مجلة المهرة للعلوم الإنسانية
مجلة علمية نصف سنوية محكمة
العدد الثاني عشر- ذي القعدة ١٤٤٣هـ-يونيو٢٠٢٢م
ISSN:2707-8655
EISSN:2707-8663

صعوبات التحقيق والإثبات في الجرائم المعلوماتية وأثرها على العدالة الجنائية

أ.د. كمال عبد الله المهلاوي(*)

الملخص:

تتسم الجرائم المعلوماتية بطبيعة خاصة تختلف تمامًا عن الجرائم التقليدية؛ لأنها تتم في عالم افتراضي، ومن ثم فقد كانت هذه الدراسة عن صعوبات التحقيق والإثبات في الجرائم المعلوماتية، وأعني بذلك تلك العقبات والعوائق التي قد تقف في طريق المحقق الجنائي أثناء مباشرته لعملية التحقيق في أي مرحلة من مراحله.

واتبعت المنهج الوصفي والتحليلي، وتوصلت إلى أن للجرائم المعلوماتية طبيعة خاصة تختلف عن الجرائم التقليدية، لذلك يجب أخذ الحذر من قبل المحققين الجنائيين في التعامل معها. وأن الجرائم المعلوماتية هي جرائم عالمية لا تعترف بالحدود السياسية والجغرافية، وهذا يتطلب وجود تعاون دولي لمكافحتها. ويتمتع المجرم المعلوماتي بذكاء بينما جهات التحقيق قد تفتقر تماما للخبرة والكفاءة في هذا المجال. ومن خلال هذه النتائج أوصي، بتدريب كل من له علاقة في عملية التحقيق في هذا النوع من الجرائم. وضرورة التعاون الدولي بين مختلف دول العالم. وضرورة تبليغ جهات التحقيق فور وقوع الجريمة من قِبَل كل من يتعرَّف إلى هذا النوع من الجرائم، لاسيما المؤسسات والشركات التجارية والبنوك وغيرها ممن يمتنع عن التبليغ بسبب خوفهم من فقد ثقة عملائهم، وخوفهم على سمعتهم. ولابد من وضع قانون إجراءات جنائية وقانون إثبات خاص بالجرائم المعلوماتية؛ نظرا لقصور كل من قانون الإجراءات وقانون الإثبات التقليديين.

الكلمات المفتاحية: الصعوبات، التحقيق؛ الإثبات، الجرائم المعلوماتية، العدالة الجنائية

(*) أستاذ القانون العام، كليات الخليج للعلوم الإدارية والإنسانية.

Difficulties of Investigation and Evidencing of Cyber-Crimes and their Impact on Criminal Justice

Prof. Kamal Abdullah Al-Mahlaawy

Abstract

Cybercrimes are of a particular nature that are completely different from traditional crimes since they occur in a virtual world. Thus, this study deals with the difficulties of investigating and evidencing on cyber-crimes, i.e., those impediments and obstacles that may stand in the way of the criminal investigator as he undertakes the investigation process at any stage of the investigation. This study followed the descriptive and analytical approach and concluded that cyber-crimes have a special nature that differ from traditional crimes. Therefore, criminal investigators must be vigilant in dealing with them. Further, cyber-crimes are global crimes that do not recognize political and geographical borders, and to this end, international cooperation to combat them is a requirement. Cyber-criminals possess intelligence, while the investigation authorities may completely lack experience and competence in this domain. In light of these results, the researcher recommends training everyone involved in the process of investigating this type of crimes. Also, there is a need for international cooperation between different countries of the world. As well as the necessity of notifying the investigation authorities immediately upon the occurrence of the crime by everyone who recognizes this type of crime, especially institutions, commercial companies, banks and others who refrain from reporting because of their fear of losing their clients' trust, and their fear for their reputation. It is also necessary to impose criminal procedures' law and a special evidencing law for cyber-crimes due to the shortcomings of both the code of procedure and the traditional evidentiary act.

Keywords: Difficulties; Investigation; Evidence, Cybercrimes, Criminal justice

ISSN:2707-8655
EISSN:2707-8663

مقدمة:

أدى التطور السريع في التقنية الحديثة وخاصة في مجال الإنترنت إلى ظهور سلبيات كثيرة بجانب إيجابياتها التي لا تخفى على أحد، ومن أبرز هذه السلبيات: استغلال المجرمين لهذه الشبكة في عملياتهم الإجرامية، ذلك لأنها شبكة دولية واسعة لا يمكن حصر كل من يستخدمها من الأفراد، وكل ما يتم فيها من عمليات، فيستطيع أي شخص أن يفعل كل ما يريد، ثم يمحو ذلك بكل سهولة ويسر.

وللجريمة المعلوماتية طبيعة خاصة تميزها عن الجريمة التقليدية، وللمجرم المعلوماتي أيضًا خصائص تميزه عن المجرم التقليدي، ولذلك يجب أن يتمتَّع المحقق الجنائي بصفات خاصة ليتمكن من فك لغز الجريمة التي أمامه، والتي يكون مسرحها جهاز الحاسب الآلي، ويتضح لنا من الواقع العملي أن المحقق الجنائي في الجرائم المعلوماتية يواجه الكثير من الصعوبات التي تُعيقه للتوصل إلى المجرم المعلوماتي.

أهمية البحث:

تتمثل أهمية هذا البحث في أنه يسعى إلى توضيح الصعوبات التي تعترض طريق المحقق الجنائي في الوصول إلى الحقيقة، بما يساهم في تقديم المشورة لجهات الاختصاص في إدراك تلك الصعوبات وحلها ليسهل القبض على هؤلاء المجرمين وتقل نسبة هذه الجرائم في المجتمع.

أهداف البحث:

يهدف البحث إلى:

1. تحري الصعوبات التي تواجه المحقق الجنائي في الجرائم المعلوماتية.
2. توضيح الصعوبات التي تواجه المحقق الجنائي في مرحلة المعاينة في الجرائم المعلوماتية.
3. توضيح الصعوبات التي تواجه المحقق الجنائي في مرحلة التفتيش في الجرائم المعلوماتية.
4. توضيح الصعوبات التي تواجه المحقق الجنائي أثناء الضبط في الجرائم المعلوماتية.

مشكلة البحث:

تكمن مشكلة البحث في الصعوبات التي تعترض المحقق الجنائي من الوصول إلى المجرم المعلوماتي. ويجيب البحث عن الأسئلة الآتية:

1. ماذا نعني بصعوبات التحقيق والإثبات في الجرائم المعلوماتية؟
2. ما هي الصعوبات التي تواجه المحقق الجنائي أثناء المعاينة في الجرائم المعلوماتية؟
3. ما هي الصعوبات التي تواجه المحقق الجنائي أثناء التفتيش في الجرائم المعلوماتية؟
4. ما هي الصعوبات التي تواجه المحقق الجنائي أثناء الضبط في الجرائم المعلوماتية.

منهج البحث:

اتبع البحث المنهج الوصفي التحليلي.

ولغرض البحث تم تقسيمه إلى مقدمة وستة مباحث وخاتمة.

المبحث الأول: (مفهوم الجرائم المعلوماتية)

المطلب الأول: تعريف الجريمة

أولا: الجريمة لغةً

الجُرْمً هو التَّعدِّي، والجُرْمً الذنب ويجمع على أجْرام، وهو الجريمة، وقد جَرَمَ يَجْرِمُ جَرْماً وأجْترم وأجْرَام، فهو مُجْرِم وجريمُ[1].

[1] لسان العرب: 12/ 91.

ISSN:2707-8655
EISSN:2707-8663

ثانيًا: الجريمة اصطلاحًا

الجريمة هي محظورات شرعية زجر الله تعالى عنها بحدٍّ أو تعذير[1].

ثالثًا: الجريمة قانونًا

هي كل فعل معاقب عليه بموجب أحكام هذا القانون أو أي قانون آخر[2]، والمقصود هنا القانون الجنائي لسنة 1991م أو أي قانون آخر غيره.

المطلب الأول: تعريف المعلوماتية

أولاً: المعلوماتية لغةً

المعلوماتية جمع معلومة من العِلْم، والعِلْمُ هو نقيض الجهل، علم علمًا وعلمَ، وعَلِم الأمْرَ وتَعَلَّمَه أي أتقنه[3].

ثانيًا: المعلوماتية اصطلاحًا

المعلوماتية هي البيانات التي تتم معالجتها لترتيبها وتنظيمها وتحليلها بقصد الاستفادة منها[4].

ثالثًا: المعلوماتية قانونًا

المعلوماتية هي نظم وشبكات ووسائل المعلومات، والبرمجيات والحواسيب والإنترنت والأنشطة المتعلقة بها[5].

---

(1) الموسوعة الفقهية: 59/16.

(2) القانون الجنائي السوداني لسنة 1991م:3.

(3) لسان العرب:12/ 417.

(4) الجرائم الإلكترونية وآثارها على النسيج الاجتماعي:31.

(5) مجلة أبحاث ودراسات التدريب والمعلومات،ج8، 2012م : 114.

رابعًا: الجريمة المعلوماتية

هي كل فعل ضارٍ يأتيه الفرد أو الجماعة عبر استعمال الأجهزة الإلكترونية، ويكون لهذا الفعل أثرٌ ضارٌ على غيره[1].

ويمكن تعريفها بأنها: كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي/ الجوالات الذكية بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي، وينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل.

المطلب الثاني: خصائص الجريمة المعلوماتية

للجريمة المعلوماتية العديد من الخصائص التي تميزها عن الجريمة التقليدية نظرًا لطبيعتها الخاصة، وهذه الخصائص تتمثل فيما يلي:

أولاً: ترتكب عن طريق الحاسب الآلي

يعد الحاسب الآلي هو السبب الرئيس في إيجاد هذا النوع من الجرائم كونه الأداة المستخدمة لارتكابها؛ لأنه يُمكِّن الأشخاص من الدخول على شبكة الإنترنت وتنفيذ الجريمة من خلالها أيًّا كانت هذه الجريمة[2].

وهذه الخاصية هي الأساس الذي تبنى عليه الخواص الأخرى؛ إذ لولاها لما وجدت هذه الجرائم العابرة للحدود التي يصعب إثباتها.

---

[1] جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية:32.

[2] قانون الحاسوب: 213.

ISSN:2707-8655
EISSN:2707-8663

ثانيًا: عابرة للحدود

عندما نقول إن الجريمة المعلوماتية جريمة عابرة للحدود فإننا نعني بذلك أنها غير محدودة أو محصورة برقعة جغرافية معينة؛ إذ يمكن أن تُرتكب الجريمة المعلوماتية في مكانٍ ما وتظهر آثارها في مكان آخر سواء أكان قريبا منه أم بعيدا، ذلك لأن شبكة المعلومات تربط بين أجهزة الحاسب الآلي المرتبطة بها في مختلف أنحاء العالم[1].

ثالثًا: لا يستخدم فيها العنف

تحتاج الجرائم التقليدية في أغلب الأحيان إلى بذل مجهود عضلي؛ كثيرا كان أو قليلا من قبل من يرتكبها كجريمة القتل وغيرها من الجرائم التقليدية، أما الجرائم المعلوماتية فكل ما تتطلبه مقدرة ذهنية وعقلية لدى الجاني، ومعرفة بتقنيات الحاسب الآلي، وتوافر العلم الكافي ببعض البرامج التشغيلية[2] التي قد يحتاجها لارتكاب هذا النوع من الجرائم.

رابعًا: صعبة الإثبات

البيئة التي تتم فيها الجريمة المعلوماتية هي بيئة افتراضية رقمية لا تترك خلفها آثارا مادية يمكن من خلالها حل لغز الجريمة المعلوماتية والوصول إلى مرتكبها، وحتى لوجدت هذه الآثار المادية فإنه يصعب المحافظة عليها كبيّنَة؛ لذلك يجب عند إيجادها أن يتم التعامل معها بواسطة مؤهلين فنيا وأكاديميا[3].

وتعود صعوبة الإثبات في الجرائم المعلوماتية:

أ. صعوبة الاحتفاظ الفني بآثارها إن وجدت.

ب. أنها تعتمد على الخداع في ارتكابها، والتضليل في التعرف على مرتكبيها.

---

(1) **التفتيش في الجرائم المعلوماتية: 27 –28.**

(2) **جرائم الحاسب الآلي والانترنت:107 –108.**

(3) **شرح قانون جرائم المعلوماتية السوداني:9.**

ج. أنها تعتمد على قمة الذكاء والمهارة في ارتكابها.

د. يلعب البعد الزمني (اختلاف المواقيت بين الدول) والمكاني (إمكانية تنفيذ الجريمة عن بعد) والقانون (أي قانون يطبق) دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم[1].

هـ. أنها تحتاج إلى خبرة فنية وتقنية من قبل المحقق الجنائي، وذلك يصعب جدًّا على المحقق الجنائي التقليدي[2]؛ لأنه يفتقر لتلك الخبرة الفنية التقنية مما يجعل تعامله مع هذا النوع من الجرائم صعبًا جدًّا.

المطلب الثالث: خصائص المجرم المعلوماتي

يطلق على المجرم المعلوماتي مصطلح (هاكرز)، وهو مفهوم لوصف الأشخاص الذين يستخدمون الحاسب الآلي في الأنشطة غير القانونية والأنشطة التدميرية[3]، ويتميز المجرم المعلوماتي بخصائص عديدة تميزه عن المجرم التقليدي وهي كالآتي:

أولاً: المجرم المعلوماتي اجتماعي

يحيا المجرم المعلوماتي– عادة– وسط المجتمع، ويمارس عمله في المجال المعلوماتي أو غيره من مجالات الحياة الأخرى، وقد يرتكب الكثيرون منهم جرائم معلوماتية بدافع الكبرياء، أو بدافع النصب، أو الحسد، أو بدافع إظهار قدرته على التفوق في هذا المجال، أو بغرض الحصول على منفعة مادية[4] أو

---

(1) الجوانب الإجرائية كجرائم الإنترنت: 40.

(2) جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها: 19.

(3) الجرائم الإلكترونية وآثارها على النسيج الاجتماعي: 22.

(4) الجرائم المعلوماتية: 77.

ISSN:2707-8655
EISSN:2707-8663

لشغفهم بالمعلوماتية، أو بغرض إضرار الغير[1] أو غيرها من الأسباب التي تدفع به إلى فعل ذلك ولو بشكل غير مستمر.

ثانيًا: المجرم المعلوماتي ذكي

يتميز المجرم المعلوماتي- غالبًا- بالذكاء، ذلك لأن هذه الجرائم لا يستطيع ارتكابها إلا من يتمتع بذكاء ومعرفة فائقين بتقنيات الحاسب الآلي؛ لأنه لا يستطيع مواجهة المصاعب التي تواجهه عند ارتكابه للجريمة المعلوماتية ما لم يكن يتمتع بالذكاء الحاد، ومن أمثلة هذه الصعوبات التي تواجهه أن يكون الحاسب الآلي محمياً بكلمة سرٍ معينة[2].

ثالثًا: المجرم المعلوماتي ذو خبرة

يتمتع المجرم المعلوماتي بخبرة فائقة في مجال الحاسب الآلي، ومهارة عالية في كيفية التعامل معه، وهذه الخبرة والمهارة تسهلان لهم عملية ارتكاب الجريمة المعلوماتية، وغالبًا يعملون كمبرمجين أو محللين أو مشغلين[3].

رابعًا: المجرم المعلوماتي لا يستخدم العنف

لا يحتاج المجرم المعلوماتي عند ارتكابه للجريمة المعلوماتية إلى استخدام العنف، فهذا النوع من الجرائم تتم عن طريق جهاز الحاسب الآلي، ويحتاج فيها إلى الذكاء الحاد فقط لا إلى غيره من الأساليب الأخرى كالعنف[4].

---

(1) **التفتيش في الجرائم المعلوماتية: 31.**

(2) **المرجع نفسه:31– 32.**

(3) **الجريمة المعلوماتية في القانون السوداني:9.**

(4) **قانون الحاسوب: 214.**

المبحث الثاني: مفهوم صعوبات التحقيق والإثبات في الجرائم المعلوماتية

المطلب الأول: تعريف الصعوبات

أولاً: الصعوبات لغةً

الصَّعْبُ خلاف السَّهْل، وصَعُب الأمر وأَصْعَبَ يَصْعُب صُعوبة صار صَعْبًا[1] وصعب تجمع على صعوبات.

ثانيًا: الصعوبات اصطلاحًا

الصعوبات هي كل موقف غير معهود لا يكفي لحله الخبرات السابقة والسلوك المألوف[2].

المطلب الثاني: تعريف التحقيق

أولاً: التحقيق لغةً

الحق نقيض الباطل، ويجمع حُقوقٌ وحِقاقٌ، حققت الرجل وأحققته إذا غلبته على الحق وأثبته عليه وحقه على الحق وأحقه عليه، وأستحقه طلب منه حقه[3].

ثانيًا: التحقيق اصطلاحاً

التحقيق هو بذل المجهود في طلب المقصود أو طلب الشيء بغالب الظن عند عدم الوقوف على حقيقته[4].

---

[1] لسان العرب: 340/7.

[2] الموسوعة الحرة، ويكبيديا.

[3] لسان العرب: 256/3.

[4] الموسوعة الفقهية: 187/10.

ISSN:2707-8655
EISSN:2707-8663

ثالثًا: التحقيق قانونًا

التحقيق هو اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة[1].

المطلب الثالث. تعريف الإثبات

أولاً: الإثبات لغةً

ثَبتَ الشيءُ يَثْبُتُ ثَباتًا وثُبوتًا فهو ثابتٌ وتثبيتٌ، وأثْبت حُجَّتَهُ؛ أي أقامها وأوضحها[2].

ثانيًا: الإثبات اصطلاحًا

الإثبات هو إقامة الدليل الشرعي أمام القاضي في مجلس قضائه على حق أو واقعة من الوقائع[3].

ثالثًا: الإثبات قانونًا

الإثبات هو أي وسيلة يتم بها إثبات أو نفي أي واقعة متعلقة بدعوى أو نزاع أمام المحكمين أو الموفقين[4].

إذن الصعوبات هي: تلك العقبات أو المعوقات التي قد تعترض طريق المحقق الجنائي أثناء سير التحقيق في أي مرحلة من مراحله – معاينة، تفتيش، ضبط – بخصوص جريمة من الجرائم المتعلقة بالحاسب الآلي.

---

(1) البوليس العلمي أو فن التحقيق:1.
(2) لسان العرب:2/ 79 –80.
(3) الموسوعة الفقهية: 232.
(4) قانون الإثبات السوداني لسنة 1994م، م4.

المبحث الثالث: المعاينة

المطلب الأول: مفهوم المعاينة

أولاً: المعاينة لغةً

العَيْنُ والمعاينة هي النظر، وقد عاينَه مُعاينة وعِيانًا أي رآه[1].

ثانيًا: المعاينة اصطلاحًا

المعاينة هي فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، مثل معاينة مكان ارتكاب الجريمة أو أداة الجريمة[2].

المطلب الثاني: أنواع المعاينة

أولاً: معاينة المكونات المادية للحاسب الآلي

تتمثل المكونات المادية في الحاسب الآلي في وحدة الإدخال (لوحة المفاتيح، الفأرة، الماسح الضوئي) ووحدة المعالجة المركزية (الذاكرة الرئيسية، وحدة الحساب والمنطق، وحدة السيطرة والتحكم)، ووحدة الإخراج (الشاشة، الطابعة، الأشرطة المغناطيسية، الأغراض المغناطيسية ووسائط الخزن الأخرى) [3].

والجرائم التي تقع على المكونات المادية للحاسب الآلي هي مثل الاعتداء على أشرطة الحاسب الآلي وكابلاته، وشاشة العرض الخاصة الطابع المادي المحسوس[4]، وعموما ليست هنالك أي صعوبة كتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينته من قبل مأموري الضبط القضائي والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين وكذلك

---

(1) لسان العرب: 55/9.

(2) التحقق وجمع الأدلة في الجرائم المعلوماتية:394.

(3) التفتيش في الجرائم المعلوماتية: 211–216.

(4) جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية:356.

ISSN:2707-8655
EISSN:2707-8663

وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها، مع إخطار النيابة العامة بذلك.

ثانيًا: المكونات غير المادية للحاسب الآلي

تتمثل المكونات غير المادية للحاسب الآلي في البيانات والبرامج، والبيانات مثل النصوص والخرائط وغيرها من البيانات التي تتحول إلى معلومات، أما البرامج فهي مثل برامج نظم التشغيل ونظم إدارة وقواعد البيانات، أو برامج تطبيقية مثل الأفراد والأجور وغيرها[1].

من الجرائم الواقعة على المكونات غير المادية للحاسب الآلي تلك الجرائم الواقعة على برامج الحاسب الآلي أو بياناته أو تتم بواسطتها، وكذلك الجرائم التي تتم عن طريق الإنترنت، ومنها أيضا جرائم التزوير المعلوماتي والتخريب الذي يتم بطريق الفيروس المعلوماتي[2].

المطلب الثالث: صعوبات المعاينة

أولاً: إحجام المجني عليهم عن الإبلاغ

المجني عليهم- في كل الجرائم بصورة عامة وفي الجرائم المعلوماتية الجرائم المعلوماتية بصورة خاصة- هم المتضررون الأساسيون من وقوع هذه الجرائم عليهم، ولذلك ينبغي أن يقوموا بإبلاغ الجهات المختصة بالتحقيق فور حدوث الجريمة، بل وينبغي عليهم أيضا أن يدلوا بأي معلومات أو وقائع قد تعرضوا لها قبل وقوع الجريمة كالتهديد والابتزاز وغيرها، حتى يسهل على الجهات المختصة القيام بالتحقيق ومساعدتهم، ويتمكنوا معهم من الوقوف على دوافع ارتكاب الجريمة[3]، وحل لغزها والوصول إلى الجاني الحقيقي، ولكن المجني عليهم في الواقع قد لا يقومون بالإبلاغ عن الجريمة، سواء أكانوا طبيعيين أم اعتباريين وذلك لعدة أسباب منها:

---

(1) ينظر: الجرائم المعلوماتية: 73.

(2) ينظر: المرجع نفسه: 183.

(3) ينظر: البينة الإلكترونية: 52.

1. افتقارهم للقدرة الفنية التي تمكنهم من كشف الجريمة[1].

2. خوفهم على سمعتهم ومكانتهم وعلى فقدهم ثقة الناس فيهم وفي كفاءتهم.

3. محاولة إخفاء أسلوب الجريمة لكي لا يتم تقليدها من قبل مجرمين آخرين.

وبسبب هذه المخاوف لا يقومون بالإبلاغ عن الجرائم التي تقع عليهم، وهذا يؤدي إلى تمادي المجرمين بنقاط الضعف في أنظمتهم[2] الأمر الذي يشجع ويدفع الكثير من الجناة على ارتكاب المزيد من الجرائم على هذه الجهات وعلى غيرها[3].

إن إحجام أو تأخر المجني عليهم بالإبلاغ عن وقوع الجريمة يؤدي إلى كثير من الأضرار والعوائق التي تقف في طريق من يقوم بعملية المعاينة وتجعل فهمها صعبًا، أكثر مما لو كان قد أُبلغ عنها فور حدوثها وانتقل فورًا إلى مسرح الجريمة.

ومن أهم السوابق القضائية التي تدور حول مشكلة عدم إبلاغ المجني عليهم والأضرار المترتبة على ذلك هي قيام مدير المبيعات في إحدى الشركات الإنجليزية وباستخدام أسماء وهمية لشركات في حسابات الشركة التي تجرى معالجتها عن طريق الحاسب، ولم يكتف بما سببه من أضرار مادية بسبب الاختلاس بل طالب بمنحه إفادة تسمح له بالعمل في شركات أخرى مقابل عدم تشهيره بالشركة[4].

ثانيًا: عدم وجود آثار مادية

الجريمة المعلوماتية ذات طبيعة مختلفة عن الجريمة التقليدية، حيث إن الجريمة التقليدية غالباً ما تترك آثاراً مادية يسهل من خلالها على المحقق الجنائي حل لغز الجريمة والوصول إلى مرتكبها في أقل وقت

---

(1) **التفتيش في الجرائم المعلوماتية: 29.**

(2) **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 110.**

(3) **الجريمة المعلوماتية في القانون السوداني: 10.**

(4) **ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: 357.**

ISSN:2707-8655
EISSN:2707-8663

ممكن، ولكن الجريمة المعلوماتية لا توجد لديها آثار مادية يمكن الوصول إلى مرتكبها بأسرع وقت؛ لأنها تتم عبر نبضات الكترونية غير ملموسة[1]، لذلك من الصعب جدًّا على المحقق الجنائي حل لغز هذا النوع من الجرائم، فالعديد من العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي لا يتطلب بالضرورة وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدًّا ومخزنًا على جهاز الحاسب الآلي، وتتوافر أمام المتعامل خيارات عديدة، وليس عليه سوى أن ينقر على الخيار الذي يريده؛ فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى، حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء أو نقلها من مكان إلى آخر بطريقة آلية وحسب الأوامر المعطاة للجهاز، ويكون الاختلاس أو التزوير بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب، أو بتعديل البرنامج المخزن في جهاز الحاسب الآلي، وبذلك تكون النتيجة مخرجات على هوى مستعمل الجهاز الذي أدخل البيانات أو عدَّل البرنامج، ولأنه لا يوجد استخدام وثائق أو مستندات ورقية فإن الجريمة تفقد آثارها المادية[2].

ثالثًا: تردد الأشخاص على مسرح الجريمة

قد تقوم أعداد كبيرة من الأشخاص بالتردد على مسرح الجريمة خلال المدة الزمنية، التي غالبًا ما تكون طويلة نسبيًّا، ما بين اقتراف الجريمة والكشف عنها؛ الأمر الذي يمنح فرصة للجاني أو الآخرين لأن يقوموا[3] بتغيير أو تلفيق أو العبث بالآثار المادية، أو زوال بعضها وهو ما يؤدي إلى الشك في

---

(1) ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: 356.

(2) ينظر: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 83 – 84.

(3) مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 101–102

الدليل المأخوذ من المعاينة[1]، ولذلك ينبغي أن يتم التبليغ بأقصى سرعة عند حدوث الجريمة، حتى لا يتم تغيير مسرح الجريمة المعلوماتية.

رابعًا: صعوبة المحافظة على الدليل المعلوماتية

تكون البيانات والمعلومات المتداولة عبر الانترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة، ولا تقرأ إلا بواسطة الحاسب الآلي ولذلك ولما تتميز به الجرائم المعلوماتية من طبيعة فنية معقدة فإنه يصعب المحافظة على الأدلة المعلوماتية ومن ثم فإننا نكون بحاجة إلى خبرة فنية معينة يتمتع بها رجال التحقيق، أو كل من يقوم ويشارك في عملية المعاينة، بحيث تتوافر لديهم المقدرات الفنية والتقنية التي تمكنهم من القيام بإجراء المعاينة على أدق وأكمل وجه[2].

خامسًا: إعاقة الوصول إلى الدليل المعلوماتي

قد يقوم المجرم المعلوماتي بإعاقة الوصول إلى الدليل المعلوماتي بشتى الوسائل، فهو بعد ارتكاب جريمته يقوم بدس برامج، أو وضع كلمات سرية كرموز تعيق من يقوم بإجراء المعاينة من الوصول إلى الدليل المعلوماتي، أو يلجأ إلى تشفير المعلومات، مما يصعب الوصول إلى دليل يدينه، وذلك لأنه من السهل على المجرم المعلوماتي في أغلب الجرائم المعلوماتية محو الدليل في زمن قياسي، ولا يستغرق ذلك سوى دقائق معدودة بالاستعانة بالبرامج المخصصة لذلك[3].

---

(1) ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون: 356.

(2) مجلة الأبحاث ودراسات التدريب والمعلومات: 119.

(3) الجريمة المعلوماتية في القانون السوداني: 11.

ISSN:2707-8655
EISSN:2707-8663

المبحث الرابع: التفتيـش

المطلب الأول: مفهوم التفتيش

أولاً: التفتيش لغةً

الفَتْشُ والتَفتْيشُ: الطلبُ والبحثُ[1].

ثانيًا: التفتْيشُ قانونًا

هو إجراء من المتحري يقوم على أساس الاطلاع على محلٍّ منح له القانون حماية خاصة، باعتباره مكمن سرِّ صاحبه. فلا يجوز كقاعدة عامة الاطلاع عليه إلا بحكم القانون أو برضا صاحبه[2].

المطلب الثاني: أنواع التفتيش

أولاً: تفتيش المكونات المادية للحاسب الآلي

قد تقع بعض الجرائم على المكونات المادية للحاسب الآلي مثل كابلاته، وشاشة العرض الخاصة به، ومفاتيح تشغيله وغيرها وذلك في حال سرقتها أو إتلافها أو اختلاسها[3].

الغرض من تفتيش المكونات المادية للحاسب الآلي هو البحث عن شيء يتصل بالجريمة المعلوماتية، التي قد وقعت، ويفيد التفتيش في كشف الحقيقة عن الجريمة المعلوماتية وعن مرتكبها، وتفتيش المكونات المادية للحاسب الآلي يتوقف على أمر واحد وهو طبيعة المكان الموجودة فيه هذه المكونات، وهل هو مكان عام أم خاص، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان له حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونًا في التشريعات المختلفة، ويجب داخل المكان الخاص التمييز بين ما إذا كانت

---

(1) لسان العرب: 175/10.

(2) قانون الإجراءات الجنائية: 294.

(3) ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 363.

هذه المكونات المادية منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب أو بنهاية طرفيه في مكان آخر كمسكن لا يخص مسكن المتهم، فإذا كانت هنالك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة؛ لذا تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما في الأماكن العامة إذا وجد شخص وهو يحمل هذه المكونات المادية أو مسيطرًا عليها أو حائزًا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال[1].

ثانيًا: تفتيش المكونات غير المادية للحاسب الآلي

لمَّا كان محل الجريمة المعلوماتية هو المكونات غير المادية للحاسب الآلي وهي البرامج والبيانات أو تمت الجريمة بواسطتها فإن ذلك يؤدي إلى سؤال مفاده: هل يمكن تطبيق القواعد التقليدية للتفتيش أم لا[2]؟.

1- برامج الحاسب الآلي

لا يحتاج الأمر إلى تقرير قواعد جديدة للتفتيش عن أدلة الجرائم التي يكون محلها برامج الحاسب الآلي كالسرقة أو الإتلاف أو استعمال هذه البرامج كأداة في ارتكاب بعض الجرائم، كالتزوير أو التلاعب في البيانات أو الإتلاف الفني للأنظمة المعلوماتية، وذلك لكفاية القواعد التقليدية لمواجهة هذه الأحوال أيًّا كانت الوسيلة المستخدمة لارتكاب الجريمة، سواء أكانت تقليدية أو كانت معلوماتية حيث يمكن إثبات الجرائم المعلوماتية عن طريق الالتجاء إلى الفنيين المتخصصين في هذا المجال.

2- بيانات الحاسب الآلي

---

(1) ينظر: الجرائم المعلوماتية على شبكة الإنترنت: 233 – 234.

(2) المرجع نفسه: 195.

ISSN:2707-8655
EISSN:2707-8663

إذا كان محل الجرائم هو البيانات المخزنة بالأنظمة المعلوماتية فإن الأمر هنا فيه بعض الصعوبات وذلك بالنظر لكونها ليست ذات طابع مادي ملموس ، ولكن يحاول بعض أهل الفقه التغلب عليها باللجوء إلى حيلة التمييز بين المعلومات وبين البيانات المعالجة آليًا، فينفي الطابع المادي عن أولها أو يؤكد للثانية طابعًا ماديًا على أساس أنها نبضات أو ذبذبات إلكترونية وإشارات أو موجات كهرومغناطيسية، قابلة لأن تسجل وتخزن على وسائط معينة، ويمكن قياسها، وبالتالي ينفون الطابع غير المادي لهذه البيانات؛ مؤكدين أنها شيء يمكن لمسه في المحيط الخارجي، وأنها كيان مادي لا يمكن جحده، مستندين في ذلك إلى حكم صدر من محكمة جنح بروكسل الذي أكد على كون هذه البيانات أشياء مادية ملموسة، وانتهوا إلى إمكانية خضوع هذه البيانات لقواعد التفتيش التقليدية وبالتالي إمكانية ضبطها[1]. إلا أن المشكلة ليست في أن هذه البيانات ذات طابع مادي أو لا، بل تكمن في وجود صعوبات وعوائق إجرائية من شأنها إعاقة خضوع البيانات المخزنة آلياً لقواعد التفتيش التقليدية، ويمكن تلخيصها فيما يلي:

أ. حالة وجود النظام المعلوماتي داخل أحد المساكن مع وجود النهاية الطرفية له في مكان آخر، الأمر الذي يعطي الجاني فرصة سانحة للتخلص من البيانات التي يستخدمها التفتيش، وهذا يتطلب منح الشخص المخول بالتفتيش السلطة الكاملة للتوصل إلى النهاية الطرفية، وتسجيل ما تحويه من بيانات تعد أدلة على ارتكاب جريمة ما دون التقيد بالحصول على إذن القاضي بذلك كما هو مقرر قانونا في حالة تفتيش منزل غير منزل المتهم.

ب. إن إذن التفتيش يشترط أن يكون محدَّدًا فيما يخص محله والأشياء التي يهدف التفتيش إلى ضبطها، ويقتصر ذلك أن يقوم مصدر الإذن بتحديد الأشياء المراد ضبطها بطريقة فنية؛ الأمر الذي لا يكون في مقدوره؛ لأنه يتطلب نوعا من المعرفة تتجاوز المعرفة العامة.

---

[1] ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 364.

ج. أن تفتيش البيانات المخزنة آليا للقيام بعملية ولوج للأنظمة المعلوماتية التي تحويها لضبط ما يعد صالحا من هذه البيانات كدليل لارتكاب جريمة ما؛ يقتضي أن يكون الشخص القائم بالتفتيش لديه معرفة كافية بكيفية التعامل مع البرامج والملفات والبيانات المخزنة بالحاسب الآلي وكذلك كيفية فك كلمة السر والمرور اللازمين للدخول إلى النظام[1].

المطلب الثالث: شروط التفتيش

عند القيام بعملية التفتيش من قبل جهاز التحقيق في جريمة من الجرائم المعلوماتية لابد من توافر العديد من الشروط في التفتيش التي منها ما هو موضوعي، ومنها ما هو شكلي، وتتمثل في الآتي:

أولاً: الشروط الموضوعية

تتمثل الشروط الموضوعية للتفتيش في: سبب التفتيش ومحله والغاية منه، والجهة المختصة بإصدار إذنه، والجهة القائمة به أو التي تباشره.

1- سبب التفتيش

سبب التفتيش يقصد به وقوع الجريمة، أي أنه لابد لكي يتم التفتيش أن تكون الجريمة قد وقعت بالفعل وليست محتملة الوقوع، والسبب في ذلك هو أن التفتيش من الإجراءات الخطيرة التي تمس حرية الأشخاص وحرمة حياتهم، فلا يجوز انتهاكها إلا إذا ارتكبت جريمة بالفعل، فلا يجوز انتهاك حرية الأشخاص ومنازلهم بمجرد وجود احتمال ارتكاب جريمة[2].

وأن تحديد وقوع جريمة من عدمه يرجع إلى مبدأ الشرعية (لا جريمة ولا عقوبة إلا بنص) هذا المبدأ تظهر أهميته بشكل كبير ونحن نتحدث عن سلوكيات جديدة لارتكاب الجرائم، والتي تتطلب من المشرع ضرورة التدخل السريع وإدخال نصوص في القانون لتجريمها خاصة عندما تعجز النصوص

[1] ينظر: جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 364 –365.

[2] ينظر: الأدلة الالكترونية وحجيتها في الإثبات الجنائي: 68–69.

ISSN:2707-8655
EISSN:2707-8663

التقليدية عن احتوائها، مثل الاعتراض غير المصرح به للاتصالات الإلكترونية أو الهجوم على مواقع الإنترنت[1].

2- محل التفتيش

يقصد بمحل التفتيش مستودع سرِّ الإنسان وهو الحاسب الآلي، وهذا المحل إما أن يكون موجودًا في مكان معين منحه القانون حرمة خاصة كالمسكن، أو بحوزة شخص كالحاسوب المحمول، ولابد من توافر شرطين فيه، هما:

أ. أن يكون المحل معينًا: يجب أن يكون المحل معينًا تعينًا نافيًا للجهالة.

ب. أن يكون المحل مما يجوز تفتيشه

قد يمنح القانون محل الجريمة حصانة معينة فيمنع إجراء تفتيشه على الرغم من توافر الشروط اللازمة للتفتيش، ويرجع ذلك إلى تعلقه بمصلحة معينة؛ عامة كانت أم فردية، يرى المشرع أنها أولى بالرعاية من مصلحة التحقيق التي تتطلب إجراء التفتيش[2]؛ أي أنه يجب أن لا يكون محل التفتيش مما يمنع تفتيشه بحصانة أو بغيرها.

3- الغاية من التفتيش

لابد أن تكون الغاية من التفتيش دائما هي ضبط أشياء تتعلق بالجريمة، التي تم التفتيش من أجلها أو أي أشياء تفيد في كشف الحقيقة، ويقع باطلا التفتيش الذي يجري لغاية أخرى خلاف ما حدده المشرع؛ لأن كل تفتيش يجري بغير أن يتبين وجه المصلحة منه يكون إجراء تحكميًّا وباطلاً[3].

---

(1) ينظر: جرائم الحاسب الآلي والإنترنت: 271.

(2) التفتيش في الجرائم المعلوماتية: 127 – 131.

(3) مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 358 – 359.

4- الجهة المختصة بإصدار إذن التفتيش

إذن التفتيش هو تفويض يصدر من سلطة التحقيق المختصة إلى أحد مأموري الضبط القضائي مخولاً إياه إجراء التفتيش التي تختص به تلك السلطة [1].

وقد نص قانون الإجراءات الجنائية السوداني لسنة 1991 في المادة 86 على من له حق إصدار إذن التفتيش:

1. يجوز لوكيل النيابة أو القاضي في أي وقت من تلقاء نفسه أو بناء على طلب من الجهة المختصة في أي دعوى جنائية أن يصدر أمرًا بإجراء التفتيش الخاص لأي مكان أو شخص من رأى أن ذلك يساعد في أغراض التحري أو المحاكمة أو التنفيذ بحسب الحال.
2. يجوز للقاضي في أي وقت بناء على طلب من الجهة المختصة أن يصدر أمرًا بإجراء التفتيش العام لأي أمكنة أو أشخاص متى رأى أن ذلك يساعد في أغراض اكتشاف الجريمة[2].

5- الجهة التي تباشر التفتيش

نصت معظم التشريعات على أن سلطة مباشرة التفتيش هي السلطة المختصة بالتحقيق وذلك لكون التفتيش إجراء من إجراءات التحقيق، وتباشر جهات التحقيق عملية التفتيش بنفسها إذا كان المكان المراد تفتيشه ضمن اختصاصها المكاني، أما إذا كان خارج نطاق اختصاصها المكاني فتقوم جهات التحقيق بإنابة السلطات التي توجد في تلك الأماكن لمباشرة التفتيش بالنيابة عنها، ويتم ذلك من خلال أحد الأمرين التاليين:

أ. الندب بالتفتيش

---

[1] **التفتيش في الجرائم المعلوماتية: 141-149.**

[2] **قانون الإجراءات الجنائية السوداني لسنة 1983م: 86.**

ISSN:2707-8655
EISSN:2707-8663

الندب بالتفتيش يعني أن يتم تكليف مأمور الضبط القضائي من قبل السلطة المختصة بالتحقيق بعمل محدد أو أكثر من أعمال التحقيق، و يترتب عليه اعتبار العمل من حيث قيمته القانونية كما لو كان صادرًا عن سلطة التحقيق المختصة.

ب. الإنابة القضائية

الإنابة القضائية هي إجراء بموجبه تُنيب محكمة التحقيق المختصة محكمة تحقيق أخرى لاتخاذ إجراء أو أكثر من إجراءات التحقيق ضمن الاختصاص المكاني للمحكمة المنابة[1].

ثالثًا: الشروط الشكلية

تتمثل الشروط الشكلية للتفتيش في وقت إجراء التفتيش، وحضور شاهدين، وتحرير محضر التفتيش، وعرض المضبوطات وقوائمها على وكيل النيابة أو القاضي[2].

المطلب الرابع: صعوبات التفتيش

نظرا لما يتميز به مسرح الجريمة المعلوماتية من طبيعة خاصة تختلف عن طبيعة مسرح الجريمة التقليدية، فقد تواجه جهات التحقيق العديد من الصعوبات أثناء إجراء عملية التفتيش، وهذه الصعوبات تتمثل فيما يلي:

أولاً: سهولة محو الدليل أو تدميره

لما كانت الجريمة المعلوماتية ترتكب بواسطة الحاسب الآلي عن طريق إشارات وأوامر معنوية تعطى من الجاني إلى الحاسب الآلي بكل سهولة ويسر، وعن طريق ضغط زر واحد تصبح مسألة التخلص من تلك الأوامر في غاية البساطة والسهولة[3]، ومن الطبيعي أيضا أن يكون من السهل على مرتكب

---

(1) التفتيش في الجرائم المعلوماتية: 155-159.

(2) قانون الإجراءات الجنائية: 303.

(3) جرائم الحاسب الآلي والانترنت: 290.

هذه الجريمة المعلوماتية محو وإتلاف وتدمير كل دليل من شأنه أن يدينه، حتى لا تتمكن جهات التحقيق من إيجاد دليل يدل على من ارتكب هذه الجريمة.

ثانيًا: حماية الدليل بواسطة كلمة السر

قد يعمد الجاني إلى وضع كلمة سرٍ معينة على جهاز الحاسب الآلي الذي ارتكبت عن طريقة الجريمة المعلوماتية حتى لا يتمكن أحد من الدخول عليه والاطلاع على ما فيه من معلومات وأدلة تدينه[1].

ثالثًا: حماية الدليل بواسطة التشفير

التشفير هو تحويل المعلومات عبر اتفاقات تحتوي على رموز غير مفهومة، بحيث يجب إعادتها إلى حالتها الأصلية لأجل قراءتها وفهمها، وقد يلجأ مرتكب جريمة من جرائم المعلوماتية إلى التشفير كوسيلة لمنع الوصول إلى الدليل الذي يدينه[2]، على الرغم من قيام بعض الجهات التي تتبنى في نشاطها نظامًا معلوماتيًا لتيسير حركتها بقصد حماية نُظُمها عن طريق التشفير وغيرها من طرق الحماية الإلكترونية الأخرى، إلا أن قراصنة الحاسب الآلي والعاملين في ذات الجهات يستطيعون اختراق هذه الأنظمة ويجعلون حمايتها لا جدوى منه، وذلك بدخولهم إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها، أو استخدمها في مؤسسات جديدة يسعون إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات لتخريب المعلومات ويقومون بعد ذلك بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانة ضدهم، ويستخدمون كلمة سر حول مواقعهم تمنع الوصول إليها أو تشفيرها لإعاقة الاطلاع على أي دليل يتخلف وراء نشاطهم الإجرامي[3].

---

(1) **التفتيش في الجرائم المعلوماتية: 223.**

(2) **الأدلة الإلكترونية وحجيتها في الإثبات الجنائي: 45.**

(3) **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 89 – 91.**

ISSN:2707-8655
EISSN:2707-8663

رابعًا: وجود فايروسات داخل الجهاز

الفيروس هو برنامج تم إعداده من قبل شخص أو أكثر لهم خبرة ودراية عاليتين بالبرمجة عن طريق استخدام تقنية متطورة بحيث يكون من خصائص هذا البرنامج الانتقال إلى أجهزة الحاسب الآلي والتكاثر والانتشار فيها، وهي برامج غير مرئية بالطرق العادية وتحتاج إلى أسلوب علمي للكشف عنها.

وتستخدم الفيروسات لغرضين؛ أحدهما: حمائي، ويكون لحماية الحاسب الآلي لما يحتويه من بيانات وبرامج من خطر النسخ غير المشروع، إذ ينتشر الفيروس بمجرد النسخ ويدمر نظام الحاسب الآلي الذي يعمل عليه، والآخر لغرض التخريب إذ يهدف واضعه لتخريب نظام الحاسب الآلي أو الحصول على منافع شخصية، وقد يقوم الجاني مرتكب الجريمة المعلوماتية بإدخال فايروس إلى الجهاز المرتكبة عن طريقه الجريمة المعلوماتية وذلك بهدف إعاقة الوصول إلى الدليل المعلوماتي الذي يدينه[1].

خامسًا: تخزين المعلومات في جهاز آخر

قد يعمد مرتكب الجريمة المعلوماتية إلى تخزين المعلومات التي قد تدينه في جهاز آخر غير الذي ارتكب به الجريمة، فإذا كان جهاز الحاسب الآلي الموجودة فيه المعلومات هو غير الجهاز الذي ارتكبت به الجريمة ويوجد في مكان آخر غير المكان الذي يوجد فيه الجهاز المخزنة فيه المعلومات ولكن داخل حدود الدولة نفسها ، ففي هذه الحالة يثار تساؤل مهم حول مدى إمكانية امتداد إذن التفتيش للحاسوب الآخر عن طريق الشبكة إذا تبين أن المعلومات المطلوب ضبطها مخزنة على ذلك الحاسوب، ويرى جانب من الفقه في ألمانيا إمكانية امتداد التفتيش إلى البيانات المخزونة في حاسوب آخر خارج موقع التفتيش.

[1] **التفتيش في الجرائم المعلوماتية: 224.**

أما إذا كان الجهاز المخزنة فيه المعلومات يقع في مكان آخر خارج حدود الدولة فيجمع الفقه على عدم إمكانية تجاوز نطاق التفتيش لحدود الدولة؛ لأن هذا النوع من التفتيش يشكل انتهاكًا لسيادة الدولة التي يقع الجهاز على أراضيها، ومخالفة لقواعد الاختصاص المكاني والولاية القضائية لقضاء الدولة، ويقول رأي آخر إنه من الممكن تفتيش الجهاز حتى ولو كان خارج حدود الدولة إذا كان الهدف منه إظهار الحقيقة[1]. ومما يعيق عملية التفتيش خارج حدود الدولة بالإضافة إلى الكشف على كل ما يشمله الجهاز من معلومات داخله هو عدم الدقة في إذن التفتيش الذي قد يصدر في هذا الصدد[2].

المبحث الخامس: الضبط

المطلب الأول: مفهوم الضبط

أولاً: الضبط لغةً

الضَّبْطُ هو لزوم الشرع وحبْسه، ضبط عليه وضبطه يضْبُط وضابطه[3].

ثانيًا: الضبط قانونًا

الضبط هو وسيلة لالتقاط الأدلة المأخوذة من التفتيش، وتثبيتها ويعتمد على تحرير أوراق رسمية بكل خطوة تأتيها جهة التفتيش بالإضافة إلى التقاط كل دليل معتبر في الإثبات[4].

---

[1] التفتيش في الجرائم المعلوماتية: 231–233.

[2] جرائم الحاسب الآلي والانترنت: 293.

[3] لسان العرب: 8/ 15.

[4] جرائم الحاسب الآلي والإنترنت: 285.

ISSN:2707-8655
EISSN:2707-8663

المطلب الثاني: أنواع الضبط

أولاً: ضبط المكونات المادية للحاسب الآلي

لا يرد الضبط بحسب الأصل إلا على الأشياء المادية، ولذلك فإنه من السهل ضبط أدلة الجرائم المعلوماتية التي يكون محل الجريمة فيها هو المكونات المادية للحاسب الآلي، مثل الجرائم التي تقع على معدات الحاسب الآلي أو كابلاته، أو أسلاكه أو مفاتيح تشغليه، أو شاشة العرض أو الدعامات المادية أو الأشرطة أو الأسطوانات أو غيرها، عن طريق إتلافها بالوسائل التقليدية، كالكسر أو الحرق أو غيرها [1]، وهنا لا توجد أية صعوبة أو مشكلة لكي نقر بصلاحية هذه الجرائم لضبط أدلتها بموجب القواعد التقليدية للتفتيش[2]، ولا يوجد أي خلاف فقهي في كيفية ضبطها[3].

إلا أن ضبط المكونات المادية للحاسب الآلي يحتاج إلى عناية خاصة من قبل القائم به، وهنا تبرز أهمية وجود الخبير المعلوماتي مع الفريق المكلف بالقيام بعملية الضبط؛ لأنه يستطيع تحديد الطريقة المناسبة لضبط مكونات للحاسب الآلي والمواد اللازمة لحفظها وتغليفها ومقاومة الكهرباء الساكنة والحرارة، مثل الأغطية البلاستيكية، وورق التغليف والصناديق الكرتونية القوية وغيرها من المواد، وعلى الخبير المعلوماتي مباشرة الضبط والنقل والتفريغ بنفسه لضمان عدم تلف جهاز الحاسب الآلي[4].

ثانيًا: ضبط المكونات غير المادية للحاسب الآلي

تتمثل المكونات غير المادية للحاسب الآلي في برامجه وبياناته، ونظرا لما تتميز به هذه المكونات من طبيعة خاصة فإن ضبطها يثير العديد من الصعوبات ومنها الآتي:

---

(1) مبادئ الإجراءات في جرائم الكمبيوتر والإنترنت: 402.

(2) جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 373.

(3) جرائم الحاسب الآلي والإنترنت: 286.

(4) التفتيش في الجرائم المعلوماتية: 226 – 267.

1- برامج الحاسب الآلي

ليست هنالك صعوبة في ضبط الجرائم وأدلتها حين يكون محلها سرقة الدعامة المادية للبرامج أو الوسائل المادية المستخدمة في نسخة بصورة غير مشروعة، أو إتلافه بوسائل تقليدية، ومن ذلك البرنامج المطبوع على (F.D) أو (C.D) [1]، ولكن تكمن الصعوبة هنا في أمرين: أولهما، نقص خبرة المحققين نظرا لقلة تدريبهم في هذا المجال، والثاني يتمثل في ما إذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الأنظمة المعلوماتية الكبيرة، أو الشبكات الكبيرة حيث يصادف الضبط فيها صعوبتين هما:

أ. يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عند دائرته لمدة زمنية قد تطول أو تقصر، مما قد يتسبب عنه أضرار للجهة مستخدمة النظام.

ب. عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق، لما يعنيه الضبط بالنسبة لها من المساس بحقوق الغير[2].

2- بيانات الحاسب الآلي

ثمة عوائق تعترض مأموري الضبط القضائي/ المحقق الجنائي عند ضبط البيانات، وذلك بغض النظر عن الخلاف القانوني الدائم حول طبيعتها؛ فيما إذا كانت من الأشياء القابلة للتملك من عدمه، وإن تلك الصعوبات العملية تحول دون ضبط البيانات التي هي دليل على ارتكاب جريمة ما في بيئة المعالجة الآلية للبيانات[3].

---

(1) مبادئ الإجراءات في جرائم الكمبيوتر والإنترنت: 211.

(2) جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 374.

(3) مبادئ الإجراءات في جرائم الكمبيوتر والإنترنت: 213.

ويجب عند ضبط المكونات غير المادية للحاسب الآلي أن نقوم بتجميعها وحصرها في حيز مادي، بمعنى أن يتم نقلها من صورتها غير المادية إلى صورة مادية، ويتم ذاك عن طريق إخراجها على ورق أو أخذ تسجيل منها أو جمعها على أقراص مرنة أو ممغنطة أو تصويرها[1].

المطلب الثالث: صعوبات الضبط

أولاً: ضخامة تكاليف جمع الأدلة

تجد جهات التحقيق نفسها مجبرة على تفتيش نظام الحاسب الآلي برمته بحثًا عن الصفحات، لاسيما عندما لا تثبت تلك الصفحات شيئًا بالإضافة إلى الحالات التي يكون فيها الحاسب الآلي متصلا بشبكات الاتصالات العالمية فتزداد الصعوبة وترتفع التكاليف، وهذا يتطلب خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجود الدليل، وأقصر وأيسر السبل لضبطه [2].

ثانيًا: نقص خبرة المحققين

يتطلب التحقيق في الجرائم المعلوماتية معامل ومختبرات خاصة، وخبراء يجمعون بين المعرفة القانونية ومهارة التحقيق وعلوم وتقنية المعلومات، وبالإضافة إلى ذلك يتطلب مواجهة التحدي الجديد بناء قدر من التعاون والثقة بين أجهزة تنفيذ القوانين والمؤسسات التي تقدم خدمات المعلومات والاتصالات [3]، ومن الصعوبات التي تواجه/ تعيق عملية التحقيق في الجرائم المعلوماتية: نقص الخبرة في مجال الحاسب الآلي لدى رجال الضبط القضائي، أو أجهزة الأمن بصفة عامة، وكذلك لدى

---

[1] **جرائم الحاسب الآلي والإنترنت: 286.**

[2] **جرائم الحاسب الآلي والإنترنت: 291.**

[3] **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 66– 67.**

أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر المعلوماتية وكيفية التعامل معها[1].

ثالثًا: مشاكل اللغة المستخدمة في التحقيق

من المعلوم أن ثورة التكنولوجيا بما أوجدته من نظم معلوماتية ذات تقنية عالية تعتمد على لغة علمية نمت وتطورت مع الاستعمال المتزايد والمتكرر، هذه اللغة بدأت بطرفين هما: المبرمج والحاسب الآلي، ثم امتدت إلى المبرمجين والعاملين في مجال تقنية المعلومات بعضهم مع بعض، ثم تعدلت وأصبحت تستخدم باختصارات معروفة عوضًا عن مصطلحات أصلية، سميت بلغة المختصرات ويتم استخدامها من قبل خبراء ومشغلي الحاسب الآلي للتفاهم بينهم، وأصبحت هذه اللغة مهمة مع ظهور جرائم الحاسب الآلي؛ ومن ثم فالواجب على جهات التحقيق والمحاكم المختصة معرفتها، وتبرز أهمية معرفتها من أن الجريمة تعتمد على تقنية معلوماتية يشار إليها برموز معروفة عند أهل التخصص، فهي وسيلة التخاطب الوحيدة المفهومة بين مرتكبي الجرائم والخبراء والمشتغلين من جهة، والنيابة العامة والمحاكم من جهة أخرى[2].

رابعًا: مسائل الاختصاص

تربط شبكات الاتصال الإنترنت بين ملايين الحواسيب الآلية حول العالم، مما يعني أنه قد ترتكب الجريمة المعلوماتية بدولة وتظهر آثارها في دولة أخرى، وقد يكون الجاني أيضًا من دولة ثالثة، ومن ثمَّ تكون الأدلة على ارتكاب الجريمة المعلوماتية موجودة خارج النطاق الإقليمي لجهة التحقيق؛ أي خارج

---

(1) **المرجع نفسه: 122.**

(2) **جرائم الحاسب الآلي والإنترنت: 295–296.**

ISSN:2707-8655
EISSN:2707-8663

صلاحيتها القانونية الجنائية، كما أن الدول تتبنى فكرة الإقليمية محددة الاختصاص، وكل القوانين عاجزة عن مواكبة التطورات والمستجدات التي أتت بها التكنولوجيا الحديثة[1].

ويلاحظ أن التشريعات الجنائية المطبقة حاليًّا في معظم دول العالم تركز على الصفة الإقليمية فيما يتعلق بتطبيق الإجراءات الجنائية عن طريق السلطات غير الوطنية، ولذلك لا تتقدم ولا تتطور التشريعات الجنائية بنفس سرعة وتقدم وتطور المعلوماتية التي شملت العالم كله، والحل الوحيد لذلك وضع اتفاقيات ثنائية أو جماعية بين الدول في مختلف أنحاء العالم لتسهيل عملية التحقيق في الجرائم المعلوماتية[2].

خامساً: ضخامة المعلومات والبيانات

يواجه رجال الضبط وسلطات التحقيق الجنائي في الجريمة المعلوماتية كمية ضخمة من المعلومات والبيانات التي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هذه الجريمة، بالإضافة إلى ضرورة توافر الخبرة الفنية في مجال الحاسب الآلي لدى رجل الضبط/ المحقق الجنائي يتعين كذلك أن يتوفر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي، أو على ديسكات أو أسطوانات منفصلة [3]، وذلك لكي يتمكن من تحديد البيانات التي تصلح كأدلة جنائية من تلك التي لا تصلح، وكثيرا ما تكون الأحزمة الأمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحتويها هذا النظام عائقًا عن الوصول إلى المعلومات في كثير من الأحيان، مما يزيد من صعوبة الأمر على المحقق الجنائي على معرفته لكلمات السر أو شفرات المرور، وهذا يتطلب يقتضي تعاون مستخدم النظام معه أو الاستعانة بذوي الخبرة في هذا المجال[4].

---

(1) **المرجع نفسه: 292-293**

(2) **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 146-147**

(3) **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت:148.**

(4) **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية: 375.**

وتعد ضخامة هذه البيانات والمعلومات عائقا أمام عملية التحقيق، وذلك لأن طباعة كل ما هو موجود على الدعامات الممغنطة لحاسب آلي متوسط العمر يتطلب مئات الآلاف من الصفحات، وقد لا تقدم هذه الصفحات أي شيء مفيد في عملية التحقيق، ولذلك ولضعف خبرة رجل الضبط/ المحقق الجنائي في مجال الحاسب الآلي فإنه يكون من الملائم وجوب ندب خبراء فنيين في مثل هذه الجرائم حتى يمكن فرز المعلومات التي يحتاجها التحقيق عن تلك التي لا يحتاج لها، وذلك يتطلب أن يكون ندب هؤلاء الخبراء وجوبيا، وتعديل كل التشريعات الجنائية التي تجعل ندبهم أمرا جوازيا للمحقق – إن شاء قبله أو رفضه– لأن طبيعة هذه الجريمة تتطلب التعامل معها بحرفية أو فنية تفوق قدرات رجل الضبط/ المحقق الجنائي التقليدية، إلا إذا كان هو مؤهلاً لذلك فيمكن حينها الاعتماد على قدراته الشخصية في ضبط وتحقيق هذه الجرائم شرط ألا يخرج عمله عن الأصول الفنية المتعارف عليها[1].

المبحث السادس: أثر الصعوبات على العدالة الجنائية

العدالة الجنائية هي ممارسة المؤسسات العدلية، ممثلة للدولة لمكافحة الجرائم والتخفيف منها، ومعاقبة من ينتهك النظام من خلال العقوبات والإصلاحات الجنائية. وبالمثل، يحق للأشخاص المشتبه في ارتكابهم جرائم المطالبة بالحماية من الانتهاكات سلطة التحقيق والادعاء.[2]

وتقوم فكرة العدالة الجنائية بغرض مكافحة الجريمة من خلال تقديم أكبر عدد من المجرمين إلى العدالة وزيادة الثقة في عدالة النظام، وتعزيز ثقة المواطنين الملتزمين بالقانون[3].

---

[1] مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت: 148–149.

[2] – https://e3arabi.com/?p=788689

[3] –https://e3arabi.com/?p=788689 –

ISSN:2707-8655
EISSN:2707-8663

إذن لا تستطيع الدولة تقديم كل من ارتكب الجريمة إلى العدالة إلا أن يكون لديها أجهزة عدلية ذات كفاءة عالية من حيث التأهيل والتدريب.

من خلال ما أوردناه في البحث ندرك أثر صعوبات بعض إجراءات التحقيق المتمثلة في المعاينة والتفتيش والضبط، وتمكن الجاني من الإفلات من المحاكمة. ويمكن أن نجمل أبرز الآثار المترتبة على هذه الصعوبات في الآتي:

1- صعوبة حل لغز هذا النوع من الجرائم على المحقق الجنائي نظرا لأن الجريمة المعلوماتية لا توجد لديها آثار مادية يمكن من الوصول إلى مرتكبها بأسرع وقت، لأنها تتم عبر نبضات الكترونية غير ملموسة[1].

2- سهولة إفلات مرتكبها من العقوبة وذلك وهذا يسهم في صعوبة عمل المحقق الجنائي؛ وذلك لسهولة تنفيذ الجريمة من قبل مرتكبها، لا سيما أنه قد يكون واحدا من موظفي الجهة، ولا يحتاج إلى أي مكونات مادية كالأوراق والمستندات لتنفيذ جريمته، كما أنه يتمكن من خلال كلمات السر أو التشفير من إخفاء جريمته.

3- استحالة فحص ودراسة كمية المعلومات والبيانات الضخمة، والتي هي في حاجة إلى كي يستخلص منها دليل هذه الجريمة.

4- كلفة مواكبة تدريب وتأهيل رجال التحقق الجنائي والقضائي على التقنيات الحديثة نظرا. للتطور المتسارع في تقنيات الحاسب وبرامجه وفي تقنيات الجريمة الالكترونية

5- ضعف الثقة في قدرات التحقيق الجنائي وهو ما سيؤدي إلى إضعاف مؤسسات الدولة العدلية في محاربة ومكافحة الجريمة.

---

[1] المرجع نفسه: 356.

خاتمة:

أولا: النتائج

1. أن الجرائم المعلوماتية ذات طبيعة خاصة، تختلف عن الجرائم التقليدية؛ لأنها تتم في عالم افتراضي وهمي غير ملموس.

2. أنها جرائم عالمية لا تعترف بالحدود الجغرافية والسياسية، الأمر الذي يثير كثيرا من المشاكل المتعلقة بالقانون الواجب تطبيقه عليها.

3. أن المجرم المعلوماتي يتمتع بذكاء حاد في مجال الحاسب الآلي، حيث تعاني جهات التحقيق من فقر ونقص شديدين في الخبرة الفنية والكفاءة في هذا المجال.

ثانيا: التوصيات

1. أوصي بضرورة أخذ الحيطة والحذر عند التعامل مع هذا النوع من الجرائم من قِبَل العاملين في عملية التحقيق، حتى لا يتم محو أو إتلاف أي دليل عن طريق الخطأ.

2. لابد من وجود تعاون دولي بين مختلف دول العالم؛ لأن هذه الجرائم هي جرائم عالمية ينبغي حلها أو مكافحتها بالتعاون بين جميع دول العالم.

3. ضرورة وضع قانون للإجراءات الجنائية وقانون للإثبات خاص بالجرائم المعلوماتية؛ نظرا لقصور كل من قانون الإجراءات الجنائية والإثبات التقليديين عن مواكبة هذا النوع من الجرائم.

4. ضرورة تدريب كل العاملين في مجال التحقيق في الجرائم المعلوماتية وتزويدهم بالخبرة والكفاءة في مجال الحاسب الآلي، وتزويدهم بصوره ومخاطره وطرق ارتكاب هذا النوع من الجرائم، وكيفية التعامل مع الأدلة إن وجدت.

ISSN:2707-8655
EISSN:2707-8663

المصادر والمراجع:

ابن منظور، لسان العرب.، دار صادر، بيروت، ط3، 1414هـ.

أسامة أحمد المناعسة – جلال مُحَمَّد الزعبي – صايل فاضل الهواوشة جرائم الحاسب الآلي والإنترنت، دار وائل للنشر والتوزيع، الأردن، ط1، 2001م .

أقيس عبد الوهاب حمد مُحَمَّد، شرح قانون جرائم المعلوماتية السوداني، السودان، ط1، 2010م.

القانون الجنائي السوداني لسنة 1991م.

الموسوعة الفقهية.

أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، مصر، 2008م.

جرائم المعلوماتية (ورشة عمل)

حاج آدم حسن الطاهر، قانون الإجراءات الجنائية، منشورات جامعة السودان المفتوحة، السودان، ط1، 2007م.

دار مسيس بهنام، البوليس العلمي أو فن التحقيق، منشأة المعارف، مصر، 1996م.

سامي جلال فقهي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، مصر، د(ط) 2011م.

عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر،2007م.

عبد المنعم عبد الحافظ إبراهيم، البينة الإلكترونية، السودان، د. ت.ط

عزة علي مُحَمَّد الحسن، قانون الحاسوب، منشورات جامعة السودان المفتوحة، السودان،ط1،2007م.

عزة علي مُحَمَّد الحسن، الجريمة المعلوماتية في القانون السوداني، الزيتونة للطباعة، السودان، 2009م.

عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، لبنان، 2003م.

قانون الإثبات السوداني لسنة 1994م.

مجلة أبحاث ودراسات التدريب والمعلومات.

مجلة العدل (العدد24، 26)

مُحَمَّد علي إبراهيم مُحَمَّد، الأدلة الإلكترونية وحجيتها في الإثبات الجنائي، السودان، ط1، 2014م.
مُحَمَّد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديد، مصر، 2011م.
مصطفى مُحَمَّد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب القانونية، مصر، 2005م.
منير مُحَمَّد الجنبيهي، و منتصر مُحَمَّد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، مصر، 2005م.
نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، دار الفكر الجامعي، مصر، ط1، 2007م.