مجلة البحث العلمي الإسلامي

Journal of Islamic Scientific Research

(JOISR)

مجلة إسلامية علمية محكمة

تعنى بالبحوث والدراسات الإسلامية

ISSN: 2708-1796 (ردمد النسخة المطبوعة)

E-ISSN: 2708-180X (ردمد النسخة الإلكترونية)

المجلد 23 – العدد 78 – فبراير 2026

Volume 23 – issue 78 – February 2026

Pages 259 - 299 الصفحات 259 - 299

# إثبات الجريمة الإلكترونية وفق النظام السعودي

# Proof of crime according to the Saudi system

DOI: https://doi.org/10.55625/joisr-7809

مروان راجي دخيل الله العرفي

Marwan Raji Dakhil Allah Al-orfi

باحث ماجستير كلية الأنظمة والاقتصاد بالجامعة الإسلامية بالمدينة المنورة

Master's Researcher in Law and Economics, Islamic University of Madinah, Saudi Arabia

Email: marwanalorfi1@gmail.com

Date of Receipt - 2025/10/21 – تاريخ الاستلام

Date of Acceptance - 2025/11/02 – تاريخ القبول

الباحث: مروان راجي دخيل الله العرفي
باحث ماجستير كلية الأنظمة والاقتصاد بالجامعة الإسلامية بالمدينة المنورة
***Researcher name : Marwan Raji Dakhil Allah Al-orfi***
البريد الإلكتروني: marwanalorfi1@gmail.com

# إثبات الجريمة الإلكترونية وفق النظام السعودي

# Proof of crime according to the Saudi system

**DOI: https://doi.org/10.55625/joisr-7809**

تاريخ الاستلام: ٢٠٢٥/١٠/٢١ / تاريخ القبول: ٢٠٢٥/١١/٢

**المستخلص**

يناقش هذا البحث طرق ووسائل إثبات الجريمة الإلكترونية، وتكمن أهمية البحث في كونه يبين ويوضح مفهوم الجريمة الإلكترونية، وبيان خصائصها، وتوضيح الفرق بينها وبين الجرائم التقليدية، والوقوف على أهم الوسائل القانونية التي يثبت بها هذا النوع من الجرائم.

كما يسعى البحث للبحث حول دراسة حلول لمشكلة الطرق المتبعة لإثبات الجريمة، وبيان مدى قوة الدليل الإلكتروني في إثبات هذه الجريمة، وقد استخدم الباحث المنهج الوصفي التحليلي للوصول إلى نتائج البحث، واستنتج الباحث أن الجرائم الإلكترونية من الجرائم التي لا تترك أثراً في الغالب حيث لا يمكن الاستشهاد بأدلة جنائية للحصول على إثبات لها وتتسم بصعوبة إثباتها حيث أنها من الجرائم المستحدثة والمتنوعة الوسائل، كما استطاع الباحث الوصول إلى الأطراف المعنيين والمسؤولين عن الجريمة الإلكترونية وتحديد مدى صلة كلا منهما بالجريمة، واستنتج الباحث أيضاً طرق الإثبات والخصائص التي تجمع الجريمة الإلكترونية بالجريمة التقليدية وبيان ما يمكن الاعتماد عليه من أدلة في كشفها.

وأوصى الباحث بالاهتمام بهذا الأمر، حيث أنه من الجرائم المستحدثة والقابلة للتحديث باستمرار؛ نظرا للتقدم السريع والملحوظ على كافة الأصعدة التقنية، والتي لا تخلو من التهديدات والمخاطر التي تؤدي إلى الجريمة الإلكترونية كما أوصى الباحث المنظم السعودي بالتحديث والتجديد الدائم والمستمر لنظام مكافحة الجرائم الإلكترونية حتى يواكب التغير والتنوع الذي يطرأ على الجريمة الإلكترونية ليستطيع المنظم الوصول إلى العقوبات الرادعة التي تحد من

انتشـار هذا النوع من الجرائـم، كما أوصى الباحث أيضاً بالاهتمام بكافة الوسائل والطرق الفنية التـي مـن شأنها التسهيل فـي الوصول إلى أدلة علـى الجريمة الإلكترونية، ودمـج ما يمكن دمجه من الوسائـل التقليدية مع الوسائل الإلكترونية للوصول إلى العدالة في إثبات الجريمة الإلكترونية والعقوبة الملائمة لها.

الكلمـات المفتاحية: الجريمة الإلكترونية – القانون الجنائـي – الإثبات الإلكتروني – إثبات الجريمة – التقنية الحديثة

**Abstract**

This research discusses the methods and means of proving cybercrime. The importance of the research lies in its clarification of the concept of cybercrime, its characteristics, its distinction from traditional crimes, and its identification of the most important legal means of proving this type of crime.

The research also seeks to explore solutions to the problem of methods used to prove cybercrime and demonstrate the strength of electronic evidence in proving this crime. The researcher used the descriptive and analytical approach to arrive at the research results. He concluded that cybercrimes are crimes that often leave no trace, as criminal evidence cannot be used to prove them. They are also difficult to prove, as they are new crimes with diverse methods. The researcher was also able to reach the parties involved and those responsible for cybercrime and determine the extent of their connection to the crime. The researcher also deduced the methods of proof and the characteristics that unite cybercrime with traditional crimes, and explained the evidence that can be relied upon to uncover them. The researcher recommended paying attention to this issue, as it is a newly emerging crime that is subject to continuous updating due to the rapid and noticeable progress in all technical fields, which are not without the threats and risks that lead to cybercrime. The researcher also recommended that the Saudi regulator constantly update and renew the system for combating cybercrimes to keep pace with the changes and diversity occurring in cybercrime, enabling the legislator to reach deterrent penalties that limit the consequences of this type of crime. The researcher also recommended that the legislator pay attention to all technical means and methods that facilitate access to evidence of cybercrime and integrate what can be combined from traditional means with electronic means to achieve justice in proving cybercrime and imposing appropriate penalties.

**Keywords:** Cybercrime - Criminal Law - Electronic Evidence - Proof of Crime - Modern Technology

**مقدمة البحث**

بسـم الله الرحمـن الرحيم والصلاة والسلام على أشرف الخلـق سيدنا محمد عليه أفضل الصلاة وأتم التسليم.

أما بعد:

فمع تقدم التكنولوجيا، والتقدم العلمي في وقتنا الحالي الذي قدم الكثير، والكثير من المزايا والخدمـات لأفراد المجتمع وجعلت الحياة بالنسبة لهـم تتسم بالانسيابية، والمرونة وكان الهدف المـراد منه هو تسهيل الحياة بالنسبة لهـم، وتطورها، ولكن بالمقابل هذا التقدم الذي حدث أتى معه؛ التطـور الفكري الإجرامي المخيف، وأصبحت أغلبية الجرائـم تتجه من الجريمة التقليدية إلـى الجريمة الإلكترونية، وتزايـد حدوث الجرائم حيث إنها أصبحت مع التقدم الإلكتروني يسهل تنفيذها، ويصعب إثباتها بسبب الكم الهائل من البيانات، وتطور الأدوات التقنية للمجرمين. ومع ظهـور التكنولوجيا بدأت تظهـر جرائم مختلفة، وجديدة عن الجرائـم التقليدية التي كان يتعامل معهـا النظام الأمنـي، والنظام القانوني، وكذلك القضائي بأساليـب معروفة من خلال حصرها؛ وتلك الجرائم الجديدة تتمثل في الجرائم الإلكترونية.

كذلك إن الأنظمة سعت لوضع قوانين وأنظمة قانونية مختصة في الجرائم الإلكترونية، ومن ذلـك المنظم السعودي الذي أصدر العديد من الأنظمة، ومنها نظام مكافحة جرائم المعلوماتية. وكذلـك إن أهميـة إثبات الجريمة بصفة عامـة بالغة من أمرها، وتكمـن أهميتها في الكشف عن الحقيقـة، والوصول إلى الوقائـع، والتعرف على الجاني من خلال معرفة المجني عليه، وذلك عبر الأدلة، حيث إنه لا جريمة دون إثبات ولا أدلة؛ ونفس الأمر ينطبق كذلك على الجريمة الإلكترونية حيث لا تطبق القوانين إلا إذا تم إثبات الجريمة أولاً[1]. ونظراً لاختلاف طبيعة الجريمة القانونية الإلكترونيـة عن الجريمـة التقليدية فقد أدى ذلك إلـى؛ إشكالية في تطبيـق النصوص التقليدية على الجرائـم الإلكترونية، واتباع نفس الأساليب، والطرق لإثبـات الجرائم الإلكترونية[2]. كذلك تتمثـل أهميـة الدليل الإلكتروني في أنه بدونه لا تكون هنـاك جريمة، حيث إنه لا جريمة بلا دليل، ولا عقـاب بلا جريمة، لذلك فإن التوصل إلـى الدليل الإلكتروني من قبل المختصين يعد العنصر الأهم، ولذلك يعد دور الخبراء التقنيين في الجريمة الإلكترونية هو الأبرز، ويكون ذلك من خلال فحصـ الأجهـزة، وتقديم تقرير مفصل بجميـع البيانات التي تم التوصل إليهـا، سواء من خلال البيانـات المتوفرة علـى الأجهزة، أو من خلال الحصـول عليها بالطرق التقنيـة المعقدة، أو من خـلال التواصل مع الشركات المستضيفة للمواقع الإلكترونية حول العالم. كذلك إنه قد تم الدمج

(١) بطيخ، حاتم أحمد محمد: تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات دراسة تحليلية مقارنة مجلة الدراسات القانونية والاقتصادية، جامعة المنوفية – كلية الحقوق، العدد ١، ٢٠٢١م،)، ص ٨٠

(٢) ال ثنيان، ثنيان ناصر : إثبات الجريمة الإلكترونية دراسة تأصيلية تطبيقية، (رسالة ماجستير)، (كلية الدراسات العليا، جامعة الأمير نايف العربية للعلوم الأمنية، الرياض، دولة المملكة العربية السعودية، (٢٠١٢م)، ص١

بين الطـرق التقليدية، والطرق الإلكترونية لاعتمادها في إثبات الجريمة الإلكترونية، حيث تمثلت طرق إثبات الجريمة الإلكترونية في الطرق التقليدية التي تتمثل في الضبط، والتفتيش، والمعاينة، وكذلك في الطرق الإلكترونية من خلال الاستعانة بالخبراء التقنيين لفحص الأجهزة، والتأكد من الرسائـل، ومكان القيام بالجريمة وذلك يرجع إلى طبيعـة الجريمة الإلكترونية التي في الغالب لا يكون فيها دليل مادي ملموس، وإنما يتم التوصل إلى الدليل من قبل الخبراء والمختصين بالتقنية بالتعـاون مع جهات التحقيق؛ حيث تقـوم الجريمة الإلكترونية على ركنيـن أساسيين هما: الركن المـادي المتمثل في الأدوات، والأجهزة، التي من خلال فحصهـا يتم التوصل إلى الدليل، والركن المعنـوي المتمثـل في العمل والإرادة لـدى الجاني. ومن خـلال الدراسة الحاليـة سيتم التعريف بالجريمة الإلكترونية وأركانها، وخصائصها، والطبيعة القانونية لها، ومن ثم بيان أهمية الإثبات، وأشخاص الجريمـة الإلكترونية، وكذلك التعريف بالدليل الإلكترونـي، وبيان خصائصه المنفرد بهـا، وتوضيح طـرق الحصول على الدليل الإلكترونـي، وطرق إثبات الجريمـة الإلكترونية ونختم نهاية بالسوابق القضائية المتعلقة بالجرائم الإلكترونية.

**أهمية البحث**

- بيان مفهوم الجريمة الإلكترونية، وتوضيح الخصائص التي تميز الجرائم الإلكترونية عن الجرائم التقليدية، وبيان الطبيعة القانونية للجريمة الإلكترونية.
- معرفة أهمية إثبات الجرائم الإلكترونية.
- معرفة أطراف الجريمة الإلكترونية، وتوضيح الفئات الخاصة بكل طرف بهم.
- بيان مفهوم الدليل الإلكتروني للجريمة، وما هي الطرق المتبعة حتى يتم الحصول على الدليل الإلكتروني الخاص بالجريمة.
- أهمية معرفة الطرق الخاصة بإثبات الجريمة الإلكترونية.

**أسباب اختيار الموضوع**

إن الذي دعاني لاختيار هذا الموضوع عدة أسباب وأهمها ما يلي:

- قلة البحث في هذا الموضوع كونه من الموضوعات المستحدثة والعصرية.
- الوقـوف علـى أهم العقبـات والتحديات التي تواجـه التعامل مع الجريمـة الإلكترونية وتحقيق العدالة فيها
- معرفة الأسس التي يبنى عليها الأخذ بالأدلة الإلكترونية أو رفضها.
- الحاجـة لزيـادة تعزيز الحماية القانونية للمجتمع، بسبـب زيادة حالات الاعتداء على الخصوصيـة التقنيـة، ممـا يجعل دراسـة وسائل إثبـات الجريمة الإلكترونيـة تسهم في دعم القانون ومكافحة الجريمة الإلكترونية.

- الرغبة بالربط بين الجانب النظري والتطبيقي حيث يهدف البحث إلى ربط النصوص النظامية مع التطبيقات القضائية، مما يحقق الفهم الواقعي لإثبات الجريمة الإلكترونية.

**أهداف البحث**

١- بيان طرق إثبات الجريمة الإلكترونية وفق النظام السعودي

٢- بيان مدى وضوح النصوص النظامية المتعلقة بإثبات الجريمة الإلكترونية

٣- توضيح ما هو الدليل الإلكتروني والفوارق بين الأدلة الإلكترونية والأدلة الغير إلكترونية

٤- إدراج عدة تطبيقات قضائية في النظام السعودي في موضوع الجرائم الإلكترونية

**إجراءات البحث**

استخدم البحث في منهجه المنهج الوصفي التحليلي وهو أسلوب من أساليب التحليل المركزي على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد، أو فترة أو فترات زمنية معلومة، وذلك من أجل الحصول على نتائج علمية، ثم تفسيرها بطريقة موضوعية، بما ينسجم مع المعطيات الفعلية للظاهرة[١]

**منهج البحث**

اعتمد الباحث في دراسته على المنهج الوصفي التحليلي، وذلك من خلال جمع المعلومات المتعلقة بموضوع إثبات الجريمة الإلكترونية من المصادر النظامية والقضائية، ثم وصفها وتحليلها للوصول إلى نتيجة علمية قانونية دقيقة. ويتمثل تطبيق هذا المنهج في الخطوات الآتية:

- الوصف:

يقوم الباحث بوصف مصطلحات البحث و بيانها و كذلك القواعد النظامية ذات العلاقة بإثبات الجرائم الإلكترونية، مثل نصوص نظام الإثبات ونظام مكافحة الجريمة المعلوماتية والأنظمة الإجرائية ذات الصلة.

- التحليل:

يعمد الباحث إلى تحليل هذه النصوص القانونية والممارسات القضائية تحليلًا قانونيًا لبيان مدى كفاية طرق إثبات الجريمة الإلكترونية وذلك في مواجهة التطورات التقنية.

**مشكلة البحث**

١- ما طبيعة الأدلة الرقمية وما مدى كفايتها ومشروعيتها للإثبات؟

٢- ما مدى قبول وسائل إثبات الجريمة الإلكترونية أمام القضاء السعودي؟

٣- ما مدى قوة الدليل الإلكتروني؟

(١) رجاء وحيد دويدري: البحث العلمي أساسياته النظرية وممارسته العملية ص ١٨٣.

**أسئلة البحث**

هناك ثلاث تساؤلات تم طرحها وسوف يتم الإجابة عنها في البحث بمشيئة الله وهي:

١- ما هي طرق الإثبات المتبعة في إثبات الجريمة الإلكترونية.

٢- من هم أشخاص الجريمة الإلكترونية.

٣- مدى قوة الدليل الإلكتروني في إثبات الجريمة الإلكترونية.

**الدراسات السابقة**

**١- الدراسة الأولى:**

عنوان الدراسة: الإثبات الجنائي في الجريمة الإلكترونية

اسم الباحث: محمد بن ناصر بن علي الرقيشي

نوع الدراسة: رسالة ماجستير

الجامعة: جامعة السلطان قابوس (سلطنة عمان)

السنة: ٢٠١٨م

**ملخص الدراسة:** لقد وضحت هذه الدراسة ماهية الإثبات الجنائي، وماهية الجريمة الإلكترونية، وكذلك وضحت الإجراءات الخاصة بجمع الدليل الإلكتروني، سواء كانت عن طريق الإجراءات التقليدية، أو الإجراءات الإلكترونية.

**٢- الدراسة الثانية:**

عنوان الدراسة: إثبات الجريمة الإلكترونية (دراسة تأصيلية مقارنة).

اسم الباحث: ثنيان ناصر آل ثنيان.

نوع الدراسة: رسالة ماجستير.

الجامعة: جامعة نايف العربية للعلوم الأمنية.

السنة: ٢٠١٢م.

**ملخص الدراسة:**

لقد توصلت هذه الدراسة إلى أن الجريمة الإلكترونية لها طبيعة قانونية، تستلزم من خلالها وسائل غير تقليدية، عن طريقها يتم الحصول على الدليل الإلكتروني، وكذلك بيان أن الجريمة الإلكترونية من أهم المعوقات التي تواجهها حتى يتم إثباتها هو عدم العثور على الدليل المادي.

**خطة البحث:**

- المبحث التمهيدي: مفهوم الإثبات وماهية الجريمة الإلكترونية.

- المطلب الأول: مفهوم الإثبات والجريمة لغة واصطلاحاً.
- المطلب الثاني: ماهية الجريمة الإلكترونية.
- المبحث الأول: أهمية إثبات الجريمة وأشخاص الجريمة الإلكترونية.
- المطلب الأول: أهمية إثبات الجريمة بصفة عامة والجريمة الإلكترونية
- المطلب الثاني: أشخاص الجريمة الإلكترونية.
- المبحث الثاني: الدليل الإلكتروني وطرق إثبات الجريمة الإلكترونية.
- المطلب الأول: ماهية الدليل الإلكتروني.
- المطلب الثاني: طرق الحصول على الدليل الإلكتروني.
- المطلب الثالث: طرق إثبات الجريمة الإلكترونية.
- المبحث الثالث: التطبيقات القضائية.

## المبحث التمهيدي

### مفهوم الإثبات وماهية الجريمة الإلكترونية

قسم هذا المبحث التمهيدي إلى مطلبين، وتم تخصيصه للتعريف بالمصطلحات الأساسية، والتمهيدية، والتي يحصل بها خطأ في بعض الأوقات، فلا بد من تعريفها بصورة صحيحة، وواضحة، حتى يتم معرفتها بشكل كامل؛ وسأقوم في هذا المبحث بمشيئة الله بتعريف مصطلح الإثبات لغة، واصطلاحاً، وماهية الجريمة لغة، واصطلاحاً وتعريف موضوعنا الأساسي، وهو الجريمة الإلكترونية، وبيان أركانها، وخصائصها، والطبيعة القانونية لها.

#### المطلب الأول: مفهوم الإثبات والجريمة لغة واصطلاحاً

إن التعريف بمصطلحات البحث هو أهم متطلب يأتي بداية البحث به، وذلك حتى يتم للفرد وضوح معنى المصطلحات التي يقوم عليها البحث، وسوف أقوم بتعريفها بمشيئة الله في هذا المطلب.

الإثبات لغة: «ثَبَتَ الشيءُ يَثْبُتُ ثَباتاً وثُبوتاً فَهُوَ ثابتٌ»[١].

الإثبات اصطلاحاً: «إقامة الدليل أمام القضاء بالطرق التي حددتها الشريعة على حق أو واقعة معينة تترتب عليها آثار»[٢].

الجريمة لغةً: «الجُرْمُ: التّعدِّي، والجُرْمُ: الذَّنْبُ، وَالْجَمْعُ أَجْرامٌ وجُرُومٌ، وَهُوَ الجَرِيمَةُ، وقد جَرَمَ يَجْرِمُ جَرْماً واجْتَرَمَ وأَجْرَم، فَهُوَ مُجْرِم وجَرِيمٌ»[٣].

الجريمة اصطلاحاً: إن تعريفات الجريمة متعددة، سواء كانت في الاصطلاح الفقهي، أو الاصطلاح القانوني ففي الاصطلاح الفقهي لها اتجاهين: خاص وعام، وبمشيئة الله سوف أذكر الاصطلاحين الفقهي، والقانوني.

الجريمة العامة في الاصطلاح الفقهي: «فالتعريف العام للجريمة أن تكون مرادفة للشر عموماً فيقال الجريمة: «هي عصيان ما أمر الله به وفعل ما نهى الله عنه». ويمكننا أيضاً أن نقول إن هذا هو تعريف علماء الأخلاق للجريمة[٤]. والتعريف الخاص للجريمة نقول بأنها: «هي العصيان الشرعي المعاقب عليه قضاء»[٥].

---

(١) ابن منظور، محمد بن مكرم بن علي أبو الفضل جمال الدين: (لسان العرب ط الثالثة (١٤١٤)، الجزء الثاني)، ص ١٩.

(٢) موسى، خالد السيد: شرح قواعد الإثبات الموضوعية: دراسة مقارنة (مكتبة القانون والاقتصاد الرياض، الطبعة الأولى، ٢٠١٤)، ص ٢١.

(٣) ابن منظور لسان العرب مرجع سابق، جزء ١٢ ص ٩١.

(٤) الزهراني، سعيد بن حسن ال يحيى: جرائم الشبكة العالمية للمعلومات (الإنترنت) (جامعة الإمام محمد بن سعود الإسلامية، الرياض، الطبعة الأولى ٢٠٢٠م)، ص ٥٣.

(٥) الزهراني: جرائم الشبكة العالمية للمعلومات، مرجع سابق، ص ٥٣.

الجريمــة وفقاً للاصطلاح القانوني: إخلال بقاعــدة قانونية ذات طابع جنائي تحظر سلوكاً معينــاً إيجابياً أو سلبياً (عـ ـلاً أو امتناع عن عمل) وترتب لمن يقع منــه الانتهاك إرادياً ومختاراً جزاء جنائياً (عقوبة أم تدبيراً احترازياً)[١].

**المطلب الثاني: ماهية الجريمة الإلكترونية**

**أولاً: الجريمة الإلكترونية:** لقد عرف النظام السعودي الجريمة الإلكترونية وهي: «أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام»[٢].

التعريــف الآخر للجريمة الإلكترونية: «هي مجموعة العناصــر المتداخلة المؤثرة في طبيعة الأفعــال الإجرامية المرتكبة والمتصلة اتصــالاً وثيقاً بالحاسب الآلي، والمعلوماتية، وهي بذلك لا يتصور وجودها دون ارتباط بالحاسوب»[٣].

**ثانياً: أركان الجريمة الإلكترونية:**

هنــاك أركان أساسية للجريمــة الإلكترونية، شأنها شأن الجرائــم التقليدية، ولكن طبيعتها تختلف، حيث يجب توافر ركنين أساسيين في الجريمة الإلكترونية؛ بالإضافة إلى ركن ثالث يتعلق بأنظمة الدول وقد يختلف من دولة لأخرى.

أمــا الركنان الأساسيان فهما الركن المادي، ويتمثل: في الاستعداد للجريمة، والتجهيز لها، واستخــدام أداة الجريمة التي تتمثل في الأجهــزة أو المواقع الإلكترونية؛ والركن الثاني هو الركن المعنــوي الذي يتمثل فــي الحالة المزاجية، والنفسية للقائم بالجريمــة الإلكترونية، والعلاقة بين المتهم والركن المادي[٤].

ويتمثل الركن الثالث: في الركن الشرعي الذي يتمثل: في اعتبار الفعل الذي قام به الشخص جريمــة إلكترونية يعاقب عليها القانــون، وهذا الركن يختلف من دولة وأخــرى، ومن نظام وآخر، حيــث قد يكون هناك فعل يُعد جريمة في دولــة، ولا يُعد جريمة في دولة أخرى. إن الركن المادي، يوضــح الفعــل الجنائي الذي قام به المجــرم؛ والشكل الخارجي له، وكذلــك نتيجة فعله، والسبب الــذي يربط الفعل بالنتيجة، فإذا لــم يتوافر فعل، أو سبب، أو نتيجة؛ فلن يقوم الركن المادي، ولا يوجد جريمة يمكن إثباتها. أما بالنسبة للركن المعنوي، يبين ما إذا كان القصد الجنائي عمدي، أم غيــر عمــدي، أو حدث بسبب خطأ ورد، أو بسبب الإجبــار، والركن المعنوي، يكمن فيه أن يكون الفاعــل عالم بالجريمة التي سوف يتم حدوثها، وأن يكون هناك إرادة لفعل هذه الجريمة؛ أما إذا

(١) مرعي، أحمد لطفي السيد: أصول علمي الإجرام والعقاب، دار الكتاب الجامعي للنشر والتوزيع، الرياض، المملكة العربية السعودية، الطبعة الأولى، ١٤٣٧)، ص ٥٠.

(٢) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/١٧/ بتاريخ ١٤٢٨هـ، المادة الأولى.

(٣) سكيكر، محمد علي الجريمة المعلوماتية وكيفية التصدي لها، (سلسلة كتاب الجمهورية، دولة مصر، ٢٠١٠)، ص ٣٦.

(٤) آل ثنيان: إثبات الجريمة الإلكترونية، مرجع سابق، ص ٢١-٢٢.

لم يتوافر علم وإرادة للجريمة؛ فلن يقوم الركن المعنوي للجريمة.

واستنتاجاً من الذي ذكر، فإن الجريمة لا قيام لها دون الركنان الأساسيان: وهما الركن المادي، والمعنوي.

**أولاً: الركن المادي:**

إن وجود الركن المادي يعتبر أمر ثابت في الجريمة، فالركن المادي هو أن يقوم الجاني بالفعل الغير مشروع، والذي من خلاله يتم الاعتداء على حق قانوني؛ فإذاً لا قيام لجريمة دون توافر هذا النشاط الخارجي المادي، ولا يتم تكون الركن المادي للجريمة إلا عن طريق قيام الجاني بالفعل الغير مشروع؛ أو أنه قام بعدم القيام بعمل يجب فعله، أي (الامتناع عن عمل) وكذلك عندما يوجد قصد الفعل الجريمة، أو نية مراده، ولكن إن لم يكن هناك فعل فهنا لن تحدث الجريمة؛ بسبب عدم وجود سلوك إجرامي حدث، لذلك لابد أن تكون النية الإجرامية حدثت على أرض الواقع، وكذلك إن النشاط المادي في الجريمة الإلكترونية يتطلب توفر بيئة ذات هيئة رقمية، وجهاز حاسوب آلي، وتوفر اتصال بشبكة الإنترنت، ويتطلب أيضاً معرفة متى يتم البدء بهذا النشاط، والشروع فيه وظهور نتيجته[1].

ويتكون الركن المادي من ثلاثة عناصر وهي:

١- السلوك الإجرامي: يمثل السلوك الإجرامي النشاط، أو الفعل الخارجي الذي يقوم به الجاني، حتى يحدث بعد ذلك بسبب هذا النشاط ضرراً، أو خطراً على المقصود من فعل الجريمة وسواء كانت إرادة الجاني أن يريد إحداث نتيجة يريدها، أم تحققت هذه النتيجة، ولكن إرادته لا تنصرف إليها. فالسلوك المادي في الجرائم الإلكترونية إنما يحتاج إلى منطق تقني، حتى يتم إحداث الجريمة الإلكترونية، وبدونه فلن يكون اتصال بالإنترنت، حتى يتم إحداث الجريمة، وسواء اتجهت الإرادة إلى قصد ارتكاب الجريمة، أو إلى تصفح الإنترنت فقط. وكذلك حتى تقوم الجريمة الإلكترونية لابد من توفر حاسوب آلي، واتصال بشبكة الإنترنت، وكذلك يفترض معرفة الجاني بأنه يقوم بهذا النشاط والمعرفة في أنه يستخدم الحاسوب الآلي، «كأن يتولى الجاني أو يرتكب الجريمة بتجهيز الحاسوب لكي يتحقق له حدوث الحاسوب فيقوم بتحميل الحاسب ببرامج اختراق، أو يقوم بإعداد هذه البرامج بنفسه أو يقوم مثلاً بتهيئة صفحات مخلة بالآداب وتحميلها على البرنامج المضيف»[2].

٢- النتيجة الإجرامية: هي الحلقة الوسطى من الجريمة، وهي من خلالها يتحقق مراد الجاني في إحداث الفعل الذي يريده، ومن خلاله يتم وقوع الجريمة بشكل نهائي، فالنتيجة

(١) إبراهيم، خالد ممدوح: الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، طبعة أولى، (٢٠٠٩)، ص ٩٨.

(٢) الحوامدة لورانس سعيد الجرائم المعلوماتية أركانها وآلية مكافحتها دراسة تحليلية مقارنة مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية، العدد ١، ٢٠١٧)، ص ١٩٧-١٩٨)

هـي إحـداث ذلك الأثـر الغير مشروع، ومـن خلاله يصبح المجـرم قد أحدث الفعـل الذي يمثل اعتـداء علـى حق يحميه القانون. والجريمـة الإلكترونية كغيرها من الجرائـم التي لابد من وجود نتيجـة إجراميـة بها، ولكنها تختلـف بالتأكيد النتيجة مـن جريمة إلى أخـرى. فعندما تتكلم عن جريمـة تزويـر للبيانات، وهي تابعة للجرائـم الإلكترونية، فنرى أن النتيجـة الإجرامية بها تكمن فـي تحريف الحقيقة، وتزويرها في البيانات، والمعلومـات التي توجد في الحاسوب، أو إنها توجد فـي الموقع الإلكترونـي، فالنتيجة هنا عن الأثر المـادي المترتب على القيام بالفعـل، أو النشاط المـادي غيـر المشروع، وهي كذلـك تنتج أثر قانوني عـن تزوير بيانات، ومعلومـات الأفراد فهذا تعـدي على خصوصيات الأفراد، وعلى معلوماتهم الخاصـة بهم سواء القيام بتعديلها، أو حذفها، أو تحريفهـا، بمـا يعتبر تعدي صريح ومخالف في القانون، وكذلك في جريمة القتل، والتي تتم عن طريق استخدام النظام المعلوماتي، وأجهزة الحاسوب، والإنترنت، فهنا النتيجة الإجرامية تكمن فـي إزهـاق روح المجني عليـه، مثلها هو عند قيام طبيـب يعمل بالمستشفى بالدخـول إلى قاعدة البيانـات، بسبـب دواء معين حتى يقوم بالتلاعـب في هذا الدواء؛ ويقوم بتغييـره، أو يقوم بتغيير الكميـة المطلوبـة منه، وبسبـب هذا التغيير يقتـل المريض، و الذي تم بسبـب دخوله على قاعدة البيانات الخاصة بالمستشفى[1].

٣- العلاقة بين السلوك، والنتيجة الإجرامية (السببية): لا قيام للجريمة إلا إذا كانت هناك علاقـة بين السلـوك الإجرامي الذي قـام به المجـرم؛ والنتيجة الإجرامية التـي تمت عن طريق السلـوك، أي (النشاط الإجرامي للمجرم) فـإذا انتفت هذه السببية بين العنصرين: (السلوك – النتيجـة) فلا مجال لمساءلة المجرم بسبب انتفاء السبب؛ الذي من خلاله حدثت هذه الجريمة، وتحققـت نتيجتهـا، والسبب الإجرامي هـو الدافع الغير مشـروع، الذي من خلالـه يقوم المجرم بالسلوك، والطرد نحو تحقيق النتيجة الإجرامية.

**ثانياً: الركن المعنوي:**

كما تم ذكره سابقاً فإن الركن المعنوي يتعلق بالحالة النفسية والمزاجية للقائم بالفعل الذي يُعد جريمة، أي أنه يتوافق مع الركن المعنوي للجريمة التقليدية، والذي يتمثل في العلم، والإرادة، حيـث لا بُد أن يكون الشخص مدركًا للفعل الذي يقوم بـه، ويعلم الآثار المترتبة عليه، ويكون لديه إرادة بفعل هذا، وليس عن طريق الخطأ، كأن يستخدم برنامجًا لا يعرف مصدره، ويكون البرنامج من برامج الاختراق، وهو لا يعلم، فبذلك لا يتوافر الركن المعنوي في الجريمة الإلكترونية. وتوافر الركن المعنوي ليس بديلاً عن الركن المادي، الذي يعد الركن الأساسي في الجريمة الإلكترونية، بـل لا بد من توافر الركنين معًا، حتى تكتمل الجريمة؛ ويتـم الحكم عليها؛ بأنها جريمة إلكترونية

(١) أحمد، أحمد محمد عبد المعبود أبو أسيد: الجريمة الإلكترونية وآلية مكافحتها في ظل القانون الدولي، (مجلة البحوث القانونية والاقتصادية، جامعة المنوفية كلية الحقوق، دولة مصر، عدد ٥٠، ٢٠١٩م)، ص ٢٠.

مكتملة الأركان، وبناء على ذلك يتم تطبيق العقوبة عليها، وفقاً لما حدده القانون.

ومما سبق يُمكن استنتاج خصائص المجرم الإلكتروني المتعلقة بالركن المعنوي، وهي:

- أن يكون الشخص عاقلًا، ومدركًا لطبيعة الفعل، وللنتائج المترتبة عليه.
- أن يكون الشخص على علم بمخاطر ما يقوم به من أعمال، وأنها تُعد جريمة.
- أن يكون الشخص لديه الإرادة للقيام بالعمل، وليس مجبرًا عليها.

ورغم أن تلك الخصائص تعني ضرورة توافر العلم والإرادة لدى الشخص القائم بالفعل الإجرامي، إلا أنها لا يُقصد بها أن تكون مبررًا للدفاع عن الشخص، ومحاولة إثبات أنه لم يكن لديه العلم والإرادة؛ وبذلك يكون الهدف التلاعب بالقوانين، واستغلال الثغرات؛ وإنما الهدف أن يكون الشخص مدركًا لما يفعل وقاصدًا الإضرار بالآخرين، لتوافر الركن المعنوي في الجريمة الإلكترونية. كذلك أن النظام السعودي لم يقتصر على القصد الجنائي العام، والتي تتفرع إلى العلم، والإرادة، بل ألزم بأن تتوافر النية لدى الجاني، ألا وهي: القصد الجنائي الخاص لدى الجاني عند دخوله الغير مشروع، و الذي يكون الغرض منه هو التهديد، أو الابتزاز، أو لغرض آخر، وهو الحصول على بيانات تتعلق بأمن الدولة سواء كان في داخلها، أو خارجها، أو لها علاقة بالاقتصاد الوطني، أو تكون نية الجاني بأن يعبث بالبيانات التي يحتويها النظام أو يعبث بالنظام بنفسه، أو أن يقوم الجاني بإتلاف الموقع الإلكتروني، والقيام بتغيير التصاميم الخاصة بالموقع نفسه؛ أو بتعديل الموقع الإلكتروني[1].

القصد الجنائي: يُقصد به تمثيل الجاني للقيام بفعل يعاقب القانون عليه، فيجب ليتوافر القصد الجنائي هو أن يكون الجاني يعلم أن الفعل الذي يريد ارتكابه يدخل من ضمن الأفعال التي يعاقب عليها القانون وتردعه. والقصد الجنائي العام يتمثل بعنصرين: وهما الإرادة والعلم.

أ- الإرادة: هي الدوافع الداخلية الإجرامية للفرد للقيام بعملية إجرامية، والتي تنتقل من إرادة معنوية نفسية إلى فعل على أرض الواقع. وإن الجرائم الإلكترونية كغيرها من الجرائم، التي يدخل فيها توافر الإرادة، فمثلاً: عند قيام الشخص بإرادته القيام بفعل التزوير، المستندات، أو معلومات متواجدة في الحاسب الآلي، أو سرقة معلومات، أو محتويات متواجدة في البريد الإلكتروني، والحصول عليها، فهنا ينطبق العنصر الأول من القصد الجنائي العام، وهو (الإرادة) لفعل الجريمة الإلكترونية.

ب- العلم هو أن يحيط الشخص بحقيقة الوضع الإجرامي الذي يريد القيام به، وما هو في القانون، وذلك أن يدرك الشخص بحقيقة هذا الفعل، وإلى أي منحنى يتجه به والعلم في الجريمة الإلكترونية، هو يوجب على الشخص أن يعلم بأن تزوير المستندات،

(١) الأحمد، وسيم حسام الدين: مكافحة الجريمة المنظمة عبر الوطنية في ضوء أحكام الشريعة الإسلامية والأنظمة السعودية (مكتبة القانون والاقتصاد الرياض، طبعة أولى، ٢٠١٦م) ص ٥٢٤.

والمعلومـات، أو سرقة هـذه المحتويات، والمعلومـات، من البريـد الإلكتروني، معاقب عليهـا في القانون، وتدخـل من ضمن الأفعـال الإجرامية الإلكترونيـة، وهنا يتم وجود وتطبيق العنصر الثاني من القصد الجنائي العام، وهو (العلم) بالجريمة الإلكترونية.

وخلاصـة القـول يُعد الركن المعنوي ركنًـا غير ملموس، وهو يتطلب خبـرة ومعرفة من قِبل المحققيـن، حيث يتم التأكد من وعي الشخص القائـم بالفعل الإجرامي، وربط دوافعه بالجريمة التي تمت من خلال العلاقة بينها، وبين ماديات الجريمة ومدى الاستفادة الواقعة عليه، بالإضافة للتأكـد من سلامتـه العقلية أيضًا؛ فإن تـم التأكد من سلامته العقلية ووجـدت علاقة بينه، وبين ماديات الجريمة، وكان هناك دوافع تتعلق بهذا الفعل الإجرامي، وبين الفاعل فإن الركن المعنوي يكون قد تحقق بجميع تفاصيله.

**ثالثاً: خصائص الجريمة الإلكترونية:**

انتشـرت العمليـة الإجرامية الإلكترونية انتشـاراً غير مسبوق؛ فالجريمـة الإلكترونية تتمتع بخصائـص ذي قـوة يسهل تنفيذها فـي أي دولة، بالرغم مـن أن الجهة التي فعلـت العملية غير متواجـدة في الدولة التي تـم التنفيذ بها. وبذلك أصبحت الجريمـة الإلكترونية شكلاً جديداً من الجرائـم العابرة للحدود الإقليمية؛ ما جعلها تتخذ طابعاً يميزها من غيرها من الجرائم[1]. فهي تملـك خصائـص منفردة بها، وليسـت كخصائص الجرائم التقليدية سـواء كان في تنفيذها، أو بأسلوبها. ويتضح لنا أن خصائص الجريمة الإلكترونية عديدة وهي:

١- استعمـال الحاسب الآلي، أو الأجهـزة المتنقلة كأدوات لارتكاب الجرائم الإلكترونية عن طريقها:

إن الجرائـم الإلكترونيـة يتم تنفيذها دائماً تقنياً عن طريـق أداة الحاسب الآلي أو الأجهزة المتنقلـة فهـي خاصية منفـردة بها. ويتخـذ المجرم هـذه الأدوات كبوابة يتم مـن خلالها البدء بالجريمـة، وهـو الحاسـوب، والأجهزة المتنقلـة فهي عن طريقهـا تمكنه من الدخـول إلى شبكة الإنترنت، وهي الأدوات الوحيدة التي تمكنه من الدخول لعالم الإجرام الإلكتروني[2].

وفـي أي مرحلـة من المراحل التي يتم فيها معالجة البيانات يمكن حدوث الجريمة فلا كلمة غير واضحة اللجوء إلى الأنظمة الأمنية التي تقف سداً عند هذه الأفعال الإجرامية[3].

٢- صعوبة إثبات الجريمة الإلكترونية:

---

(١) المقصودي، محمد بن أحمد علي الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً، المجلة العربية للدراسات الأمنية، الرياض، العدد ٧٠، ٢٠١٧ م)، ١١٣.

(٢) منير، محمد الجنبيهى ممدوح محمد الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م)، ص ١٤.

(٣) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ٨٥.

عندمـا نتحدث عـن إثبات الجريمة الإلكترونيـة، فنحن نتحدث عن أصعـب الجرائم إثباتاً فهي تتسم بالصعوبة البالغ من أمرها، حيث أن الجريمة الإلكترونية عندما تقع يمكنك العثور على الأفعال التي ساهمت في إحداث الجريمة؛ لكن لا يمكنك العثور على فاعل الأفعال الغير شرعية إلا بصعوبـة بالغة، فللأسف في الجريمة الإلكترونية عملية تتبع المجرم المرتكب للأفعال الإجرامية الإلكترونيـة تتسـم بصعوبة قصوى؛ وللأسـف أن المجرم الإلكتروني بإمكانـه أن يمحو الأدلة، أو الإثباتات التي تكون في سبب العثور فهنا تزداد، وتكمن خطورة هذا الأمر.

فالجريمة الإلكترونية تتميز بصفة أنها مخفية، ومعنى هذه الجملة أي أنها (لا تترك وراءها آثـاراً مادية) يمكن تتبعها فهي ذات خطـورة عالية من أمرها، ويصعب اكتشافها، ويصعب كذلك معرفة مـكان التعامل معها، وتحديد مكان وقوعها بسبب الكمية الكبيرة من البيانات، والمتداخلة مع بعضها البعض[1].

٣- إنها جريمة ليست محصورة على منطقة جغرافية معينة:

تتسم الجريمة الإلكترونيـة بعالميتها الإجرامية: حيث يمكن فعلها في دولة، ووقوع الجريمة فـي دولة أخرى، ويتم القبض على المجرم في الأمر عـن طريق التحري، والتنسيق ما بين الدول. فالجريمـة الإلكترونية عابرة للقارات، فلا تعترف بحدود بين الدول، فهي تعتبر صفة جديدة على صفات الجرائم الإلكترونية الأخرى، وعن طريق هذه الصفة يمكن ارتكاب التعدي على بيانات أي شخصـ في أي دولة؛ أو انتحـال صفته، أو سرقة بطاقات الائتمـان، أو تزوير وإتلاف المستندات الإلكترونية، أو ارتكاب الجريمة المنتشرة بشكل كبير، وهي غسيل الأموال، وهذا عن طريق وجود الأمـوال في دولة مـا، ودخولها بطرق مشروعة في دولة أخرى، بالرغم من عدم مشروعية الأصل، وهي الأموال[2].

٤- الجريمة الإلكترونية ذات قوة ناعمة:

إن الجريمـة الإلكترونيـة ليسـت كالجريمـة التقليديـة التـي هي أكثـر عنفاً مـن الجريمة الإلكترونيـة؛ فالجريمة التقليدية تحتـاج إلى عمل مادي، وقوة بدنية حتى تتم الجريمة؛ وهذا على عكـس التقليدية الإلكترونيـة التي تحتاج إلى فكـر عميق، وذكاء، وقوة فكريـة علمية ومعرفية في الحاسـوب، والأجهزة المتنقلة، ومجهود ذهني فالمجرم الإلكتروني يحتاج هذه الصفات حتى يتم عمل الجريمة الإلكترونية الغير مشروعة.

والقصـد من كلمة ناعمة هي أن المجـرم الإلكتروني يقوم بالجريمة دون مجهود مادي؛ فهو عن طريق جهاز الحاسوب الآلي، يمكنه فعل الجريمة بخفية، وهذا على خلاف المجرم التقليدي، الذي لا يمكنه إيقاع العملية الإجرامية دون وجود مجهود بدني، ومادي.

(١) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ٧٩.

(٢) إبراهيم الجرائم المعلوماتية، مرجع سابق، ص ٧٧.

٥- خطورة الجريمة الإلكترونية:

تتسم الجريمة الإلكترونية بالخطورة العالية على جميع الأفراد، والمؤسسات فهي من جهة الأفراد يكمن ضررها في سيطرتها على العقل البشري، والسيطرة على الحياة الشخصية، والعملية لدى الفرد، ويكمن كذلك ضررها على الاقتصاد في وقوع الضرر على المؤسسات بذاتها، وعليه فإن الخطورة تتسع إلى الأمن القومي، والاقتصادي للدولة.

**رابعاً: الطبيعة القانونية للجريمة الإلكترونية:**

تدخل الجريمة الإلكترونية ضمن نطاق فرع القانون الجنائي، و على وجه الخصوص ضمن نطاق قانون العقوبات الخاص بالجرائم الإلكترونية، أو المعلوماتية[١]، فهي ذات خواص مميزة عن الجريمة التقليدية سواء في نوع الجرائم، أو التنفيذ، أو الإثبات، أو حتى في الأنظمة المتعلقة بالجرائم، حيث إن الجرائم الإلكترونية لها نظام خاص بها، و هو (نظام مكافحة جرائم المعلوماتية)، وقام النظام بتعريف البيانات التي إذاً تتم من خلالها الجريمة الإلكترونية وهي: «المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها»[٢]. يترتب على ذلك أن هذه البيانات هي الوسيلة التي إذا تم انتهاكها تحدث الجريمة الإلكترونية، وإن الجريمة الإلكترونية هي جريمة متعددة في وقت واحد، ومعنى هذا هو حدوث أكثر من جريمة في وقت واحد تحت مسمى الجرائم الإلكترونية، والمثال على هذا هو حدوث نقل المعلومات، وسرقتها، وتغيير نظم المعلومات الخاصة بالحاسب الآلي فهنا نرى وقوع ثلاث جرائم إلكترونية في وقت واحد.

وبناء على نظام مكافحة جرائم المعلوماتية السعودي، نرى أنه وضع الهدف الأساسي له، هو الحد من الجريمة الإلكترونية، وذلك حتى يتم الأمن والسلامة للجميع من الجرائم الإلكترونية، وذلك بناءً على نص المادة الثانية وهي[٣]:

- «المساعدة على تحقيق الأمن المعلوماتي.
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
- حماية المصلحة العامة، والأخلاق، والآداب العامة.
- حماية الاقتصاد الوطني».

ولا بد من الإشارة إلى أن القواعد القانونية الإجرامية الإلكترونية تتميز عن نظيرتها القواعد

(١) المقصودي، الجرائم المعلوماتية، مرجع سابق، ص ١١٠-١١١.

(٢) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م / ١٧ بتاريخ ١٤٢٨هـ، المادة الأولى، فقرة ٤.

(٣) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/ ١٧ بتاريخ ١٤٢٨هـ، المادة الثانية.

التقليديــة؛ فلا يمكن تطبيق القواعد، أو النصوص القانونيــة للجريمة التقليدية على الإلكترونية، وهــي بالأصل ليست مخصصــة حتى يتم تطبيقها علــى الجريمة الإلكترونيــة، وبالإضافة إلى أن النصوصــ القانونية للجريمة التقليدية تم وضعها بحسب معايير معينة سابقة، وحيث إن الجريمة الإلكترونيــة لها طابع خاص بهــا سواء من حيث كيفية وقوعها، أو إثباتهــا، أو الوصول إلى الفاعل للفعــل الغير مشروع. ويترتــب على تطبيق النصوص التقليدية على الجريمــة الإلكترونية كثيرٌ من المشــكلات، ومنهــا أن الجاني في الجرائــم الإلكترونية يمكنه محو جميع الآثــار نتيجة فعله الغير مشــروع، وكذلك محو جميع الأدلة التي يمكن الاستفادة منهــا في الوصول إليه فتطبيق النصوص التقليدية في هذا الموضع يمثل مشكلة كبرى، وهذا يعبر عما تم القول به سابقاً وهو عدم إمكانية تطبيق النصوص التقليدية على الجرائم الإلكترونية[1].

ونستخلصــ من هذا، وكما تــم القول سابقاً أن الجريمة الإلكترونيــة لها طابع قانوني تتميز به، وخاص بها.

### المبحث الأول

### أهمية إثبات الجريمة وأشخاص الجريمة الإلكترونية

إن الإثبــات بشكل عام يمثل نتيجة كل جريمة، فهو الفاصل في القضايا سواء كانت الجنائية أم المدنيــة وهــي الأدلة التي من خلالها يتم الوصول إلى الحقيقة فهي تحمي صاحب الحق عندما تتواجــد لديه الأدلة، ويتــم إثباتها عن طريقها، وفــي واقعنا الحالي التكنولوجــي أصبحت معرفة أهميــة الإثبات الإلكتروني تنال أهمية كبيرة، حيــث أن في الواقع الحالي أصبحت أغلبية الجرائم تُفعــل عــن طريق أجهــزة الحاسوب، والأجهــزة المتنقلة، فلابد مــن معرفة مدى أهميــة الإثبات الإلكترونــي في إثبات الجرائــم الإلكترونية. وبالإضافة إلى معرفــة أشخاص الجريمة الإلكترونية فهــي مثل الجرائم الأخرى لديها طرفــان ألا، وهما: «المجرم الإلكتروني - المجني عليه» وبالطبع أشخاصــ الجريمة الإلكترونية ليس مثل بقية أشخاص الجرائم الأخرى فهم مغايرون عنها، ولهم صفات وملامح، وفئات، وأدوات تخالف البقية.

وسيتــم بمشيئــة الله فــي هــذا المبحث توضيــح أهميــة الإثبات بصفــة عامــة، والجنائي، والإلكتروني، وكذلك شــرح أشخاص الجريمة الإلكترونية بشكل مفصل، وتوضيح الفئات الخاصة بهم.

(١) المقصودي، الجرائم المعلوماتية، مرجع سابق، ص ١١.

**المطلب الأول: أهمية الإثبات بصفة عامة وإثبات الجريمة الإلكترونية**

إن الإثبات من الوسائل الرئيسية، والثابتة حتى يتم الكشف عن تفاصيل الجريمة، وأطرافها فلا بد من ذكر أهميتها، وهذا ما سوف نتحدث عنه بمشيئة الله

## أولاً: أهمية الإثبات بصفة عامة

إن الإثبـات بصفة عامة هو الطريق، أو الوسيلة التي تقود القاضي نحو الحقيقة فإن الإثبات هو المعنى الحقيقي للعدالة فعن طريقه يتم وضع الحقوق، والعقوبات في موضعها الأصلي فعندما يتعرض الشخص للظلم، أو انتهاك الحقوق أو تعرضه لإحدى الجرائم التقليدية، أو الإلكترونية فيجب عليه اللجوء للقضاء، و تقديم الأدلة التي يملكها للقاضي، وحينها يرى القاضي كفاءة الأدلة، وهل هي تؤخذ بها كدليل، أم أنها ليست كافية أن تكون دليل لإثبات التهمة، فالقاضي يتم تقييده بالأقوال والأدلة المقدمة لديه، فلا يكون له الحق في أن يحكم بهواه، أو بعاطفته فيجب عليه التفكير بمنطقية، وأن يتحرى بدقة في الحكم الذي سوف يصدره. ويسعني القول إن الإثبات هو خاتمة القضايا في جميع فروع القانون، وهو الشيء الذي من خلاله يمكن للشخص أن يدافع به عن حقوقه التي سرقت منه. ومن خلال الإثبات يتم الحكم في القضية عن طريق القاضي، بعد معاينة أقوال، وأدلة أطراف القضية ثم إذا رأى من حكم ضده أن القاضي لم يحكم بالحق يمكنه إحالة الحكم من محكمة الدرجة الأولى، وهي من صدرت الحكم إلى الاستئناف، ثم بعد ذلك إلى المحكمة العليا؛ حتى ينال كل امرئ حقه الحقيقي على أكمل وجه. وكذلك إن الإثبات لا يرد على الحق ذاته، فالحق لا يمكن أن يكون محلاً للإثبات فهو الطريق الذي يقوده صاحب الحق للإثبات. فمحل الإثبات هو أساس مصدر الحق للإثبات، ومصدر الحق لا يخرج من وسيلتين، وهي أن يكون تصرفاً قانونياً أو واقعة قانونية[1].

### ثانياً: أهمية الإثبات الجنائي

إن الإثبات الجنائي من خلاله يتم «التوصل بإجراءات الخصومة الجنائية للكشف عن الحقيقة التي يبني عليها الحكم»[2].

إن ما ينال أهميةً في هذا المشروع هو الإثبات الجنائي الذي يبلغ أهمية كبيرة عن مسائل الإثبات في القانون المدني، وأولها: هو أهمية بحث القاضي عن الحقيقة المطلقة التي تعتمد على الجزم، واليقين التام في إصدار الحكم على المتهم، حيث أن في الإثبات المدني القاضي إذا لم يتوصل إلى الحقيقة المطلقة، يقوم على الموازنة، والتحكيم العقلي الذي يراه صحيحاً، ويتم

(١) سويلم، محمد أحمد: الوجيز في قواعد الإثبات على ضوء نظام المرافعات الشرعية السعودي، دار النشر الدولي، الرياض، الطبعة الأولى ، ١٤٣٨ هـ)، ص ١٨.

(٢) امسيويط، انتصار احميدة محمد التحول في نظام الإثبات الجنائي، مركز الدراسات العربية، مصر، طبعة أولى، ١٤٣٨هـ)، ص ١٢.

عـن طريقه الحكـم، ولكن هذا الأسلوب بالتأكيد التام أنه ليس متواجد في الإثبات الجنائي، فعلى القاضـي أن يبحـث بالحقيقة بنفسه، ويقوم بالتحري على أكمل وجه، ويعاين الأدلة معاينة دقيقة، و يقوم بالبحث عن الركن المادي والمعنوي للمجرم الذي فعل الجريمة لما يتسبب؛ هذان الركنان فـي تغيير مرتكب الجريمـة الحقيقي، ومصدر الجريمة نفسه بعد ذلك يتـم الحكم، وفي القانون الجنائـي هناك عدة مبـادئ قانونية يتم الاعتماد عليهـا، و منها «المتهم برئ حتـى تثبت إدانته» ففي الإثبات الجنائي لأطراف القضية أن يقدموا ما لديهم من أدلة، وأقوال، وشهود، ومن خلالها يتـم الإثبـات الجنائي عن طريـق القاضي، وإصدار الحكـم فالإثبات: هو الهـرم الرئيسي للحكم الجنائـي. فالمراد هو أن على القاضي الذي يملك إصدار الحكم في القضية الجنائية أن لا يحكم في القضية، أو أن يفصل في الدعوى، إلا بدليل إثبات واضح وقاطع يبرر به إما الإدانة، أو البراءة، فهـذه هي وظيفة القاضي، وعندما يقوم بهـذا الأمر عليه أن يوازن في الأدلة المقدمة له بين التي هـي ضد؛ أو مع المتهم، وبيـن واجب هو مناط بفعله، وواجب آخر، وهـو إرضاء الجانب الإنساني للطبيعة البشرية، فهذا ما يجب عليه فعله قبل أن يقوم بالحكم في القضية المرادة[1].

### ثالثاً: أهمية إثبات الجريمة الإلكترونية

تعـد الجرائم الإلكترونية من أبرز معالم العصر الحديـث، حيث أن مسألة الإثبات الجنائي في هذا النوع من الجرائم تثير صعوبة بالغة أمام جهات التحقيق، وأجهزة العدالة الجنائية، وذلك بسبب أن محل الجريمة ذات طبيعة معنوية، ومتعلقة بالمعالجة الآلية التي تخص البيانات، وليست ذات طبيعـة مادية[2]. فلذلك لابد من أهمية إثبـات الجريمة الإلكترونية في الأفعال حتى تتماشى معهـا خطـوة تلي الخطوة؛ والقيام بتحليلها من المختصين حتى يتـم الوصول إلى الجاني مرتكب الجريمـة الإلكترونية، فلهذا أهمية إثبات الجريمة مهمـة للغاية وكذلك أنها بالطبع أن تختلف في عملية إثباتها عن الجرائم التقليدية من حيث الأدلة، والمعاينة، ولذلك في الواقع الحالي حان الآن لتطويـر الأنظمة التي تختص بالجريمة الإلكترونية، حيـث أن مع تقدم الأجهزة تقنياً الحاسوبية، والمتنقلـة فـلا بد من وضع حد لقفل الثغرات، التي من خلالها يقـوم المجرم الإلكتروني بعملياته الإجرامية؛ والتي كانت موجودة في الأنظمة السابقة، حتى يتم مواكبة التطور التقني الذي نعيشه.

وإن الجرائم المادية يمكن إثباتها بسبب الآثار الملحوظة التي تتركها وراءها، فهو أمر مسهل، وميسـر حيث يمكن السعي وراءها، حتى الوصول للجاني، وذلك على عكس الجرائم المعنوية التي بالغالب لا يكون وراءها أثر، والآثار هي المعلومات، والبيانات التي يتم تداولها عن طريق الحاسب الآلـي ومـن خلالها تحدث العمليـات الإلكترونية، حيث أنهـا تكون على شكل رمـوز، ونبضات يتم

(١) سويلم، الوجيز في قواعد الإثبات، مرجع سابق، ص ١٩.

(٢) عمري محمد محمود الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية : دراسة مقارنة مجلة العلوم القانونية والسياسية دولة العراق، العدد ٢، ٢٠١٦)، ص ٢٩٥.

تخزينهـا في وسائط لكـن إن الإنسان لا يمكنه أن يقوم بقراءة هـذه البيانات، والمعلومات إلا عن طريـق وسيلـة واحدة، وهي الحواسيب التـي تحفظها[1]. لكن الصعوبة تكمن فـي الركن المعنوي للجرائـم الإلكترونية، بسبب عدم إمكانية معرفة الشخص الحقيقي الذي فعل الجريمة بسبب أنه مخفى ولا يمكن لأحد العثور عليه، لكن بالطبع أنه غير مطلق، ويمكن العثور عليه بتطبيق الوسائل التقنية، التي من خلالها يمكن كشفه.

كذلك إن المسببات التي تجعل من الإثبات الإلكتروني ذا صعوبة خمسة أسباب:[2]

١- أنه بعد حدوث ارتكاب الجريمة الإلكترونية لا يكون هناك أثر لها.

٢- «صعوبة الاحتفاظ الفني بآثارها إن وجدت».

٣- المحقـق الإلكترونـي ليس كالمحقق التقليـدي، فهو يحتاج إلى أن يملـك خبرة ذات بعد فني، وتقني من الصعب أن يتعامل معها المحقق التقليدي.

٤- عند ارتـكاب الجريمة الإلكترونيـة، وحصولها يـجأ منفذ الجريمة الـى تضليله؛ وخداع الجهة التي تحقق في الجريمة حتى لا يتم العثور عليه.

٥- حتـى يتم ارتكاب الجريمـة الإلكترونية، لا بد أن يكون المنفذ فـي قمة الذكاء، والمهارة اللازمة.

**المطلب الثاني: أشـ اص الجريمة الإلكترونية**

لا شـك بإن لكل جريمـة سواء كانت إلكترونيـة، أو تقليدية أشخاص يطلـق عليهم المجرم، أو الجانـي، والمجنـي عليه، وسوف نتحدث بالتفصيل بمشيئة الله فـي هذا المطلب عن أشخاص الجريمة الإلكترونية، والفئات الخاصة بهم وهم (المجرم الإلكتروني - المجني).

**أولاً: الفرق بين المجرم الإلكتروني والمجرم التقليدي:**

إن المجـرم لا يوجـد تعريف مثبت عنه، ولكنـه يتميز عن المجرم التقليـدي، أو العادي من حيث المفهوم، وذلك بالطبع بسبب الفرق الشاسع بين الجريمة الإلكترونية، والتقليدية. فالمجرم الإلكتروني يتميز بعدة خصائص، وسمات شخصية تجعل منه ذو أهمية كبرى في عالم الجرائم[3]

ففي عالم الجريمة الإلكترونية نحن أمام مجرم محترف، ويملك مهارات تقنية على مستوى

(١) سقف الحيط، عادل عزام: جرائم القدح والذم والتحقير المرتكبة عبر الوسائط الإلكترونية شبكة الإنترنت وشبكة الهواتف النقالة: دراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن، مشار إليه عمري الإثبات الجزائي، مرجع سابق، ص ٢٩٥

(٢) الجنبيهي الجنبيهي جرائم الإنترنت، مرجع سابق، ص ١٩.

(٣) ربيعي، حسين المجرم المعلوماتي شخصيته وأصنافه (مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، الجزائر، العدد ٤٠، ٢٠١٥م)، ص ٢٨٧.

عـال، وعلى علـم تقني كبير في نظم الحاسب، وفـي الأجهزة الإلكترونية المتنقلـة[1]. وكذلك إن المجـرم الإلكترونـي يتميز عـن المجرم التقليـدي في التنفيذ؛ ففـي الجريمـة التقليدية نرى أن المجـرم التقليـدي يقوم بالجريمة علـى أرض الواقع، ويمكـن كشفه، والإمساك بـه لكن المجرم الإلكترونـي لا يمكـن كشفه، على الحقيقة إلا بصعوبة بالغة من أمرهـا، وكذلك في عملية الإثبات على المجرم، فهناك فرق شاسع فيما بينهم، حيث أن المجرم الإلكتروني يتم إثبات جرمه بتتبعه التقنـي؛ وآثار دخوله للمواقـع الإلكترونية، لكن للأسف عملية الحصول علـى المجرم الإلكتروني تتسـم بصعوبة، ولا بد من وجـود قدرة ذهنية، وتحليلية، وخبرة تقنية حتـى يتم الإمساك به، أما بالنسبـة للمجرم التقليدي فيتم عن طريـق الأقوال، والشهود والأدلة الواقعيـة والإمساك به، يتم بسهولة في غالب الأمر، وهذا التمييز الجوهري بينه وبين المجرم الإلكتروني.

**ثانياً: شخصية المجرم الإلكتروني:**

لقد عرّف النظام السعودي الشخص المجرم الإلكتروني وهو: «أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة»[2]. ويكمن بداية فعل المجرم الإلكتروني هو في الدخول الغير مشروع ولقـد قام بتعريفـه كذلك نظام جرائـم المعلوماتية السعـودي: «دخول شخصـ بطريقة متعمدة إلـى حاسـب آلي، أو موقـع إلكتروني أو نظام معلوماتي، أو شبكة حاسبـات آلية غير مصرح لذلك الشخص بالدخول إليها»[3].

إن شخصيـة المجرم الإلكتروني شخصية فريدة من نوعها، فهـو ليس كالمجرم التقليدي، بالرغـم مـن أنهم يشتركون في نفس المعنى، ألا وهو الفعل الغيـر مشروع، لكن ليس بينهم علاقة تشابه بشكل شبه كامل.

وبالطبـع إن المجرم الإلكتروني بسبب أفعالـه الغير مشروعة التي يؤديها تجعل منه شخص يمتلك صفات يتميز بها عن البقية؛ حيث أن المجرم الإلكتروني بسبب خبرته الكبيرة، والمختلفة عن الآخرين، ولذلك إن الخبرة الواسعة التي يتميز بها المجرم الإلكتروني في المسائل المعلوماتية، والتي عن طريقها يمكنه تحريف معلومات أو بيانات، أو سرقتها، أو إتلاف أنظمة معلوماتية فهذي تجعـل من المجرم الإلكتروني شخص مخيف وفـي ذات الوقت شخص لا يمكن السيطرة عليه، أو مراقبته في جميع الأوقات، فهو شخص متخفي، وليس ظاهر مثل المجرم التقليدي.

كذلـك إن طبيعة العنف الـذي يفعله المجرم الإلكتروني في مجـال الحاسب الآلي، لا يمكن تصـور مـداه حيـث أن العنـف حدوثه على هيـكل الحاسـوب الآلي، وليـس بالمعلومـات الخاصة بالحاسـوب والمثال على ذلك هو القيام بإتلاف وحدة المعالجة المركزية، فهنا يكون الإتلاف قد

(١) المقصودي، الجرائم المعلوماتية، مرجع سابق، ص ١٠٧.

(٢) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م / ١٧ بتاريخ ١٤٢٨ ، المادة الأولى، فقرة ١.

(٣) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م / ١٧ بتاريخ ١٤٢٨ ، المادة الأولى.

وقع على هيكل الحاسوب الآلي، وهنا تكمن محل الجريمة، وليس في المعلومات[1].

**ثالثاً: فئات المجرمين الإلكترونيين**

ينقسم المجرمون الإلكترونيون إلى فئتين وهما:

الفئة الأولى من المجرمين الإلكترونيين (الهاكرز): إن المجرمين الذين ينتمون لفئة الهاكرز يصنفون أنهم ضمن الأقل خبرة، وخطورة في الإجرام الإلكتروني فهم لديهم خبرة بالإمكان تسميتها بالمعتبرة مثل المعرفة بمكونات، ووظائف الحاسب الآلي ونظم المعلومات فهؤلاء يمارسون إجرامهم بغرض الهواية فهم أغلبية حياتهم يعيشونها في هذا المجال الإجرامي حيث أنهم لا يدركون مدى نتيجة الإجرام الذي يمارسونه إلا بعد وقوع الفعل، ومثلما قلنا فهؤلاء الفئة يعتبرون من الأقل خطورة حيث أنهم ممارستهم مجال نظم المعلومات بسبب إشباع فضولهم القوي في هذا المجال لكن مع مرور الأيام لا شك أن هذه الفئة سوف تتعمق بشكل مخيف في مجال الحاسب الآلي، وتنتقل من الفئة الأقل خطورة إلى فئة أكبر خطورة أي تصبح الفئات المحترفة بمجال الحاسب الآلي[2]. لكن يجب العلم في الهاكرز كذلك إنهم يصنفون ضمن الأذكياء فهم أغلبية أعمالهم تتجه إلى القيام بدرء الأخطار، أو أنهم يقومون بإصلاحات، وعمليات تحسين في مجال الحاسب الآلي، لكن هذا الأمر لا يغير من قيام بعضهم من هذه الفئة بعمليات غير شرعية أي إجرامية.

الفئة الثانية من المجرمين الإلكترونيين وهم الكراكر: إن توجه هؤلاء الأشخاص المندرجين تحت هذه الفئة يصنفون بأعلى مراحل مستوى المهارة في مجال الحاسب الآلي ككل فاستعمالهم لمجال الحاسب الآلي من أجل التخريب، والاختراق والابتزاز فهم يقومون بهذه الأفعال لأسباب غير مقنعة، وغير إيجابية.

كذلك إنه بسبب المهارة الكبرى التي يملكونها يسمح لهم بسهولة باقتحام الأنظمة الحاسوبية، وكذلك إنهم يمتلكون القدرة الكافية للاقتحام، والتخريب في مجال الأنظمة الحاسوبية، وبالطبع إن هناك قدرة أمنية للأنظمة الحاسوبية لكن هذا لا يسبب لهم أي صعوبة إلا عندما يكون النظام الأمني عالي، وعلى مستوى رفيع من درجات الحماية فهنا يمكن القول إنهم يواجهون بعض الصعوبة لكن للأسف بغالب الأمر يقومون بتعديتها، وإحداث أفعالهم الغير شرعية، وبغالب الأمر عند إحداث فعل إجرامي مثل القيام بتحويل، أو بتحريف المحتوى، أو بسرقة المعلومات الخاصة بالبرامج فتكون هذه الفئة الإجرامية هي الفاعلة لهذا الفعل الغير شرعي[3].

---

(١) المقصودي الجرائم المعلوماتية، مرجع سابق، ص ١٠٧.

(٢) شوقي، يعيش تمام: الجريمة المعلوماتية دراسة تأصيلية مقارنة سلسلة مطبوعات المخبر، جامعة محمد خيضر بسكرة الجزائر، الطبعة الأولى، ٢٠١٩م)، ص ٢٢-٢٣.

(٣) شوقي، الجريمة المعلوماتية، مرجع سابق، ص ٢٣.

**رابعاً: المجني عليه في الجريمة الإلكترونية:**

إن صاحب فعل الجريمة الإلكترونية إما أن يكون صاحب صفة طبيعية، أو معنوية، ومن المتصور هو أن يكون ضحية الإجرام الإلكتروني شخص ذو صفة طبيعية أم ذو صفة اعتبارية فهي لا تخصص وقوع الجريمة على أحد ما، وهذا يعني أن الجريمة الإلكترونية تقع على أي شخص دون تحديد. لكن يمكن القول إن الإجرام الإلكتروني يقع على الأفراد الاعتباريين بكثرة، ونقصد بالاعتباريين: الشركات والمؤسسات الخاصة بالدولة والمؤسسات ذات الملكية الخاصة فهنا يمكن القول إنها تتعرض بشكل أكبر من الأشخاص الطبيعيين حيث إنها تُستهدف بشكل أكبر بسبب؛ قيمة المحتويات والمعلومات والبيانات التي لديها، والتي بعضها تتصف بسرية مما يجعل المجرم الإلكتروني يستهدفها بشكل أكبر، وكذلك الأموال التي تعتبر الهدف الأول للمجرمين الإلكترونيين حيث إن بعضهم يدخل عالم الإجرام الإلكتروني بسبب الأموال التي يريد الحيازة عليها، ومن خلالها يريد الوصول لمرحلة الثراء الغير مشروع.

وللأسف إذا نظرنا لدور المجني عليه في الجريمة الإلكترونية نرى أن دوره سلبي، وغير واضح بشكل كبير، وهذا بسبب أن المجني عليه عندما يُستهدف من المجرم الإلكتروني يميل إلى التكتم عنها، وأن لا يتحدث سواء عنها، أو عن آثارها خصوصاً عندما تحدث الجريمة في الحصول على بياناته، أو معلوماته السرية التي تملك أهمية عالية، أو عندما تتعلق بسرقة أمواله، وهنا عندما ينفذ المجرم الإلكتروني فعله الغير المشروع يفعل المقايضة الغير مشروعة حيث مقابل هذه المعلومات، والبيانات لصاحبها الشرعي يتم إعطاء المجرم أموال لا يستحقها، أو يتم تنفيذ طلبات يريدها، وللأسف يجبر المجني عليه في بعض الأحيان بسبب أهمية هذه المعلومات، والبيانات وخوفه من تسريبها، وانتشارها[1]، وبعض الأوقات تكون هذه البيانات، أو المعلومات تختص بحياته الشخصية مثل اختراق الحاسوب الآلي الخاص به، أو الأجهزة المتنقلة، والحصول على صور أو فيديوهات شخصية فلا يمكنه اللجوء إلى فعل آخر بينه، وبين المجرم الإلكتروني حيث يتم ابتزاز المجني عليه ببيع معلوماته، أو بياناته لغير أصحابها إذا لم يسلم الأموال المطلوبة من طرف المجرم، أو لم يتم تنفيذ طلباته الأخرى. كذلك هناك مشكلة كبرى في الإثبات، وهي أن المجني عليه يلاقي صعوبة كبرى في الإثبات المادي للجريمة الإلكترونية بسبب خوفه من المساءلة القانونية، وخوفه بسبب إلقاء المسؤولية عليه كمجني عليه، وهذا بسبب أنه يمكن أن يكون هو المسؤول عن المعلومات، أو البيانات، أو هو من له سلطة على هذه المعلومات، والبيانات فعندما يتم اختراقها يتم إلقاء اللوم عليه، وهذا يجعل منه الطرف الأضعف في هذه الجريمة الإلكترونية فهذه السلطة التي يمكن أن يكون مالكها المجني عليه في وقت الاختراق تجعل منه هو من يمتلك إصدار القرارات والإجراءات اللازمة في وقت حدوث الجريمة الإلكترونية حتى يتم

(١) المقصودي، الجرائم المعلوماتية، مرجع سابق، ص ١١٠.

تلاشي، أو تخفيف الأضرار الناتجة عن هذا الفعل الغير مشروع[1].

**خامساً: فئات المجني عليه:**

إن مع تطور الوسائل الإلكترونية تعددت فئات المجني عليه، والخطر امتد من الأشخاص الطبيعيين إلى الأشخاص الاعتباريين. وتقسم فئات المجني عليه إلى:[2]

- الأشخاص ذو الصفة الطبيعية.
- الأجهزة العسكرية: وهي المواقع الإلكترونية الخاصة بوزارتي الدفاع والداخلية.
- المؤسسات المتخصصة مالياً، والقطاعات الحكومية.

**أولاً: الأشخاص الطبيعيين:**

لا شك أن الجريمة الإلكترونية ليست محصورة في خطرها على الأجهزة العسكرية، والمؤسسات المالية، والقطاعات الحكومية فقط بل تصل إلى الشخص الطبيعي.

ويتم ذلك عن طريق:

- اختراق الأجهزة، والحواسيب الشخصية لدى الشخص الطبيعي، والتمكن من الوصول إلى معلومات سرية، أو خاصة، أو إتلاف البريد الإلكتروني، وذلك عبر نشر فيروسات في البريد، ويترتب عليه الدخول غير الشرعي للجاني فالبريد الإلكتروني هو من أهم وسائل وصول الجاني للأجهزة الخاصة للأفراد، والوصول لمعلوماتهم الشخصية.
- عملية النصب، والسرقة التي تقع على الأشخاص الطبيعيين، وذلك يتم عن طريق شبكات الإنترنت بسبب؛ ربط بعض الأشخاص بحسن نية بطاقات الشخصية عبر مواقع الإنترنت بغرض الشراء منها، ويتم النصب عليهم بحجة استمرارية عملية الشراء، ونتيجة لذلك يتم سرقة معلومات حساباته البنكية، وسرقة الأموال المتواجدة بها عن طريق المجرم الإلكتروني.

**ثانياً: الأجهزة العسكرية**

انتقلت الحرب العسكرية، والتجسس من الوجود المادي للإفراد إلى الحرب الإلكترونية، والتجسس الإلكتروني ما بين الدول، وهذا نتيجة للتقدم الإلكتروني الذي حدث فالتقدم الإلكتروني لم يقتصر فقط على المنشآت ذات الصفة المدنية، أو التجارية بل امتد للقطاعات العسكرية، وأصبحت الدول تهتم بها بشكل رئيسي، وأساسي، وقوي جداً، وترتب على ذلك أن الدول أصبحت تزود الأجهزة العسكرية بأقوى درجات التشفير، وأعلاها حماية لمواقعها الإلكترونية، وذلك تفادياً لاختراقها فهي حاجز الحماية للمعلومات السرية، والأمنية للدولة، ويؤدي اختراق حاجز

(١) المقصودي، الجرائم المعلوماتية، مرجع سابق، ص ١١٠.

(٢) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ١٥٠-١٥١-١٥٣.

الحماية الإلكترونية للدولة إيقاعها بكثير من المشاكل منها؛ معرفة الدول المعادية لها المعلومات الأمنيــة للدولة، والسرية بالإضافة إلى الكشف عن المواقع الأمنية الحساسة التي بداخلها، فكلما ازدادت صلابــة التشفير كلما ارتفع سقف الحماية لدى مواقــع الأجهزة العسكرية، ودرجة الأمان لها، وصعب اختراقها.

**ثالثاً: المؤسسات المتخصصة مالياً، والقطاعات الحكومية:**

تعتبــر جرائــم الاختراق من أشــد الجرائم وقوعــاً، وأكثرها ضــرراً بالخصوص عندما تقع هــذه الجريمة على المؤسسات التابعة للحكومة مثل الوزارات، وكذلك عندما تقع على مواقع تقدم الخدمات الإلكترونية للمجتمع، أو عندما تقع على مؤسسات اعتبارية، وخاصة مثل البنوك، وغيرها مــن المؤسســات الخاصة. وتعــد المؤسسات المالية، والتــي تمتثل بالشــركات، والبنوك التجارية مــن أكثــر الجهات التي يتــم استهدافها بكثرة عن طريــق المجرمين الإلكترونييــن، وهذا نتيجة؛ لكميــة الأمــوال المتواجدة بها فهــي بيئة جاذبة لمرتكبــي الجرائم الإلكترونيــة فأكثر المجرمين الإلكترونييــن يكون هدفهم هــو: الاستيلاء على الأموال المتواجدة فــي المؤسسات المالية، وذلك عن طريق السرقة، أو النصب، أو الاحتيال[1].

والخلاصــة أن جميــع الدول لم يسلــم أي منها من جريمة الاختراق الواقــع على المؤسسات التابعة لها كحكومة، أو التابعة لأفراد اعتباريين فهذه الجريمة من أكثر الجرائم وقوعاً عليها.

**المبحث الثاني**

**ماهية الدليل الإلكتروني وطرق الحصول عليه ووسائل إثبات الجريمة الإلكترونية**

إن الجريمة الإلكترونية كالجريمة التقليدية تحتاج إلى أدلة يتم عن طريقها ثبوت الجريمة، ولكــن بالطبع ليس بأدلة مادية بل أدلة إلكترونية، وذلك بسبب؛ الطبيعة التي نشأت منها الجريمة الإلكترونيــة، وعليه فإنه حتى يتــم إثبات الجريمة الإلكترونية لابد مــن أن تكون مستندة إلى دليل إلكترونــي، وهذا بسبب أن الدليــل الإلكتروني يتم بواسطته؛ إثبات الجريمة الإلكترونية. بالإضافة إلــى أن هناك طرقاً خاصة يتم عن طريقها الحصــول على الدليل الإلكتروني، وبعضها يتشابه مع الجريمة التقليدية، وبعضها يختلف، وكذلك إن هناك بالطبع طرقاً تنفرد بها الجريمة الإلكترونية لإثباتها. لذلك سوف نتحدث بإذن الله في هذا المبحث عن مفهوم الدليل الإلكتروني، وخصائصه، وماهــي الطرق الخاصة بالحصول علــى الدليل الإلكتروني، وعن الطرق التــي يتم الاستناد عليها لإثبات الجريمة الإلكترونية.

**المطلب الأول: مفهوم الدليل الإلكتروني وخصائصه**

إن الدليــل الإلكتروني مثل ما ذكرنا مسبقاً دليل يختلــف بطبيعته عن الدليل التقليدي سواء

(١) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ١٥٠.

مـن حيث المفهـوم، أو الخصائصـ لذلك سـوف نوضح في المبحـث المفهوم الخاصـ بالدليل الإلكتروني، والخصائص التي ينفرد بها.

**أولاً: مفهوم الدليل الإلكتروني:**

أي «معلومـات سـواء كانت من صنع الإنسان أو تـم استخلاصها من الحاسوب وبشكل يمكن قراءتـه أو تفسيره من أشخاص لديهم مهـارات في إعادة تشكيل المعلومات، بمساعدة من برامج الكمبيوتر»[1].

ونستنتـج من هذا التعريـف أن الأدلة الإلكترونية هي عبارة عن معلومات، أو محتويات تعتبر وسائـل رئيسية، ومن خلالها يتم إثبـات الجريمة الإلكترونية. وكذلك أن الدليل الإلكتروني مقسم إلـى مجموعتيـن وبناء عليه يتم الحصول على الأدلة الإلكترونية حيث من خلالها يتم الوصول إلى المجرم الإلكتروني، وهي[2]:

١- السجلات التي تم حفظها في الحاسب الآلي، والأجهزة المتنقلة، وهي:

• رسائـل البريد الإلكتروني فهذه الرسائـل بمثابة وثائق بالإضافة أنه يمكن من خلالها العثـور علـى المجرم الإلكترونـي، وكذلك الحسابـات السحابية مثل (iCloud) فهـذه الحسابات يتـم عـن طريقها تخزين جميع الصور، والملفـات المتواجدة في الهاتـف، ويترتب على ذلك أنها تعتبر وثائق يمكن الاستناد عليها كأدلة إلكترونية.

• جميع المحادثات التي تمت عبر الإنترنت، وبرامج التواصل الاجتماعي فهذه المحادثات تضل محفوظة في جهاز الحاسب الآلي، والأجهزة المتنقلة.

• الملفـات الخاصـة بالبرامج التي تتواجـد في الكمبيوتر، ومنها ملفـات برنامج معالج النصوص (word).

٢- سجلات تكونت عن طريق الحاسب الآلي:

• الملفـات المخزنـة للبرامج المحملة على الحاسوب الآلي، والتي تربط ما بين النظام، والبرامج التي تم تحميلها.

• ملفـات السجـل الخاص بالأحداث، وهـو (LOG)، وهذا الملف عـن طريقه يتم عرض جميـع العمليـات التي حدثت سواء كانت بالنظام، أو بالبرنامج الـذي تم تحميله فهو أشبه بالتتبع بسبب عرضه للتاريخ، والوقت الخاص بالحدث.

**ثانياً: خصائص الدليل الإلكتروني:**

لمـا كان مـن شأن الأدلة الإلكترونيـة إثبات صحة الجريمة الالكترونيـة من عدمها، وكذلك

(١) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ١٧٨.

(٢) إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص ١٧٨.

تثبيت التهمة على فاعلها من براءته فلا بد من وجود خصائص عدة تتميز بها الأدلة الالكترونية. وهي:

١- الدليل الإلكتروني من الأدلة العلمية:

إن الدليل الإلكتروني من الأدلة التي يتم استخراجها من بيئة افتراضية تقنية فهو يحتاج إليها بسبب الطبيعة التي يتكون منها، وهي تقنية المعلومات، وكذلك إن الدليل الإلكتروني من الأدلة الغير مادية أي أن المعلومات، والبيانات التي يتكون عن طريقها الدليل الإلكتروني هي أدلة الكترونية غير ملموسة، وارتباط الدليل الإلكتروني بالدليل العلمي هو بناء على؛ الأدوات التقنية، وبرامج متخصصة فبلاهما لا يمكن استخراج البيانات، والمعلومات المتواجدة في جهاز الحاسوب، أو الجهاز المتنقل، والتي عن طريقها يتم استخراج الدليل الإلكتروني، وعليه فإن الأدوات التقنية، والبرامج هي: وسائل علمية، وهذا هو الرابط المشترك الرئيسي ما بين الدليل الإلكتروني، والعلمي، وعدم وجود المتخصصين التقنيين، وعدم وجود الوسائل والأساليب العلمية التقنية يعني عدم استخراج المحتويات المتواجدة في الجهاز الإلكتروني[١].

٢- الدليل الإلكتروني من الأدلة التقنية:

يعتبر الدليل الإلكتروني دليل غير ملموس، وغير مادي، وهذا ما يجعله دليلاً تقنياً متميزاً به حيث أن الدليل الإلكتروني لا يمكن قراءته مجرد النظر إليه، وفهمه فهو حتى يتم وضوحه يحتاج إلى؛ مختصين ذو قيمة فنية، وعلمية، والاحتياج العلمي سببه هو؛ الاستناد إلى البيئة التي أتى منها الدليل الإلكتروني، أو التقني فالتقنية الأساس التي تقوم عليه هو الأساس العلمي. كذلك إن الأدلة التقنية هي ليست أدلة مادية يمكن معرفتها مجرد المشاهدة لها مثل السلاح، والمتفجرات وغيرها من الوسائل المادية التقليدية التي توضح المجرم أو تقرب من معرفته، بينما الأدلة التقنية تنتج عن طريق؛ وقوع الجريمة على البريد الإلكتروني وشبكات الإنترنت والحاسوب الآلي والخوادم الخاصة به، والأجهزة المتنقلة، وطريقة وقوعها هي التي تجعلها في مرتبة صعبة للغاية لكشفها، ومثل ما ذكرنا بالسابق حيث أنها تحتاج إلى مختصين ذوي قيمة عالية فنية وتقنية وعلمية، وذلك بسبب السرعة الفائقة التي تحدثها الوسائل الخاصة بالتقنية كذلك شبكات الإنترنت التي ليست لها حدود مكان، وزمان[٢].

٣- الدليل الإلكتروني ذا تنوع وتطور:

يعتبر الدليل الإلكتروني كمصطلح شامل للبيانات الرقمية سواء كانت للشكل الخاص بها، أو أنواعها فهذه البيانات بالإمكان أن يتم تداولها تقنياً، وكذلك إن هذه البيانات تساعد

(١) المعمري، مسعود بن حميد الدليل الإلكتروذ لإثبات الجريمة الإلكترونية مجلة كلية القانون الكويتية العالمية، كلية القانون الكويتية العالمية، ٣، ٢٠١٨م)، ١٩٧ - ١٩٨.

(٢) المعمري، الدليل الإلكتروني، مرجع سابق، ص ١٩٩.

علـى الوصول إلى الجاني، وهـذا بسبب علاقة من نوع معين للبيانـات بالجريمة التي تم وقوعها، وكذلك إن هذه البيانات تكون لها صلة متصلة بالضحية أي المجني عليه، وبناء على ما سبق تكمن خاصية تنوع الدليل الإلكتروني فتنوع الدليل يمكن ظهوره بعدة أشكال مختلفة فهي تظهر على شكل تعرضـ الخـوادم للاختراق والعطل فهنا فـي هذا الشكل لا يمكن للشخص قـراءة هذه الهيئة من الدليـل الإلكتروني، وبينما هنا شكل من أشكال الدليل الإلكتروني التي بالإمكان قراءته عن طريق الأشخاص، وهي التي تظهر على صورة صور تم تخزينها بالحاسب الآلي، أو تم تخزينها في البريد الإلكترونـي، وكذلك إن الدليل الإلكترونـي يعتبر من الأدلة المتطورة بطبيعتهـا، ويتزايد تطورها أكثـر فأكثر فمن حيث الجرائم المستحدثة يتـم استخدامها بها، والمثال على ذلك هو في جريمة النصب حيث سابقاً ارتكابها يتم عن طريق الوسائل التقليدية، والتي بعد ذلك يكون نتيجتها ظهور دليل أو أدلة مادية على ارتكابها بينما في الوقت الحالي مع التقدم التقني المذهل الذي في بعض الأوقـات يكن في صالحنا، وبعضها يكن ضدنا أصبحت ترتكب جريمة النصب عن طريق الوسائل التقنيـة سواء كان عـن طريق الحاسب الآلي، أو الأجهزة المتنقلـة، والخلاصة من ذلك أن مجال الأدلة الإلكترونية يتطور أكثر فأكثر، والجرائم تواكب التطور معه[1].

٤- الدليل الإلكتروني يصعب التخلص منه:

يعتبـر الدليـل الإلكتروني مـن أصعب الأدلـة التي يصعـب التخلص منها، وكذلـك إن هذه الخاصيـة مـن أهـم الخصائص على الإطلاق مـن بين خصائـص الدليل الإلكترونـي، وإن هذه الخاصيـة تعتبـر من المميزات العظيمة التي يتمتع بها الدليـل الإلكتروني. وهذا على عكس الأدلة التقليدية التي يسهل التخلص منها مثل التخلص من حمل الأسلحة، أو حرق الوثائق، والمستندات التـي تشكل فارق في الجريمة، وكذلك إن هذا الأمر ينطبق حتى على بصمات الأصابع التي يسهل إخفاءها، أو مسحها، بينما هذا الأمر ليس متواجد في الدليل الإلكتروني حيث حتى لو قام الجاني بحـذف برامج الحاسـوب الآلي، أو الملفـات المتواجدة بالحاسـوب، أو مسح البيانـات التي قام بتحميلهـا عن طريـق شبكة الإنترنت، أو الغـاء ارتباطه في شبكات Wi-Fi فلـن يستطيع إزالتها، أو يصعـب أن يقـوم بالتخلص منها عن طريـق الأدوات الخاصة بالحذف، وذلـك بسبب الطبيعة الخاصـة للتكنولوجيا التي تحفظ جميع مـا يستخدمه الفرد في الحاسوب الشخصي، والتي يمكن استردادهـا بسهولة، وعليه حتى لو قـام الجاني باستخدام أدوات متواجدة فـي التقنية وهي التي تتمثـل بالحـذف، أو الإزالـة، أو الإلغاء فلن تجدي معـه نفعاً، ولا تشكل عائقـاً للحكومة، أو الجهة المختصـة في استـرداد المعلومات، والبيانات التي تم حذفها، أو تـم إزالتها من الجهاز الذي تم حدوث الجريمة عن طريقها، وحيث أنها تملك برامج، وأدوات متخصصة في استرجاع المحتويات المطلوبـة. كذلك إن صعوبة التخلص من الدليل الإلكترونـي تترتب على فعله مسائل قانونية ذات

(١) المعمري الدليل الإلكتروني، مرجع سابق، ص ١٩٩.

أهميــة كبرى حيث إنهــا تكون؛ جريمة مستقلة بحد ذاتها عند ارتــكاب الجاني برامج تساعد على حــذف البيانــات والمعلومات المتواجدة فــي الجهاز حتى يتخلص منها فهنــا نكون بصدد جريمة جديــدة مستقلــة، وهي البرامج المستخدمة لحــذف المحتويات المتواجدة فــي الجهاز فتقع على الجاني العقوبات المترتبة على استعمالها[١].

**المطلب الثاني: طرق الحصول على الدليل الإلكتروني**

حيث إن طبيعة الدليل الإلكتروني تختلف عن طبيعة الدليل العادي، فعليه إن طرق الحصول عليــه تختلف أيضا، وهذا الاختلاف ليس كلي بل ببعض الطرق والإجراءات المتبعة، والتي تختص بالجوانب الإلكترونية.

حيــث تقســم طرق، وإجــراءات الحصــول على الدليــل الإلكترونــي إلى ثلاث طــرق، وعبر إجــراءات تتمثــل في إجراءات الضبط، والتفتيش، وإجراءات الاستعانة بالخبــرة التقنية الفنية، وإجــراءات التأكــد من مدى الحجية القانونية لقوة الدليل الإلكتروني[٢]. وبناء على ذلك يتضح أن هناك أوجه اتفاق بين طرق الحصول على الدليل الإلكتروني والدليل التقليدي، وذلك في إجراءات الضبط، والتفتيش، وكذلك التأكد من مدى قوة الدليل بالإضافة لمشروعية الحصول على الدليل، وبالرغــم مــن التشابه في طرق الحصــول على الدليــل إلا أن هناك بعض الاختلافــات في تنفيذ الطريقة والإجــراءات المتبعة؛ وأوجه الاختلاف في الحصول علــى الدليل الإلكتروني، والتقليدي الطريقة التي تتمثل في الاستعانة بالخبرة التقنية، والفنية. ومن خلال ما سبق يمكن تقسيم طرق الحصول على الأدلة الإلكترونية إلى طرق إجرائية وطرق فنية.

**أولاً: الطرق الإجرائية:**

تتمثل الطرق الإجرائية في الحصول على الدليل الإلكتروني في اتباع نفس إجراءات الحصول علــى الدليل المادي التقليــدي، إلا أن طبيعة التطبيــق مختلفة، حيث تتمثل الطــرق الإجرائية في الضبط والمعاينة والتفتيش، وتختلف تلك الإجراءات من نظام لآخر ومن دولة لأخرى، حيث نصت بعض الأنظمــة على تعيين فرق ضبطية يتم منحها ميزة الضبــط القضائي في جرائم المعلومات بشرط أن يكون الأشخاص المنتمين لتلك الفرق من المتخصصين قانونيا وتقنيا أو تنتمي لجهات تقنيــة مثــل هيئة الاتصــالات والمعلومات، ومــن تلك الأنظمة النظــام المصــري [٣]؛ في حين أن النظام السعودي لم يشر إلى ذلك صراحة وإنما أعطى حق المتابعة وتقديم المساعدة في مراحل الضبط والمساعدة لهيئة الاتصالات وتقنية المعلومات[٤]. كما أن لمرحلة التفتيش شروط خاصة

(١) المعمري الدليل الإلكتروني، مرجع سابق ، ص ١٩٩- ٢٠٠.

(٢) بطيخ، تطور السياسة التشريعية، مرجع سابق، ص ٨٠.

(٣) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨، المادة ١٢.

(٤) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨، المادة ١٣.

لا بـد من مراعاتها في الحصـول على الدليل الإلكتروني، ومن ذلك الحفاظ على السرية واحترام الخصوصية، بحيث إن كان البحث والتفتيش مختصًا بجهاز حاسوب فإن التفتيش يكون في حدود الملفات المتعلقة بالقضية ولا يصح الاطلاع على باقي الملفات دون إذن إن لم تتعلق بالقضية، كما لا يحق مشاركة أي خصوصيات خارج حدود القضية؛ وقد أكد النظام السعودي ذلك بالإشارة إلى حقـوق الملكية الفكرية، واحترام الاتفاقات الدوليـة والتي منها الخصوصية[1]. وقد سمح النظام السعودي بمصادرة جميع الأجهزة والأدوات التي تم استخدامها في الجريمة الإلكترونية من أجل الوقوف على الحقائق واستخراج الأدلة الإلكترونية من خلال المتخصصين التقنيين[2].

**ثانياً: الطرق الفنية:**

وتتمثل الطرق الفنية التقنية في الاستعانة بخبراء تقنيين لفحص الأجهزة، ومعاينة الأدوات التـي تـم استخدامها في الجريمة الإلكترونيـة، وغالبا يكون الخبراء التقنيـون من هيئات رسمية تابعـة للدولة، وهي فـي المملكة العربيـة السعودية (هيئـة الاتصالات وتقنيـة المعلومات). وبعد الاستعانـة بالخبـراء الفنيين يتم فحص الأجهزة، والأدوات المتعلقـة بالجريمة الإلكترونية، ومن ثـم يكـون الفحص قائما علـى جانب تقني احترافي ويبـدأ بحذف أي اتصـال خارجي قد يتم مع الأجهـزة حتى لا يتحكم أحد من الخارج في السيطـرة على الأجهزة، وحذف ما فيها من أدلة؛ ثم يبدأ الفحص في الملفات ذات الصلة بالقضية حتى يستخرج الدليل، وفي بعض الأوقات قد يكون الدليـل متوقفا على موافقة أمنية من قبل السيرفرات المستضيفة على المستوى الدولي، وفي تلك الحالـة يتم إعداد تقرير وطلـب رسمي يتم توجيهه من الجهة المختصة للشركة أو الدولة الأخرى إن لـم يكن هناك قدرة لتخطي حاجز الأمان للوصـول إلى البيانات. ثم تكون المرحلة الأخيرة أن يقـوم الفريـق التقني بإعداد تقرير شامـل عن جميع الملاحظات، والأدلـة، وتسجيل جميع الأدلة بالتوقيـت والتاريخ الخاص بها، ومن ثم تقديم ذلك إلى الفريق القضائي أو جهة التحقيق. ويجب أن تكـون الطرق الفنية للحصول على الدليل الإلكترونـي موثوقة وموضح فيها أساليب البحث عن الدليـل والطرق المتبعة وذكر البرامج المستخدمة، والتأكد مـن استخدام تقنيات حديثة لا تؤدي إلى تغيير أو حذف الأدلة أو تعديلها ومن تلك التقنيات Write Blocker Digital Images Hash وكذلك توثيق جميع العمليات من خلال الكود وخوارزمية Hash، والتي يمكن من خلالها استخراج نسخـة مطابقـة للأصل من الدليل الإلكتروني[3]. ومما سبق يمكـن القول بأن طرق الحصول على الدليل الإلكتروني تتمثل في طريقتين أساسيتين، الأولى متشابهة مع الدليل التقليدي وهي الضبط والمعاينـة والتفتيش، ولكـن الآلية تكون مختلفة لطبيعـة الجريمة الإلكترونيـة، ومن ثم مصادرة الأجهـزة والأدوات المستخدمـة؛ والطريقة الثانيـة متمثلة في الاستعانة بالخبـراء التقنيين وهي

(١) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨، المادة ١٢.

(٢) نظام مكافحة جرائم المعلوماتية الصادر بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨، المادة ١٢.

(٣) بطيخ، تطور السياسة التشريعية، مرجع سابق، ص ٩٢.

طريقــة مختلفــة عن الدليــل التقليدي لكنها تعد مثــل الاستعانة بالأطبــاء الشرعيين في الجريمة التقليديــة لرفــع البصمات أو تشريــح الجثث لاستنتاج الدليــل من المعلومات. ويمكــن القول بأن طــرق الحصول على الدليل الإلكتروني تتمثل في طرق يسيــرة وأخرى معقدة، أما الطرق اليسيرة فــلا تحتاج إلى خبراء تقنيين وهي تتمثــل في الملفات الفعالة والملفــات المؤرشفة؛ بينما الطرق المعقــدة التي تحتاج إلى الاستعانــة بالخبراء التقنيين فتتمثل في الملفات والبيانات الممسوحة أو التــي تحتــوي على جدار حماية من الصعب تجاوزه[1]. وينبغــي أن تكون جميع تلك المراحل قائمة علــى قواعــد وأسس وطرق قانونيــة شرعية، ويكون ذلــك من خلال عدم التعــدي على خصوصية الأشخاص وأن يكون التفتيش بإذن مسبق ومرتبطا بالجريمة.

**ثالثاً: مدى قوة الدليل الإلكتروني:[2]**

ترتبط قوة الدليل بقوة المعلومــات المستخرجة من الجهاز الإلكتروني، والتي تتعلق بطبيعة الجريمــة، حيــث كلما كانــت المعلومات شاملــة ودقيقة كانــت قوة الدليــل أقوى، بينمــا إن تخلل المعلومــات لبســ أو شبهــة تعديل أو تغيير فإن قــوة الدليل تضعف، كما أن قــوة الدليل الإلكتروني ترتبط بالأدلة غير الإلكترونية إن وجدت، حيث إن كان هناك دليل غير إلكتروني يتوافق مع الدليل الإلكترونــي فــإن الدليل الإلكتروني يكتسب قــوة في الحجية والإثبات، بينما عــن تواجد دليل غير إلكتروني يخالف الدليل الإلكتروني فإن الأمر يترك في عدد من الأنظمة إلى القاضي، وفي الغالب يأخذ القضاة بالأدلة غير الإلكترونية إن خالفت الأدلة الإلكترونية. أيضًا من الأمور التي تؤثر على قــوة الدليــل الإلكتروني طريقة الحصول عليه، فــإن كانت الطريقة تمت على نهــج قانوني شرعي بالالتــزام بجميــع الضوابط واتباع جميع الإجــراءات فإن الدليل الإلكترونــي يكتسب قوة وحجية، بينمــا إن لم يتم الالتزام بالطــرق القانونية، والشرعية في الحصول علــى الدليل الإلكتروني فإنه يضعــف ولا يحتــج به فــي الإثبات. ومما سبــق يتضح أن الدليــل الإلكتروني إن تــم الحصول عليه بالطــرق القانونية، والشرعية، وتم توثيق جميع الإجراءات التي تمت خلال عملية استخراجه، وتم التأكيــد على صحته، وعدم التعديــل فيه، وأنه لا يُخالف دليلا غير إلكتروني فإنه يكون دليلا قويا؛ بينما إن افتقد لتلك الشروط فإنه يضعف ولا يكون دليلا في إثبات الجريمة الإلكترونية.

**المطلب الثالث: طرق إثبات الجريمة الإلكترونية**

إن الجريمــة الإلكترونية نوع مــن الجرائم التي أصبحت منتشرة فــي العصر الحديث الذي يُعرف بعصر الثورة التكنولوجية، ومثل تلك الجرائم يحتاج إلى طرق إثبات خاصة بها تختلف عن طرق الإثبات الخاصة بالجرائم التقليدية.

---

(١) عبد الباقي مصطفى: التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين دراسة مقارنة مجلة دراسات علوم الشريعة والقانون ٤ ، ٢٠١٨م)، ص ٢٩٢.

(٢) ال ثنيان، إثبات الجريمة الإلكترونية، مرجع سابق، ص ٧٤-٨٤.

ونظرا لاختلاف الجرائم الإلكترونية، والأدلة الخاصة بها التي في الغالب تتمثل في بيانات، وأجهـزة رقمية، فإنهـا تكون في حاجة إلى نيابة متخصصة، أو لديها مستشارون متخصصون في التقنيـة من أجل تحليل الأدلة، واستنتاجهـا، ومن ثم إثبات الجريمة؛ وقد تتمثل الأدلة في وحدات تخزيـن مؤقتة، أو دائمة، وملفات فعالة أو مؤرشفـة أو ممسوحة؛ وهي نوعان إما أدلة يتم إنشاؤها مثـل الملفـات والوسائط، وحفظها علـى الأجهزة، أو أدلة لا يتـم إنشاؤها مثل ملفـات التسجيل، وملفـات تعريـف الارتباط[١]. حيـث تتمثل الأدلة التي يتـم إنشاؤها في الأعمـال التي للشخص أو العنصـر البشري المستخدم تدخل فيهـا، ومنها أن يقوم الشخص بإنشاء ملـف للكتابة داخله أو إعـداد جداول حسابيـة كانت أو تحتوي على بيانات مثـل ملفات الإكسل على سبيـل المثال، أو أن يقـوم بإنشـاء ملف ويضع فيه صـور، أو مقاطع صوتية قد يكون لها علاقـة بالجريمة؛ ومن ثم يتم حفـظ تلك الملفات أو المستندات على الجهـاز الإلكتروني، وعند العودة إليها وفحصها تعد دليلا علـى الجريمـة. بينما تتمثل الأدلة التي لم يتم إنشاؤها في تلك البيانات، أو الملفات التي لا علاقة للعنصـر البشـري والشخص المستخدم فيهـا، وإنما هي ملفـات ارتباط وبيانات يتـم أرشفتها، وحفظهـا تلقائيا من قبل البرامـج، والسيرفرات التي تستضيف تلك المواقـع والتطبيقات، ومنها أن يتـم حفـظ تواقيت الدخول إلـى الموقع، والأماكن التي تم فتح الموقـع أو التطبيق من خلالها، وهـذه بروتوكـولات تنظيم، وحماية تقنيـة لا يتدخل الإنسان فيها وإنما تتـم بطريقة تلقائية، وتعد الأدلـة التي يتـم إنشاؤها من خلال العنصر البشـري أسهل في الوصول إليهـا، وكذلك أسهل في حذفهـا من قبل الشخص؛ بينما الأدلة التي لا يتم إنشاؤها أكثر صعوبة في الحصول، وتحتاج إلى اتفاقيات دولية ولا يتم الحصول عليها إلا بضوابط، وفي أضيق الحدود نظرًا لعنصر الخصوصية والسريـة[٢] . ولذلك تواجـه عملية إثبات الجرائـم الإلكترونية بعض التحديـات والصعوبات عن الجرائـم التقليديـة، وذلك يرجع لعدة أسباب منهـا أنها تفتقد إلى الآثـار المعروفة في الجريمة التقليديـة وخاصة أنها تخلو في الغالب مـن البصمات والشواهد المادية بالإضافة إلى عدم توافر الخبـرة الكاملة والمعرفة والإتقان للأساليب التقنية لدى أجهـزة البحث الجنائي والنيابة العامة والقضاء[٣].

وتتمثل طرق إثبات الجرائم الإلكترونية في نوعين من الطرق، وهما:

**النوع الأول: طرق الإثبات التقليدية:**

وفيهـا يتم اتبـاع الأساليب والوسائل الخاصـة بالاستدلال وإثبات الجريمـة، وهي الأساليب المعروفة والتي لا فرق بينها وبين الجريمة التقليدية سوى في آلية التطبيق، وهي:

(١) عبد الباقي، التحقيق في الجريمة الإلكترونية، مرجع سابق، ص ٢٩٢.

(٢) عبد الباقي، التحقيق في الجريمة الإلكترونية، مرجع سابق، ص ٢٩٢.

(٣) البداينة، ذياب الجرائم الإلكترونية المفهوم والأسباب كلية العلوم الاستراتيجية، الملتقى العلمي الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، عمان، الأردن ٢٠١٤م)، ص ١٥.

- تلقـي البلاغ نتيجة للضبط، وهي من الأساليب القليلـة والتي تواجه صعوبات في الجرائم الإلكترونيـة، حيـث تتم تلـك الجرائم في سرية تامـة وكذلك لا تترك أثـرا ماديًا لذا من الصعب البلاغ عن تلك الجرائم، لكنها تعد المرحلة الأولى للاستدلال.
- معاينـة وضبط وتفتيش الأجهـزة الإلكترونية محل الجريمة، وهي في الغالب لا تكون ثابتة ولا تعتمد على مكان محدد وأداة للجريمة مثل ما يحدث في الجرائم التقليدية.
- الاعتمـاد علـى شهادة الشهود، وهـي أيضا من الأساليب التي تواجـه صعوبة في الجرائم الإلكترونية نظرا لسرية الجرائم الإلكترونية وعدم ترك أثر مادي عليها.

وهـذا النـوع من الإجـراءات والطرق يتم غالبًـا مع الأدلة التـي يتم إنشاؤها نظـرًا لسهولة الحصول عليها.

**النوع الثاني: طرق الإثبات الرقمية:**

والطـرق الرقمية أو الإلكترونية هي الطـرق المستحدثة التي يتم من خلالها إثبات الجرائم الإلكترونية وهي طرق فنية تقنية تحتاج إلى خبرة واستعانة بالمتخصصين التقنيين، وهي:[1]

- الاطـلاع على الـ IP الخاصـ بالجهاز، وبالشخص المستخدم لـه، ومن خلال ذلك يمكن التأكد من العلاقة بين البيانات، والجهاز، أو الشخص المستخدم لها.
- استخـدام ملفـات الكوكيـز، والبروكسي وهـي بروتوكولات تقنيـة تقوم بحفـظ البيانات والتوقيتات.
- اعتراضـ الاتصـالات والتواصل مع الجهات المسؤولة عن استضافـة المواقع أو الشبكات سـواء الاتصالات أو السيرفـرات والداتا سنتر، ويكون ذلك بالتعـاون بين الدول حيث إن استضافة بعض المواقع يكون في دول خارج الدولة التي تمت فيها الجريمة.
- المراقبة الإلكترونية وهي مسؤولية تقع على عاتق الجهات الأمنية التي تتمتع بخبرة تقنية، ولا يكون ذلك إلا في حدود معينة وبضوابط ينص عليها القانون حتى لا تدخل ضمن تعدي وتجاوز الخصوصية.

وهـذا النوع من الإجراءات، والطـرق يتم في الغالب مع الأدلة التي لم يتـم إنشاؤها، وذلك نظـرا لصعوبة الحصـول عليها، حيث إنها تتطلـب جانب تقني، وكذلك موافقـات، واتفاقات بين الـدول يمكن مـن خلالها الرجوع إلى الشـركات المستضيفـة للمواقع الإلكترونيـة، والداتا سنتر المسؤولـة عن السيرفرات حول العالم، وطلب تلك البيانات؛ ولا يتم الموافقة على ذلك دائما إنما يكـون في حدود ضيقة لعدم تجاوز السريـة، والخصوصية؛ وهنا يأتي الـدور التقني المتخصص الذي يحاول الوصول إلى تلك البيانات، وتحليلها للتوصل إلى الأدلة. ومن خلال الدمج بين الطرق

(١) عبد الباقي، التحقيق في الجريمة الإلكترونية، مرجع سابق، ص ٢٩٢.

التقليدية، والطرق الرقمية الحديثة يمكن إثبات الجريمة الإلكترونية وتأخذ الأدلة حجيتها.

**المبحث الثالث**

**التطبيقات القضائية للجريمة الإلكترونية في المملكة العربية السعودية**

بنـاء علـى ما سبـق، وبعد أن تم عرض موضوع إثبـات الجريمة الإلكترونيـة ترغب بعرض السوابـق القضائيـة التي لهـا علاقة بالجرائـم الإلكترونية، والتـي تم حدوثهـا بالمملكة العربية السعودية، وبعد أن تم البحث في مجلة الأحكام القضائية رأينا عدداً يعتبر قليلاً، وذلك بالمقارنة مـع عدد الجرائـم الإلكترونية التي تحدث سواء كانت سرقة، أو نصبـاً، أو احتيالاً، أو اختراقاً، أو تشهيـراً، أو نشر مواد إباحية، وكذلك أن المجلة لم تكن شاملة لجميع الجرائم الإلكترونية، ولهذا تـم الاقتصار على عرض تطبيقات قضائية لنوعين مـن الجرائم الإلكترونيـة وهما جريمة نشر المواد الإباحية وجريمة التشهير وتم تقسيم المبحث الى مطلبين:

**المطلب الأول: القضية الأولى**[1]

ملخص التطبيق القضائي:

قيـام المدعي العام (أ) بإقامـة دعوى ضد المدعى عليه، وذلك بسبـب قيام المدعى عليه ببيـع الأفـلام الإباحية، وحيازتهـا وتخزينها، والقيـام بتجهيز بمـا يمس القيم الدينيـة والآداب العامة، وذلك عن طريق استعماله لشبكة الإنترنت بعد ذلك قام المدعي العام (أ) بطلب العقوبة عليـه، وذلك بالاستناد على المادة السادسة من نظام مكافحة جرائم المعلوماتية، وبعد ذلك أقر المدعى عليه بصحة الدعوى بعد عرضها عليه.

الأدلة والقرائن:

١. المحضر الخاص بالمشاهدة لفة رقم (٣).

٢. إقرار واعتراف المتهم (ب) الذي ينشر ويبيع المواد الإباحية.

٣. المتهم (ب) أقدم على هذا الفعل المحرم شرعاً، والغير مشروع والذي يُعاقب عليه الشرع وقـام بالفعل وهو بكامـل أهليته التي يعتبرها الشرع، وهذا يستوجـب إرسال المتهم الى المحكمة الجزائية، وذلك استناداً للمادتين (١٢٨-١٢٦) من النظام الخاص بالإجراءات الجزائية.

الأسانيد الشرعية والنظامية:

النظام الخاص بمكافحة الجرائم المعلوماتية السعودي (المادة السادسة).

التفاصيل الخاصة بالقضية

(١) مجلة الأحكام القضائية ١٤٣٥ هـ ، المجلد الثالث عشر، صك رقم: ٣٤٥٤٢٩١٩ ، بتاريخ ١٤٣٥/٥/٢هـ ، و تم تأييد الحكم من محكمة الاستئناف بقرار رقم : ٣٥٢٢٨٨٢٦ ، بتاريخ ١٤٣٥/٤/١١هـ .

فـي يـوم الأربعاء الساعـة العاشرة والربع، والـذي يوافق ١٤٣٥/٣/١٤ هـ افتتحت الجلسة الأولـى، وحضـر فيهـا المدعي العـام (أ) وهو مدعي عام يمثـل دائرة الادعاء العـام لفرع الهيئة بمنطقة الجوف، وقام بتجهيز لائحة دعوى، وتقديمها ضد المدعى عليه (ب).

رفعت الدعوى بعد أن قام أحد المواطنين برفع بلاغ على المتهم (ب) لهيئة الأمر بالمعروف والنهي عن المنكر، وذلك لبيعه؛ ذواكر خاصة بالحاسب الآلي تحتوي على أفلام إباحية.

تم التأكد من صحة البلاغ المقدم من المواطن عن طريق بيع المتهم لذاكرتين، وتم إيقافه وقـام المتهـم بالإفادة بأنه يبيع الأفـلام الإباحية عن طريق تخزينها فـي الذواكر، وبيع الذواكر، وبعد ذلك تم القبض عليه، وتم تسليمه لشرطة العزيزية.

تم إيقاف المتهم عبر المستند النظامي وهو (القرار الوزاري رقم ١٩٠٠ المبني على المادة ١١٢ من نظام الإجراءات الجزائية).

الحكم:

افتتح القاضي الجلسة في يوم الأربعاء ١٤٣٥/٣/١٤هـ. في الساعة العاشرة صباحاً.

حضـر المدعي العـام (أ)، وحضـر المدعى عليـه (ب)، وأقر المدعى عليـه (ب) بدعوى المدعـي العـام (أ) جملـة، وتفصيلاً. وتحدث المدعـى عليه (ب) بأنه غيـر محصن، وكذلك لا توجد عليه سابقة قضائية، وأنه نادم على فعله، وتائب الى الله عز وجل، وقد قرر القاضي، وذلك بنـاء علـى أن الشـرع قد حرم الفواحش ما ظهر منهـا، وما بطن، وحرم كل وسيلـة تؤدي إلى هذا الفعل، وكذلك أن التعزير وجد في كل معصية من المعاصي ليس لها حد، وليس لها كفارة، وكذلك بالاستنـاد على المـادة السادسة مـن النظام الخاص بمكافحـة الجرائم المعلوماتيـة السعودي، وتطابقها على المدعى عليه (ب) وقد حكم القاضي على المدعى عليه (ب):

١. جلـد المدعـى عليه (ب) وهـو المتهم ثلاثمائة جلـده تقم على بدنه، وتكـون على خمس دفعات بالتساوي والمدة تكون عشرة أيام بين كل دفعة، ودفعة.

٢. سجن المتهم (ب) سنة كاملة، وتكون مدة الإيقاف محتسبة منها.

٣. الجهـاز الذي كان بحوزة المتهم (ب) والذي يحتوي على المواد الإباحية، وتمت الإشارة عليه في الدعوى يتلف، ويمسح ما يوجد به من مواد غير مشروعة محرمة شرعاً.

٤. تغريم المتهم (ب) مبلغ قيمة خمسة آلاف ريال، ويتم إيداعها في الخزينة العامة.

٥. توقيع المتهم (ب) على تعهد بشأنه عدم رجوعه على الفعل المحرم شرعاً مرة أخرى.

هنـاك رأي خاص بالقاضي ألا، وهو: بعد انتهاء فترة المحكومية الخاصة بالمتهم (ب) يتم إبعاده الى بلاده، وإن وجد شيء عليه أو له يتم الانتهاء منه.

تم النطق بالحكم في الساعة العاشرة والنصف بتاريخ ١٤٣٥/٣/١٤ هـ.

تـم عرضـ الحكم على أطـراف القضية، وهم المدعـي العام والمدعى عليـه، ولم يقتنعون بالحكـم الـذي نطـق بـه القاضي فـي محكمة الدرجـة الأولـى، وطلبوا رفـع الحكم إلـى محكمة الاستئناف، وذلك بلا لائحة اعتراضية من الطرفين.

حكم الاستئناف:

اطلعـوا قضـاة الاستئناف علـى الحكم الذي تم رفعـه عن طريق القاضـي لمحكمة الدرجة الأولـى، وذلك استجابة لطلب طرفـي القضية، وقد صادق قضاة محكمـة الاستئناف على الحكم الذي صدر من محكمة الدرجة الأولى.

العلاقة بين السابقة القضائية والبحث:

إن جريمة نشر المواد الإباحية من أنواع الجرائم الإلكترونية حيث أن هذه الجريمة المحرمة شرعـاً قبل كل شيء من أكثر الجرائـم انتشاراً للأسف في العالم بصفـة عامة والمجتمع العربي بصفـة خاصة، وذلك الانتشار يتم عن طريق النشـر عبر شبكات الإنترنت أو التواصل الاجتماعي مثـل تويتـر، وغيره من البرامج التي تحتمل الاستعمال السيء، والجيـد أو تحميل المواد الإباحية، وتخزينهـا بذاكـرة، وبيعها. ولذلك أنا أرى أن حكم القاضي صحيـح، وموافق للشرع حيث أن هذه الجريمة لابد من رادع قوي لها حتى يتم تقليل مرتكبيها فمدى قوة الردع هو الحاجز ما بين المقبل على الارتكاب والجريمة المحرمة شرعاً.

**المطلب الثاني: القضية الثانية**[1]

ملخص التطبيق القضائي:

قام المدعي العام (أ) برفع دعوى ضد المدعى عليه (ب)، وذلك بسبب قيام المدعى عليه، وهـو المتهم (ب) بتصوير فتـاة صغيرة، ونشر صورها، وكذلك حيـازة المتهم (ب) على مقاطع جنسية في الجوال الذي يملكه، وكذلك بعد أن تم عرض الدعوى على المدعى عليه (ب) اعترف، وأقر بصحة العرض. وطالب المدعي العام (أ) بعدة طلبات توقع على المتهم.

الطلبات:

١. الحكـم على المدعى عليه (ب) بالعقوبة الموجودة في نظام مكافحة جرائم المعلوماتية السعودي.

٢. الحكم على المتهم (ب) بالعقوبة التعزيرية.

٣. مصادرة الجوال الخاص بالمتهم (ب) والذي يحتوي على مقاطع جنسية.

الأدلة والقرائن:

(١) مجلة الأحكام القضائية عام ١٤٣٥ هـ ، المجلد الثالث عشر، صك رقم : ٣٥١٦٥٩٣٢ ، بتاريخ ١٣/٤/١٤٣٥ هـ ، وتم تأييد الحكم من محكمة الاستئناف بقرار رقم: ٣٥٢١١١٦٤ ، بتاريخ ١٠/٤/١٤٣٥هـ.

١. اعتراف المتهم (ب) بالتحقيق.

٢. المحضر الخاص بالقبض.

٣. محضر خاص بشاهدة الجوال الخاص بالمتهم.

الأسانيد الشرعية والنظامية:

١. قول الله تعالى ﴿قُلْ إِنَّمَا حَرَّمَ رَبِّيَ الْفَوَاحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَ﴾.

٢. القاعدة الفقهية: (لا عذر لمن أقر).

٣. المادة الثالثة والمادة الثالثة عشر من النظام الخاص بمكافحة جرائم المعلوماتية السعودي.

التفاصيل الخاصة بالقضية:

افتتح القاضي في المحكمة العامة بمحافظة ينبع الجلسة، وذلك في يوم الأربعاء الموافق ١٤٣٥/٣/٢١ هـ وفي الساعة (١١:٤٥) صباحاً، وحضر المدعي العام، وهو الذي يمثل دائرة الادعاء العام لدائرة التحقيق، والادعاء العام في محافظة ينبع.

في تاريخ ١٤٣٥/٣/٩ هـ أتى للدوريات بلاغ من مواطن بتصوير المتهم (ب) فتاة صغيرة عمرها لا يتجارز ١١ سنة وتم التصوير عن طريق الجوال الخاص بالمتهم (ب)، وفي المحل الذي يعمل به.

انتقلت الدوريات إلى الموقع الذي أتاهم في البلاغ، وتم إلقاء القبض على المتهم (ب)، وبحوزته الجوال الذي تم تصوير الفتاة منه، وبعد الاطلاع على الجوال وجد أن هناك صورة لفتاة عمرها لا يتجاوز الحادية عشر سنة، وهي داخل المحل، وكذلك وجد داخل الجوال الخاص بالمتهم (ب) ملف يوجد به مقطع، وهو يقوم بدلك ذكره داخل مكان يشابه دورة المياه، وكذلك وجد في الجوال نفسه للمتهم (ب) صورة لفتيات. واعترف المدعى عليه (ب) وهو المتهم بارتكاب هذه الجرائم، وأقر بصحة الأدلة والقرائن التي عليه.

الحكم:

افتتح القاضي الجلسة بتاريخ ١٤٣٥/٣/٢١ هـ في الساعة (١١:٤٥) وبناء على الأدلة، والقرائن المعروضة، وبناء على طلبات المدعي العام (أ) وهو الذي يمثل دائرة الادعاء العام، وبناء على ارتكاب المدعى عليه (ب) فعلاً محرماً شرعاً قد حكم القاضي على المتهم (ب):

١. بعقوبة تعزيرية زاجرة له وتردع غيره، وهي تعزيره بجلده خمسين جلده وتكرر عليه ثلاث دفعات، وتكون بين كل دفعة، وأخرى عشرة أيام، وهذا بسبب أنه يحوز على مقطع جنسي يرتكبه بنفسه بالإضافة لصور فتيات متبرجات في الجوال الذي يملكه.

٢. مصادرة الهاتف المحمول الذي يملكه، والذي تم استخدامه في الجريمة.

٣. سجن المتهم (ب) لمدة ثلاثة أشهر، ويتم احتساب مدة الإيقاف لهذه القضية.

٤. إلقاء غرامة على المتهم (ب) بمبلغ قدره مئتي ريال، ويدفع هذا المبلغ لبيت مال المسلمين، وذلك بالاستناد على المادة الثالثة لنظام مكافحة جرائم المعلوماتية السعودي.

وبعد أن تم عرض الحكم الذي حكم به القاضي على المدعى عليه (ب) اقتنع به، ولكن المدعي العام (أ) لم يقتنع به بالأحكام الصادرة من القاضي، وقرر المعارضة بلا لائحة. تم تحرير في ١٤٣٥/٣/٢٦ هـ.

الحكم الصادر من الاستئناف:

افتتح قضاة الاستئناف القضية، والتي تم إحالتها من رئيس محكمة الاستئناف، وذلك بناء على المعاملة التي وردت من المحكمة العامة بمحافظة ينبع. وبعد أن تم الاطلاع من قضاة الدائرة الجزائية الأولى على الحكم الذي صدر من قاضي المحكمة العامة بمحافظة ينبع تم الإقرار على الحكم الذي صدر بالأكثرية.

العلاقة بين السابقة القضائية والبحث:

بلا شك أن جريمة التشهير من أنواع الجرائم الإلكترونية، وهي من أكثر الجرائم انتشاراً في الوطن العربي، ويجب أن تكون هناك عقوبات رادعة وقوية حتى يتم تقليل مرتكبي هذه الجريمة، وأنا أوافق القاضي فيما صدره من حكم قضائي على المتهم (ب) بل لا يوجد هناك مانع من أن تكون العقوبة أكثر قوة على المجرم حتى لا يحاول ارتكاب الجريمة مرة أخرى، وبالإضافة أنه عند التعرض لمثل هذا النوع من الجرائم المحرمة شرعاً، والغير مشروعة قانوناً يجب التحرك سريعاً نحو الجهة المختصة حتى يتم القبض على المجرم، وهذا هو الطريق الصحيح لتقليل هذا النوع من الجرائم.

**الخاتمة**

إن الحمد لله، والشكر له على نهاية هذا المشروع، وإتمامه في موضوع إثبات الجريمة الإلكترونية، والذي تم به استعراض المفردات الخاصة بالإثبات والجريمة، وكذلك عرض أهمية الإثبات، وبيان أشخاص الجريمة الإلكترونية، وتوضيح الفئات الخاصة بهم، أيضاً التعريف بالدليل الإلكتروني، وبيان خصائصه، وتوضيح الطرق الخاصة للحصول على الدليل الإلكتروني، وبالإضافة إلى عرض طرق إثبات الجريمة الإلكترونية.

- **ومن خلال بحثي قد توصلت إلى هذه النتائج:**

١. أن الجرائم الإلكترونية من الجرائم التي في الغالب لا تترك أثراً يمكن مشاهدته عند ارتكابها بالإضافة إلى أنها من الجرائم المعقدة حتى يتم اكتشافها، وذلك إذا قارنا

الحـالات التي تـم فيها اكتشاف الجرائـم الإلكترونيـة بالحالات التي تـم فيها اكتشاف الجرائم التقليدية نجد أن هناك فرقاً شاسعاً، وكذلك إن الجرائم الإلكترونية هي عابرة للـدول، ومعنى هذا هو: إمكانية قيام المجـرم بفعل الجريمة في دولة، والمجني عليه في دولة أخرى.

٢. إن الجرائم الإلكترونية تتسم بصعوبة إثباتها، وهذه من أكثر العوائق للجريمة الإلكترونية، والتـي تواجهها الجهات المختصة، والتي يواجهها ضحيـة هذه الجريمة كذلك إن إثبات الجريمة الإلكترونية يستلزم وجود خبرة فنية، وجهد كبير وكثيف.

٣. في الماضي كان التركيز على أهمية إثبات الجريمة الإلكترونية شبه معدوم، وذلك بسبب عدم كثرة الاستعمال التكنولوجي في المجتمع، ولكن مع سيطرة التقنية على العالم أجمع أصبحـت أهمية إثبات الجريمـة الإلكترونية تضاهي أهمية إثبـات الجريمة التقليدية بل حتـى بنفس المستوى التي يكون لإثبات الجريمة التقليدية بالإضافة إلى أن عدد الجرائم الإلكترونية أصبح يضاهي عدد الجرائم التقليدية بل هي أكثر بسبب سهولة فعل الجريمة الإلكترونية.

٤. توصلـت في بحثي إلى توضيح فئات أشخاص الجريمـة الإلكترونية بالتفصيل وكذلك إن توضيح الفئات الخاصة بأشخاص الجريمة الإلكترونية له أهمية كبيرة، وقوية للغاية فمن خلالهـا يسهـل على الفرد، وعلى الجهـات المعنية معرفة ما هي الفئـة التي تندرج تحت شخصية المجرم الإلكتروني وما هي الفئة التي تندرج تحت شخصية المجني عليه.

٥. إن الحصـول على الدليل الإلكترونـي للجريمة يتطلب طرقاً معينة وهـي إجرائية وتقنية وقد جرى توضيحها بالتفصيل في بحثي، وبناء على ذلك فالإجرائية تكمن في اتباع نفس الطـرق التي يتم اتباعها عند الحصول على الدليل التقليـدي بينما الطرق التقنية، وهي التـي تكمن في الاستعانة بمختصيـن ذو خبرة فنية، وتقنية عالية بل كلاهما يكمل الآخر للوصول للدليل الإلكتروني المراد.

٦. تتميـز الجريمـة الإلكترونيـة بطـرق إثبات إحداهمـا تتشابه مـع طرق إثبـات الجريمة التقليديـة وإحداهما مختلفة عن الجريمة التقليدية وتكمن طـرق الإثبات بطرق الإثبات التقليديـة وهي الطرق الرئيسية للإثبات في الجريمـة التقليدية، وطرق الإثبات الرقمية وهي التي تتميز بها الجريمة الإلكتروني كوسيلة لإثبات الجريمة الإلكترونية.

٧. إنه عندما يتم الدمج ما بين طرق الإثبات التقليدية، وطرق الإثبات الرقمية يكون الوصول للمتهم والأدلة أسرع، وأقوى سواء من حيث الأدلة، أو من حيث الكشف عن المتهم.

- **التوصيات:**

١. أوصى بالعمل على زيادة الاهتمام على مراقبة جميع ما يدخل في مجال شبكات الإنترنت،

وهـذا يعطي الجهات المختصـة نتيجة، وهي الحصول على أي أثر يؤدي إلى القبض على المجرم الإلكتروني، وذلك عن طريق الحصول على الموقع الذي يعمل منه أو الكشف عن اسمه الشخصي، والحقيقي أو الكشف عن الجهاز الذي يعمل عن طريقه.

٢. أوصي المنظـم السعودي بتجديد النظـام الخاص بمكافحة جرائـم المعلوماتية، وذلك بسبـب قدم النظام الذي صدر في عام ١٤٢٨هـ وعـدم مواكبته لتطور العصر الإجرامي التقنـي فمن بعد عـام ١٤٢٨هـ أتت العديد من الطرق، والتغييـرات الحديثة، والتطورات المذهلة للتقنية بشكل عام، وللجرائم الإلكترونية بشكل خاص فمواكبة العصر الإجرامي الحالي أصبحت واجبة بسبب تطور طرق فعل الجريمة الإلكترونية، وطرق الحصول على الأدلة الخاصة بها.

٣. أوصـي بتشديد العقوبات على المجرم الإلكتروني بصفـة عامة، وبصفة خاصة لمرتكب جريمـة نشر المـواد الإباحية ولجريمـة التشهير فهاتـان الجريمتان من أكثـر الجرائم انتشـاراً فـي المجتمع، وضرراً، وتأثيراً عليه كذلك أن جريمـة نشر المواد الإباحية تؤدي إلـى فساد العقـول، وإفساد صحة الشخص، وكذلك إن جريمـة التشهير تؤدي إلى كشف أسرار المنازل، ونشـر الأمور الخاصة بالأسر فلذلك أوصي بإيقاع أقصى العقوبات على مرتكبي هذه الجرائم.

٤. أوصـي بالاهتمـام بالطرق الفنية الخاصـة بالحصول على الدليـل الإلكتروني، وتطورها حتى يتم التقليل من عدد الجريمة الإلكترونية، وسهولة الوصول للمتهم عند ارتكابها.

٥. أوصـي بعـدم فصل طرق الإثبات التقليديـة عن طرق الإثبات الرقميـة، وذلك بسبب أن كلاهما مكملان لبعضهما والدمج ما بينهم يُسرع من الكشف عن تفاصل الجريمة.

## قائمة المراجع

### أولاً: الكتب:


• رجـاء، وحيـد دويدري، البحث العلمي أساسيته النظريـة وممارسته العملية،(٢٠٠٠)، الطبعة الأولى، دار الفكر المعاصر، دولة لبنان.

• الجنبيهي، منير محمد الجنبيهي، ممدوح محمد. (٢٠٠٦م). جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها. الإسكندرية، دولة مصر: دار الفكر الجامعي.

• إبراهيـم، خالـد ممدوح. (٢٠٠٩م). الجرائم المعلوماتيـة (الإصدار الطبعة الأولى). الإسكندرية، دولة مصر: دار الفكر الجامعي.

• ابـن منظـور، محمـد بن مكرم بن علي أبـو الفضل جمال الديـن. (١٤١٤ هـ). لسان العرب (الإصدار الطبعة الثالثة الجزء الثاني ص ١٩).

• الأحمـد، وسيم حسـام الدين. (٢٠١٦م). مكافحة الجريمة المنظمة عبر الوطنية في ضـوء أحـكام الشريعة الإسلامية والأنظمـة السعودية (الإصدار الطبعة الأولـى). الرياض، دولة المملكة العربية السعودية: مكتبة القانون والاقتصاد.

• الزهرانـي، سعيـد حسـن آل يحيـى. (٢٠٢٠م). جرائـم الشبكة العالميـة للمعلومات (الإنترنـت) دراسـة فقهيـة تأصيليـة تطبيقية (الإصـدار الطبعـة الأولى). جدة، دولـة المملكة العربية السعودية: دار الأوراق.

• امسيويـط، انتصـار احميـدة محمد. (١٤٣٨هـ). التحول في نظـام الإثبات الجنائي (الإصدار الطبعة الأولى). دولة مصر: مركز الدراسات العربية.

• خالـد السيـد موسـى. (٢٠١٤م). شـرح قواعد الإثبـات الموضوعيـة: دراسة مقارنة (الإصدار الطبعة الأولى). الرياض، دولة المملكة العربية السعودية: مكتبة القانون والاقتصاد.

• سقـف الحيـط، عادل عزام. (٢٠١١م). جرائم الذم والقـدح المرتكبة عبر الوسائط الإلكترونيـة: شبكـة الإنترنـت والهواتف النقالـة وعبر الوسائـط التقليدية والآليـة والمطبوعات: دراسة قانونية مقارنة (الإصدار الطبعة الأولى). دولة الأردن: دار الثقافة والنشر والتوزيع.

• سكيكر، محمد علي. (٢٠١٠م). الجريمة المعلوماتية وكيفية التصدي لها. دولة مصر: سلسلة كتاب الجمهورية.

• سويلم، محمد أحمد. (١٤٣٨ه). الوجيز في قواعد الإثبات على ضوء نظام المرافعات الشرعيـة السعـودي (الإصدار الطبعة الأولـى). الرياض، دولـة المملكة العربيـة السعودية: دار النشر الدولي.

• شوقي، يعيش تمام. (٢٠١٩م). الجريمة المعلوماتية: دراسة تأصيلية مقارنة (الإصدار الطبعة الأولى). بسكرة، الجزائر: سلسلة مطبوعات المخبر.

• مرعـي، أحمـد لطفي السيـد. (١٤٣٧هـ). أصـول علمي الإجرام والعقـاب (الإصدار الطبعة الأولى). الرياض، دولة المملكة العربية السعودية: دار الكتاب الجامعي.

**ثانياً: الرسائل الجامعية:**

• آل ثنيـان، ثنيـان ناصـر. (٢٠١٢م). إثبـات الجريمـة الإلكترونيـة (دراسـة تأصيلية مقارنـة). رسالة ماجستير، جامعـة نايف العربية للعلوم الأمنية، الرياض، دولة المملكة العربية السعودية.

**ثالثاً: المجلات والبحوث العلمية:**

• أحمـد، أحمـد محمد عبـد المعبود أبو أسيـد. (٢٠١٩م). الجريمـة الإلكترونية وآلية مكافحتها في ظل القانون الدولي. مجلة البحوث القانونية والاقتصادية، العدد ٥٠.

• البداينــة، ذياب موســى. (٢٠١٤م). الجرائم الإلكترونية: المفهوم والأسباب. الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية.

• الحوامــدة، لورانــس سعيــد أحمــد. (٢٠١٧م). الجرائــم المعلوماتيــة أركانهــا وآلية مكافحتها: دراسة تحليلية مقارنة. مجلة الميزان للدراسات الإسلامية والقانونية، العدد ١.

• المعمري، مسعود بن حميد. (٢٠١٨م). الدليل الإلكتروني لإثبات الجريمة الإلكترونية. مجلة كلية القانون الكويتية العالمية، العدد ٣.

• المقصــودي، محمد بن أحمد بن علــي. (٢٠١٧م). الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونياً. المجلة العربية للدراسات الأمنية، العدد ٧٠.

• بطيــخ، حاتــم أحمد محمــد. (٢٠٢١م). تطور السياســة التشريعية في مجال مكافحة تقنية المعلومات: دراسة مقارنة. مجلة الدراسات القانونية والاقتصادية، العدد ١.

• ربيعــي، حســن. (٢٠١٥م). المجــرم المعلوماتــي: شخصيتــه وأصنافــه. مجلة العلوم الإنسانية، العدد ٤٠.

• عبــد الباقــي، مصطفــى. (٢٠١٨م). التحقيــق في الجريمــة الإلكترونيــة وإثباتها في فلسطين: دراسة مقارنة. مجلة دراسات علوم الشريعة والقانون، العدد ٢.

• عمري، محمد محمود. (٢٠١٦م). الإثبات الجزائي الإلكتروني في الجرائم المعلوماتية: دراسة مقارنة. مجلة العلوم القانونية والسياسية، العدد ٢.

**رابعاً: الأنظمة واللوائح:**

• قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥. (٢٠١٨م).

• نظــام مكافحــة جرائــم المعلوماتية الصــادر بالمرسوم الملكي رقــم م/١٧ . (٨ ٣، ١٤٢٨هـ).

**خامساً: الأحكام والقرارات:**

• مجلــة الأحكام القضائية صك رقــم: ٣٥١٦٥٩٣٢. (١٠ ٥، ١٤٣٥هـ.). مجلة الأحكام القضائيــة عام ١٤٣٥ هــ ، المجلد الثالث عشر، صك رقــم: ٣٥١٦٥٩٣٢، بتاريخ ١٣/٤/١٤٣٥هـ، وتم تأييد الحكم من محكمة الاستئناف بقرار رقم: ٣٥٢١١١٦٤،.

• مجلــة الأحكام القضائية، صك رقم: ٣٤٥٤٢٩١٩. (١١ ٤، ١٤٣٥هـ.). مجلة الأحكام القضائيــة ١٤٣٥هــ، المجلــد الثالــث عشر، صــك رقــم: ٣٤٥٤٢٩١٩، بتاريــخ ٢/٥/٤٣٥هـ، وتم تأييد الحكم من محكمة الاستئناف بقرار رقم: ٣٥٢٢٨٨٢٦.