراسة

نظرا لما تحتاجه الجرائم الإلكترونية من بحث وتحليل لموضوعاتها كونها من الجرائم المستحدثة ، فقد تم الاعتماد في دراستنا هذه على المنهج الوصفي التحليلي ، حيث تم وصف الجريمة الإلكترونية ، وبيان خصائصها ، بالإضافة إلى بيان إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية بشيء من التفصيل.

الفصل الثاني

ماهية الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية

لقد شهد العالم تطورا هائلا وسريعا في العديد من المجالات ، لاسيما التطور الحاصل في تكنولوجيا المعلومات والمتمثل بظهور الهواتف الذكية والحواسيب ، وظهور ما يعرف بالشبكة المعلوماتية وغيرها من الوسائل التكنولوجية الحديثة.

وهذا التطور الهائل الذي ظهر في العالم أجمع بخصوص التكنولوجيا ، والذي أدى إلى تطور مختلف مجالات ونواحي الحياة ، صاحبه تطور في عالم الجريمة ، حيث ظهرت جرائم لم تكن موجودة من قبل وأهم هذه الجرائم هي الجريمة الإلكترونية.

وسنتناول في هذا الفصل ماهية الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، وذلك من خلال مباحث ثلاث على النحو التالي:

المبحث الأول : ماهية الجريمة الإلكترونية

المبحث الثاني : ماهية الاستدلال في الجرائم الإلكترونية

المبحث الثالث : ماهية التحقيق الابتدائي في الجرائم الإلكترونية

المبحث الأول

ماهية الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة التي يتميز بها العصر الحديث ، والتي تشكل خطرا على الأفراد والمجتمعات لما تتميز به من خصائص ، وفي هذا المبحث سنتناول تعريف الجريمة الإلكترونية وذلك في المطلب الأول , وفي المطلب الثاني نذكر خصائص الجريمة الإلكترونية ، أما المطلب الثالث فنبين فيه الطبيعة القانونية للجريمة الإلكترونية.

المطلب الأول

تعريف الجريمة الإلكترونية

لم يستقر الفقه على وضع تعريف محدد للجريمة الالكترونية ، وذلك بسبب التطور الدائم لها ولقد انقسم الفقه في تعريف الجريمة الإلكترونية إلى عدة اتجاهات ومنها :

الاتجاه الأول : يعرف الجريمة الإلكترونية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحول عن طريقه"[1].

ويعرفها أصحاب هذا الاتجاه أيضا بأنها "الاستخدام غير المشروع للحاسبات والتي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية"[2].

الاتجاه الثاني : ويعرف الجريمة الإلكترونية بأنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا"[3].

---

[1] رستم ، هشام محمد فريد (1992) . **قانون العقوبات " مخاطر تقنية المعلومات "** . مصر : مكتبة الآلات الحديثة بأسيوط ، ص31.

[2] حجازي ، عبدالفتاح بيومي (2006) . **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي** . ط1 ، الاسكندرية : دار الفكر الجامعي ، ص21.

[3] الشواء ، سامي (1993) . "الغش المعلوماتي كظاهرة إجرامية مستحدثة" ، **مؤتمر الجمعية المصرية للقانون الجنائي ، 25-28 أكتوبر ، القاهرة ، ص516.**

الاتجاه الثالث: ويعرفها بأنها " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي"[1].

ونجد أن أصحاب الاتجاه الأول قد اعتمدوا معيار موضوع الجريمة في تعريفهم للجريمة الإلكترونية والتي تقع على الحاسب أو نظامه , أما أصحاب الاتجاه الثاني فاعتمدوا في تعريفهم للجريمة الإلكترونية على المعرفة بتقنية المعلومات ، في حين اعتمد أصحاب الاتجاه الثالث على معيار الوسيلة المستخدمة في ارتكاب الجريمة.

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[2].

كما عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا سنة 2000م ، الجريمة المعلوماتية بأنها " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية , أو داخل نظام حاسوب , والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية "[3].

وقد عرفت منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة الجريمة الإلكترونية بأنها : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الإلكترونية"[4].

---

[1] ابراهيم ، راشد بشير (2008) . "التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة ابوظبي" ، **مجلة دراسات إستراتيجية** ، العدد (131) ، ص23.

[2] عياد ، سامي علي حامد (2007) . **الجريمة المعلوماتية وإجرام الانترنت** . مصر : دار الفكر الجامعي ، ص38.

[3] المناعسة ، أسامة احمد (2001) . **جرائم الحاسب الآلي والانترنت** . ط1 ، الأردن : دار وائل ، ص77.

[4] عبابنة ، محمد أحمد (2005) . **جرائم الحاسوب وأبعادها الدولية** . ط1 ، عمان : دار الثقافة ، ص17.

ومن خلال دراستنا للتعريف نجد أن المشرع الأردني لم يورد أي تعريف للجريمة الإلكترونية ، لذلك يرى الباحث أنه وبالرغم من أن وضع تعريف للجريمة الإلكترونية ليس من مهمة المشرع ، إلا أنه يقع على عاتقه وضع تعريف خاص بها ؛ كونها من الجرائم المستحدثة ، وذلك لتمهيد الطريق أمام السلطات المختصة في تطبيق القانون.

المطلب الثاني
خصائص الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية من الجرائم المستحدثة ، والتي تتميز بطابع خاص يميزها عن الجرائم التقليدية ، فهذه الجرائم لا عنف فيها ولا وجود لأي آثار للدماء ، أو القتلى والجرحى كما في جرائم القتل والإيذاء ، فهي لاتترك أي أثر من الآثار التي تخلفها الجرائم التقليدية ؛ وسبب ذلك يرجع إلى أنها ترتكب في الخفاء بعيدا عن الأنظار ، ولقدرة الجاني على إتلاف أي دليل قد يعد سببا لاكتشاف جريمته في لحظات قصيرة.

فالتطور التكنولوجي الهائل الذي لامس جميع مجالات ونواحي الحياة ، أتاح المجال للمجرم الإلكتروني القيام بأعماله الجرمية بطريقة أسهل وأيسر وأقل خطرا ، كما وفر له هذا التطور القدرة على محو الأدلة التي من الممكن أن تكون سببا لإدانته ، الأمر الذي أدى إلى صعوبة اكتشاف مثل هذه الجرائم ، وجميع هذه الإمكانيات المتاحة للمجرم الإلكتروني نتيجة التطور التكنولوجي ترجع إلى الخصائص التي تمتاز بها هذه الجرائم ومن تلك الخصائص ما يلي :-

أولا : جرائم عابرة للحدود (ذات بعد دولي)

تعد هذه الجرائم ذات طابع دولي ، حيث أن الجريمة يمكن ارتكابها في دولة ما ويكون تأثيرها الجرمي في دولة أخرى ، ويظهر ذلك بوضوح في الجرائم المرتكبة بوساطة الشبكات الإلكترونية بمختلف أنواعها كالانترنت ، وشبكات الاتصالات الدولية[1].

فيرى الباحث أن الحدود الدولية أصبحت اليوم وكأنها غير موجودة أمام الجرائم الإلكترونية ، إذ بإمكان المجرم الإلكتروني أن يقوم بارتكاب جريمته أو سرقة المعلومات ، ونقلها ، وتبادلها

---

[1] الفقي ، عمرو عيسى (2006) . **الجرائم المعلوماتية** . الاسكندرية : المكتب الجامعي الحديث ، ص32.

عن بعد دون التأثر بالحدود الدولية ، كما أصبح بالإمكان القيام بالفعل الجرمي في دولة ما ، وتحقق النتيجة الجرمية في دولة أخرى.

ثانيا : سهولة وسرعة تنفيذها

تعتبر الجرائم الإلكترونية من الجرائم التي لا تتطلب شدة أو عنف لتنفيذها أو مجهودا كبيرا ، فهي تنفذ بوقت وجهد أقل من الجهد المبذول في ارتكاب الجرائم التقليدية ، إذ لا تحتاج إلى استخدام القوة العضلية كما في جرائم الإيذاء والقتل ، أو الحاجة إلى استخدام أدوات للكسر والخلع كما في جرائم السرقة [1]، وغيرها الكثير من الجرائم التي تحتاج لجهد أكبر لاستخدامها مقارنة بالجرائم الإلكترونية التي لا تحتاج أحيانا إلا لخطوات بسيطة عبر جهاز الحاسوب لارتكابها وبسرعة عالية جدا.

ثالثا : جرائم ناعمة

تتميز الجرائم الإلكترونية بأنها جرائم ناعمة ؛ وذلك لأنها لا تحتاج للعنف والشدة في ارتكابها ، وإنما للضغط على مجموعة من الأزرار الخاصة بجهاز الحاسوب مع الاستعانة ببعض البرامج التي تساعد المجرم على ارتكاب جريمته[2].

بالإضافة إلى أن الجاني قد يقوم بجريمته بشكل غير ملحوظ لتمتعه بالقدرات الفنية التي تمكنه من ارتكاب جريمته بدقة ، بحيث لا يستطيع المجني عليه ملاحظة ذلك ، ومن الأمثلة على

---

[1] المسند ، صالح بن محمد ، والمهيني عبدالرحمن بن راشد (2013) . "جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات" ، **المجلة العربية للدراسات الأمنية والتدريب** ، المجلد 29 ، العدد (15).

[2] رستم ، هشام محمد فريد (1994) . **الجوانب الإجرائية للجرائم المعلوماتية** . أسيوط : دار النهضة العربية ، ص16.

ذلك قيام الجاني بإرسال فيروسات إلى جهاز المجني عليه أو سرقة بياناته والتجسس عليه دون علمه[1].

رابعا : عدم لجوء ضحايا الجريمة الإلكترونية للقضاء

إن معظم الضحايا في الجرائم الإلكترونية لا يلجؤون للقضاء من أجل تقديم الشكاوى ؛ ويرجع السبب في ذلك أحيانا إلى خوفهم من التعرض للتشهير عبر مواقع التواصل الاجتماعي[2]، خاصة فيما إذا كانوا متعرضين لجرائم الابتزاز الإلكتروني ، لذلك نجد أن معظم جرائم الابتزاز الإلكتروني وغيرها من الجرائم الماسة بسمعة المجني عليه لا تكتشف إلا بعد وقت طويل من ارتكابها.

خامسا : تستخدم الأجهزة الذكية في ارتكابها

تعتبر الأجهزة الإلكترونية الذكية بمختلف أنواعها من أجهزة حاسوب ، وهواتف محمولة ، وأجهزة لابتوب ، من وسائل ارتكاب الجريمة الإلكترونية ؛ كونها تحتوي على شبكة الانترنت ، وأنظمة المعلومات ، وعليه فإن لتلك الأجهزة دور بارز في ارتكاب الجريمة الإلكترونية ويتمثل بالأدوار الثلاثة التالية[3]:

- قد تكون تلك الأجهزة الذكية هدفا للجريمة الإلكترونية ، بمعنى أن الجريمة تقع على الجهاز من أجل الحصول على البيانات والمعلومات المخزنة بداخله ، أو إتلافها ، وذلك عن طريق الدخول الغير مشروع لنظام الجهاز المستهدف.

---

[1] بلواضح ، الطيب (2020) . **الجريمة في الفضاء الإلكتروني** . ط1 ، عمان : دار وائل للنشر والتوزيع ، ص41-42.

[2] يوسف ، اميرة فرج (2011) . "الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت" ، ص157.

[3] الشريم ، صالح خميس راشد يوسف (2020) . **الإطار القانوني لوسائل البحث والتحري عن الجرائم الإلكترونية** . (رسالة ماجستير) ، جامعة عمان الأهلية ، عمان ، الأردن ، ص25-26.

- قد تكون تلك الأجهزة وسيلة أساسية يتم ارتكاب الجريمة الإلكترونية من خلالها ، بحيث تكون تلك الأجهزة أداة لارتكاب الجريمة الإلكترونية ، ومن الأمثلة على ذلك ، جريمة الاحتيال الإلكتروني ، واحتيال نظام الاتصالات والصراف الآلي.
- قد يكون لتلك الأجهزة دورا ثانويا في الجريمة الالكترونية ، وذلك من خلال استخدامها كوسيلة ثانوية في ارتكاب الجريمة الإلكترونية ، بمعنى أن الجريمة الإلكترونية كان من الممكن ارتكابها بوسيلة أخرى ولكن وقع الاختيار على أحد هذه الأجهزة ليتم تنفيذها من خلاله ، كجريمة غسل الأموال ، وجرائم إباحية الأطفال.

لذلك يرى الباحث أن بعض هذه الخصائص التي تتميز بها الجرائم الإلكترونية عن غيرها من الجرائم التقليدية ، قد تعتبر عوائق وصعوبات أمام اكتشاف رجال الضابطة العدلية لهذه الجرائم أثناء قيامهم بعملهم.

المطلب الثالث

الطبيعة القانونية للجريمة الإلكترونية

إن حديثنا عن الطبيعة القانونية للجريمة الإلكترونية يقودنا للحديث عن الوضع القانوني للبرامج والمعلومات ، فهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأي طريقة كانت ؟

تباينت الآراء والاتجاهات حول تحديد الطبيعة القانونية للجريمة الإلكترونية ، إذ يرى الاتجاه الأول أن الأشياء المادية فقط هي التي تعتبر قابلة للحيازة والاستحواذ عليها ، وأن الأشياء يجب ان يكون لها كيان مادي ملموس حتى يستطيع الآخرين من الاستحواذ عليها ، وبما أن البرامج والمعلومات تعتبر من الأشياء الغير محسوسة ، فإنه لا يمكن حيازتها أو الاستحواذ عليها إلا إذا كانت مخزنة على أسطوانة ، أو شريط ممغنط ، أو أي أداة تخزين أخرى.[1]

أما الاتجاه الثاني فيرى أن البيانات والمعلومات المخزنة على جهاز الحاسوب تمتلك قيمة إقتصادية ، بالتالي فهي تقبل الحيازة والاستحواذ عليها ، وكما يقول الأستاذان "Catala و Vivant" في مؤلفاتهم بوجود علاقة تبني بين الشيء ومالكه ، وأن ذلك ينطبق على العلاقة بين المعلومات ومالكها ، وبالتالي فإن المعلومات عبارة عن مال يقبل الحيازة والاستحواذ عليه ، وذلك بناءا على قيمته الاقتصادية بغض النظر عن طبيعته المادية.[2]

وهناك من يرى وجوب التفرقة بين أدوات الحاسب الآلي التي لها قيمة مالية بصفتها المادية ، كوحدة الإدخال ، ووحدة العرض البصري ، وبين الوسائل المستخدمة في حفظ بيانات

---

[1] المطردي ، مفتاح بوبكر (2012) . "الجريمة الإلكترونية" ، **المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان ، ص17.**

[2] سلامة ، محمد عبدالله (2007) . **موسوعة الجرائم المعلوماتية** . ط1 ، مصر : المكتب العربي الحديث ، ص43-44.

ومعلومات الحاسب الآلي ، والتي تكون قيمتها المالية الحقيقية بما تحتويه من مضمون معنوي ، كالشريط الممغنط ، أو الأسطوانة الممغنطة وغيرها من الوسائل ، بالتالي فإنه من المنطق القول أنه عند حدوث سرقة لإحدى هذه الوسائل مثلا ، فإن السرقة تكون لما هو مسجل على تلك الوسائل من بيانات ومعلومات لا من أجل أداة التخزين كالشريط ، أو الأسطوانة الممغنطة .[1]

إن التحليل المنطقي يرفض الأخذ بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي للبرامج والمعلومات ، وأنها لا يمكن أن تكون شيئا ملموسا محسوسا ، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه بتشغيل جهاز الحاسوب ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من جهاز الحاسوب إلى ذهن المتلقي ، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقته ، وبالتالي لها كيان مادي يمكن الاستحواذ عليه (البرامج والمعلومات) ، وطالما أن موضوع الحيازة (أي المعلومات) غير مادي ، فإن واقعة الحيازة تكون من نفس الطبيعة أي غير مادية (ذهنية) ، وبالتالي يمكن حيازة المعلومات بواسطة الالتقاط الذهني عن طريق البصر.[2]

---

[1] الزعبي ، جلال محمد ، والمناعسة ، أسامة (2013) . **جرائم تقنية نظم المعلومات الإلكترونية** ، ط1 . الأردن : دار الثقافة للنشر والتوزيع ، ص36-37.

[2] قشقوش ، هدى حامد (1992) . **جرائم الحاسب الإلكتروني في التشريع المقارن** . القاهرة : دار النهضة العربية ، ص51-52.

المبحث الثاني

ماهية الاستدلال في الجرائم الإلكترونية

تمر الإجراءات الجزائية التي يقوم بها رجال الضابطة العدلية عند وقوع جريمة ما بمجموعة من المراحل منها مرحلة جمع الأدلة والتي تعرف بمرحلة الاستدلال ، إذ تعتبر هذه المرحلة من المراحل المهمة التي تمر بها الدعوى الجزائية ، وسنتناول في هذا المبحث مفهوم الاستدلال في الجرائم الإلكترونية وذلك في المطلب الأول ، وفي المطلب الثاني شروط إجراءات الاستدلال في الجرائم الالكترونية.

المطلب الأول

مفهوم الاستدلال في الجرائم الإلكترونية

تعددت آراء الفقهاء في تعريفهم لإجراءات الاستدلال في الجرائم الإلكترونية ، حيث عرفت مرحلة التحري والاستدلال على أنها " إجراءات تمهيدية لإجراء الخصومة الجنائية ومستمرة بعدها وضرورة لازمة لتجميع الآثار والأدلة والمعلومات بهدف إزالة الغموض والملابسات المحيطة بالجريمة وملاحقة مرتكبيها"[1]

وعرفت أيضا بأنها " مجموعة من الإجراءات الجوهرية غير المنظورة يتوخى فيها مأمور الضبط القضائي أو مرؤوسهم الصدق والدقة في التنقيب عن الحقائق المتعلقة لموضوع معين واستخراجها من مكمنها في إطار القانون.[2]

أما بالنسبة للشخص القائم بمهمة البحث والتحري عن الجرائم الإلكترونية ، فنلاحظ أن المشرع الأردني قد عالج ذلك في مواده القانونية من خلال النص صراحة في الفقرة الأولى من

---

[1] محدة ، محمد (1991-1992) . **ضمانات المشتبه فيه أثناء التحريات الأولية** . ط2 ، الجزائر : دار الهدى ، ص22.

[2] مرسي ، عبد الواحد إمام . **الموسوعة الذهبية في التحريات** . مصر : دار المعارف والمكاتب الكبرى للنشر والتوزيع ، ص66.

المادة الثامنة من قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م[1]على أن مهمة البحث والتحري والاستقصاء عن الجرائم والقبض على الفاعلين تناط برجال الضابطة العدلية.

ومن خلال التعريفات السابقة يرى الباحث أن الاستدلال هو عبارة عن مجموعة من الإجراءات ، يقوم بها أعضاء الضبط القضائي بعد ارتكاب الجريمة ، وتهدف إلى جمع الأدلة اللازمة للوصول للحقيقة.

[1] المادة (1/8) "موظفو الضابطة العدلية مكلفون باستقصاء الجرائم وجمع الاستدلالات والأدلة المادية والقبض على فاعليها وإحالتهم على المحاكم الموكول إليها أمر معاقبتهم".

المطلب الثاني

شروط إجراءات الاستدلال في الجرائم الإلكترونية

ويشترط في الاستدلال مجموعة من الشروط لضمان سلامة الإجراءات وعدم بطلانها ومن هذه الشروط ما يلي[1]:

1. أن تتعلق إجراءات الاستدلال بجريمة قد وقعت فعلا ، إذ يعتبر الإذن بمباشرة إجراءات الاستدلال باطلا فيما لو صدر تمهيدا لضبط جريمة محتملة الوقوع.
2. يجب أن تكون مرحلة جمع الأدلة ضمن إطار مشروع ومتفق مع القانون.
3. أن يتقيد مأمور الضبط القضائي بقواعد الاختصاص النوعي والمكاني ، فيجب أن يتقيد مأمور الضبط القضائي بقواعد الاختصاص النوعي ، ومعنى ذلك أنه لا يجوز لمأموري الضبط ذوي الاختصاص النوعي الخاص أن يقوموا بإجراءات التحري بصدد جريمة أخرى غير تلك المتعلقة بأعمال وظائفهم ولو في دوائر اختصاصهم[2]، بالإضافة إلى التقيد بالاختصاص المكاني من حيث مكان وقوع الجريمة ، ومكان القبض على المتهم إذ لا يجوز تجاوز الاختصاص المكاني تحت طائلة بطلان الإجراءات.
4. أن تكون إجراءات الاستدلال المتبعة بشأن الجريمة ذاتها لا بشأن جريمة أخرى ، مهما كانت الصلة بينهما ، فيجب أن يكون لكل جريمة إجراءات استدلال خاصة بها.

---

[1] قادري ، سارة (2014) . **أساليب التحري الخاصة في قانون الإجراءات الجزائية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر ، ص16-17.

[2] فاروق ، ياسر الأمير (2009) . **مراقبة الأحاديث الخاصة في الإجراءات الجنائية** . ط1 ، جامعة القاهرة : دار المطبوعات الجامعية ، ص403.

المبحث الثالث

ماهية التحقيق الابتدائي في الجرائم الإلكترونية

بعد الانتهاء من مرحلة جمع الاستدلالات يتم الانتقال إلى مرحلة التحقيق الابتدائي في الجريمة الإلكترونية ، ولبيان ماهية التحقيق الابتدائي في الجرائم الإلكترونية تم تقسيم هذا المبحث إلى مطلبين ، بحيث تناولنا في الأول منهما مفهوم التحقيق الابتدائي في الجرائم الإلكترونية ، وفي المطلب الثاني العناصر الأساسية للتحقيق الابتدائي في الجرائم الإلكترونية.

المطلب الأول

مفهوم التحقيق الابتدائي في الجرائم الإلكترونية

يعرف التحقيق إصطلاحا على أنه :" الجهد المبذول لكشف غموض الجرائم وتحديد شخصية مرتكبيها وإثبات التهمة عليهم بما يقدم من أدلة إثبات وهو العلم الذي يوضح الوسائل الفنية التي على هداها يمارس العاملون في حقل مكافحة الجريمة وضبطها وتحقيقها اختصاصاتهم التي خولها لهم القانون عند وقوع الجريمة وتصديهم لمواجهتها".[1]

ولقد تعددت التعريفات حول مفهوم التحقيق الابتدائي في الجرائم الإلكترونية وتنوعت حيث يعرف " بأنه عمل قانوني يقوم به المختصون في ضبط الجرائم المعلوماتية من فاعل ودليل إلكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذا النوع من الجرائم لإقامة العدل"[2].

---

[1] القحطاني ، عبدالله بن حسين الجراف (2014) . **تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية** . (رسالة ماجستير) ، جامعة نايف للعلوم الأمنية ، الرياض ، ص12-13.

[2] موسى ، مصطفى محمد (2009) . **التحقيق الجنائي في الجرائم الإلكترونية** . ط1 ، القاهرة : مطابع الشرطة ، ص166.

كما عرف بأنه " مجموعة من الإجراءات القضائية التي تباشر عند وقوع جريمة ، وتختص باتخاذها سلطة معينة هي النيابة العامة ، بهدف الكشف عن الحقيقة في جريمة قد وقعت ، لإتخاذ الإجراء المقتضى قانونا في مثل هذه الأحوال"[1].

[1] الجوخدار ، حسن (2008) . **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية ، دراسة مقارنة** . الأردن : دار الثقافة للنشر والتوزيع ، ص11.

المطلب الثاني

العناصر الأساسية للتحقيق الابتدائي في الجرائم الإلكترونية

هناك مجموعة من الإجراءات التي يجب الالتزام بها عند القيام بالتحقيق الابتدائي في الجرائم الإلكترونية ، ومن هذه الإجراءات ما يكون قبل البدء بالتحقيق الابتدائي ، ومنها ما يكون أثناء القيام به.

أولا : الإجراءات التي يجب الالتزام بها قبل البدء بالتحقيق الابتدائي في الجرائم الإلكترونية

هناك مجموعة من الإجراءات التي يجب الالتزام بها قبل البدء بالتحقيق ومنها[1]:

1. فصل التيار الكهربائي عن مكان جمع الاستدلالات لمنع الجاني من قيامه بمحو أدلة الجريمة.
2. الحصول على كلمات المرور الخاصة بأجهزة الحاسب الآلي من الموظفين ، ومن ثم إبعادهم عن تلك الأجهزة.
3. الأخذ بعين الإعتبار صعوبة بقاء الدليل على أجهزة الحاسب الآلي لمدة طويلة ، لذا يجب القيام بإجراءات التحقيق الابتدائي بأقصى سرعة ممكنة للحصول على الأدلة اللازمة قبل ضياعها.

ثانيا : الإجراءات التي يجب مراعاتها أثناء التحقيق الابتدائي في الجرائم الإلكترونية

يقع على عاتق الجهات المختصة بالتحقيق عند البدء بالتحقيق الابتدائي في الجرائم الإلكترونية مراعاة ما يلي[2]:

---

[1] السوفي ، نور الهدى (2017) . **التحقيق في الجريمة المعلوماتية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر ، ص14.

[2] سعيداني ، نعيم (2013) . **آليات البحث والتحري عن الجرائم المعلوماتية** . (رسالة ماجستير) ، جامعة الحاج لخضر ، ص113-114.

1. القيام بفحص البرامج الموجودة على أجهزة الحاسب الآلي كالبرامج الحسابية التي من الممكن أن تكون قد استخدمت في جريمة الاختلاس المعلوماتي.
2. إنشاء نسخة إحتياطية من الأقراص الصلبة أو الأسطوانية المرنة قبل القيام بإستخدامها ، بالإضافة إلى التأكد من دقة النسخ.
3. حفظ الأجهزة الحاسوبية والمعدات التي يتم ضبطها بطريقة فنية وصحيحة.

ونلاحظ أن المشرع الأردني في الفقرتين (أ) و (ب) من المادة 13 من قانون الجرائم الإلكترونية لسنة 2015م[1]، قد سمح لرجال الضابطة العدلية بعد الحصول على الإذن من الجهات الرسمية ، الدخول لأي مكان تشير الأدلة لاستخدامه بارتكاب أي من الجرائم ، وتفتيشه ، وضبط الأجهزة والبرامج وغيرها من الوسائل المستخدمة في ارتكابها.

[1] المادة (13/أ) "مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية ، يجوز لموظفي الضابطة العدلية ، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة ، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم ، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص".

(13/ب) "مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة ، وبإستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها".

الفصل الثالث

إجراءات الاستدلال في الجرائم الإلكترونية

تعد مرحلة الاستدلال من المراحل التمهيدية للدعوى الجنائية ، وبالإضافة إلى ذلك فهي تتصل مباشرة بحرية الفرد وحقه في الحياة بأمان بعيدا عن أي اعتداءات من قبل السلطات العامة ، كما وتعد هذه المرحلة من إجراءات العدالة الجنائية الهامة والأكثر حساسية وخطورة ، كونها تعتبر بداية الطريق أمام تحقيق العدالة الجنائية وحماية حقوق الأفراد في المجتمعات ، والسبيل لمكافحة الجرائم بمختلف أنواعها , كما وتعتبر هذه المرحلة من أهم المقاييس التي تبين كفاءة رجالات الأجهزة الأمنية وقدرتهم على تحقيق الأمن والأمان ومكافحة الجريمة والحد منها , وضبط مرتكبيها وتقديمهم للمحاكم المختصة.[1]

وسنتناول في هذا الفصل إجراءات الاستدلال في الجرائم الإلكترونية ، وذلك من خلال مبحثين مستقلين على النحو التالي:

المبحث الأول : تلقي البلاغ والمعاينة في الجرائم الإلكترونية

المبحث الثاني : وسائل جمع الأدلة في الجريمة الإلكترونية

[1] محمد ، محمد نصر (2012) . "التحقيق الجنائي بين الواقع والقانون دراسة تطبيقية على أنواع البصمات وحجتها" ، المجلد 21 ، العدد (83) ، ص113-114.

المبحث الأول

تلقي البلاغ والمعاينة في الجرائم الإلكترونية

تجدر الإشارة إلى أن تلقي البلاغ والمعاينة من المواضيع الهامة التي يقوم بها رجال الضابطة العدلية في مجال مكافحة الجريمة الإلكترونية وجمع الأدلة من مسرح الجريمة ، ولما لها من أهمية بالغة في هذا المجال سيتم تناولها في هذا المبحث ، وذلك من خلال مطلبين مستقلين ، بحيث تناول الأول منهما الحديث عن تلقي البلاغ في الجرائم الإلكترونية ، أما المطلب الثاني فتناولنا فيه الحديث عن المعاينة في الجرائم الإلكترونية.

المطلب الأول

تلقي البلاغ في الجرائم الإلكترونية

من مهام رجل الضابطة العدلية تلقي البلاغات والشكاوى التي ترد إليه بخصوص الجرائم الواقعة على أفراد المجتمع ، ليقوم بدوره بالتأكد من وقوع الجريمة وجمع الأدلة التي تثبت وقوعها واكتشاف مرتكبها ، فما هو مفهوم البلاغ ؟ وما هي العناصر التي ينبغي أن تتوافر في البلاغ عن الجرائم الإلكترونية ؟

وقبل الإجابة عن الأسئلة السابقة لا بد لنا من الإشارة إلى أن الكثير من الجرائم الإلكترونية عادة لا يتم الإبلاغ عنها من قبل المجني عليه في الجريمة ، ولا تصل إلى علم السلطات المختصة ؛ ويرجع السبب في ذلك إلى أن المجني عليه يخشى أحيانا من تعريض سمعته للتشويه ، أو إلحاق الضرر بمكانته الإجتماعية.

وعلى الرغم من ذلك ، يقع على عاتق رجال الضابطة العدلية لدى علمهم أو ورود بلاغ إليهم بوقوع أحد الاشخاص ضحية في جريمة إلكترونية ، أن يقوموا بتلقي البلاغ والتأكد من صحته ومن ثم القيام بإجراءات الاستدلال للحصول على أدلة إثبات وقوع الجريمة والسعي لمعرفة فاعلها.

فالبلاغ هو " إخبار السلطات المختصة عن وقوع جريمة ، أو أنها على وشك الوقوع ، أو أن هناك إتفاقا جنائيا أو أدلة أو قرائن أو عزما على إرتكابها أو وجود خوف من أنها ارتكبت."[1]

وعليه فإنه يجب على مأمور الضابطة العدلية لدى ورود بلاغ إليه بقيام شخص بممارسة أنشطة إجرامية تقع ضمن الجرائم الإلكترونية ، أن يقوم بممارسة اختصاصاته والصلاحيات الممنوحة له بموجب أحكام القانون ، وعليه فينبغي أن يتضمن البلاغ عن أي جريمة تندرج تحت الجرائم الإلكترونية على مجموعة من العناصر نذكر منها:[2]

أولا : تحديد مكان وقوع الجريمة ، فيجب على المبلغ أن يقوم بتحديد المكان الذي وقعت فيه الأفعال غير المشروعة ووصفها قدر الإمكان للتمكن من الوصول إليها كوصف موقع الشركة ، أو عنوانها ، أو البنك ، أو المنزل الذي تعرض للاعتداء.

ثانيا : تحديد نوع الجريمة ، فبالإضافة إلى تحديد مكان وقوع الجريمة يقع على عاتق المبلغ أن يبين نوع الجريمة المرتكبة ، وما إذا كانت اعتداء على مال أم تزوير البطاقة الائتمانية أو جرائم اختراق وتعطيل وإعاقة المواقع والاعتداء على البيانات والمعلومات الإلكترونية.

ثالثا : تحديد محل الجريمة ، إذ يجب على المبلغ بعد قيامه بتحديد مكان ونوع الجريمة أن يحدد أيضا لرجال الضابطة العدلية المختصين الجهاز أو الأجهزة التي وقعت عليها الجريمة ، والموقع الذي استهدفته تلك الجريمة.

---

[1] هروال ، نبيلة هبة (2013) . **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات** . الاسكندرية : دار الفكر الجامعي ، ص177.

[2] ابراهيم ، راشد بشير (2008) . **التحقيق الجنائي في جرائم تقنية المعلومات** . ط1 ، أبو ظبي : مركز الإمارات للدراسات والبحوث الاستراتيجية ، ص48-49.

المطلب الثاني

المعاينة في الجرائم الإلكترونية

تعتبر المعاينة من الإجراءات الأولية للاستدلال في الجرائم الإلكترونية ، وهي حجر الأساس في الكشف عن الجريمة ، ففيها قد يتم الحصول على المعلومات والأدلة التي يستند عليها رجال الضابطة العدلية في متابعة الجريمة الإلكترونية ، وضبط الجناة ، والتحقيق معهم ، وصولا إلى توديعهم للقضاء لتتم محاكمتهم ، وسنتناول في هذا المطلب مفهوم المعاينة في الجرائم الإلكترونية وذلك في الفرع الأول ، أما الفرع الثاني فتناولنا فيه قواعد المعاينة في الجرائم الإلكترونية.

الفرع الأول

مفهوم المعاينة في الجرائم الإلكترونية

هناك العديد من التعريفات التي بينت مفهوم المعاينة حيث عرفت بأنها " إثبات الحالة التي يكون عليها مسرح الجريمة عند إنتقال المحقق إليه وإثبات ما به من آثار وحالة الأشخاص المتواجدين به والتحفظ على كل ما من شأنه أن يغير في كشف الحقيقة"[1].

كما يقصد بالمعاينة بأنها "الإجراء الذي يتضمن وصف مكان الحادث بما فيه من أشياء وأشخاص والفحص الدقيق لكافة المحتويات بهدف كشف مخلفات وآثار الجاني بالمكان والتي تشير إلى شخصيته أو شركائه وما يفيد في إثبات ارتكاب الجريمة وتوضح قدرا من الاستنتاجات المنطقية التي تشكل في حد ذاتها الأساس الذي تقوم عليه التحقيق والبحث التالية"[2].

---

[1] سند ، نجاتي سيد أحمد (2008) . **مبادئ الإجراءات الجنائية في التشريع المصري** . جامعة الزقازيق : كلية الحقوق ، ص530.

[2] كامل ، محمد فاروق عبدالحميد (1999) . **القواعد الفنية والشرطية للتحقيق والبحث الجنائي** . الرياض : جامعة نايف العربية للعلوم الأمنية ، ص66.

وتتم المعاينة في الجريمة الإلكترونية عن طريق الانتقال إلى مكان وقوعها ، ولكن يختلف الانتقال لمسرح الجريمة بحسب طبيعة الجريمة الإلكترونية المرتكبة ، فإذا ارتكبت الجريمة على المكونات المادية لأجهزة الحاسوب أو ملحقاته كالأشرطة والأقراص الممغنطة مثلا ، فعلى رجال الضابطة العدلية أن ينتقلوا إلى مسرح الجريمة المادي والذي يحتوي على أجهزة الحاسوب أو ملحقاته لمعاينته والتحفظ على الأدلة المادية فيه وضبطها[1] ، أما إذا كانت الجريمة الإلكترونية واقعة على البيانات والمعلومات المخزنة في الأجهزة الإلكترونية ، أي المكونات غير المادية لأجهزة الحاسوب ، فيتم الانتقال إلى مسرح الجريمة عن طريق الانترنت بواسطة أجهزة الحاسوب المنتشرة في مقاهي الانترنت ، أو الأجهزة الخاصة بسلطات الاستدلال لإجراء المعاينة الافتراضية[2].

وينبغي على رجال الضابطة العدلية عند وقوع الجريمة الإلكترونية التفرقة بين مسرحين[3]، الأول تقليدي ، وهو المسرح الذي يضم المكونات المادية الملموسة والذي يشبه مسرح الجريمة التقليدية بحيث يترك الجاني فيه آثار عدة كالبصمات والوسائط التخزينية للحاسب الالي[4] ، وأما الثاني فهو المسرح الافتراضي (الإلكتروني) ، والذي يضم البيانات الرقمية التي توجد داخل جهاز

---

[1] أبو حطب ، ياسر محمد الكومي محمود (2014) . **الحماية الجنائية والأمنية للتوقيع الإلكتروني** . الاسكندرية : منشأة المعارف ، ص243.

[2] عاكوم ، وليد (2003) . "التحقيق في جرائم الحاسوب" ، **المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، 26-28 أبريل ، دبي ، الإمارات العربية المتحدة.**

[3] الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان ، ص57.

[4] مصطفى ، عائشة بن قارة (2010) . **حجية الدليل الإلكتروني في مجال الإثبات الجنائي** . الاسكندرية : دار الجامعة الجديدة للنشر ، ص84.

الحاسب الآلي ويتم التعامل مع هذا المسرح من قبل ذوي الخبرة والمتخصصين في التعامل مع الأدلة الإلكترونية[1].

الفرع الثاني

قواعد المعاينة في الجرائم الإلكترونية

يتعين على رجال الضابطة العدلية عند إجراء المعاينة لمسرح الجريمة الإلكترونية القيام بما يلي:

1. معرفة مكان وقوع الجريمة ، وعدد الأجهزة المتوقع تفتيشها ، وأنواعها ، والأجهزة المتصلة بها[2].
2. تصوير الحاسب الآلي الذي ارتكبت الجريمة الإلكترونية من خلاله ، والأجهزة الطرفية ، والملحقات التي تتصل به ، والمحتويات التي بداخله مع ضرورة توثيق الوقت والمكان الذي تم التقاط الصور فيه.[3]
3. التواني في نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء الاختبارات اللازمة ؛ للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا تؤدي إلى إتلاف البيانات المخزنة نتيجة تداخل المجالات المغناطيسية مع بعضها البعض[4].

---

[1] حنفي : حازم محمد (2017) . **الدليل الإلكتروني ودوره في المجال الجنائي** . ط1 ، القاهرة : دار النهضة العربية ، ص55-56.

[2] أبو حطب ، ياسر محمد الكومي محمود (2014) . **الحماية الجنائية والأمنية للتوقيع الإلكتروني** . الاسكندرية : منشأة المعارف ، ص245.

[3] حجازي ، عبدالفتاح بيومي (2002) . **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت** . مصر : دار الكتب القانونية ، ص213.

[4] حنفي ، حازم محمد (2017) . **الدليل الإلكتروني ودوره في المجال الجنائي** . ط1 ، القاهرة : دار النهضة العربية ، ص59.

4. تأمين كافة الاحتياجات اللازمة لتشغيل وفحص أجهزة الحاسوب المستخدمة في الجريمة ، ولضبط الأدلة ونقل البيانات والمعلومات المخزنة فيها[1].
5. حفظ محتويات سلة المهملات من الأوراق الملقاة والممزقة والشرائط والاقراص الممغنطة غير السليمة أو المتلفة لفحصها ، ومضاهاة ما عليها من بصمات من الممكن أن يكون لها علاقة بالجريمة المرتكبة[2].

---

[1] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص58.

[2] الطحطاوي ، أحمد يوسف (2015) . **الأدلة الإلكترونية ودورها في الإثبات الجنائي** . القاهرة : دار النهضة العربية ، ص135.

المبحث الثاني
وسائل جمع الأدلة في الجريمة الإلكترونية

تتوافر أمام رجال الضابطة العدلية مجموعة من الوسائل للبحث والتحري عن الجرائم الإلكترونية ، ونتناول منها الإرشاد الجنائي عبر الشبكة الإلكترونية وذلك في المطلب الأول من هذا المبحث ، والمراقبة الإلكترونية لشبكة الانترنت في المطلب الثاني ، أما المطلب الثالث فنتناول فيه اعتراض المراسلات عبر الشبكة الإلكترونية.

المطلب الأول
الإرشاد الجنائي عبر الشبكة الإلكترونية

"يعد الإرشاد الجنائي عبر الشبكة الإلكترونية من الوسائل الهامة التي يعتمد عليها رجال الضابطة العدلية في البحث عن الأدلة وجمع التحريات حول الجريمة الإلكترونية المرتكبة ، لما لهذه الوسيلة من دور بارز في استقصاء الجرائم والكشف عنها ، إذ إن معظم المؤسسات الضبطية في مختلف أنحاء العالم تقوم باستخدامه ، وذلك عن طريق تجنيد مصادرها للدخول إلى العالم الافتراضي ، بهدف البحث عن الجرائم الإلكترونية وكشف مرتكبيها لتقديمهم للمحاكم المختصة ، كما يمكن أن يقوم رجال الضابطة العدلية بالبحث والتحري بأنفسهم عن الجرائم الإلكترونية في العالم الافتراضي من خلال الحصول على إذن رسمي لمباشرة مهامه في البحث والتحري عن تلك الجرائم ومرتكبيها ، ويجب أن يتضمن الإذن على رقم الحاسوب وصلاحيته للعمل وخلوه من العوائق التكنولوجية واحتواءه على برمجيات أصلية وليست منسوخة ، فضلا عن ذكر أرقامها المتسلسلة ورقم الترخيص بها وتاريخه وجهة إصدارها ، ثم يجلس بعد ذلك أمام حاسوب متصل

بالشبكة الإلكترونية للقيام بعمله بالبحث والتحري ، وذلك من خلال دخوله في نقاشات مع الغير باستخدام أسماء مستعارة لأشخاص أو لهيئات مختلفة عبر قاعات الدردشة وحلقات النقاش".[1]

ويتولى مهمة الإرشاد الجنائي أحد مأموري الضبط القضائي ، وقد يكلف بها غيره من ذوي المعرفة بتقنية المعلومات ، ولا يباشر المرشد عمله إلا بعد الحصول على إذن رسمي من السلطات المختصة ، وبعدها يقوم المرشد الجنائي بالولوج في شبكة الانترنت بغية الكشف عن الجريمة وبيان فاعلها ، إذ يقوم بالدخول في نقاشات مع الغير عبر قاعات وأماكن الدردشات الخاصة بالمتهمين ، وبدء النقاش معهم للحصول على النوايا الإجرامية التي يخفونها والتحري عن الجرائم التي ارتكبوها ومن ثم تزويد الجهات المختصة بكل إجراءات التحري التي قام بها[2].

ويرى الباحث أن نظام الإرشاد الجنائي من أهم الأنظمة التي ينصح باتباعها للاستدلال على الجرائم الإلكترونية ، لما لهذا النظام من دور بارز في الكشف عن الجريمة وتقديم فاعلها للقضاء.

---

[1] هروال ، نبيلة هبة (2013) . **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات** . الاسكندرية : دار الفكر الجامعي ، ص195-196.

[2] محمد ، أكرم البكوش راشد (2012) . **المواجهة الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلال** . (رسالة ماجستير) ، جامعة طرابلس ، طرابلس ، ليبيا.

المطلب الثاني

المراقبة الإلكترونية لشبكة الانترنت

يقصد بهذه المراقبة العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء أكان شخصا أم مكانا أم شيئا كان بحسب طبيعته مرتبط بالزمن والتاريخ والوقت الذي وقعت به الجريمة لتحقيق غرض أمني أو لأي غرض آخر.[1]

وتعد المراقبة الإلكترونية من المصادر الهامة لعملية البحث والتحري ، والتي يتم القيام بها باستخدام تقنية المعلومات ، بهدف جمع البيانات والمعلومات اللازمة عن المشتبه بهم في ارتكاب الجرائم الإلكترونية ، كما تعتبر هذه الوسيلة من الوسائل التي تشكل خطرا على حق الأفراد في الخصوصية ، والذي يعتبر من الحقوق المقدسة التي ضمنها كل من القانون والدستور وتعهد بحمايتها ، لذلك تم وضع القيود على هذه الوسيلة من خلال ربطها بموافقة السلطات القضائية المختصة ، إذ لا يجوز مباشرتها قبل الحصول على إذن من الجهات المختصة[2].

ولا يمكن الاستغناء عن عملية المراقبة في مجال مكافحة الجريمة الإلكترونية ، "خصوصا وأن المنظمات الإجرامية أصبحت اليوم تمتلك وسائل حديثة في مجال المواصلات والاتصالات بالإضافة إلى قيامها باستخدام التقنية الحديثة في تبادل المعلومات دون أن تتعرض للكشف من قبل الأجهزة المختصة بالملاحقة ، لذلك أصبح من الضروري أن تستخدم أجهزة الأمن نفس الوسائل في عملية المراقبة والتنصت على اتصالاتهم ورصدها وتحليلها لكشفهم وتقديمهم للعدالة.[3]

---

[1] موسى ، مصطفى محمد (2003) . **المراقبة الإلكترونية عبر شبكة الانترنت** . ط1 ، القاهرة : دار الكتب والوثائق المصرية ، ص192.

[2] موسى ، مصطفى محمد (2003) . **المراقبة الإلكترونية عبر شبكة الانترنت** . ط1 ، القاهرة : دار الكتب والوثائق المصرية ، ص192.

[3] الجدال ، عامر مصباح . **الجريمة المنظمة** . ص358.

ويرى الباحث أن عملية المراقبة من المصادر الهامة للتحري والتي يستعين بها رجال الضابطة العدلية في مجال التقصي عن الجرائم ، إذ لا يمكن الاستغناء عنها لما لها من دور هام في جمع الأدلة حول الجريمة المرتكبة ، وأن هذه العملية يجب أن تتم تحت إشراف سلطة مختصة للحفاظ على حرية الفرد وحقه في الخصوصية.

المطلب الثالث

اعتراض المراسلات عبر الشبكة الإلكترونية

تعتبر عملية اعتراض المراسلات من الإجراءات الحديثة التي تقوم بها سلطات الاستدلال والتحقيق في سبيل جمع الأدلة وكشف الغموض عن الجريمة ، وسنتناول في هذا المطلب مفهوم اعتراض المراسلات وذلك في الفرع الأول ، وفي الفرع الثاني خصائص اعتراض المراسلات ، أما الفرع الثالث فنتناول فيه القيود الواردة على عملية اعتراض المراسلات.

الفرع الأول

مفهوم اعتراض المراسلات

يقصد باعتراض المراسلات أنه " اعتراض أو تسجيل أو نسخ للمراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية ، وهي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض"[1].

وقد عرفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بسترسبورغ في 2006/10/6م لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها " عملية مراقبة سرية المراسلات السلكية واللاسلكية ، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة ".[2]

---

[1] بطاش ، صفيح (2018) . **أساليب التحري الخاصة وضمانات حقوق الإنسان** . (رسالة ماجستير) ، المركز الجامعي أحمد زبانة – غليزان ، الجزائر ، ص8.

[2] بوكر ، رشيدة (2012) . **جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن** . ط1 ، بيروت : منشورات الحلبي الحقوقية ، ص442.

ويرى الباحث من خلال التعريفات السابقة أن عملية اعتراض المراسلات هي إجراء يتم على المحادثات السرية الخاصة بالأفراد باسخدام وسائل تكنولوجية حديثة للحصول على الدليل في الجريمة والكشف عن الحقيقة.

الفرع الثاني
خصائص اعتراض المراسلات

يتضمن إجراء اعتراض المراسلات خصائص معينة وتتمثل هذه الخصائص بما يلي:

1. تمس عملية اعتراض المراسلات بحق الشخص في سرية الحديث

فعلى الرغم من أن هذا الإجراء يساعد سلطات الاستدلال والتحقيق في الكشف عن الجريمة ، إلا أنه ينتهك حرمة الحياة الخاصة وحق الإنسان في سرية حديثة.[1]

2. اعتراض المراسلات يتم بالخفاء ودون علم صاحبها

فمن أهم الخصائص التي تميز إجراء اعتراض المراسلات أنها تتم بالخفاء ودون علم صاحب الشأن بها ، ولو علم بها لانتفت هذه الخاصية منها.[2]

3. الهدف من عملية اعتراض المراسلات الحصول على دليل غير مادي

تعتبر تقنية التنصت على الأحاديث الهاتفية للآخرين من الأدلة الغير مادية التي تنبعث من عناصر شخصية مما يصدر عن الآخرين من أقوال وأحاديث تقنع قاضي التحقيق بطريقة غير مباشرة وتفيد في كشف الغموض عن الجريمة المرتكبة[3].

---

[1] قادري ، سارة (2014) . **أساليب التحري الخاصة في قانون الإجراءات الجزائية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر.

[2] قادري ، سارة (2014) . **أساليب التحري الخاصة في قانون الاجراءات الجزائية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر.

[3] فاروق ، ياسر الأمير (2009) . **مراقبة الأحاديث الخاصة في الإجراءات الجنائية** . ط1 ، جامعة القاهرة : دار المطبوعات الجامعية ، ص165.

الفرع الثالث

القيود الواردة على عملية اعتراض المراسلات

على الرغم من أن عملية اعتراض المراسلات تسهم في الكشف عن الغموض في العديد من الجرائم الإلكترونية ، إلا أنها تشكل إنتهاكا لحرمة الحياة الخاصة للأفراد وتعتدي على سرية اتصالاتهم ، لذلك فقد تم وضع عددا من القيود القانونية التي تضمن عدم تعسف سلطات الاستدلال والتحقيق وهذه القيود هي[1]:

1. موافقة السلطات القضائية المختصة

فيجب أن يوجد أمر قضائي صادر حسب الأصول كي تتمكن الجهات المختصة من مباشرته. ولقد نص الدستور الأردني في مواده على ذلك صراحة حيث نصت المادة 18[2] منه على عدم جواز خضوع المراسلات البريدية للمراقبة أو الاطلاع عليها إلا بعد الحصول على أمر قضائي يتفق مع أحكام القانون.

2. تسبيب اللجوء إلى اعتراض المراسلات

فيجب أن يرتبط الأمر القضائي الصادر باعتراض المراسلات بوجود مصلحة مباشرة مرجوة من هذا الاعتراض ، وأن الدليل الذي يمكن الحصول عليه بعد إجراء الاعتراض يمكن أن يؤثر في مسار القضية المنظورة.

3. سرية الإجراءات أثناء القيام بعملية اعتراض المراسلات

فينبغي أن تنفذ هذه العملية بسرية تامة دون علم صاحب العلاقة ، ولا يجوز إفشاء المحتوى الذي تم اعتراضه للعامة ، وإنما يعرض على الجهات المعنية به فقط دون غيرها.

---

[1] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص94-98.

[2] المادة (18) من الدستور الأردني "تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية وغيرها من وسائل الاتصال سرية لا تخضع للمراقبة أو الاطلاع أو التوقيف أو المصادرة إلا بأمر قضائي وفق أحكام القانون".

ونجد أن المشرع الأردني قد عاقب الموظف الذي يقوم بنشر أو إشاعة محتوى الرسائل التي يتم الحصول عليها أثناء القيام بعملية اعتراض المراسلات ، وذلك بموجب الفقرة (ب) من المادة 65 من قانون الاتصالات الأردني لسنة 1995م.[1]

[1] المادة (65/أ) من قانون الاتصالات الأردني "للهيئة الحق بتعقب مصدر أي موجات راديوية للتحقق من ترخيص ذلك المصدر دون أن يعتبر ذلك خرقا لسرية الرسائل أو مخالفة لأحكام القوانين النافذة".
(65/ب) "لا يجوز نشر او إشاعة مضمون الرسائل التي تم إلتقاطها في معرض تتبع مصدر الرسالة بموجب الفقرة (أ) من هذه المادة ويعاقب الموظف الذي يقوم بنشر أو إشاعة مضمون تلك الرسائل بالعقوبات المقررة قانونا".

الفصل الرابع

إجراءات التحقيق الابتدائي في الجرائم الإلكترونية

وإجراءات التحقيق في الجرائم الإلكترونية متعددة ، ومنها التفتيش ، والخبرة ، والشهادة ، والاستجواب وسنتناول في هذا الفصل إجراءات التحقيق في الجرائم الإلكترونية وذلك من خلال مباحث ثلاث مستقلة على النحو التالي:

المبحث الأول : التفتيش في الجرائم الإلكترونية

المبحث الثاني : إجراءات التحقيق الشخصية في الجرائم الإلكترونية

المبحث الثالث : صعوبات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية

المبحث الأول

التفتيش في الجرائم الإلكترونية

يعتبر التفتيش من أهم الإجراءات التي تباشرها سلطات البحث والتحقيق في مواجهة الجريمة الإلكترونية بهدف الكشف عن الجريمة والتصدي لها ، وسنتناول في هذا المبحث ماهية التفتيش في الجرائم الإلكترونية وذلك في المطلب الأول ، أما المطلب الثاني فنتناول فيه محل التفتيش في الجرائم الإلكترونية.

المطلب الأول

ماهية التفتيش في الجرائم الإلكترونية

يعتبر التفتيش من أهم الإجراءات التي يقوم بها المحقق بغية الوصول إلى الأدلة اللازمة لإدانة الجاني في الجريمة ، فما هو مفهوم التفتيش ؟ وما هي شروطه ؟

الفرع الأول

مفهوم التفتيش في الجرائم الإلكترونية

عرف الفقه التفتيش بأنه " إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه".[1]

كما عرف بأنه " بحث بوليسي أو قضائي عن عناصر الدليل في جريمة ما ويمكن وفقا لقواعد قانونية خاصة أن ينفذ في المسكن الخاص بأي شخص أو في أي مكان آخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة "[2]

---

[1] عبد الستار ، فوزية (1986) . **شرح قانون الإجراءات الجنائية** . القاهرة : دار النهضة العربية ، ص278-279.

[2] انظر : Lexique de termes Juridique au Code de Dalloz Penale, 2004,101 ed e .

وعرف أيضا بأنه " البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه أو الاطلاع على محل منح القانون حماية خاصة كونه مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الانترنت ".[1]

ويرى الباحث من خلال التعريفات السابقة أن التفتيش هو وسيلة من الوسائل الهامة لإثبات الجريمة الإلكترونية ، والهدف منه جمع أدلة الجريمة الإلكترونية من برامج وملفات وبيانات تم استخدامها بشكل غير مشروع من قبل الجاني في الجريمة الإلكترونية لتحقيق مكاسب خاصة به.

الفرع الثاني
شروط التفتيش في الجرائم الإلكترونية

يعتبر التفتيش من الإجراءات الجوهرية اللازمة للتحقيق في الجرائم الإلكترونية ويهدف للحصول على الأدلة التي تكشف الحقيقة في الجريمة الإلكترونية ، إلا أن للتفتيش شروط وضمانات خاصة به تحفظ حقوق الأفراد وحرياتهم وحرمة مساكنهم ، وتضمن عدم استغلال جهات التحقيق للسلطات الممنوحة لهم بموجب القانون ، ويمكن تقسيم هذه الشروط إلى شروط شكلية وأخرى موضوعية نتناولها كما يلي :-

أولا: الشروط الشكلية للتفتيش في الجرائم الإلكترونية

هناك شروط تضمن صحة الإجراءات المتخذة في التفتيش ويجب الالتزام بها عند إجراء التفتيش على الأجهزة الإلكترونية ومنها:-

1. **إجراء التفتيش بحضور المتهم أو من ينوب عنه**

إن معظم التشريعات لا تجيز إجراء التفتيش إلا بحضور المتهم أو من ينوب عنه وإلا اعتبر التفتيش باطلا[1].

---

[1] الطوالبة ، علي حسن محمد (2004) . **التفتيش الجنائي على نظم الحاسوب والانترنت** . ط1 ، الأردن : عالم الكتب الحديث ، ص12-13.

ولقد أورد المشرع الأردني هذا الشرط في المادة 83 من قانون أصول المحاكمات الجزائية لسنة 1961م[2] ، إذ نصت على وجوب إجراء التفتيش بحضور المشتكى عليه فإذا تعذر حضوره وجب حضور مختار محلته أو من يقوم مقامه أو اثنين من أقاربه أو شاهدين يستدعيهما المدعي العام.

2. الميقات الزمني لإجراء التفتيش في الجرائم الإلكترونية

اختلفت التشريعات في تنظيمها للوقت الذي يجوز فيه إجراء التفتيش ، فهناك من حدده بأوقات النهار فقط مع وجود بعض الاستثناءات في ذلك[3]، وهناك من حصره خلال فترة زمنية معينة فحدد وقت البداية والنهاية المسموح بها إجراء التفتيش[4]، ومنهم من ترك أمر ذلك لتقدير القائم بالتفتيش لاختيار الوقت المناسب للتنفيذ ضمن المدة المحددة بالإذن مثل القانون الأردني[5].

---

[1] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص42.

[2] المادة (1/83) "يجري التفتيش بحضور المشتكى عليه إذا كان موقوفا".

(2/83) "فإن لم يكن موقوفا وأبى الحضور أو تعذر عليه ذلك أو كان موقوفا خارج المنطقة التي يجب أن يحصل التفتيش فيها أو كان غائبا يجري التفتيش بحضور مختار محلته أو من يقوم مقامه أو بحضور اثنين من أقاربه أو شاهدين يستدعيهما المدعي العام".

[3] نصت المادة (53) من قانون الإجراءات الجنائية القطري على أنه " لا يجوز أن يجري تفتيش المساكن إلا نهارا ، ويجوز التفتيش ليلا إذا كانت الجريمة متلبسا بها ، أو إذا اقتضت مصلحة التحقيق ذلك ، ويثبت ذلك في محضر التحقيق".

[4] نصت المادة (59) من قانون الإجراءات الجنائية الفرنسي " باستثناء حالة المطالبة المقدمة من داخل المنزل أو الاستثناءات التي ينص عليها القانون لا يجوز بدء عمليات البحث والزيارات المنزلية قبل الساعة 6 صباحا وبعد الساعة 9 مساء.....".

[5] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص40-41.

إذ نلاحظ أن المشرع الأردني قد أورد في الفقرة الثالثة من المادة 87 من قانون أصول المحاكمات الجزائية الأردني لسنة 1961م[1] مدة التفتيش القانونية والتي حددها بسبعة أيام من تاريخ صدور أمر التفتيش وإلا اعتبر باطلا.

3. محضر التفتيش في الجرائم الإلكترونية

إن تحرير محضر التفتيش من الشروط الجوهرية التي يجب مراعاتها عند القيام بعملية التفتيش ، وذلك لتوثيق ما أسفر عنه التفتيش من أدلة ، بالإضافة لتدوين الوقت والمكان الذي تم فيه التفتيش[2].

"ولا يلزم القانون وجود شكلا أو شروطا خاصة في محضر التفتيش ، وإنما يكفي أن يتوافر فيه ما تتطلبه القواعد العامة في المحاضر عموما ، كالكتابة باللغة الرسمية ، تاريخ تحريره ، توقيع محرره ، ويتضمن كافة إجراءات التفتيش.[3]

وكذلك الأمر عند القيام بإجراء التفتيش في الجرائم الإلكترونية ، إذ يجب وجود شخص متخصص في مجال تقنية المعلومات عند تحرير محضر التفتيش ؛ وذلك لتمكين سلطة التحقيق والمحكمة من الاطلاع على ما تم من إجراءات صحيحة وإحاطتهم بتقنية المعلومات.[4]

وقد تنبه المشرع الأردني لهذا الشرط ، وذلك في الفقرة الأولى من المادة (87) من قانون أصول المحاكمات الجزائية الأردني والتي نصت على أنه " يصطحب المدعي العام كاتبه ويضبط او يأمر

---

[1] المادة (3/87) "في جميع الأحوال ، يجب أن يكون أمر التفتيش مسببا ولا يجوز تنفيذه بعد مرور سبعة أيام من تاريخ صدوره تحت طائلة البطلان".

[2] الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان ، ص80.

[3] غلاب ، فايز محمد راجح (2011) . **الجرائم المعلوماتية في القانون الجزائري واليمني** . (أطروحة دكتوراة) ، جامعة الجزائر1 ، الجزائر ، ص338.

[4] حسين ، سامي جلال فقي (2011) . **التفتيش في الجرائم المعلوماتية** . مصر : دار الكتب القانونية ودار شتات للنشر والبرمجيات ، ص171.

بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة وينظم بها محضرا ويعنى بحفظها وفقا لأحكام الفقرة الأولى من المادة (35).

ثانيا: الشروط الموضوعية للتفتيش في الجرائم الإلكترونية

وهي القواعد اللازمة لإجراء التفتيش وغالبا ما تكون قبل البدء بعملية التفتيش كسبب التفتيش ، ومحله في الجرائم الإلكترونية.

1. سبب التفتيش في البيئة الإلكترونية

يعتبر عنصر السبب من العناصر اللازمة للقيام بإجراء التفتيش ، ومن الضمانات القانونية لصحة مشروعيته ، ويتحقق بوقوع جريمة وُجه الإتهام فيها إلى الشخص أو الأشخاص المراد تفتيشهم بناءا على أدلة معقولة ، وإلا فإن إجراء التفتيش يكون باطلا لإنتفاء السبب الذي يبرره[1].

وعليه فإن سبب التفتيش في الجرائم الإلكترونية يجب أن يستند على ثلاثة شروط ، ومنها وقوع جريمة إلكترونية من نوع الجنحة أو الجناية ووفق الأفعال التي يحددها المشرع في هذا المجال ، بالإضافة إلى إتهام أحد الأشخاص بارتكاب الجريمة الإلكترونية أو الاشتراك بها ، ويكون ذلك بناءا على أدلة كافية تشير بأن المتهم هو من قام بارتكاب الجريمة ، وأما الشرط الثالث فهو ضرورة توافر أدلة أو قرائن جدية لدى سلطات التحقيق على وجود بيانات أو معلومات أو معدات بحوزة المتهم أو غيره تفيد في إظهار الحقيقة.[2]

---

[1] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص31.

[2] حسين ، سامي جلال فقي (2011) . **التفتيش في الجرائم المعلوماتية** . مصر : دار الكتب القانونية ودار شتات للنشر والبرمجيات ، ص117-126.

أما المشرع الأردني فقد نص على وجوب تسبيب أمر التفتيش ، وذلك في الفقرة الثالثة من المادة 87 من قانون أصول المحاكمات الجزائية الأردني لسنة 1961م[1].

2. محل التفتيش

ويقصد بمحل التفتيش عموما بأنه المستودع الذي يحتفظ فيه الشخص بأشيائه المادية التي تتضمن أسراره ، والسر الذي يوفر القانون له الحماية هو المكان الذي يتوافر به حرمة خاصة من الاعتداء عليها ، كالمسكن والمكالمات والرسائل الشخصية والشخص نفسه ، ومحل التفتيش في الجريمة الإلكترونية هو الجهاز الإلكتروني والشبكات المرتبطة به وما يرتبط بهما من ملحقات مادية وتقنية.[2]

فمحل التفتيش في الجرائم الإلكترونية قد يكون متعلقا بمكان معين كمسكن المتهم أو بشخص معين ، ومن الضروري قبل البدء بإجراء التفتيش مراعاة طبيعة المكان الذي توجد فيه الوسائل الإلكترونية المراد تفتيشها ، بالإضافة لمراعاة الضمانات القانونية المحيطة به[3].

---

[1] المادة (3/87) "في جميع الأحوال ، يجب أن يكون أمر التفتيش مسببا ولا يجوز تنفيذه بعد مرور سبعة أيام من تاريخ صدوره تحت طائلة البطلان".

[2] قنديل ، أشرف عبدالقادر (2015) . **الإثبات الجنائي في الجريمة الإلكترونية** . الاسكندرية : دار الجامعة الجديدة ، ص149.

[3] جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر ، ص35.

المطلب الثاني

محل التفتيش في الجرائم الإلكترونية

ينصب محل التفتيش في الجريمة الإلكترونية على جهاز الحاسوب بمكوناته المادية والمعنوية وشبكات الاتصال الخاصة به ، وفي هذا المطلب سنتناول تفتيش المكونات المادية للحاسب الآلي وذلك في الفرع الأول ، وفي الفرع الثاني تفتيش المكونات المعنوية للحاسب الآلي ، أما الفرع الثالث فتناولنا فيه تفتيش شبكات الحاسب الآلي.

الفرع الأول

تفتيش المكونات المادية للحاسب الآلي

يقسم التفتيش من حيث محله إلى قسمين ، وذلك وفقا للقواعد العامة للتفتيش بحيث ينصب الأول منهما على المساكن وهو إجراء من إجراءات التحقيق تقوم به الجهات المختصة بالبحث في مسكن شخص ما عن أشياء تتعلق بجناية أو جنحة قامت دلائل قوية على حيازته لها ، وأما الثاني فينصب على الأشخاص وهو إجراء من إجراءات التحقيق يتم القيام به بهدف ضبط ما يحوزه الشخص الخاضع للتفتيش من أشياء تفيد في كشف الحقيقة"[1]

والتفتيش الواقع على الكيانات المادية لجهاز الحاسوب في الجرائم الإلكترونية يخضع لذات الإجراءات القانونية والقواعد العامة للتفتيش[2] ، أي أن حكم تفتيش المكونات المادية متوقف على طبيعة المكان الذي توجد فيه تلك الكيانات ، فإذا كانت موجودة بحوزة أحد الأشخاص في مكان عام وسواء أكان عام بطبيعته كالطرق العامة والحدائق العامة والمتنزهات أو كان المكان عام بالخصوص كمقاهي الانترنت ووسائل النقل العامة فإنها تخضع للحالات التي يجوز فيها تفتيش

---

[1] حنفي ، حازم محمد (2017) . **الدليل الإلكتروني ودوره في المجال الجنائي** ، ط1 . القاهرة ، دار النهضة العربية ، ص40.

[2] الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان ، ص66.

الأشخاص[1] ، أما إذا كانت موجودة في مكان خاص كمنزل الجاني أو أحد ملحقاته فإنها تخضع للحالات التي يجوز فيها تفتيش المساكن مع ضرورة الانتباه فيما إذا كانت تلك الكيانات منفصلة أو متصلة بجهاز حاسوب آخر موجود في مكان غير منزل المتهم ، فإذا كانت متصلة فيتعين تفتيش تلك الكيانات الأخيرة ولكن ضمن الحالات التي يجوز فيها تفتيش تلك الأماكن[2].

وتفتيش المكونات المادية لجهاز الحاسوب لا يكون بالبحث عن الآثار المادية والبصمات كما هو حاصل في الجرائم التقليدية بل يكون بالبحث عن الأجهزة المستخدمة في ارتكاب الجريمة الإلكترونية والملحقات المرتبطة بها ، كالبحث عن طابعة أو جهاز ماسح ضوئي تم استخدامه للقيام بجريمة تزوير.[3]

الفرع الثاني

تفتيش المكونات المعنوية للحاسب الآلي

والمكونات المعنوية تعرف بأنها : "مجموعة من البرامج والأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات"[4]

وعلى الرغم من أن تفتيش المكونات المادية للحاسب الآلي تخضع لنفس قواعد التفتيش في الجرائم التقليدية إلا أن المشكلة تثور فيما يتعلق بتفتيش المكونات المعنوية للحاسب الآلي ، حيث

---

[1] هروال ، نبيلة هبة (2013) . **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات** . الاسكندرية : دار الفكر الجامعي ، ص237.

[2] الطوالبة ، علي حسن محمد (2004) . **التفتيش الجنائي على نظم الحاسوب والانترنت** . ط1 ، الأردن : عالم الكتب الحديث ، ص82.

[3] الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان ، ص67.

[4] عفيفي ، كمال عفيفي (2007) . **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون** . ط2 ، دمشق : منشورات الحلبي القانونية ، ص61.

ثار جدل فقهي واسع حول مدى جواز تفتيش تلك المكونات المعنوية لضبط الأدلة منها ، وهل يمكن تطبيق قواعد التفتيش التقليدية عليها ؟

وانقسم الفقه إلى اتجاهات عدة منها :

- **الاتجاه الأول:** يرى أن هذه المكونات المعنوية لا تصلح بطبيعتها لأن تكون كذلك، معتبرا أن الهدف من التفتيش هو القيام بضبط أدلة مادية وأن ذلك يتطلب وجود أحكام خاصة تتلاءم مع هذه المكونات المعنوية.[1]
- **الاتجاه الثاني:** يرى أن المكونات المعنوية تتشابه مع الكيانات المادية لجهاز الحاسوب من حيث خضوعها للتفتيش وأحكامه ، على اعتبار أن تلك البيانات قابلة للتخزين على وسائط مادية كالأشرطة الممغنطة والأقراص وغيرها من أدوات التخزين بالتالي فإنها تعتبر صالحة للضبط والتفتيش.[2]
- **الاتجاه الثالث:** ويرى أن ضبط الأدلة الإلكترونية يمكن أن يتم من مختلف أشكال البيانات التي تحتويها الأجهزة الإلكترونية ، ويستند هذا الاتجاه في رأيه إلى النصوص الجنائية التي تنص على ضبط أي شيء يمكن أن يفيد في كشف الحقيقة ، وبالتالي يشمل ذلك البيانات الإلكترونية بمختلف أنواعها.[3]

كما ذهب رأي في الفقه إلى جواز تفتيش وضبط البيانات الموجودة في أجهزة الحاسوب بمختلف أشكالها ، ويستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن

---

[1] رستم ، هشام محمد فريد (1995) . "جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة" ، **مجلة الدراسات القانونية** ، العدد (17) ، ص64 وما يليها.

[2] أرحومة ، موسى مسعود (2009) . "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" ، **المؤتمر المغاربي الأول حول المعلوماتية والقانون ، 28-29 / 10 / 2009م ، طرابلس ، ص7.**

[3] يوسف ، أمير فرج (2016) . **الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها** . ط1 ، الاسكندرية : مكتبة الوفاء القانونية ، ص310.

بضبط (أي شيء) ، فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المادية والمعنوية بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسوب غير المرئية أو غير المادية ، ولذلك فإنه يقترح أصحاب هذا الرأي على مواجهة هذا القصور التشريعي بالنص صراحةً على جواز تفتيش المكونات المعنوية لجهاز الحاسوب.[1]

ونجد أن المشرع الأردني قد نص في المادة 87 من قانون أصول المحاكمات الجزائية الأردني رقم 9 لعام 1961م[2] على أن للمدعي العام أن يضبط أو يأمر بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة ، فنجده قد استعان بلفظ الأشياء بشكل عام ، وهذا اللفظ يشمل جميع الأدلة المادية والمعنوية.

كما نجد أن المشرع الأردني قد نص صراحة على جواز تفتيش الأجهزة الإلكترونية التي أشارت الأدلة إلى استخدامها بارتكاب جريمة إلكترونية ، حيث نصت المادة 13 من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015[3] على ذلك.

---

[1] ابراهيم ، خالد ممدوح (2010) . **فن التحقيق الجنائي في الجرائم الإلكترونية** . الاسكندرية : دار الفكر الجامعي ، ص197.

[2] المادة (1/87) "يصطحب المدعي العام كاتبه ويضبط أو يأمر بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة وينظم بها محضرا ويعنى بحفظها وفقا لأحكام الفقرة الأولى من المادة (35)".

[3] المادة (13/أ) "مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية ، يجوز لموظفي الضابطة العدلية ، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة ، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم ، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص".

(13/ب) "مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة ، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب

ويرى الباحث بعد النظر في القواعد العامة للتفتيش والضبط في قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م ، أن تلك القواعد لا تصلح للتطبيق على تلك المكونات المعنوية لجهاز الحاسب الآلي ، لذلك فإن الباحث يوصي المشرع الأردني بضرورة وضع قانون خاص يتعلق بإجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية أو تعديل القواعد العامة الواردة في قانون أصول المحاكمات الجزائية الأردني لتشمل تلك الجرائم الإلكترونية.

كما يرى الباحث بجواز تفتيش تلك المكونات المعنوية بعد الحصول على إذن رسمي من الجهة المختصة ، وذلك لأن التفسير المنطقي لقصد المشرع الأردني من عبارة الأشياء والواردة بنص المادة 87 من قانون أصول المحاكمات الجزائية الأردني[1] هي جميع الأدلة التي تساهم في إظهار الحقيقة دون التطرق لطبيعتها المادية أو المعنوية ، وقد أحسن المشرع الأردني عندما نص في أحد مواده[2] على جواز تفتيش تلك المكونات المعنوية وحسم الجدل في ذلك.

ويواجه المحققين عند قيامهم بتفتيش الكيانات المعنوية وجود أنظمة حماية تمنع دخولهم إلى البيانات المخزنة في جهاز الحاسوب ككلمات المرور مثلا ، ومن هنا يثور تساؤل هام جدا وهو هل يجوز إجبار المتهم على الإفصاح عن كلمة السر ليتمكن المحقق من الوصول إلى الأدلة المحتملة على الجهاز أم أن ذلك الإجراء يعد باطلا ؟

أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها".

[1] المادة (1/87) "يصطحب المدعي العام كاتبه ويضبط أو يأمر بضبط جميع الأشياء التي يراها ضرورية لإظهار الحقيقة وينظم بها محضرا ويعنى بحفظها وفقا لأحكام الفقرة الأولى من المادة (35)".

[2] انظر المادة (13) من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015م.

إختلفت آراء الفقهاء في الإجابة على ذلك التساؤل وانقسمت إلى اتجاهين[1]:

الرأي الأول : يرى أصحاب هذا الرأي بعدم جواز إجبار المتهم على تقديم المعلومات التي تحتاجها الجهات المختصة للدخول إلى النظام المعلوماتي الخاص به ، وذلك استنادا إلى القاعدة الجنائية التي تنص بعدم جواز إجبار المتهم على الإجابة عن الاعترافات التي تؤدي إلى إدانته وأن من حقه الصمت والامتناع عن الإجابة دون أن يفسر ذلك ضد مصلحة المتهم.

أما الرأي الثاني فيرى أنه وعلى الرغم من عدم جواز إجبار المتهم على الإدلاء بأقواله ضد نفسه إلا أن ذلك لا يمنع من إجبار المتهم على تقديم المعلومات التي تحتاجها السلطات المختصة من أجل الدخول إلى النظام المعلوماتي الخاص به ، وذلك قياسا على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته.

وفي الحقيقة فإن الباحث يؤيد الرأي الأول ؛ ذلك لأن المتهم ليس مجبرا على الإدلاء بكلمات المرور أو ما شابهها من وسائل تتيح لرجال الضابطة العدلية الدخول إلى الأنظمة الخاصة به والبحث فيها عن دليل لإدانته ، وذلك قياسا على عدم جواز إجبار المتهم على الاعتراف وإعطاء أدلة من شأنها أن تثبت إدانته.

الفرع الثالث

تفتيش شبكات الحاسب الآلي

"يثير إخضاع شبكات المعلومات المتصلة بأجهزة الحاسوب الآلية العديد من الصعوبات ، والتي تتعلق بالدرجة الأولى بالطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي على أدلة عبر شبكات حاسوبية في أماكن غير معروفة وبعيدة عن موقع التفتيش ، فقد يكون موقع

[1] أحمد ، جمال زين العابدين أمين (2021) . "الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية" ، **مجلة مستقبل العلوم الاجتماعية** ، العدد (4) ، ص99-100.

التفتيش الفعلي لتلك المعلومات ضمن اختصاص قضائي آخر يتبع لدولة أو عدة دول أخرى وهو ما يزيد الأمر تعقيدا باعتبار الشبكة المعلوماتية ممتدة عبر أنحاء العالم.[1]

فكيف يمكن تفتيش هذه الشبكات فيما لو كانت متصلة بجهاز الحاسوب المأذون بتفتيشه وهل يمتد إذن التفتيش إليها أم لا ؟

أ- حالة اتصال جهاز المتهم بجهاز آخر داخل إقليم الدولة

ففي مثل هذه الحالة هل يمتد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم أم لا ؟

إن خضوع الجهاز المتصل بجهاز المتهم للتفتيش يتحدد وفق المكان الذي يوجد به ذلك الجهاز ، فلا تثور المشكلة فيما إذا كان مكان الجهاز المتصل بجهاز المتهم يخضع لنفس النظام القانوني والولاية القضائية التي يخضع لها جهاز المتهم ، ولكن تظهر المشكلة بوضوح فيما إذا كان مكان تواجد الجهاز المتصل بجهاز المتهم لا يخضع لنفس النظام القانوني والولاية القضائية التي يخضع لها جهاز المتهم ، بالإضافة إلى عدم وجود نص قانوني يجيز امتداد التفتيش على المكانين بإذن قضائي واحد ، فعندها لا يجوز أن يمتد التفتيش إلى الجهاز أو الأجهزة المتصلة بجهاز المتهم إلا بناءا على إذن قضائي من الجهة المختصة بالمكان المراد تفتيشه[2].

ب- حالة اتصال جهاز المتهم بجهاز آخر خارج إقليم الدولة

يقوم مرتكبي الجرائم الإلكترونية أحيانا بتخزين المعلومات والبيانات في شبكات وأنظمة معلوماتية خارج إقليم الدولة عن طريق استخدام شبكات اتصال دولية من أجل عرقلة إجراءات التحقيق ، الأمر الذي يشكل عائقا أمام سلطات التحقيق في تعقب الأدلة الإلكترونية ، وفي هذه الحالة لا

---

[1] المعمري ، عادل عبدالله خميس (2013) . "التفتيش في الجرائم المعلوماتية" ، **مجلة الفكر الشرطي** ، المجلد 22 ، العدد (86) ، ص262.

[2] الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان ، ص72-73.

يمكن أن يمتد إذن التفتيش إلى جهاز حاسوب يقع خارج الإقليم الجغرافي للدولة التي صدر من قبلها الإذن بالتفتيش ، وذلك لتمسك كل دولة بسيادتها الإقليمية إلا في ظل وجود إتفاقيات ثنائية بين الدول تجيز ذلك الإجراء والذي يعرف بالتفتيش العابر للحدود.[1]

وقد ساهمت الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) عام 2001م في هذا المجال , فقد نصت المادة 32 منها على ما يلي:

"يجوز لدولة طرف , دون ترخيص من دولة طرف أخرى:

أ- النفاذ إلى بيانات كومبيوتر مخزنة متاحة للعموم (مصدر مفتوح) بغض النظر عن مكان تواجد البيانات جغرافيا.

ب- النفاذ إلى بيانات كومبيوتر مخزنة موجودة لدى دولة طرف أخرى أو تلقيها ، من خلال نظام كومبيوتر داخل أقاليمها ، في حال حصول تلك الدولة الطرف على الموافقة القانونية والطوعية للشخص الذي يتوفر على السلطة القانونية للكشف عن تلك البيانات لتلك الدولة الطرف عبر نظام الكومبيوتر المذكور."

---

[1] هروال ، نبيلة هبة (2013) . **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات** . الاسكندرية : دار الفكر الجامعي ، ص240.

المبحث الثاني

إجراءات التحقيق الشخصية في الجرائم الإلكترونية

وتتمثل إجراءات التحقيق الشخصية بالخبرة والشهادة والاستجواب والتي نتناولها في ثلاثة مطالب ، بحيث نتناول في المطلب الأول الخبرة في الجرائم الإلكترونية ، وفي المطلب الثاني الشهادة في الجرائم الإلكترونية ، أما المطلب الثالث فنتناول فيه الاستجواب في الجرائم الإلكترونية.

المطلب الأول

الخبرة في الجرائم الإلكترونية

تعتبر الخبرة من الإجراءات التي تعين جهات التحقيق على أداء مهامها ، فعند وقوع جريمة ما قد تستعين تلك السلطات بالخبراء وأهل الاختصاص ، وفي هذا المطلب سنتحدث عن مفهوم الخبرة وذلك في الفرع الأول ، وأهم شروطها في الفرع الثاني.

الفرع الأول

مفهوم الخبرة في الجرائم الإلكترونية

لقد أورد الفقه للخبرة تعريفات عديدة فهي "إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء ، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم.[1]

كما عرفت بأنها "الاستشارة الفنية التي يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته ، نحو المسائل التي يحتاج تقديرها لمعرفة خاصة ودراية علمية أو فنية

---

[1] فرغلي ، عبدالناصر محمد محمود (2008) . "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية" ، **المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ، 12-14 نوفمبر ، الرياض ، المملكة العربية السعودية ، ص23.**

لا تتوفر لديه بحكم عمله وثقافته ، أما الخبير فهو كل شخص له دراية خاصة بمسألة من المسائل.[1]

وتجدر الإشارة إلى أن الخبير "هو الشخص الذي تعمق في دراسة عمل من الأعمال الإلكترونية وتخصص في أدائه فترة زمنية طويلة مما أكسبه خبرة عملية بحيث أصبح ملما بتفصيلاته مما جعله متفوقا على الشخص العادي وجعله قادرا على إبداء الرأي الإلكتروني الرقمي في الأمور المتصلة بهذا العمل.[2]

فيتضح من التعريفات السابقة أن الخبرة لها أثرها البارز في الكشف عن الأدلة التي تحتاجها سلطات التحقيق للوصول لحقيقة الجريمة وإزالة الغموض الذي يكتنفها.

إن المحقق الجنائي يقوم في سبيل الكشف عن غموض الجريمة ومعرفة فاعلها بمجموعة من الإجراءات اللازمة لذلك كالاستعانة بالخبراء والمتخصصين في هذا المجال ، وذلك تحقيقاً لمبدأ التخصص ، ولأن الخبرة من التقديرات المادية أو الذهنية التي يبديها أصحاب الفن او الاختصاص في مسألة فنية ما لا يستطيع المحقق في الجريمة معرفتها وبمعلوماته الخاصة سواء أكانت تلك المسألة الفنية مرتبطة بشخص المتهم أم بجسم الجريمة أم المواد المستعملة في ارتكابها أم آثارها.[3]

---

[1] الطحطاوي ، أحمد يوسف (2015) . **الأدلة الإلكترونية ودورها في الإثبات الجنائي** . القاهرة : دار النهضة العربية ، ص304.

[2] يوسف ، أمير فرج (2016) . **الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها** ، ط1 ، الاسكندرية : مكتبة الوفاء القانونية ، ص328.

[3] العكيلي ، عبد الأمير ، وحربة ، سليم (2009) . **شرح قانون أصول المحاكمات الجزائية** . بيروت.

الفرع الثاني

شروط الخبرة في الجرائم الإلكترونية

نظرا لما للخبرة من أهمية بالغة في مجال التحقيق في الجرائم الإلكترونية فهي تخضع لمجموعة من الشروط ومنها[1] :

1. أن يكون الخبير قادرا على إتقان مأموريته دون أن يؤدي ذلك إلى تدمير أو تلف الأدلة المتحصل عليها من الوسائل الإلكترونية.
2. الإلمام بتركيب جهاز الحاسوب وصناعته وبنظم تشغيله الرئيسية والفرعية.
3. طبيعة البيئة التي يعمل بها جهاز الحاسوب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل التي يتم استخدامها في ذلك.
4. قدرة الخبير على نقل أدلة الإثبات الغير مرئية وتحويلها إلى أدلة يمكن قراءتها مع إثبات أن البيانات والمعلومات الموجودة في المخرجات الورقية تتطابق مع تلك الموجودة على الجهاز أو نظام الشبكة.

---

[1] جواحي ، عبد الستار (2015) . **جرائم الحاسوب ، دراسة مقرنة بين الشريعة الإسلامية والقانون الجزائري** . (رسالة ماجستير) ، جامعة الشهيد حمه لخضر ، الوادي ، ص90.

المطلب الثاني

الشهادة في الجرائم الإلكترونية

إن شهادة الشهود تلعب دورا هاما في إبراز الحقيقة ولها أهمية خاصة في الجرائم الإلكترونية لما تقدمه من معلومات تفيد سلطات التحقيق في الوصول للحقيقة ، ونبين في هذا المطلب مفهوم الشهادة في الجرائم الإلكترونية وذلك في الفرع الأول ، أما الفرع الثاني فنتناول فيه بيان الشهود في الجريمة الإلكترونية والالتزامات المترتبة عليهم.

الفرع الأول

مفهوم الشهادة في الجرائم الإلكترونية

ويقصد بالشهادة بأنها : "الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها".[1]

ويقصد بالشاهد في الجرائم الإلكترونية بأنه الشخص الفني الذي يمتلك الخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي وشبكاته ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي حيث يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله.[2]

وبالنظر إلى التعريفات السابقة يتضح لنا أن الشاهد الإلكتروني يجب أن يكون صاحب خبرة ومن ذوي الاختصاص في مجال تقنية المعلومات وعلم الحاسوب.

---

[1] مصطفى ، عائشة قارة (2010) . **حجية الدليل الإلكتروني في مجال الإثبات الجنائي** .الاسكندرية : دار الجامعة الجديدة للنشر ، ص125.

[2] محمد ، سعيد (2005) . **الجرائم الإلكترونية وآليات الحصول على الدليل فيها** . ط1 ، دار النشر الذهبي ، ص30-53.

الفرع الثاني

الشهود والتزاماتهم في الجريمة الإلكترونية

وكما ذكرنا سابقا فإن الشاهد المعلوماتي يجب أن يكون من أصحاب الخبرة ومن المتخصصين في مجال تكنولوجيا المعلومات ، فمن هو الشاهد ؟ وما هي الالتزامات المترتبة عليه؟

أولا: الشهود في الجريمة الإلكترونية

والشاهد في الجريمة الإلكترونية يكون من ضمن الفئات التالية :

1. مشغلو الجهاز الإلكتروني

وهم أصحاب الخبرة الذين تكون لديهم الدراية التامة بتشغيل الجهاز الإلكتروني والمعدات والملحقات المتصلة به واستخدامها ، وإدخال البيانات ونقلها من وإلى الجهاز.[1]

2. المبرمجون

وهم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج وينقسمون إلى فئتين ، مخططو البرامج التطبيقية ويقومون بالحصول على خصائص النظام المطلوب ، مخططو برامج النظم ويقومون باختيار وتعديل وتصحيح برامج النظام الحاسب الداخلية وإدخال أي تعديلات أو إضافات.[2]

3. المحللون

والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراسة هذه البيانات ، ومن ثم تحليلها أي تقسيمها إلى وحدات منفصلة وإستنتاج العلاقات الوظيفية من هذه

---

[1] فهمي ، محمد (1991) . **الموسوعة الشاملة لمصطلحات الحاسب الآلي الإلكتروني** . مصر : مطابع المكتب المصري الحديث ، ص23.

[2] الشريم ، صالح خميس راشد يوسف (2020) . **الإطار القانوني لوسائل البحث والتحري عن الجرائم الإلكترونية** . (رسالة ماجستير) ، جامعة عمان الأهلية ، عمان ، الأردن ، ص 56-57.

الوحدات ، كما يقوم بتتبع البيانات داخل النظم عن طريق ما يسمى بمخطط تدفق البيانات ، واستنتاج الأماكن التي يمكن معالجتها بواسطة الحاسب الآلي.[1]

4. مديرو النظم

وهم الذين يوكل إليهم أعمال الإدارة في النظم المعلوماتية.[2]

5. مهندسو الصيانة والاتصالات

وهم المسؤولين عن أعمال الصيانة الخاصة بتقنيات الجهاز الإلكتروني بمكوناته وشبكات الاتصال المتعلقة به.[3]

ثانيا: التزامات الشاهد في الجريمة الإلكترونية

هناك عدة التزامات تترتب على الشاهد في الجريمة الإلكترونية وهي كالآتي:

1. حضور الشاهد

فيجب على الشاهد عندما يستدعيه المدعي العام أو جهة التحقيق أن يلتزم بالحضور بالوقت والمكان المحدد وألا يتخلف عن ذلك وإلا عوقب حسب القوانين.

وقد تناول المشرع الأردني هذا الالتزام وأجبر الشاهد على الحضور عندما يطلبه المدعي العام للإدلاء بشهادته وخلافا لذلك يعاقب قانونا ، حيث نصت المادة 75 من قانون أصول المحاكمات الجزائية على ما يلي: "كل من يدعى لأداء الشهادة مجبر على الحضور أمام المدعي

---

[1] أحمد ، هلالي عبداللاه (2000) . **إلتزام الشاهد بالإعلام في الجريمة المعلوماتية** . القاهرة : دار النهضة العربية ، ص24.

[2] أحمد ، هلالي عبداللاه (2000) . **إلتزام الشاهد بالإعلام في الجريمة المعلوماتية** . القاهرة : دار النهضة العربية ، ص24.

[3] محمود ، عبدالله حسين علي (2003) . "إجراءات جمع الادلة في مجال جريمة سرقة المعلومات" ، **المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، 26-28 أبريل ، دبي ، الإمارات العربية المتحدة ، ص616.**

العام وأداء شهادته وللمدعي العام في حالة تخلف الشاهد عن الحضور أن يقرر إحضاره ويغرمه حتى خمسين دينارا وله أن يعفيه من الغرامة إذا كان تخلفه بسبب معقول...."

2. حلف اليمين

فيجب على الشاهد في الجريمة الإلكترونية أن يحلف اليمين القانونية على القيام بعمله بصدق وأمانة ، وعدم الإبطاء عن تقديم كل ما يتوفر لديه من معلومات تفيد في كشف الغموض عن الجريمة والوصول للحقيقة متى ما طلب منه ذلك ، وإذا إمتنع عن ذلك عوقب بجريمة الإمتناع عن الشهادة.

وقد نصت المادة 165 من قانون أصول المحاكمات الجزائية الأردني على أنه "إذا امتنع الشاهد بغير مبرر قانوني عن أداء اليمين أو عن الإجابة على الأسئلة التي توجهها إليه المحكمة فيجوز لها أن تودعه السجن مدة لا تتجاوز شهرا واحدا....."

3. الالتزام بقول الحقيقة

ويوجب هذا الالتزام الشاهد بالصدق في كل ما يصدر عنه من أقوال لضمان سلامة وصحة شهادته وضمان الوصول إلى الحقيقة ، وعليه يجب على الشاهد أن يذكر البيانات والمعلومات الصحيحة والسليمة فقط والتي تصف ما حدث فعلا وفي حالة عدم الالتزام بذلك فاننا سنكون امام تضليل للعدالة ، كون الشاهد يلعب دورا هاما في كشف غموض الجريمة الإلكترونية من خلال تسهيل الوصول للأدلة الجنائية الرقمية عن طريق الإفصاح عن كلمات المرور والشيفرات التي تشكل عائقا أمام الجهات المختصة في الوصول للأدلة.[1]

وقد نصت المادة (71) من قانون أصول المحاكمات الجزائية الأردني على "يتثبت المدعي العام من هوية الشاهد ثم يسأله عن إسمه وشهرته وعمره ومهنته وموطنه وهل هو في خدمة أحد

---

[1] أحمد ، هلالي عبداللاه (1997) . **إلتزام الشاهد بالإعلام في الجرائم المعلوماتية** . ط1 ، مصر : دار النهضة العربية ، ص63-64.

الفريقين أو من ذوي قرباه وعن درجة القرابة ويحلفه بأن يشهد بواقع الحال بدون زيادة أو نقصان ويدون جميع ذلك في المحضر".

المطلب الثالث

الاستجواب في الجرائم الإلكترونية

"يعتبر الاستجواب من إجراءات التحقيق الابتدائي في كافة الجرائم بغض النظر عن نوع الجريمة ، ويهدف إلى البحث عن كافة أنواع الأدلة الجنائية من أجل عرضها على المتهم ومواجهته بها والتحقيق معه من أجل الوصول للحقيقة ، أو إلى اعتراف المتهم بالتهم المنسوبة إليه في الجريمة ، كما ويتاح للمتهم عند القيام بهذا الإجراء الفرصة للدفاع عن نفسه ودفع ما نسب إليه من تهم.[1]

فبعد أن ينتهي قاضي التحقيق من إجراءات التفتيش والضبط وسماع الشهود يقوم بالاطلاع على التقارير المقدمة إليه من الخبراء في الجريمة الإلكترونية ، ومن ثم يبدأ باستجواب المتهم ومناقشته بشأن الادلة التي تم التوصل إليها من قبل الجهات المختصة ، فما هو الاستجواب ؟ وما هي القواعد التي تحكمه ؟

وللإجابة عن الأسئلة السابقة تم تقسيم هذا المطلب إلى فرعين لبيان مفهوم الاستجواب في الجرائم الإلكترونية وذلك في الفرع الأول ، أما الفرع الثاني فتناولنا فيه قواعد الاستجواب في الجرائم الإلكترونية.

الفرع الأول

مفهوم الاستجواب في الجرائم الإلكترونية

يعرف الاستجواب بأنه " مناقشة المتهم بالتهم والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده والمتهم حر في الإجابة عن الأسئلة الموجهة عليه ولا يعد امتناعه قرينة ضده ، وهو

---

[1] الجوخدار ، حسن (2011) . **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية** . ط2 ، الاردن : دار الثقافة للنشر والتوزيع ، ص234.

وسيلة تمحيص للتهم أو لنفيها عنه فهو طريق من طرق تقصي الحقيقة ومصدر من مصادر الاثبات وليس وسيلة إثبات.[1]

ويعرف أيضا بأنه " مناقشة المحقق للمتهم بأدق تفاصيل التهمة المنسوبة إليه من خلال مواجهته بالأدلة والشبهات القائمة ضده ، وللمتهم أن لا يعترف بما وجه له من أدلة إن كان منكرا لها ، أو أن يسلم بها إن كان معترفا بما نسب إليه".[2]

ونلاحظ مما سبق أن الاستجواب قد يعتبر وسيلة لإثبات الجرم المرتكب من قبل المتهم في الجريمة فيما إذا اعترف بالجرم المسند إليه ، وقد يعتبر وسيلة دفاع فيما لو أنكر المتهم الجرم المسند إليه.

الفرع الثاني

قواعد الاستجواب في الجرائم الإلكترونية

يلتزم المحقق عند إجراء الاستجواب بالعديد من الضوابط التي تحكم عمله قبل البدء بهذا الإجراء وأثناء القيام به ، وجميع تلك الضوابط تتشابه مع قواعد الاستجواب التقليدية والتي تضمن صحة الاستجواب من الناحية القانونية وهذه القواعد هي[3]:

أولا : القواعد التي يلتزم بها المحقق قبل إجراء الاستجواب:

1. أن تكون لديه المعرفة الكافية بأقوال الشهود الذين تم سماعهم وبأقوال المتهمين كذلك.
2. قراءة تقارير الخبرة الفنية قراءة جيدة والفهم الدقيق لما تحتويه.

---

[1] بوسقيعة ، أحسن (2009) . **التحقيق القضائي** . ط7 ، الجزائر : دار هومة للنشر والتوزيع ، ص45.

[2] بخي ، فاطمة الزهراء (2014) . **إجراءات التحقيق في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامع الملية ، الجزائر ، ص90.

[3] ابراهيم ، خالد ممدوح (2010) . **فن التحقيق الجنائي في الجرائم الإلكترونية** . ط1 ، الاسكندرية : دار الفكر الجامعي ، ص245-246.

3. تحديد النتائج التي تم التوصل إليها من عمليات التفتيش والضبط الواقعة على الأجهزة الإلكترونية.

4. وضع خطة من قبل المحقق لتنفيذها عند البدء بالاستجواب.

ثانيا : القواعد التي يلتزم بها المحقق عند البدء بالاستجواب:

1. دعوة المحامي من أجل حضور الاستجواب وذلك في حال قيام المتهم بتعيين محامي لنفسه.

2. فصل المتهمين عن بعضهم البعض من قبل المحقق في حال تعددهم.

3. استجواب المتهم خلال مدة أقصاها 24 ساعة.

ونجد أن المشرع الأردني قد عالج هذه المسالة من خلال نص المادة 63 من قانون أصول المحاكمات الجزائية لسنة 1961م[1] ، حيث وضع شروطا عديدة على المحقق في مرحلة الاستجواب ، ومنها التثبت من هوية المتهم وأن يتلو عليه التهمة المنسوبة إليه ، ويطلب الإجابة عنها مع تمكين المتهم بتوكيل محامي خلال 24 ساعة.

---

[1] المادة (1/63) "عندما يمثل المشتكى عليه أمام المدعي العام يتثبت من هويته ويتلو عليه التهمة المنسوبة إليه ويطلب جوابه عنها منبها إياه أن من حقه أن لا يجيب عنها إلا بحضور محام ، ويدون هذا التنبيه في محضر التحقيق فإذا رفض المشتكى عليه توكيل محام أو لم يحضر محاميا في مدة أربع وعشرين ساعة يجري التحقيق بمعزل عنه".

(2/63) "يجوز في حالة السرعة بسبب الخوف من ضياع الأدلة وبقرار معلل سؤال المشتكى عليه عن التهمة المسندة إليه قبل دعوة محاميه للحضور على أن يكون له بعد ذلك الاطلاع على إفادة موكله".

(3/63) "إذا أدلى المشتكى عليه بإفادة يدونها الكاتب ثم يتلوها عليه فيوقعها بإمضائه أو ببصمته ويصدق عليها المدعي العام والكاتب وإذا امتنع المشتكى عليه عن توقيعها بإمضائه أو ببصمته يدون الكاتب ذلك بالمحضر مع بيان سبب الامتناع ويصادق عليها المدعي العام والكاتب".

(4/63) "يترتب على عدم تقيد المدعي العام بأحكام الفقرات 1 و 2 و 3 من هذه المادة بطلان الإفادة التي أدلى بها المشتكى عليه".

المبحث الثالث

صعوبات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية

إن سلطات الاستدلال والتحقيق الابتدائي تواجه العديد من المشكلات فيما يتعلق بالجرائم الإلكترونية ، بدءا من العقبات التي تواجهها في الحصول على الدليل ، ووصولا إلى إثبات الجريمة الإلكترونية وتحويلها للقضاء ، وكل ذلك يرجع إلى الخصائص التي تتميز بها هذه الجرائم عن الجرائم التقليدية ، والتي تشكل عائقا كبيرا في وصول هذه السلطات إلى مرادها ألا وهو محاربة الجريمة الإلكترونية ومعاقبة مرتكبيها.

فالجرائم الإلكترونية تثير العديد من الصعوبات التي تمنع من مكافحتها ، كالصعوبات التي تواجه سلطات الاستدلال والتحقيق في الكشف عن الجريمة والصعوبات المتعلقة بنصوص التجريم الجزائية وصعوبات التفتيش العابر للحدود وصعوبات تحديد الاختصاص بالتحقيق في الجرائم الإلكترونية والتي نبينها في ثلاثة مطالب وكما يلي:-

المطلب الأول : الصعوبات التي تواجه سلطات الاستدلال والتحقيق الابتدائي في الكشف عن الجريمة الإلكترونية

المطلب الثاني : صعوبات التفتيش العابر للحدود

المطلب الثالث : صعوبات تحديد القانون الواجب التطبيق في الجرائم الإلكترونية

المطلب الأول

الصعوبات التي تواجه سلطات الاستدلال والتحقيق الابتدائي في الكشف عن الجريمة الإلكترونية

هناك العديد من الصعوبات التي تعيق عمل المحققين أثناء قيامهم بتعقب الجرائم الإلكترونية ، لذلك تم تقسيم هذا المطلب إلى ثلاثة فروع بحيث تناولنا في الفرع الأول الصعوبات التي تتعلق بضبط الأدلة في الجرائم الإلكترونية ، وفي الفرع الثاني الصعوبات التي تتعلق بعنوان المجرم الإلكتروني ، أما الفرع الثالث فتناولنا فيه الصعوبات المتعلقة بالامتناع عن التبليغ بوقوع الجريمة الإلكترونية :-

الفرع الأول

ضبط الأدلة في الجرائم الإلكترونية

إن الجاني في الجريمة الإلكترونية يتميز بالذكاء والخبرة في مجال الجرائم الإلكترونية ، ويعمد إلى إعاقة عمل جهات التحقيق في وصولهم إلى الدليل الذي يثبت إدانته ، فيقوم بوضع أنظمة حماية على الأنظمة والملفات التي تحوي الدليل على إرتكابه الجريمة الإلكترونية ، كأن يضع كلمات سرية تمنع دخول الآخرين إلى تلك الأنظمة أو الملفات ، أو أن يقوم بتشفيرها ، كما بإمكانه القيام بإتلاف جميع الأدلة بعد ارتكابه للجريمة ، "فعلى سبيل المثال ، تطلب إيقاف الهاكر "حمزة بن دلاج" الجزائري الجنسية ، والمتهم باختراق 217 بنكا حول العالم ، إلى ثلاث سنوات من التعقب من قبل مكتب التحقيقات الفيدرالي الأمريكي وإلى تنسيقا دوليا حتى استطاعت قوات الأمن ببانكوك إيقافه"[1].

---

[1] انظر المقال الإلكتروني : "بعد اختراقه عشرات البنوك الهاكر الجزائري حمزة بن دلاج في قبضة الFBI" المنشور في موقع : "www.mbc. net".

وهناك مجموعة من الأمور التي تعيق سلطات الاستدلال والتحقيق أثناء قيامها بجمع الأدلة ومن هذه الأمور ما يلي :-

1. صعوبة الوصول إلى الدليل لقيام الجاني في أغلب الأحيان بوضع أنظمة حماية على الملفات التي تحوي الأدلة أو تشفيرها كما ذكرنا سابقا .
2. سهولة القيام بمحو الدليل وتدميره بوقت قصير ، فالجاني في الجريمة الإلكترونية يستطيع القيام بمحو الدليل القائم ضده وتدميره بفترة زمنية قصيرة بحيث يصعب على سلطات التحقيق كشف الجريمة إذا علمت بها.[1]
3. معظم البيانات والمعلومات التي يتم تداولها عبر جهاز الحاسوب والشبكة المعلوماتية هي عبارة عن رموز يتم تخزينها على أدوات التخزين المتعددة كالوسائط الممغنطة وغيرها والتي من غير الممكن الوصول إليها إلا عن طريق جهاز الحاسوب ومن قبل أشخاص لديهم الخبرة في التعامل مع مثل تلك الأجهزة.[2]

ويرى الباحث بعض الحلول التي من الممكن أن تساعد في حل تلك المعوقات وهي كالآتي :-

1. الإسراع وعدم التواني في تتبع الأدلة الجرمية من قبل المحققين ، وعدم إتاحة الفرصة أمام المجرمين في كسب الوقت وإتلافهم للأدلة.
2. تعزيز التعاون الدولي في مجال التحقيق بالجرائم الإلكترونية ، وتبادل الخبرات بين سلطات التحقيق المختصة بمثل هذه الجرائم في الدول كافة.

---

[1] مطر ، حسين خليل . "إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية" ، العدد (36) ، ص400.

[2] ابراهيم ، راشد بشير (2008) . "التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي" ، **مجلة دراسات إستراتيجية** ، العدد(131) ، ص90.

الفرع الثاني
عنوان المجرم الإلكتروني

فعند ارتكاب الجريمة الإلكترونية يحاول الجاني قدر الإمكان بإخفاء هويته ، ليصعب على رجال التحقيق من الوصول إليه ، وذلك عن طريق استخدامه لحواسيب الغير أو حواسيب مقاهي الإنترنت المنتشرة في معظم المدن والتي لا تقوم بالتحقق من هوية زائريها .

وتعتبر تقنية المعلومات مجال استثمار لذلك نجد أن الشركات تتسابق في تبسيط الإجراءات وتسهيل إستخدام البرامج والأجهزة وملحقاتها وزيادة المنتجات ، ويكون جل اهتمامها بتقديم الخدمات دون التركيز على الجانب الأمني فعلى سبيل المثال مستخدمو شبكة الإنترنت عبر مزودي الخدمة وبطاقات الإنترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الإنترنت ، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة.[1]

فضلا عما تقدم ، فإن الجهات المختصة تواجه صعوبة في الوصول إلى الأدلة الرقمية ، وتتمثل تلك الصعوبة في قيام الجناة المتمرسين في ارتكاب الجرائم الإلكترونية بإخفاء هوياتهم للحيلولة دون تعقبهم من قبل السلطات المختصة بحيث تبقى أنشطتهم الجرمية غير مكشوفة لدى تلك السلطات ، ومن الأمثلة على ذلك قيام الجاني باستخدام أجهزة الحاسوب المتواجدة في الأماكن العامة أو المنتشرة في مقاهي الانترنت كون تلك المقاهي لا تقوم بتسجيل أسماء زوارها او التأكد من هوياتهم ، بالإضافة إلى إمكانية استخدام الخط الواحد من خطوط شبكة الانترنت من قبل أكثر من شخص في نفس الوقت مما يجعل من مراقبة المشتبه فيه أمرا أكثر صعوبة.[2]

---

[1] الحلبي ، خالد عياد (2011) . **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت** . ط1 ، الأردن : دار الثقافة للنشر والتوزيع ، ص223.

[2] أحمد ، هلالي عبد اللاه . مرجع سابق ، ص١٦٠.

الفرع الثالث

الامتناع عن التبليغ بوقوع الجريمة الإلكترونية

إن معظم المجني عليهم في الجرائم الإلكترونية يمتنعون عن التبليغ بوقوع الجريمة عليهم ، وذلك خوفا من تعرض سمعتهم للتشويه ، فأغلب المؤسسات والبنوك التي تقع ضحية للجرائم الإلكترونية تخفي ذلك لعدم رغبتها بالظهور بمظهر غير لائق أمام الغير ، وللحفاظ على سمعتها ومكانتها وثقة عملائها بها ، مما يصعب اكتشافها من قبل سلطات الاستدلال والتحقيق.

ويرجع سبب الامتناع عن التبليغ عن الجريمة الإلكترونية أحيانا إلى خوف بعض الجهات المتعرضة للضرر من الحرمان من الخدمة ، وذلك لأن الإفصاح من قبل الضحية عن التعرض لجريمة إلكترونية قد يؤدي أحيانا إلى حرمانه من خدمات معينة تتعلق بالنظام المعلوماتي ، فعلى سبيل المثال قد يتم حرمان الموظف من خدمات معينة على الانترنت أو من خدمات الانترنت بشكل عام فيما لو تعرض لجريمة إلكترونية بسبب قيامه بزيارة أماكن أو مواقع غير مسموح بزيارتها ، وقد يرجع سبب الامتناع عن التبليغ عن الجريمة الإلكترونية أيضا إلى عدم معرفة الضحية بوقوع الجريمة أصلا وعدم القناعة أنها من الممكن أن تحدث في مؤسسته.[1]

---

[1] ابراهيم ، خالد ممدوح (2010) . **فن التحقيق الجنائي في الجرائم الإلكترونية** . الاسكندرية : دار الفكر الجامعي ، ص67-68.

المطلب الثاني

صعوبات التفتيش العابر للحدود

قد يتطلب الأمر في أحيان كثيرة عند وقوع جريمة إلكترونية البحث والتفتيش في أنظمة معلوماتية عديدة للحصول على الأدلة وكشف مرتكبي هذه الجرائم ، ومن أهم الصعوبات التي تواجه سلطات التحقيق في الجرائم الإلكترونية مسألة التفتيش عن الأدلة ، خاصة إذا تطلب الأمر حصول جهات التحقيق على إذن بالتفتيش خارج إقليم الدولة التي يصدر عن جهاتها المختصة الإذن بالتفتيش ، والذي يسمى بالتفتيش العابر للحدود ، والذي لا يمكن الحصول عليه لتمسك كل دولة بمبدأ السيادة الإقليمية.

فأبرز الصعوبات التي تواجه سلطات الاستدلال والتحقيق حالة ما إذا كان حاسوب المتهم متصلا بحاسوب آخر موجود خارج إقليم الدولة ، حيث يقوم بعض الجناة بإخفاء الأدلة أحيانا في حاسوب يقع في إقليم دولة أخرى ، محاولة منهم في تعقيد الأمر على المحققين من الوصول إلى الأدلة.

وقد اختلفت الاتجاهات حول مدى امتداد التفتيش لأجهزة الحاسوب الأخرى خارج الدولة ومنها[1]:

– الاتجاه الأول: يرفض امتداد التفتيش لأجهزة الحاسوب المتصلة بحاسوب المتهم والموجودة خارج إقليم الدولة ، وذلك بحجة أن امتداد التفتيش هذا يؤدي إلى انتهاك سيادة دولة أخرى ويشكل اعتداء على ولايتها ، بالتالي فإن الأمر يتطلب حسب رأي أصحاب هذا الاتجاه لجوء سلطات التحقيق إلى اتباع الإجراءات المعتادة بطلب الإنابة أو المساعدة القضائية من السلطات المختصة في الدولة الأخرى ، ولا يقر أصحاب هذا الاتجاه ذلك الإجراء إلا في ظل وجود اتفاقية دولية ثنائية

[1] أحمد ، هلالي عبداللاه . مرجع سابق ، ص79.

أو متعددة الأطراف وإلا يعتبر الإجراء باطلا وغير مشروع ، وهذا الاتجاه يعبر عن الرأي السائد في الفقه الألماني.

– الاتجاه الثاني: يؤيد امتداد التفتيش لأجهزة الحاسوب المتصلة بجهاز المتهم والموجودة خارج إقليم الدولة ، ويعتمد هذا الاتجاه في رأيه على أساس واقعي ، بحيث ان المدافعين عنه يحاولون التعامل بواقعية مع ما يواجه سلطات التحقيق من صعوبات ، وقد أخذ القانون الفرنسي بهذا الاتجاه وذلك من خلال المادة (17) من قانون الأمن الداخلي الفرنسي ، كذلك فإن المادة (32) من الاتفاقية الأوروبية للجرائم الإلكترونية تجيز الدخول إلى الشبكة المعلوماتية التابعة لدولة أخرى من أجل القيام بالتفتيش والضبط متى ما كان هذا الإجراء متعلق ببيانات أو معلومات مباحة للجمهور ، وفي حالة الحصول على رضا صاحب أو حائز هذه البيانات بالتفتيش[1]، في حين يتوقف الأمر في الولايات المتحدة الأمريكية على وضع الشخص الذي ينفذ التفتيش ، فإذا كان قبل مباشرته يعلم بأن البيانات والمعلومات المراد بحثها مخزنة بعيدا في نطاق دولة أخرى ، فعندئذ يستلزم التماس طلب مساعدة يتم توجيهه إلى سلطات الدولة الأخرى ، أما إذا كان القائم بالتفتيش يجهل أو ليس في وسعه معرفة أن البيانات المراد تفتيشها خارج المنطقة ، فإن ما يسفر عنه التفتيش من ضبط لا يهدر، ويمكن قبوله والركون إليه في الإثبات بوصفه دليلا مشروعا متى ما اطمأنت إليه المحكمة.

ونلاحظ أن الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) والمنعقدة بتاريخ 2001/11/23م ، قد جاءت للحد من مشكلة تنازع الاختصاص واحترام مبدأ سيادة الدول ، حيث نصت الفقرة الخامسة من المادة 22 منها على ما يلي:

---

[1] بوحويش ، عطية عثمان محمد (2009) . **حجية الدليل الرقمي في إثبات جرائم المعلوماتية** . (رسالة ماجستير) ، أكاديمية الدراسات العليا ، بنغازي ، ص105.

"في حال مطالبة أكثر من دولة طرف بالولاية القضائية على جريمة تقرها هذه الاتفاقية ، تقوم الدول الأطراف المعنية ، عند الاقتضاء ، بالتشاور بغرض تحديد الولاية القضائية الأنسب للمقاضاة".

ولكن نرى أن المشكلة لا زالت قائمة على الرغم مما جاءت به الاتفاقية الأوروبية ، ذلك لأن التشاور بين الدول يحتمل القبول والرفض ، ولا أعتقد بأن تجيب الدول بالقبول والتنازل عن مبدأ السيادة الإقليمية للدولة.

المطلب الثالث

صعوبات تحديد القانون الواجب التطبيق في الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية من أكثر الجرائم التي يصعب معها تحديد السلطة صاحبة الاختصاص في التحقيق بها على المستوى الدولي ؛ لما لها من ميزات تمكنها من الانتقال عبر الدول دون التأثر بحدود الدول وسيادتها الاقليمية ، فمن الممكن أن ترتكب الجريمة الإلكترونية في دولة ما ولكن تظهر نتائجها الجرمية في دولة أو عدة دول أخرى ، كما لا يمكن لدولة ما أصدرت الحكم بالإدانة على أحد مرتكبي هذه الجرائم ، أن تلزم الدولة التي يتواجد بها المجرم على تطبيق العقوبة عليه وذلك احتراما لسيادة تلك الدولة ، وتطبيقا لمبدأ إقليمية النص الجزائي الذي ينص على أن قواعد القانون الجنائي لا تطبق إلا في حدود الإقليم الخاضع لسيادة الدولة.

كما أن الدول تختلف عن بعضها البعض في موضوع الجرائم الإلكترونية من حيث اعتبار الفعل المرتكب عبر شبكة الإنترنت والحواسيب جريمة أم لا ، ويرجع سبب ذلك إلى القيم القانونية والسياسية والأخلاقية والثقافية لكل دولة ، ولاختلاف مفهوم الجريمة الإلكترونية في دولة ما عن غيرها من الدول ، فقوانين الدول تختلف عن بعضها البعض " ففي حين يجيز بلد مثل هولندا تعاطي المخدرات فإن معظم بلدان العالم تجرمه ، وفي حين تجيز بعض الدول الغربية لعب القمار فإن دولا أخرى تمنعه ، وذات الأمر ينطبق على مواقع الإنترنت الإباحية"[1].

وكذلك الأمر ما حصل في القضية المتعلقة بمحرك البحث "yahoo" ، حينما أصدرت المحكمة الابتدائية بباريس قرارا بتاريخ 2000/11/21م يجبر شركة ياهو بالعمل على إيجاد الحلول التي تمنع مستخدمي شبكة الانترنت القاطنين بفرنسا من الدخول إلى موقع البيع بالمزاد العلني والذي تعرض فيه بضائع لها علاقة بالنازية وهو مما يجرمه القانون الفرنسي ، وقد كان

---

[1] حجازي ، عبدالفتاح بيومي (2002) . **الأحداث والانترنت** . مصر : دار الفكر الجامعي ، ص314.

القرار مرفقا بتقرير صادر عن هيئة من الخبراء يبين الطريقة الفنية التي يمكن اتباعها لتنفيذ هذا القرار ، وعلى الرغم من ذلك فإن القضاء الأمريكي قد رفض اعتماد هذا الحل لمخالفته للفصل الأول من الدستور الأمريكي الذي ينص على حرية التعبير[1].

[1] الكسراوي ، الهاشمي (2006) . "الجريمة المعلوماتية" ، **مجلة القضاء والتشريع** ، العدد (7) ، ص21.

الفصل الخامس

الخاتمة

بعد دراسة إجراءات الاستدلال والتحقيق في الجرائم الإلكترونية توصل الباحث إلى جملة من النتائج والتوصيات نتناولها كما يلي:

النتائج

1. أن المشرع الأردني لم ينص على قانون خاص ينظم إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية ، وترك أمر تنظيم تلك الإجراءات للقواعد العامة الواردة في قانون أصول المحاكمات الجزائية الأردني رقم (9) لسنة 1961م.
2. أن إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية تعترضها صعوبات عديدة وتحتاج إلى خبرة فنية من قبل سلطات الاستدلال والتحقيق من أجل القيام بها بهدف الوصول إلى حقيقة الجريمة المرتكبة وضبط فاعليها.
3. عدم إمكانية إتباع الإجراءات التقليدية في مواجهة الجرائم الإلكترونية لما تثيره من إشكاليات نتيجة طبيعتها غير المادية ، وما تنتجه من أدلة غير ملموسة.

التوصيات

1. يوصي الباحث بضرورة إصدار قانون خاص بدل نظام إستخدام وسائل التقنية الحديثة في الإجراءات الجزائية لعام 2018م ، أو تعديله أو تعديل نصوص قانون أصول المحاكمات الجزائية لتشمل الجرائم الإلكترونية.
2. يوصي الباحث بضرورة قيام المشرع الأردني بإنشاء هيئة متخصصة للنظر بالجرائم الإلكترونية بحيث يتميز أعضاؤها بالإضافة إلى الخبرة القانونية بالخبرة الفنية التي تساعد على القيام بإجراءات الاستدلال والتحقيق الابتدائي بصورة أكثر سهولة ويسر.
3. يوصي الباحث بضرورة إنشاء أقسام خاصة تابعة لوحدة مكافحة الجرائم الإلكترونية في جميع وحدات مديرية الأمن العام للنظر في هذه الجرائم.
4. يوصي الباحث بضرورة إطلاق الحملات الوطنية لرفع مستوى الوعي الاجتماعي حول مخاطر الجريمة الإلكترونية.

قائمة المراجع

أولا : الكتب القانونية

- ابراهيم ، خالد ممدوح (2010) . **فن التحقيق الجنائي في الجرائم الإلكترونية** . الاسكندرية : دار الفكر الجامعي.
- ابراهيم ، خالد ممدوح (2010) . **فن التحقيق الجنائي في الجرائم الإلكترونية** . ط1 ، الاسكندرية : دار الفكر الجامعي.
- ابراهيم ، راشد بشير (2008) . **التحقيق الجنائي في جرائم تقنية المعلومات** . ط1 ، أبو ظبي : مركز الإمارات للدراسات والبحوث الاستراتيجية.
- أبو حطب ، ياسر محمد الكومي محمود (2014) . **الحماية الجنائية والأمنية للتوقيع الإلكتروني** . الاسكندرية : منشأة المعارف.
- أحمد ، هلالي عبداللاه (2000) . **إلتزام الشاهد بالإعلام في الجريمة المعلوماتية** . القاهرة : دار النهضة العربية.
- أحمد ، هلالي عبداللاه (1997) . **إلتزام الشاهد بالإعلام في الجرائم المعلوماتية** . ط1 ، مصر : دار النهضة العربية.
- الجدال ، عامر مصباح . **الجريمة المنظمة.**
- الجوخدار ، حسن (2011) . **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية** . ط2 ، الأردن : دار الثقافة للنشر والتوزيع.
- الجوخدار ، حسن (2008) . **التحقيق الابتدائي في قانون أصول المحاكمات الجزائية ، دراسة مقارنة** . الأردن : دار الثقافة للنشر والتوزيع.

- الحلبي ، خالد عياد (2011) . **إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت** . ط1 ، الأردن : دار الثقافة للنشر والتوزيع.
- الزعبي ، جلال محمد ، والمناعسة ، أسامة (2013) . **جرائم تقنية نظم المعلومات الإلكترونية** ، ط1 . الأردن : دار الثقافة للنشر والتوزيع.
- الطحطاوي ، أحمد يوسف (2015) . **الأدلة الإلكترونية ودورها في الإثبات الجنائي** . القاهرة : دار النهضة العربية.
- الطوالبة ، علي حسن محمد (2004) . **التفتيش الجنائي على نظم الحاسوب والانترنت** . ط1 ، الأردن : عالم الكتب الحديث.
- العكيلي ، عبد الأمير ، وحربة ، سليم (2009) . **شرح قانون أصول المحاكمات الجزائية** . بيروت.
- الفقي ، عمرو عيسى (2006) . **الجرائم المعلوماتية** . الاسكندرية : المكتب الجامعي الحديث.
- المناعسة ، أسامة احمد (2001) . **جرائم الحاسب الآلي والانترنت** . ط1 ، الأردن : دار وائل.
- بلواضح ، الطيب (2020) . **الجريمة في الفضاء الإلكتروني** . ط1 ، عمان : دار وائل للنشر والتوزيع.
- بوسقيعة ، أحسن (2009) . **التحقيق القضائي** . ط7 ، الجزائر : دار هومة للنشر والتوزيع.
- بوكر ، رشيدة (2012) . **جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن** . ط1 ، بيروت : منشورات الحلبي الحقوقية.

- حجازي ، عبدالفتاح بيومي (2002) . **الأحداث والانترنت** . مصر : دار الفكر الجامعي.
- حجازي ، عبدالفتاح بيومي (2002) . **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت** . مصر : دار الكتب القانونية.
- حجازي ، عبدالفتاح بيومي (2006) . **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي** . ط1 ، الاسكندرية : دار الفكر الجامعي.
- حسني ، محمود نجيب (1988) . **شرح قانون الإجراءات الجنائية** . القاهرة : دار النهضة العربية.
- حسين ، سامي جلال فقي (2011) . **التفتيش في الجرائم المعلوماتية** . مصر : دار الكتب القانونية ودار شتات للنشر والبرمجيات.
- حنفي ، حازم محمد (2017) . **الدليل الإلكتروني ودوره في المجال الجنائي** . ط1 ، القاهرة : دار النهضة العربية.
- رستم ، هشام محمد فريد (1994) . **الجوانب الإجرائية للجرائم المعلوماتية** . أسيوط : دار النهضة العربية.
- رستم ، هشام محمد فريد (1992) . **قانون العقوبات " مخاطر تقنية المعلومات "** . مصر : مكتبة الآلات الحديثة بأسيوط.
- سلامة ، محمد عبدالله (2007) . **موسوعة الجرائم المعلوماتية** . ط1 ، مصر : المكتب العربي الحديث.
- سند ، نجاتي سيد احمد (2008) . **مبادئ الإجراءات الجنائية في التشريع المصري** . جامعة الزقازيق : كلية الحقوق.

- عبابنة ، محمد أحمد (2005) . **جرائم الحاسوب وأبعادها الدولية** . ط1 ، عمان : دار الثقافة.
- عبد الستار ، فوزية (1986) . **شرح قانون الإجراءات الجنائية** . القاهرة : دار النهضة العربية.
- عفيفي ، كمال عفيفي (2007) . **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون** . ط2 ، دمشق : منشورات الحلبي القانونية.
- عياد ، سامي علي حامد (2007) . **الجريمة المعلوماتية وإجرام الانترنت** . مصر : دار الفكر الجامعي.
- فاروق ، ياسر الأمير (2009) . **مراقبة الأحاديث الخاصة في الإجراءات الجنائية** . ط1 ، جامعة القاهرة : دار المطبوعات الجامعية.
- فهمي ، محمد (1991) . **الموسوعة الشاملة لمصطلحات الحاسب الآلي الإلكتروني** . مصر : مطابع المكتب المصري الحديث.
- قشقوش ، هدى حامد (1992) . **جرائم الحاسب الإلكتروني في التشريع المقارن** . القاهرة : دار النهضة العربية.
- قنديل ، أشرف عبدالقادر (2015) . **الإثبات الجنائي في الجريمة الإلكترونية** . الاسكندرية : دار الجامعة الجديدة.
- كامل ، محمد فاروق عبدالحميد (1999) . **القواعد الفنية والشرطية للتحقيق والبحث الجنائي** . الرياض : جامعة نايف العربية للعلوم الأمنية.
- محدة ، محمد (1991-1992) . **ضمانات المشتبه فيه أثناء التحريات الأولية** . ط2 ، الجزائر : دار الهدى.

- محمد ، سعيد (2005) . **الجرائم الإلكترونية وآليات الحصول على الدليل فيها** . ط1 ، دار النشر الذهبي.
- مرسي ، عبد الواحد إمام . **الموسوعة الذهبية في التحريات** . مصر : دار المعارف والمكاتب الكبرى للنشر والتوزيع.
- مصطفى ، عائشة بن قارة (2010) . **حجية الدليل الإلكتروني في مجال الإثبات الجنائي** . الاسكندرية : دار الجامعة الجديدة للنشر.
- موسى ، مصطفى محمد (2009) . **التحقيق الجنائي في الجرائم الإلكترونية** . ط1 ، القاهرة : مطابع الشرطة.
- موسى ، مصطفى محمد (2003) . **المراقبة الإلكترونية عبر شبكة الانترنت** . ط1 ، القاهرة : دار الكتب والوثائق المصرية.
- هروال ، نبيلة هبة (2013) . **الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات** . الاسكندرية : دار الفكر الجامعي.
- يوسف ، أمير فرج (2016) . **الإثبات الجنائي للجريمة الإلكترونية والاختصاص القضائي بها** . ط1 ، الاسكندرية : مكتبة الوفاء القانونية.

ثانيا : الأبحاث والدراسات والمقالات المنشورة في الدوريات والمجلات العلمية

- أحمد ، جمال زين العابدين أمين (2021) . "الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية" ، **مجلة مستقبل العلوم الاجتماعية** ، العدد (4).
- ابراهيم ، راشد بشير (2008) . "التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي" ، **مجلة دراسات استراتيجية** ، العدد(131).

- الكسراوي ، الهاشمي (2006) . "الجريمة المعلوماتية" ، **مجلة القضاء والتشريع** ، العدد (7).
- المسند ، صالح بن محمد ، والمهيني عبدالرحمن بن راشد (2013) . "جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات" ، **المجلة العربية للدراسات الأمنية والتدريب** ، المجلد 29 ، العدد (15).
- المعمري ، عادل عبدالله خميس (2013) . "التفتيش في الجرائم المعلوماتية" ، **مجلة الفكر الشرطي** ، المجلد 22 ، العدد (86).
- رستم ، هشام محمد فريد (1995) . "جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة" ، **مجلة الدراسات القانونية** ، العدد (17).
- محمد ، محمد نصر (2012) . "التحقيق الجنائي بين الواقع والقانون دراسة تطبيقية على أنواع البصمات وحجتها" ، المجلد 21 ، العدد (83).
- مطر ، حسين خليل . "إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية" ، العدد (36).
- يوسف ، أميرة فرج (2011) . "الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت".

ثالثا : رسائل الماجستير والدكتوراة

- الرقيشي ، محمد بن ناصر بن علي (2018) . **الإثبات الجنائي في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامعة السلطان قابوس ، سلطنة عمان.
- السوفي ، نور الهدى (2017) . **التحقيق في الجريمة المعلوماتية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر.

- الشريم ، صالح خميس راشد يوسف (2020) . **الإطار القانوني لوسائل البحث والتحري عن الجرائم الإلكترونية** . (رسالة ماجستير) ، جامعة عمان الأهلية ، عمان ، الأردن.
- القحطاني ، عبدالله بن حسين الجراف (2014) . **تطوير مهارات التحقيق الجنائي في مواجهة الجريمة المعلوماتية** . (رسالة ماجستير) ، جامعة نايف للعلوم الأمنية ، الرياض.
- بخي ، فاطمة الزهراء (2014) . **إجراءات التحقيق في الجريمة الإلكترونية** . (رسالة ماجستير) ، جامع الملية ، الجزائر.
- بطاش ، صفيح (2018) . **أساليب التحري الخاصة وضمانات حقوق الإنسان** . (رسالة ماجستير) ، المركز الجامعي أحمد زبانة – غليزان ، الجزائر.
- بوحويش ، عطية عثمان محمد (2009) . **حجية الدليل الرقمي في إثبات جرائم المعلوماتية** . (رسالة ماجستير) ، أكاديمية الدراسات العليا ، بنغازي.
- جمال ، إبراهيمي (2018) . **التحقيق الجنائي في الجرائم الإلكترونية** . (أطروحة دكتوراة) ، جامعة مولودي معمري ، الجزائر.
- جواحي ، عبد الستار (2015) . **جرائم الحاسوب ، دراسة مقرنة بين الشريعة الإسلامية والقانون الجزائري** . (رسالة ماجستير) ، جامعة الشهيد حمه لخضر ، الوادي.
- سعيداني ، نعيم (2013) . **آليات البحث والتحري عن الجرائم المعلوماتية** . (رسالة ماجستير) ، جامعة الحاج لخضر.
- غلاب ، فايز محمد راجح (2011) . **الجرائم المعلوماتية في القانون الجزائري واليمني** . (أطروحة دكتوراة) ، جامعة الجزائر 1 ، الجزائر.

- قادري ، سارة (2014) . **أساليب التحري الخاصة في قانون الإجراءات الجزائية** . (رسالة ماجستير) ، جامعة قاصدي مرباح ، ورقلة ، الجزائر.
- محمد ، أكرم البكوش راشد (2012) . **المواجهة الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلال** . (رسالة ماجستير) ، جامعة طرابلس ، طرابلس ، ليبيا.

رابعا : البحوث المقدمة في المؤتمرات العلمية

- أرحومة ، موسى مسعود (2009) . "الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية" ، **المؤتمر المغاربي الأول حول المعلوماتية والقانون ، 28-29 / 10 / 2009م ، طرابلس.**
- الشواء ، سامي (1993) . "الغش المعلوماتي كظاهرة إجرامية مستحدثة" ، **مؤتمر الجمعية المصرية للقانون الجنائي ، 25-28 أكتوبر ، القاهرة.**
- عاكوم ، وليد (2003) . "التحقيق في جرائم الحاسوب" ، **المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، 26-28 أبريل ، دبي ، الإمارات العربية المتحدة.**
- فرغلي ، عبدالناصر محمد محمود (2008) . "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية" ، **المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ، 12-14 نوفمبر ، الرياض ، المملكة العربية السعودية.**
- محمود ، عبدالله حسين علي (2003) . "إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات" ، **المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، 26-28 أبريل ، دبي ، الإمارات العربية المتحدة.**

- المطردي ، مفتاح بوبكر (2012) . "الجريمة الإلكترونية" ، **المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية ، السودان.**

خامسا : المراجع القانونية

- الدستور الأردني
- قانون أصول المحاكمات الجزائية رقم (9) لسنة 1961م
- قانون الجرائم الإلكترونية لسنة 2015
- قانون الاتصالات الاردني
- قانون الاجراءات الجنائية القطري
- قانون الاجراءات الجنائية الفرنسي

سادسا : المراجع الالكترونية

- انظر : Lexique de termes Juridique au Code de Dalloz Penale, 101, e ed 2004.
- انظر المقال الالكتروني : "بعد اختراقه عشرات البنوك الهاكر الجزائري حمزة بن دلاج في قبضة الFBI" المنشور في موقع : "www.mbc. net".
- Internet " www.businessdictionary.com "
- Computer من موقع : www.techopedi
- a.comhttps://lawyeregypt.net
- https://portal.arid.my