
# صعوبات التعامل مع مسرح الجريمة الإلكترونية

# (دراسة مقارنة)

**بحث للنشر في المجلة**

**إعداد الباحث**

**محمد يوسف النعيمي**

**٢٠١٨م**

**بِسْمِ اللَّـهِ الرَّحْمَنِ الرَّحِيمِ**

(وَمَن يَتَّقِ اللَّهَ يَجْعَل لَّهُ مِنْ أَمْرِهِ يُسْرًا (٤) ذَٰلِكَ أَمْرُ اللَّهِ أَنزَلَهُ إِلَيْكُمْ ۚ وَمَن يَتَّقِ اللَّهَ يُكَفِّرْ عَنْهُ سَيِّئَاتِهِ وَيُعْظِمْ لَهُ أَجْرًا (٥))

سورة الطلاق

# الإهداء

إلى كل من علمني حرفاً من طفولتي إلى الآن

إلى والديَّ وإخوتي وزوجتي وأبنائي وأقاربي وجميع من تعاونوا معي

إلى أساتذتي الذين تعاونوا معي وبالأخص إلى أستاذي الفاضل

**(أ.د تامر محمد محمد صالح)**

وإلى جميع الأساتذة في كلية القانون في جامعة المنصورة.

إليكم جميعاً أهدي هذا البحث

# شكر وتقدير

أتقدم بجزيل الشكر والتقدير إلى الدكتور المشرف

**(أ.د تامر محمد محمد صالح)**

لإشرافه على رسالتي هذه منذ كانت فكرة حتى أصبحت بحثاً عليماً متكاملاً

كما أتوجه بالشكر الجزيل للسادة أعضاء لجنة الحكم والمناقشة

لتفضلهم وقبولهم مناقشة رسالتي هذه

ولكل من ساندي طيلة إعداد هذا البحث

لكم مني جزيل الشكر والتقدير وعظيم الامتنان

-

# ملخص

أدى تطور التقنيات الحديثة والطابع الرقمي لشبكات الاتصال وأجهزة الحاسب الآلي إلى تطور الاستخدامات الإلكترونية لتلك الوسائل على نطاق واسع ، سواء على الصعيد الوطني أو الدولي، على نطاق القانون الجنائي وترتب عليه ذلك ظهور جرائم المعلوماتية، التي ترافقت مع ظهور العديد من الصعوبات التقنية والقانونية عند معاينة مسرح الجريمة الإلكترونية.

تتمثل أهمية الدراسة في التعرف على الصعوبات الفنية والقانونية التي تواجه مأمور الضبط القضائي أثناء التعامل مع مسرح الجريمة الإلكترونية، من خلال التعرف على الصعوبات المرتبطة بطبيعة هذه الجريمة والصعوبات التي تترافق مع الوسيلة التي ترتكب فيها الجريمة وهي التقنيات الحديثة والبحث في موقف المشرع الاماراتي من تلك الصعوبات.

تتمثل مشكلة البحث في الصعوبات القانونية والتقنية التي تواجه جهة الضبط القضائي عند معاينة مسرح الجريمة الإلكترونية.

وفي نهاية البحث توصلنا إلى ضرورة سن تشريع خاص بالإجراءات الجزائية في الجرائم الإلكترونية للتخلص من الصعوبات القانونية والتقنية التي تواجه مأمور الضبط القضائي عند معاينة مسرح الجريمة الإلكترونية.

# Abstract

**The development of modern technologies and the digital nature of communication networks and computers has led to the widespread development of the electronic uses of these means, both nationally and internationally, in the scope of criminal law. This has resulted in the advent of cybercrime, which was accompanied by the emergence of many technical and legal difficulties Electronic crime scene.**

**The importance of the study is to identify the technical and legal difficulties faced by the judicial control officer in dealing with the electronic crime scene by identifying the difficulties associated with the nature of this crime and the difficulties that accompany the means of committing the crime.**

**The problem of research is the legal and technical difficulties facing the judicial authority when examining an electronic crime scene.**

**At the end of the research, we reached the need to enact legislation on criminal procedures in cybercrime to eliminate the legal and technical difficulties facing the judicial control officer when examining the electronic crime scene.**

# مقدمة

إنّ التطورات الحديثة في تقنية المعلومات أحدثت تغيّرات مستمرة ومضطردة في أساليب العمل والميادين كافة إذ أصبحت عمليّة انتقال المعلومات عبر الشبكات المحليّة والدوليّة وأجهزة الحاسب من الأمور الروتينيّة في عصرنا الحالي وإحدى علامات العصر المميّزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلّبات الحياة العصريّة من خلال تقليل حجم الأعمال وتطوير أساليب توفير المعلومات؛ حيث أنّ انتشار أنظمة المعلومات الإلكترونيّة أدّت إلى أن تكون عرضةً للاختراق؛ لذلك أصبحت هذه التقنية سلاحاً ذو حدين تحرص المنظمات على اقتنائه وتوفير سبل الحماية له.

ولم يعد خافيا ما تخطى به برامج الحاسب الآلي من أهمية في شتى مناحي الحياة العلمية، وقيامها بالكثير من المهام بسرعة فائقة ودقة متناهية لذلك فإنه ينبغي مسايرة التقدم المتسارع لهذه البرامج، وتوفير الحماية القانونية اللازمة لها، لأن المميزات الكثيرة للحاسب الآلي جعلت الاستعانة به واستخدامه أمراً ضرورياً في كافة المجالات، وأنظمة الاتصالات خصوصاً بعد ظهور شبكة المعلومات الدولية (الإنترنت)[1] والتي جعلت العالم يبدو كقرية صغيرة فأي إنسان يستطيع التجول في أنحاء العالم عبر هذه الشبكة وهو في بيته دون عناء.

---

[1] الإنترنت هي شبكة الاتصالات الأم التي تربط بين جميع أجهزة وشبكات الكمبيوتر في العالم كله مع بعضها. Net Work of all Network بما في هذه الشبكات من معلومات وأجهزة وأفراد يعملون عليها، وغالباً ما يشار

حيث أصبحت التقنيات الحديثة وخاصة الحاسب الآلي وسيلة لارتكاب الجرائم الإلكترونية، وهو ما يثير العديد من الصعوبات التي تواجه جهة الضبط القضائي عند معاينة مسرح الجريمة ومنها الصعوبات التقنية والصعوبات القانونية، وهذا ما سنبينه من خلال هذا البحث.

## مشكلة البحث:

تتمثل مشكلة البحث في الصعوبات التي تواجه جهة الضبط القضائي عند معاينة مسرح الجريمة الإلكترونية، التي تختلف تماماً عن الصعوبات التي تواجههم عند معاينة مسرح الجريمة التقليدية، لأن الجريم الإلكترونية ترتكب في فضاء افتراضي وباستخدام وسائل التقنيات الحديثة، كما أن هناك مشكلة تتعلق بالصعوبات القانونية التي تواجه جهة الضبط القضائي عند معاينة مسرح الجريمة الالكترونية، ولاسيما أن القواعد الواردة في قانون الإجراءات الجزائية الاتحادي هي للجرائم التقليدية.

## أهمية البحث:

إن أهمية هذا البحث ترجع إلى أهمية الموضوع الذي تتناوله وهو الكشف عن الصعوبات التي تواجه جهة الضبط القضائي أثناء معاينة مسرح الجريمة الإلكترونية، ويمكن تقسيم أهمية الدراسة إلى أهمية نظرية وأهمية تطبيقية، على النحو التالي:

---

غليها بلفظ The Net أي الشبكة. راجع في ذلك: أيمن سيد دوريش: المرجع الكامل لخدمات الإنترنت، شعاع للنشر والعلوم، القاهرة، ١٩٩٨ م، ص ٩. مصطفى السيد، دليلك الشامل إلى شبكة الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، ١٩٩٧ م، ص ١٤ وما بعدها. خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، دار النهضة العربية، القاهرة، ط ١، ٢٠١٢ م، الصفحة برمز (ز).

١- **الأهميـــة النظريـــة:** تتمثـل فـي التعـرف علـى الصـعوبات الفنيـة والقانونيـة التـي تواجـه مـأمور الضـبط القضـائي أثنـاء التعامـل مـع مسـرح الجريمـة الإلكترونيـة، مـن خـلال التعـرف علـى الصـعوبات المرتبطـة بطبيعـة هـذه الجريمـة والصـعوبات التـي تترافـق مـع الوسـيلة التـي ترتكـب فيهـا الجريمـة وهـي التقنيـات الحديثـة والبحـث فـي موقف المشرع الاماراتي من تلك الصعوبات.

٢- **أمـا الأهميـة التطبيقيـة:** فتتمثـل فـي مجموعـة التوصـيات التـي سـتقدمها الدراسـة، والتـي يمكـن الاسـتفادة منهـا فـي تفعيـل التعامـل مـع الصـعوبات التـي تواجـه جهـة الضـبط القضـائي عنـد التعامـل مـع مسـرح الجريمـة الإلكترونيـة فـي دولـة الإمـارات العربية المتحدة.

## أهداف البحث:

يسعى هذا البحث إلى تحقيق هدف أساسي، وهو التعرف على الصعوبات التي تواجه جهة الضبط القضائي عند التعامل مسرح الجريمة الإلكترونية، وينبثق من هذا الهدف الأساسي عدة أهداف فرعية يمكن بلورتها على النحو التالي:

١- التعرف على الصعوبات الفنية التي تترافق مع طبيعة الجريمة الإلكترونية.

٢- التعرف على الصعوبات القانونية التي تواجه جهة الضبط القضائي أثناء التعامل مع مسرح الجريمة الإلكترونية.

٣- التعرف على الصعوبات التي تواجه الدليل الإلكتروني الذي يتم الحصول عليه عند معاينة مسرح الجريمة الإلكترونية.

## منهج البحث:

سوف يعتمد الباحث في هذه الدراسة على المنهج الاستقرائي التحليلي المقارن، إذ سيقوم الباحث بجمع المعلومات والحقائق ثم العمل على تحليلها تحليلاً موضوعياً، وذلك من أجل التعرف على الصعوبات التي تواجه مأمور الضبط القائي عند التعامل مع مسرح الجريمة الإلكترونية في التشريع الإماراتي وعدد من التشريعات العربية والأجنبية، وبتحليل هذه الإجراءات سوف يتوصل الباحث للعديد من النتائج والتوصيات التي يمكن أن يستفيد منها العاملين في مجال البحث الجنائي، ولاسيما في مجال مواجهة صعوبات الاستدلال في مسرح الجريمة الإلكترونية في دولة الإمارات العربية المتحدة.

## تقسيم البحث

المبحث الأول: الصعوبات الفنية أثناء التعامل مع مسرح الجريمة الإلكترونية.

- المطلب الأول: الصعوبات المتعلقة بطبيعة الجريمة الإلكترونية.
- المطلب الثاني: الصعوبات المتعلقة بوسائل ارتكاب الجريمة الإلكترونية.

المبحث الثاني: الصعوبات القانونية أثناء التعامل مع مسرح الجريمة الإلكترونية.

- المطلب الأول: الصعوبات الإجرائية.

- المطلب الثاني: الصعوبات القضائية.

الخاتمة تتضمن:

أولاً: النتائج.

ثانياً: التوصيات.

# المبحث الأول

## الصعوبات الفنية أثناء التعامل مع مسرح الجريمة الإلكترونية

**تمهيد وتقسيم:**

تظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجب مسرح، فعلى للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيداً لفحصها لبيان مدى صحتها في الإثبات، فليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث ينذر أن يتخلف عن ارتكابها آثاراً مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة اكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها، ويكتنف مسرح الجريمة الإلكترونية العديد من الصعوبات الفنية التي تشكل عائقاً أمام جهة الضبط القضائي أثناء معاينة مسرح الجريمة، وسنبين في هذا المبحث تلك الصعوبات من خلال تقسيمه لمطلبين على النحو التالي:

- **المطلب الأول:** الصعوبات المتعلقة بطبيعة الجريمة الإلكترونية والمجرم الإلكتروني.
- **المطلب الثاني:** الصعوبات المتعلقة بوسائل ارتكاب الجريمة الإلكترونية.

# المطلب الأول

## الصعوبات المتعلقة بطبيعة الجريمة الإلكترونية والمجرم الإلكتروني

جرائم الإنترنت تعتبر تهديداً مباشراً أو غير مباشر لتقدم البشرية بواسطة أعمال إجرامية يقوم بها أشخاص يسيئون استخدام التكنولوجيا الحديثة، وهذه الجرائم تتسم بالصعوبة والتعقيد.

كما أن ملاحقة مرتكبيها لا تكاد تخلو من هذه الصعوبة حيث أنهم يتصفون بصفات تختلف عن تلك التي يتصف بها مجرمو الجرائم التقليدية وذلك من حيث أنهم في الغالب أفراد ذوي مكانة في مجتمعهم، ويتمتعون بقدر كاف من العلم، وذلك لما تستلزمه هذه الجرائم من إلمام بمهارات ومعارف فنية في مجال أنظمة الحاسب الآلي والإنترنت، وغالباً ما يكونوا متخصصين في هذا المجال[١]. وكثير من مجرمي المعلومات عائدون إلى الإجرام، وعلى قدر من الذكاء مصحوب باحتراف في مجال المعلومات ومتكيف مع المجتمع[٢]، ومتوسط أعمارهم ما بين ١٨ سنة إلى ٤٦ سنة، وجرائم الإنترنت تتسم بسمات تكاد تخلو منها الجرائم التقليدية ومن أهم هذه الخصائص:

**١- خفاء الجريمة:**

تتسم الجرائم الناشئة ع استخدام الإنترنت بأنها مستترة خفية في أغلبها حيث أن المجني عليه لا يلاحظها غالباً مع أنها قد تقع أثناء وجوده على الشبكة ولكن لا يكون عالماً بها ولا ينتبه إليها إلا

---

[١] د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠١٥م، ص ١٠.

[٢] وليد عالكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو، ٢٠٠٠، ص٨٥.

بعد فترة من وقوعها، وفي بعض الأحيان لا يكتشف أمرها، ويعود ذلك إلى تعامل الجاني مع نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب، كما أن توافر المعرفة والخبرة الفنية لدى الجاني في هذا المجال يؤدي إلى صعوبة اكتشاف جريمته، وذلك باتباعه لطرق وأساليب لا يفطن إليها المستخدم العادي للشبكة، ومن أمثلتها إرسال فيروسات المدمرة، وسرقة الأموال والبيانات الخاصة، أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم، ثم قيامه بدس بعض البرامج الخاصة وتغذيتها ببعض البيانات التي تؤدي إلى عدم شعور المجني عليه بوقوع هذه الجرائم[١].

**٢- سرعة التطور في ارتكاب الجريمة:**

التطور السريع التي تشهده تكنولوجيا المعلومات أرخى بظله على الجرائم الناشئة عن الإنترنت حيث أن أساليب ارتكابها دائماً في تطور مستمر، وأن المجرمين في مختلف أنحاء العالم يستفيدون من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم[٢].

**٣- أقل عنفاً في التنفيذ:**

جرائم الإنترنت لا تحتاج إلى عنف عند تنفيذها، أو مجهوداً كبيراً، وإنما تنفذ بأقل جهد ممكن يقوم به الجاني ويعتمد فيها بشكل رئيسي على الخبرة في المجال المعلوماتي، وهذا عكس الجرائم التقليدية التي تحتاج إلى عنف ودماء ومجهود كبير يقوم به الجاني غالباً في الوصول إلى غايته[٣].

---

[١] المستشار محمد عبيد الكعبي : الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، ، دار النهضة العربية، القاهرة، ٢٠١٥م، ص ٣٦.

[٢] المستشار محمد عبيد الكعبي، المرجع السابق، ص ٣٧.

[٣] المستشار محمد عبيد الكعبي، المرجع السابق، ص ٣٧.

**٤- عابرة الحدود:**

أطلق البعض على شبكة الإنترنت أنها الإمبراطورية التي لا تغيب عنها الشمس، ذلك أن هذه التقنية أذابت الحدود الجغرافية بين دول العالم ولم تعد الجريمة تخضع لنطاق إقليمي محدود، وإنما أصبحت الجريمة تقع في بلد وتمر عبر بلد آخر وتتحقق نتيجتها في بلد ثالث أو عدة بلدان وكل ذلك في ثوان معدودة، وصارت أكثر من دولة مسرحاً لتلك الجريمة هذا وقد لا يقتصر الضرر المترتب على الجريمة على المجني عليه وحده وإنما قد يتعداه إلى متضررين آخرين في دول عدة، وهذا هو الملاحظ من خلال جرائم نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني أو السياسي أو الثقافي أو التربوي أو الاقتصادي[١]، لذلك فإنه يجب إيجاد تعاون دولي لمكافحة هذه الجرائم عن طريق المعاهدات والاتفاقيات الدولية.

**ومنه نرى** أن الجرائم الإلكترونية تتسم بخصائص تميزها عن الجرائم التقليدية، فهي أكثر شيوعاً على النطاق الدولي، كما أنها لا تقف عند حدود زمانية أو مكانية محددة، فهي من الجرائم العابرة للقارات، وترقى إلى مستوى الجرائم المنظمة، وإن أهم سمات الجرائم الإلكترونية أنها تتم عبر وسائل إلكترونية لختة بعيدة كل البعد عن الوسائل التي تستخدم في الجرائم التقليدية، وهذا ما يفسر لنا خطورة هذه الجرائم ويمكن تلخيص هذه الصعوبات في عاملين رئيسيين هما[٢]:

---

[١] د. محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو، ٢٠٠٠.

[٢] هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط ، ١٩٩٤، ص ٥٩ وما بعدها.

١) تكمن الصعوبة الأولى في قلة الآثار المادية التي قد تتخلف عن الجرائم التي تقع على برامج الحاسب الآلي وبياناته أو بواسطتها.

٢) الأعداد الكبيرة من الأشخاص الذين قد يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة نسبيا وذلك ما بين اقتراف الجريمة والكشف عنها الأمر الذي يمنح فرصة الحدوث تغيير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها وهو ما يلقي ظلال من الشك على الدليل المستقي من المعاينة.

وتوجد بعض القواعد والإرشادات الفنية التي يجب إتباعها عند إجراء معاينة لمسرح جرائم الحاسب الآلي وتتمثل هذه الإجراءات فيما يلي[1]:

أ- ملاحظة طريقة إعداد نظام الحاسب الآلي بعناية بالغة.

ب- يجب أن يلاحظ وان يتم إثبات الحالة التي تكون عليها توصيلات أسلاك الحاسب الآلي والتي تكون متصلة بمكونات النظام، وذلك و حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.

ت- عدم التسرع في نقل أي مادة معلوماتية" من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للمعلومات المخزنة.

---

[1] هلال بن محمد بن حارب البوسعيدي، هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٢٤٨.

ث- حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة أو المحطمة ورفع البصمات التي قد تكون على صله بالجريمة المرتكبة.

ج- القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع ومضاهاة البصمات التي قد تكون موجودة عليها.

ح- يجب أن تقتصر عملية المعاينة على مأموري الضبط سواء كانوا من الباحثين أو المحققين ممن تتوافر فيهم الكفاءة العملية والخبرة الفنية في مجال الحاسبات الآلية واسترجاع المعلومات ممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة.

خ- تتم معاينة قواعد المعلومات من الجهة المختصة بها للتأكد من أنها لم تتعرض لأي تلاعب في محتواها وذلك بمعرفة مأمور الضبط القضائي.

د- استخراج تقرير مفصل من النظام عن أي تغيير يكون قد وقع.

ذ- التأكد قبل كل شيء عن نظام الأمان الموجود على الحاسب الآلي.

**<u>ومما سبق من معطيات نرى</u>** أن مسرح الجريمة الإلكترونية له طبيعة خاصة، بحيث يصعب التعامل مع مسرح الجريمة الإلكترونية بالطرق التقليدية للتعامل مع مسرح الجريمة

التقليديـة، فمسـرح الجريمـة التقليديـة يمكـن تقييمـه ماديـاً عـن طريـق الأدلـة والبصـمات وغيرهـا مـن الأدلـة الجنائيـة فـي مسـرح الجريمـة التقليديـة، بينمـا مسـرح الجريمـة الإلكترونيـة يـتم عبـر تقنيـة المعلومـات، والجريمـة الإلكترونيـة تـتم عبـر واقـع افتراضـي يصـعب معـه التعامـل مـع مسـرح الجريمـة، كمـا أن المجـرم فـي الجريمـة الإلكترونيـة يكـون متخفيـاً ويصـعب الوصـول إليـه، كمـا أن طبيعـة الجريمـة الإلكترونيـة تمكـن الجـاني مـن إلغـاء الأدلـة وحـذها بسـرعة وسهولة، وهذا ما يشكل صعوبة للتعامل معلا تحديد أبعاد الجريمة الإلكترونية.

## المطلب الثاني

## الصعوبات المتعلقة بوسائل ارتكاب الجريمة الإلكترونية

الحـق أن تطبيـق القواعـد التقليديـة المتعلقـة بـالتفتيش لا تسـمح بمـد التفتـيش الواقـع علـى المعطيـات المخزنـة فـي الأجهـزة الموجـودة بمكـان محـدد إلـى المعطيـات الموجـودة فـي الأجهـزة

المرتبطة بها، وذلك لأن التفتيش بالمفهوم التقليدي يرتبط بالمكان المسموح إجراء التفتيش به، وتجاوز هذا المكان للتفتيش إلى غيره دون سند قانوني صريح يعرض التفتيش والضبط الناجم عنه للبطلان، ويفوت بالتالي إمكانية اللجوء إلى إجراء مهم كالتفتيش في مكافحة الجريمة الإلكترونية والمعاقبة عليها. الأمر الذي حدا بالمشرع في بعض الدول إلى تشريع ما يمكن أن يطلق عليه "التفتيش عن بعد"[1].

وأن البيانات والمعلومات المتداولة عبر شبكة الإنترنت تكون على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي ،والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمراً صعباً ،لاسيما وأن الجاني يتعمد عدم ترك أثر لجريمته، إضافة إلى ذلك ما يتطلبه من فحص دقيق لمسرح الجريمة من قبل المختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة إلكترونياً[1] .

فالجريمة الإلكترونية تتم خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت، مما جعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل من العثور على الدليل المادي على الجريمة أمراً غاية في الصعوبة[2].

---

[1] يجدر التنويه إلى أن بعض الدول مازالت تعتمد تطبيق القواعد التقليدية للتفتيش على التفتيش غير المباشر أو التفتيش عن بعد، من هذه الدول يمكن الإشارة إلى ألمانيا وكندا وإسبانيا وإيطاليا والبرتغال.

[1] داود سليمان علي الحمادي، أحكام جريمة التزوير الإلكتروني، دار النهضة العربية، القاهرة، ٢٠١٦، ص ١١٣.

[2] داود سليمان علي الحمادي، المرجع السابق، ص ١١٣.

ويتطلب الأمر في كثير من الأحيان ولوج البيئة المعلوماتية بحثاً عن الآثار المعنوية وكشف مرتكبي هذه الطائفة من الجرائم وتعقبهم ،ومع ذلك فإن التفتيش وما في حكمه في نطاق هذه البيئة ينظر إليه في كثير من الأحيان على أنه غير مجد لما يكتنفه من صعوبات أثناء تنفيذه، وبالذات ما يتم في الفضاء الافتراضي ( في بيئة الإنترنيت) مقارنة بالجرائم التقليدية، فضلاً عما يثيره تفتيش المكونات المنطقية للحاسوب، والمتمثل في المعلومات والبيانات المعالجة إلكترونياً، من جدل كبير حول صلاحيتها لأن تكون موضوعاً للتفتيش والضبط من عدمها فلاشك في أن إثبات الأمور المادية التي تترك آثاراً ملحوظة يكون سهلاً ميسوراً ،بعكس إثبات الأمور المعنوية فإنه يكون في غاية الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، باعتبار أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن قراءتها أو إدراكها إلا من خلال الحاسبات الآلية[1] وعموماً ،فإن الطبيعة غير المادية للبيانات التي يحتويها الحاسب الآلي والطبيعة المعنوية لوسائل نقل هذه المعطيات تطرح العديد من مشاكل الإثبات ،فقيام المجرمين بإخفاء جرائمهم أو على الأقل إزالة آثارها يعد من العوامل التي تعيق البحث عن الحقيقة، فالتزوير الإلكتروني عادة يتم خفية عن طريق التلاعب بالمعطيات والبيانات التي يحويها البرنامج الإلكتروني، فالتعديلات التي يجريها المتهم في الملفات لا تترك آثاراً، على خلاف تلك التي تترتب على تزوير المستندات الورقية، يضاف إلى ذلك أن التخزين الإلكتروني للمعطيات يجعلها غير

---

[1] د علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، الجزء الأول، محور القانون الجنائي، أكاديمية شرطة دبي، ٢٠٠٣، ص ٢١٦.

مرئية، وغير مفهومة بالعين المجردة، ويشكل انعدام الدليل المرئي والمفهوم عقبة كبيرة أمام اكتشاف الجرائم وضبط الأدلة [٢].

ومن المعروف أن الحاسب الألي يتكون من مكونات مادية ومكونات منطقية كما أن له شبكات اتصالات بصرية سلكية ولا سلكية، سواء كان ذلك على المستوى المحلي أو المستوى الدولي[3].

وفيما يتعلق بإمكانية التفتيش وضبط الأدلة راي جانب من الفقه الجنائي أنه متى كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم يمتد حتى يشمل البيانات الإليكترونية بمختلف أشكالها.

وفي حكم للمحكمة الاتحادية العليا جاء فيه:" لما كان من المقرر قانونا أن جرائم السب الواردة في المادة ٢٠ من المرسوم بقانون رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات قد اشترط المشرع لقيامها وانطباق النص عليها أن يتم السب بواسطة شبكة المعلومات أو أيه وسيلة تقنية معلومات ، وأن يتاح للمستخدمين الآخرين الدخول على الشبكة وتبادل المعلومات ، إذ عرفت المادة الأولى من ذات القانون شبكة المعلومات بأنها ارتباط مجموعتين أو أكثر من البرامج المعلوماتية يتيح للمستخدمين الدخول وتبادل المعلومات ، وعرفت وسيلة تقنية المعلومات بأنها " أية أداة مغناطيسية ..." بما مؤداه أن المشرع جعل من انتشار الجريمة عبر الفضاء الإلكتروني علة التجريم لخطورتها على

---

[٢] د جميل عبد الباقي الصغير، أدلة لإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية – القاهرة ٢٠٠٢م ص. ١١٣

[3] الدكتور/ عبد اللاه حسين محمود.: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية" دار النهضة العربية، القاهرة، سنة ٢٠٠٣. ص ٣٧٢

الأفراد والمجتمع، في حين أن جريمة السب الواردة في المادة ١/٣٧٤ من قانون العقوبات هي جرائم تتم بواسطة الهاتف بين شخصين أو أكثر يحددهم المتصل ولا تخرج عن نطاق المتصلين ولا تسمح للآخرين الدخول وتبادل المعلومات فيها، ولما كان برنامج الواتساب من البرامج التي تستخدم بواسطة الهاتف حصرا وهو ارتباط بين شخصين أو أكثر يحدد المرسل إليه دون أن يتاح للآخرين غير المعنيين بالأرسال الدخول على البرامج وتبادل المعلومات الواردة فيه شأنه في ذلك شأن الرسائل النصية ومن ثم فإن استخدام برنامج الواتساب في السب يندرج ضمن الجرائم الواردة بالمادة ١/٣٧٤ من قانون العقوبات وتخرج من نطاق التجريم الوارد بالمادة ٢٠ من المرسوم بقانون سالفة الذكر. ولما كان ذلك وكان الحكم المطعون فيه إذ عدل وصف الواقعة المنسوبة إلى المطعون ضدها من تهمة السب باستخدام وسيلة تقنية المعلومات المنصوص عليها بالمادة ٢٠ من المرسوم بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات إلى تهمة السب باستخدام الهاتف المعاقب عليها بالمادة ١/٣٧٤ من قانون العقوبات فإنه يكون قد صادف صحيح الواقع والقانون ويغدو النعي الوارد بوجه هذا النعي على غير أساس خليقا برفض الطعن" [1].

[1] الطعن رقم ٢٦١ لسنة ٢٠١٧ جزائي، جلسة الأثنين الموافق ١٨ من سبتمبر سنة ٢٠١٧.

## المبحث الثاني

## الصعوبات القانونية أثناء التعامل مع مسرح الجريمة الإلكترونية

**تمهيد وتقسيم:**

هناك العديد من الصعوبات القانونية المتعلقة بالتعامل مع مسرح الجريمة الإلكترونية، ولعل أهما هو الطبيعة القانونية للجريمة الالكترونية، التي تتطلب إجراءا معاينة خاصة تختلف عن تلك الواردة في قانون الإجراءات الجزائية الاتحادي.

على سبيل المثال لا يقتصر التفتيش في مجال الجرائم الإلكترونية على ذاك الذي يكون محله المكونات المادية للحاسوب، فتفتيش هذه المكونات، بأوعيتها المختلفة، فهو إن اتصل بالبحث عما

يمكن أن يفيد في كشف الحقيقة المتعلقة بجريمة إلكترونية، لا يخرج عن نطاق الشكل التقليدي للتفتيش[1]. غير أن محل التفتيش في مجال الجريمة الإلكترونية يمتد ليطال الحاسوب والشبكة بسائر مكوناتها كالخادم ومزود الخدمة والمضيف وغيرها من الملحقات التقنية وسنبين في هذا المبحث الصعوبات الاجرائية وتلك المتعلقة بالدليل الالكتروني عند معاينة مسرح الجريمة الالكترونية من خلال مطلبين على النحو التالي:

- **المطلب الأول:** الصعوبات الإجرائية.
- **المطلب الثاني:** الصعوبات القضائية.

## المطلب الأول

## الصعوبات الإجرائية

أمام حجم هذه الظاهرة كان لزاماً على الدول أن تتحرك لحماية مجتمعاتها في مواجهة الجرائم الإلكترونية. فجرى إبرام اتفاقية دولية خاصة بمكافحة الجريمة الإلكترونية في ٢٣ نوفمبر ٢٠٠١، هذه الاتفاقية التي باتت تعرف باتفاقية بودابست هي أول الاتفاقيات الدولية التي اختصت بمكافحة الجريمة الإلكترونية، تمت تحت إشراف المجلس الأوروبي، ووقعت عليها (٣٠) دولة من بينها أربع

[1] يتعين على القائم بالتفتيش أن يراعي الاشتراطات القانونية في حالة إجراء التفتيش في المنازل التي حددتها المادة (٥١) وما يليها من قانون الإجراءات الجزائية.

دول من خارج أعضاء المجلس كانت قد شاركت في إعداد الاتفاقية وهي الولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا، ودخلت الاتفاقية حيز النفاذ في ٢٠٠٧/١/١[1].

وفي هذا السياق أصدرت دولة الإمارات العربية المتحدة القانون رقم (٢) لسنة ٢٠٠٦ المسمى قانون مكافحة جرائم تقنية المعلومات[2].

وما يمكن أن يلاحظ على هذا القانون أنه أغفل النص على القواعد الإجرائية التي يمكن إتباعها في إثبات الجرائم الإلكترونية. ومعلوم أن هذه الجرائم، وعلى وجه الخصوص تلك التي يكون الإنترنت محلها أو وسيلة ارتكابها، لا تطرح المعاقبة عليها من ناحية إشكالية التجريم فحسب، وإنما تتضمن تحدياً مهماً أيضاً فيما يتعلق بالإجراءات الجزائية[١].

وفي ظل هذا الوضع التشريعي، وعلى ضوء الصعوبات التي تعترض ملاحقة الجريمة الإلكترونية والحصول على أدلتها، فإننا سنتناول في هذا الجزء إجراءات تفتيش نظام نُظم الحاسوب والإنترنت في التشريع الإماراتي، وذلك على النحو التالي:

**أولاً: ملائمة طرق التحقيق التقليدية للتطبيق في مجال جرائم تقنية المعلومات:**

---

[1] د. محمد عبيد سعيد سيف: مشروعية الدليل في المجالين الجنائي والتأديبي "دراسة مقارنة بالتطبيق على تشريعات دولة الإمارات العربية المتحدة"، رسالة درجة الدكتوراه في علوم الشرطة، أكاديمية مبارك للأمن، كلية الدراسات العليا، القاهرة، بدون تاريخ، ص ١٣٦.

[2] القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات.

[١] د. أحمد ضياء الدين محمد خليل: قواعد الإجراءات الجنائية ومبادئها في القانون المصري، مطبعة كلية الشرطة، القاهرة، ٢٠٠٤م، ص٣١٦.

يقوم الإثبات الجزائي على مبدأ حرية الإثبات الذي يسمح للقاضي بأن يستند في حكمه إلى الأدلة التي يتم الحصول عليها من خلال الاستدلال أو التحقيق[٢].

ويدخل ضمن هذه الأدلة المعطيات المخزنة في الحاسوب، بما في ذلك تلك الناتجة عن الاتصال بشبكة الإنترنت. وأن هذه المعطيات، التي تدخل في مجال ما يسمى الدليل الإلكتروني[3]، وسيلة ضرورية، لا يمكن تجاوزها، لملاحقة الجرائم الإلكترونية والمعاقبة عليها.

وبالإمكان، إثبات الجريمة الإلكترونية، أي الحصول على الأدلة الإلكترونية من خلال إجراءات التحقيق التقليدية، فبإمكان المحقق في مجال الجريمة الإلكترونية القيام بالتفتيش في النظام الحاسوبي، وضبط المعطيات التي يمكن الحصول عليها، وأخيراً اعتراض الاتصالات. فلا تخلو هذه الوسائل التقليدية من أهمية كبيرة في إثبات الجريمة الإلكترونية، وذلك على الرغم من العقبات التي قد تعترض استخدامها في هذا المجال،

ولكن في الحقيقة أن الصعوبة لا تكمن فيما إذا كانت هذه المعلومات ذات طابع مادي أولا ولكن تكمن بصفة أساسية في صعوبات إجرائية عدة منها ما يلي:

---

[٢] شريطة أن يراعي القاضي مبدأ المواجهة الذي يتطلب أن يعلم المتهم بالدليل المقدم ضده وتمكينه من مناقشة كل ما يقدم من أدلة خلال جلسات المحاكمة.

[3]يُقصد بالدليل الإلكتروني، المسمى (Electronic evidence) أو(Digital evidence) المعلومات (في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال أو صور أو غيرها من الأشكال) المخزنة في الحاسوب أو ملحقاته (أسطوانات أو أقراص مرنة أو غيرها من وسائل تقنية المعلومات) أو المنقولة عبر شبكات الاتصال، التي يمكن تجميعها وتحليلها بقصد إثبات وقوع الجريمة ونسبتها إلى مرتكبها.

أ- حالة وجود النظام المعلوماتي في داخل أحد المساكن مع وجود النهاية الطرفية له في مكان آخر، الأمر الذي يعطي الجاني فرصة سانحة للتخلص من المعلومات التي يستهدفها التفتيش، خاصة إذا كان الجاني ممن لدية الخبرة في التعامل مع الحاسب الآلي.

ب- أما فيما يتعلق بإذن التفتيش فتبدو الصعوبة في هذا الصدد في اشتراط أن يكون هذا الإذن محددا فيما يخص محله والأشياء التي يهدف التفتيش إلى ضبطها، حيث يجب أن يكون مصدر إذن التفتيش ذا ثقافة فنية عالية تتجاوز المعرفة العامة أو السطحية.

ت- يقتضي التفتيش عن المعلومات المخزنة آليا القيام بعملية ولوج للأنظمة الحاسوبية التي تحد بها لضبط ما يعد صالحا كدليل أو قرينة لارتكاب جريمة ما، وهذا يقتضي من الشخص القائم بالتفتيش معرفة كيفية التعامل مع برامج وملفات المعلومات المخزنة بالحاسب الألي وكذا كلمة السر والمرور اللازمين للدخول للنظام[1].

وللتغلب على الصعوبات سالفة الذكر لجا المشرع في عدة دول أخرى إلى تقرير بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة الحاسوبية وشاركه في ذلك الفقه.

[1] الدكتور/ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصطلحات الفنية، مكتبة الأهرام، القاهرة، ٢٠٠٠، ص ٣٣٨.

## المطلب الثاني

## الصعوبات المتعقلة بالدليل الإلكتروني

## المتحصل من مسرح الجريمة الإلكترونية

إذا كانت الوسائل التقليدية قد تكفي لإثبات الجرائم التقليدية، إلا أنها قد تعجز عن إثبات الجرائم التي تُرتكب بالوسائل الإلكترونية، فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ويجب لمنطقية هذا الدليل ومصداقيته أن تكون ولادة طبيعية بحيث أن الحقيقة التي يعبر عنها تصل إلى القاضي من تلقاء ذاتها ولا يتعجل هذا الأخير الوصول إليها، لأنه إن فعل ذلك قبل أن تصل هذه

الحقيقة التي يعبر عنها تصل إلى القاضي من تلقاء ذاتها، فإن الدليل الإلكتروني يصبح نتيجة لذلك، ومن ثم فإن الحقيقة التي تنبعث منه – وهذا حاله – تكون زائفة وغير معبرة عن واقع الدعوى.

إن انتشار شبكة الإنترنت والحاسب فتح مجالات عديدة للاستفادة منها، ولكن في نفس الوقت أدى إلى نشر ثقافة منافية لعادات وطبائع الكثير من المجتمعات وخصوصاً العربية نتيجة للانفتاح الذي فرضته هذه التقنيات وأيضاً نتيجة إلى توفيرها المعلومات التي يمكن استخدامها فيما يحقق مصلحة للبشرية وأيضا ما يحقق ضرراً لها مؤسسة لانتشار نوع جديد من الجريمة وهو الجريمة الإلكترونية[١].

**١ – الدليل الإلكتروني دليل علمي:**

إن البيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلاً للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص ميزته عن الدليل الجنائي حيث يتكون هذا الدليل من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقني يتعامل معه، وهذا يعني أنه كدليل يحتاج إلى بيئته

[١] د. مصطفى محمد موسى: أساليب إجرامية بالتقنية الرقمية (دراسة مقارنة)، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٥ ، ص ٥٩.

التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على دليل الدليل الإلكتروني [2].

**٢-الدليل الإلكتروني دليل تقني:**

فهو مستوح من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الإلكترونية في العالم الافتراضي، وهذا العالم كامن في هذا الحاسي الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها، فالأدلة الرقمية ليست مثل الدليل العادي، فلا تنتج التقنية سكيناً يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو بصمة أصبع... وإنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر غير شبكات الاتصال متعدية لحدود الزمان والمكان[1].

**٣ -الدليل الإلكتروني يصعب التخلص منه:**

وتعد من أهم خصائص الدليل الإلكتروني، بل إنه يمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن أيضاً التخلص من بصمات الأصابع بمسحها من موضعها، بالإضافة إلى أنه في بعض الدول الغربية

---

[2] Eoghan Casey: Digital evidence and forensic science, computer and the Internet, computer crime, 1st ed. Academic Press – USA UK 2000.P.9

[1] د. ممدوح عبد الحميد عبد المطلب، وزبيدة محمد جاسم وعبد الله عبد العزيز: نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في الفترة من ١٠-١٢ مايو ٢٠٠٣م، ص ٢٢٤٠.

يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة بل إن نشاط الجاني نحو الدليل يشكل كدليل أيضاً، فنسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقاً كدليل إدانة ضده[2].

**٤- الدليل الإلكتروني قابل للنسخ:**

حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغير عن طريق نسخ طبق الأصل من الدليل[1].

**٥- السعة التخزينية العالية:**

يمتاز الدليل الإلكتروني بالسعة التخزينية العالية، فآلة الفيديو الرقمية، يمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين بيانات عديدة...الخ[2].

---

[2]- د. ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد إله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في ١٠ – ١٢ مايو ٢٠٠٣، ص ٢٢٤٠.

[1]عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري – الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية – المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي – جامعة نايف العربية للعلوم الأمنية – الرياض – ٢٠٠٧، ص ١٥.

**٦- رصد المعلومات وتحليلها:**

الدليل الإلكتروني يرصد معلومات عن الجاني ويحللها في ذات الوقت، حيث يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته، وبعض الأمور الشخصية عنه، لذا، فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي[3].

هذه الخصائص سبغت على الدليل الإلكتروني طابعاً متميزاً، جعلته يتميز بذاتية خاصة مختلفة عن الأدلة التقليدية.

وفي ذلك السياق نصت المادة (٧) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة على أنه: "يعاقب بالسجن المؤقت كل من حصل أو استحوذ أو عدّل أو أتلف أو أفشى بغير تصريح بيانات أو مستند إلكتروني أو معلومات إلكترونية عن طريق الشبكة المعلوماتية أو موقع إلكتروني أو نظام المعلومات الإلكتروني أو وسيلة تقنية معلومات وكانت هذه البيانات أو المعلومات تتعلق بفحوصات طبية أو تشخيص طبي أو علاج أو رعاية طبية أو سجلات طبية"[١].

---

[2]د. ممدوح عبد الحميد عبد المطلب، وزبيدة محمد جاسم وعبد الله عبد العزيز: نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مرجع سبق ذكره، ص ٢٢٤١.

[3]د. ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد رقم ٤، المحور الأمني والإداري، تاريخ الانعقاد: ٢٦-٢٨ أبريل ٢٠٠٣م، دبي، الإمارات العربية المتحدة، ص ٦٤٩-٦٥٠.

[١] المادة (٧) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة.

ونجد أن المشرع الإماراتي تناول ذلك في المادة (٩) من القانون الإماراتي التي نصت على أنه: "يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسون الف درهم ولا تتجاوز خمسمائة الف درهم أو بإحدى هاتين العقوبتين كل من تحايل على العنوان البروتوكولي للإنترنت باستخدام عنوان وهي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها"[٢].

ولا شك في أن الجرائم التي تقع على بطاقات الإئتمان تتميز بطبيعة خاصة، مما يتطلب إتباع طرق بحث وتحري مختلفة عن طريق بحث وإثبات الجرائم التقليدية، وذلك بالنظر إلى المفهوم الجديد لهذه الجرائم والتي يتعرض محلها لعمليات تزييف وتحايل مستحدثة بفضل التقنيات التكنولوجية المستحدثة، وهو ما قد يترتب عليه ظهور مجرم جديد ومفاهيم جديدة للجريمة ومسرح يتسع لها قد يسع العالم كله.

وفي ذلك السياق نصت المادة (١٢) من القانون الاتحادي على أنه: "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة إئتمانية أو إلكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني، وتكون العقوبة الحبس مدة لا تقل عن ستة اشهر والغرامة التي لا تقل عن مائة الف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير، أو الاستفادة مما تتيحه من خدمات. فإذا توصل من ذلك إلى الاستيلاء

---

[٢] المادة (٩) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة.

لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين ...."[1].

## الخاتمة

تختلف الجريمة الالكترونية عن الجريمة التقليدية من حيث خصائصها، ولاسيما أنها تتم في فضاء افتراضي، فهي لا تقف عند حدود جغرافية معينة، كما أنها بذات الوقت ترتكب من قبل اشخاص محترفون، وهذا بحد ذاته يشكل صعوبة في معاينة مسرح الجريمة الالكترونية، مايتطلب تطوير قواعد الاجراءات الجزائية حتى تكون ملائمة للتطبيق على هذا النوع من الجرائم، وما يزيد الامر صعوبة في مرحلة الاستدلال عن الجرائم الالكترونية هو أن الادلة من الممكن أن يتم حذفها بسهولة، والتخلص منها، وهذا الأمر يتطلب من مأمو الضبط القضائي خبرة فنية متطورة، لذلك تعمد بعض جهات الضبط القضائي الى الاستعانة بالخبراء الفنيين لاسترجاع الأدلة الالكترونية ونسخها وتحوليها لأدلة مادية يسهل التعامل معها كدليل للإثبات في الجرائم الالكترونية، وقد جاء هذا البحث ليبين طبيعة الصعوبات في مرحلة معاينة مسرح الجريمة الالكترونية.

في نهاية البحث توصلنا لجملة من النتائج والتوصيات ، هي التالي:

---

[1] المادة (١٢) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة.

## أولا: النتائج.

١. تعتبر الجريمة الالكترونية من الجرائم المستحدثة التي ارتبط وجوها بظهور شبكة الانترنت وتطور التقنيات الحديثة، كما أن للجرائم الالكترونية خصائص تنفرد بها عن الجرائم التقليدية من حيث الوسيلة المستخدمة بارتكاب الجريمة، اضافة إلى جملة من الصعوبات التي تترافق مع طبيعة هذه الجريمة، ولاسيما في مرحلة الاستدلال والتعامل مع مسرح الجريمة الالكترونية.

٢. إن من أبرز الصعوبات التي تواجه جهات الضبط القضائي هي صعوبة الكشف عن مرتكب الجريمة الألكترونية، وغالبا" مايكون المجرم المعلوماتي من ذوي الخبرة الفنية العالية، حيث أنه يستطيع التخلص من أدلة الإدانة بسهولة.

٣. هناك صعوبة تتمثل في طبيعة التعامل مع مسرح الجريمة الالكترونية، اذ أنها ترتكب باستخدام التقنيات الحديثة وخاصة اجهزة الحاسب الآلي والهواتف الذكية، وهو مايشكل عقبة أمام مأمور الضبط القضائي عند معاينة مسرح الجريمة الإلكترونية حيث أن التفتيش في هذه الأجهزة يصطدم بمسألة المساس بخصوصيات الأفراد، وقد يصل إلى مرحلة المساس بالخصوصية.

## ثانيا: التوصيات.

١. ضرورة سن تشريع خاص بإجراءات التعامل مع مسرح الجريمة الإلكترونية، وخاصة في مرحلة الاستدلال، لأن قواعد الاستدلال في قانون الإجراءات الجزائية الاتحادي وقانون

الإجراءات الجنائية المصري هي للتعامل مع مسرح الجريمة التقليدية التي تختلف فيها الوسائل عن تلك التي ترتكب بواسطتها الجريمة الالكترونية.

٢. ضرورة تدريب مأموري الضبط القضائي على كيفية معاينة مسرح الجريمة الالكترونية، لأنها تتطلب توافر خبرة فنية معينة وخاصة فيما يتعلق باسترجاع الملفات المحذوفة وتحويلها لأدلة مادية يسهل استخدامها كدليل للإدانة.

٣. ضرورة تشكيل هيئات قضائية متخصصة بالنظر في الجرائم الالكترونية، تكون قادرة

# قائمة المراجع:

## المراجع العامة:


١. أيمن سيد دوريش: المرجع الكامل لخدمات الإنترنت، شعاع للنشر والعلوم، القاهرة، ١٩٩٨ م.

٢. د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠١٥م.

٣. خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، دار النهضة العربية، القاهرة، ط ١، ٢٠١٢ م.

٤. داود سليمان علي الحمادي، أحكام جريمة التزوير الإلكتروني، دار النهضة العربية، القاهرة، ٢٠١٦.

٥. الدكتور/ عبد اللاه حسين محمود: الجوانب الموضوعية والإجرائية لجرائم المعلوماتية" دار النهضة العربية، القاهرة، سنة ٢٠٠٣.

٦. الدكتور/ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصطلحات الفنية، مكتبة الأهرام، القاهرة، ٢٠٠٠.

٧. المستشار محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ٢٠١٥م.

٨. مصطفى السيد، دليلك الشامل إلى شبكة الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، ١٩٩٧ م.

٩. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط ، ١٩٩٤.

## المراجع المتخصصة:

١. د. أحمد ضياء الدين محمد خليل: قواعد الإجراءات الجنائية ومبادئها في القانون المصري، مطبعة كلية الشرطة، القاهرة، ٢٠٠٤م.

٢. د. جميل عبد الباقي الصغير، أدلة لإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية – القاهرة ٢٠٠٢م.

٣. د. مصطفى محمد موسى: أساليب إجرامية بالتقنية الرقمية (دراسة مقارنة)، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٥.

٤. هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، القاهرة، ٢٠٠٩.

## البحوث والرسائل العلمية:

١. د. محمد عبيد سعيد سيف: مشروعية الدليل في المجالين الجنائي والتأديبي "دراسة مقارنة بالتطبيق على تشريعات دولة الإمارات العربية المتحدة"، رسالة درجة الدكتوراه في علوم الشرطة، أكاديمية مبارك للأمن، كلية الدراسات العليا، القاهرة، بدون تاريخ.

**الندوات والمحاضرات:**

١. عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري – الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية – المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي – جامعة نايف العربية للعلوم الأمنية – الرياض – ٢٠٠٧.

٢. د. علي محمود حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، الجزء الأول، محور القانون الجنائي، أكاديمية شرطة دبي، ٢٠٠٣.

٣. د. محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو، ٢٠٠٠.

٤. د. ممدوح عبد الحميد عبد المطلب، وزبيدة محمد جاسم وعبد الله عبد العزيز: نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية

الإلكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في الفترة من ١٠-١٢ مايو ٢٠٠٣م.

٥. د. ممدوح عبد الحميد عبد المطلب: استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي، مركز البحوث والدراسات، العدد رقم ٤، المحور الأمني والإداري، تاريخ الانعقاد: ٢٦-٢٨ أبريل ٢٠٠٣م، دبي، الإمارات العربية المتحدة.

٦. وليد عالكوم، مفهوم وظاهرة الإجرام المعلوماتي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، مايو، ٢٠٠٠.

**القوانين:**

١. القانون الاتحادي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات العربية المتحدة.

٢. قانون الإجراءات الجزائية الاتحادي.

٣. قانون الإجراءات الجنائية المصري.

**الأحكام قضائية:**

١. الطعن رقم ٢٦١ لسنة ٢٠١٧ جزائي، جلسة الأثنين الموافق ١٨ من سبتمبر سنة ٢٠١٧.

**مراجع أجنبية:**

1. Eoghan Casey: Digital evidence and forensic science, computer and the Internet, computer crime, 1st ed. Academic Press - USA UK 2000.

## الفهرس