Researcher Journal for Legal Sciences, ISSN: 5960-2706, Vol. 5, No. 2, December 2024, Pages 153-170
DOI: https:// doi.org/10.37940/JRLS.2024.5.2.9

Mechanisms for Obtaining Digital Evidence and Using It as Means of Proof in Cybercrimes

Noorhan Mhammed AlRubayee
Uruk University College of Law, Baghdad
norhanalrubayee3@gmail.com

Article Info.

Article Progress:

Received
4/8/2024

Accepted
13/11/2024

Publishing
10/12/2024

First Author
0009-0007-7921-2127

Abstract

With the rapid technological advancement and the emergence of cyberspace, cybercrimes have become a serious threat in the modern era. Perpetrators exploit modern electronic means such as the internet, fax, and other communication tools, which expands the scope of the crimes beyond national borders. These crimes characterized by innovation and evolution, which make it difficult to categorize them within traditional criminal descriptions. Legal bodies face challenges in tracking these crimes, as new technologies surpass the traditional capabilities and procedures. This situation requires updating the criminal laws to reflect legal accuracy and account for the dimensions of modern technology, as well as cooperating with international treaties to achieve justice.

Digital evidence is among the most important developments in contemporary criminal proof, as new technologies influence the process of criminal investigation. Crime-fighting entities find it challenging to apply traditional methods of proof due to the difficulties associated with examining data related to electronic means. These challenges require an update to traditional legal methods and the development of investigation procedures to adapt to the new difficulties in the realm of cybercrime.

Citation: Noorhan Mhammed AlRubayee, Mechanisms for Obtaining Digital Evidence and Using It as Means of Proof in Cybercrimes, Researcher Journal for Legal Sciences, ISSN: 5960 2706, Vol. 5, No. 2, December 2024, Pages 153-170.

Publisher: College of Law, University of Fallujah

Keywords: Digital evidence, Cybercrime, Means of proof.

آليات الحصول على الأدلة الرقمية واستخدامها كوسائل إثبات في الجرائم الإلكترونية

نورهان محمد الربيعي
كلية القانون جامعة اوروك\ بغداد
norhanalrubayee3@gmail.com

معلومات المقالة

تاريخ الاستلام
2024/8/4

تاريخ القبول
2024/11/13

تاريخ النشر
2024/12/10

الخلاصة

مع التقدم التكنولوجي السريع وظهور الفضاء الإلكتروني، أصبحت الجرائم الإلكترونية تهديدًا حقيقيًا في العصر الحديث. يستخدم مرتكبو هذه الجرائم وسائل إلكترونية مثل الإنترنت والفاكس ووسائل الاتصال الأخرى، مما يوسع نطاق الجرائم لتتجاوز الحدود الوطنية. تتميز هذه الجرائم بالابتكار والتطور، مما يجعل من الصعب إدراجها ضمن الأوصاف الجنائية التقليدية. تواجه الأجهزة القانونية تحديات في ملاحقة هذه الجرائم، حيث تتفوق التقنيات الحديثة على الإمكانات والإجراءات التقليدية. يتطلب هذا التطور تحديث القوانين الجنائية لتكون دقيقة وتعكس تأثير التكنولوجيا الحديثة، إضافة إلى التعاون مع المعاهدات الدولية لضمان تحقيق العدالة.

تعد الأدلة الرقمية من أهم التطورات في الإثبات الجنائي بالعصر الحديث، حيث تؤثر التقنيات الجديدة على عملية الإثبات. تواجه جهات مكافحة الجريمة صعوبة في استخدام الأساليب التقليدية للإثبات بسبب التحديات المرتبطة بفحص البيانات المتعلقة بالوسائل الإلكترونية. تتطلب هذه التحديات تطوير الأساليب القانونية التقليدية، وتحديث إجراءات البحث والتحقيق لمواجهة الجرائم الإلكترونية بفعالية.

الكلمات المفتاحية: الدليل الرقمي، الجرائم المعلوماتية، وسائل الاثبات.

كيفية الاستشهاد لهذا البحث باللغة العربية: نورهان محمد الربيعي، آليات الحصول على الأدلة الرقمية واستخدامها كوسائل إثبات في الجرائم الإلكترونية، *مجلة الباحث للعلوم القانونية*, م 5، عدد 2، 2024

1- مقدمة

تطورت الوسائل الإلكترونية بشكل كبير في العصر الحديث، مما أدى إلى تأثيرها الكبير على حياة المجتمعات والشعوب. فبفضل هذا التطور وانتشار الوسائل الإلكترونية في مختلف جوانب الحياة، أصبح بالإمكان للأفراد التعامل مع التكنولوجيا بسهولة، وذلك بفضل سهولة الوصول إليها واستخدامها. على الرغم من المزايا الكبيرة التي جلبتها هذه الوسائل والتي ساهمت في تطور البشرية في مختلف المجالات، إلا أن هناك استخدامًا سلبيًّا لهذه التكنولوجيا. فقد أدى انتشار الوسائط الإلكترونية إلى ظهور أنماط جديدة من الجرائم التي كانت غير معروفة في الماضي. وتمثلت هذه الجرائم فيما يعرف بالجرائم الإلكترونية، والتي أصبحت ترتكب عبر الوسائط الإلكترونية وتتطلب مهارات تقنية لارتكابها.

تعدُّ التكنولوجيا الرقمية وسيلة مثالية لارتكاب الجرائم بعيدًا عن أعين الأجهزة الأمنية، مما يسمح للمجرمين بالقيام بأعمال غير مشروعة دون مخاوف من العقاب. وتشكل هذه الجرائم خطرًا كبيرًا على الأمن الإلكتروني للمجتمعات، خاصة في المنطقة العربية بشكل عام وبعض الدول مثل العراق والإمارات العربية المتحدة بشكل خاص.

رغم الجهود التي تبذلها الدول لمواجهة هذه الجرائم ومكافحتها، إلا أنها ما زالت تشكل تحديًا كبيرًا نظرًا لتطورها المستمر وصعوبة إثباتها بشكل قانوني. لذلك، تأتي أهمية التشريعات الجزائية في مواجهة هذه الجرائم، حيث تحتاج الدول إلى تحديث قوانينها وتكنولوجيتها الجنائية لمواكبة التطورات السريعة في عالم التكنولوجيا الرقمية.

من هذا المنطلق، يأتي دور الأدلة الرقمية كأداة حاسمة في إثبات وقوع الجريمة ونسبتها إلى الفاعل، ولكن يجب أن تواكب هذه الأدلة التطورات التكنولوجية وتكون متوافقة مع القوانين والتشريعات الجديدة. من المهم أن تتخذ الدول إجراءات جادة لمواجهة هذا التحدي، بما في ذلك تحسين التشريعات الجزائية وتطوير القدرات التقنية للأجهزة القضائية، بالإضافة إلى تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.

وهكذا، يمكن أن تسهم الأدلة الرقمية بشكل كبير في تعزيز حرية القاضي الجزائي في اتخاذ قراراته بناءً على حقائق موضوعية ومتابعة للتطورات التكنولوجية. لهذا السبب، سأركز في هذا البحث على موضوع الإثبات الجنائي باستخدام الأدلة الرقمية، نظرًا لأهميتها الكبيرة، وسأعتمد المنهج المقارن كواحد من الأساليب المتبعة. وبناءً على ذلك، سنقوم بمقارنة عمليات الإثبات الجنائي باستخدام الأدلة الرقمية في التشريعات المتعلقة بجمهورية العراق ودولة الإمارات العربية المتحدة.

1-1. أهمية البحث:

في الوقت الحاضر، أصبحت دراسات الإثبات الجنائي بالأدلة الرقمية ذات أهمية بالغة نتيجة لزيادة الجرائم الإلكترونية واستخدام الأدلة الرقمية في التحقيقات. التطور التقني الحديث يفتح أفاقًا جديدة لأشكال جرائم جديدة تعتمد على التكنولوجيا الحديثة، مما يتطلب ابتكار وسائل جديدة للإثبات. يسهم تبادل المعرفة حول مكافحة جرائم المعلوماتية في وضع تشريعات مناسبة وتقديمها بكفاءة أمام المحاكم.

2-1. أهداف البحث:

يسعى البحث الى تحقيق الأهداف التالية:

1- توضيح مفهوم الأدلة الرقمية وأنواعها، مع إبراز خصائصها الفريدة.
2- بيان مدى أهمية الدليل الرقمي في إثبات الجرائم المعلوماتية.
3- كيف يمكن استخراج الدليل الرقمي لوصف دليل اثبات أمام القضاء.

3-1. مشكلة البحث:

في ظل التطور السريع في التكنولوجيا الرقمية وتزايد الاعتماد على الإنترنت في الحياة اليومية، ارتفعت وتيرة الجرائم الإلكترونية بشكل ملحوظ. هذه الجرائم تتطلب أساليب متطورة لجمع الأدلة الرقمية التي يمكن استخدامها كوسائل إثبات في المحاكم. ومع ذلك، يواجه المحققون وصناع القرار القانوني صعوبات عديدة تتعلق بآليات جمع هذه الأدلة، الحفاظ على سلامتها، وضمان قبولها في المحاكم. تكمن المشكلة الرئيسية في كيفية تطوير وتحسين آليات الحصول على الأدلة الرقمية بما يضمن فعاليتها كوسائل إثبات في الجرائم الإلكترونية، مع مراعاة الصعوبات القانونية والتقنية، وسيتم معالجة هذه الإشكالية على ضوء القانون العراقي والمقارن.

ويتفرع عن الإشكالية المذكورة التساؤلات التالية:

1. هل توجد صعوبات قانونية وتقنية تواجه جمع الأدلة الرقمية في الجرائم الإلكترونية؟
2. هل تستخدم أدوات برمجية وأجهزة معينة لاستخراج الأدلة من الأجهزة الرقمية؟
3. هل نص المشرع على الآليات والأساليب المتعلقة باستخراج الدليل الجنائي الرقمي؟
4. هل تحتاج النصوص المتعلقة باستخراج الدليل الجنائي الرقمي إلى تقنين صريح ومحدد؟

5. هل هناك آليات تعاون بين الجهات القانونية والتقنية لضمان جمع الأدلة الرقمية بشكل قانوني وفعّال؟

1-4. منهجية الدراسة:

نظرًا لطبيعة الدراسة ولغرض الوصول إلى تحقيق أهداف الدراسة، فإن الباحثة سوف تستخدم في هذا البحث منهجًا وصفيًّا تحليليًّا بالإضافة إلى المنهج المقارن، وذلك من خلال العمل على تحليل مفاهيم الدليل الجزائي الرقمي، و بيان خصائصه وانواعه، وكيفية استخلاص الدليل الجزائي الرقمي، وتحليل المضمون بالتطبيق على النصوص القانونية وهذا من خلال بحث عن موقف المشرع العراقي و الإماراتي من الدليل الجزائي الرقمي، ومن ثم تحليل هذا الموقف لبيان أوجه النقص به، حيث يعد هذا المنهج من المناهج المناسب لهذه الدراسة من خلال تناول مشكلة الدراسة ووضع الحلول العلاجية لها.

1-5. خطة البحث:

انطلاقًا من أهداف البحث، ومشكلة البحث، فقد تم تقسيم الدراسة على الاقسام الآتية:

2- ماهية الأدلة الرقمية

تمهيد وتقسيم :

نظرًا لكون الدليل الرقمي من بين الأدلة الجنائية التي ظهرت نتيجة لتطوّر الجريمة الإلكترونية، وبما أنه يشكل الوسيلة الرئيسية لإثبات هذه الجرائم، كان من الضروري فهم معنى الدليل الرقمي ومفهومه لتسهيل توضيح جميع الجوانب المتعلقة به. ولكي نعكس تميزه عن غيره من الأدلة الجنائية، يجب التركيز على خصائصه البارزة، يتسم الدليل الرقمي بالقدرة على توثيق الأنشطة الرقمية بدقة فائقة، مما يسهم في توفير صورة شاملة وموثوقة للأحداث. كما يتميز بقدرته على توفير سجلات دقيقة للتفاعلات عبر الإنترنت، وهذا يسهم في فحص وتحليل تفاصيل الجريمة بشكل شامل.

تعتبر الصفات التقنية المتقدمة للدليل الرقمي، مثل التوقيت الدقيق والتوقيع الرقمي، عناصر أساسية تعكس تفوقه التكنولوجي. يتيح الدليل الرقمي أيضًا التحقق من صحة البيانات وتأكيدها بشكل فوري، مما يعزز قوته كأداة قانونية فعّالة. وفي ظل تعدد تصنيفاته وأنواعه، يظهر أن تقدير قيمته القانونية يتوقف على القدرة على توظيفه بشكل فعّال لتحليل وتفسير الوقائع الجنائية بما يتناسب مع التصنيف الجنائي للجريمة المعنية.

وبناءً على ذلك، سنقوم في هذا المطلب بتوضيح مفهوم الأدلة الرقمية من خلال استعراض الفرعين التاليين:

2-1. تعريف الدليل الرقمي :

يُعدُّ مصطلح "الدليل الجنائي" من الألفاظ الرئيسية في ميدان القانون الجنائي، وذلك خاصةً عند الحديث عن مسألة الإثبات، حيث يعد ضروريًا لتوجيه التهمة إلى المتهم. ورغم أن فقهاء القانون الجنائي قد ناقشوا مصطلح الدليل الجنائي بتفصيل، إلا أنني اخترت التركيز على تفحص التعاريف بشكل تتابعي، مع العلم بأن الدليل الجنائي الرقمي يمثل فرعًا من فروع الدليل الجنائي، وهو أحد أشكاله. وبالتالي، يبدو غير مناسب التناول المفصل للفرع دون الرجوع إلى المصطلح الأساسي. ولكي نحقق هدف فهم الدليل الجنائي بشكل كامل، سيتم التركيز على التعريف المتعلق بالدليل وهذا كالآتي:

2-1/1. تعريف الدليل الجنائي اصطلاحًا:

"هو ما يلزم من العلم به علم الشيء آخر"، أي أن الدليل هو ما يمكن التوصل به إلى معرفة الحقيقة[1].

2-1/2. عريف الدليل الرقمي اصطلاحًا:

"هو ذبذبات أو نبضات إلكترونية مسجلة على وسائط أو دعائم مادية"، أو أنه " الدليل الذي تم الحصول عليه بوسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنيت والأجهزة الإلكترونية الملحقة والمتصلة به وشبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة"[2].

عرف المشرع الاماراتي وفق المادة الأولى من مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، دليل الجنائي الرقمي بأنه:

أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

(1) - أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، ج1، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية،1993، ص177.

(2) - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، ط1، دار الثقافة للنشر والتوزيع الأردن،2011، ص 230.

لم يقم المشرع العراقي بتعريف الدليل الرقمي بشكل صريح، وذلك بسبب عدم صدور قانون متخصص لمكافحة الشائعات والجرائم الإلكترونية حتى الآن. ولا يزال المشرع العراقي يؤجل إصدار قانون ينظم الجرائم المعلوماتية نتيجة الظروف الحالية التي تمر بها البلاد. ورغم تقديم مشروع قانون يتضمن 33 مادة إلى مجلس النواب، إلا أنه تم إلغاؤه بسبب الضغوط التي مارستها بعض النقابات الحزبية. يُعزى تأجيل هذا القانون إلى عدم مراعاة المعايير والمبادئ التشريعية اللازمة.

لكن هذا لا يعني أن الجرائم الإلكترونية لا تخضع للقانون، حيث يتم تطبيق القوانين التالية عليها:

1. **قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.**
2. **قانون أصول المحاكمات الجزائية رقم (23) لسنة 1971.**
3. **قانون الإثبات العراقي رقم (107) لسنة 1979**، حيث نصت المادة 27 منه على أن "البرقيات تعتبر ذات حجية كسندات عادية إذا كان أصلها المودع في مكتب الإصدار موقعًا من مرسلها."
4. **قانون المطبوعات رقم (206) لسنة 1968**، والذي ينظم الصحف والمجلات ويُستند عليه في ما ينشر على مواقع الإنترنت، بما في ذلك وسائل التواصل الاجتماعي.
5. **قانون مكافحة الإرهاب رقم (13) لسنة 2005**، حيث جرمت المادة الأولى منه "كل فعل إجرامي يطال الممتلكات العامة أو الخاصة أو يثير الرعب والخوف بأي وسيلة كانت"، بما في ذلك الجرائم الإرهابية الإلكترونية.

2-2. أنواع الأدلة الرقمية وخصائصها

وسائل الإثبات تأثرت بشكل كبير بثورة المعلومات والتكنولوجيا، حيث أدى التوافق المتنامي بين خصائص الدليل وطبيعة الجرائم إلى ظهور الدليل الرقمي. يتكون الدليل الرقمي من ثلاثة أنواع مختلفة: الأول يتضمن مخرجات ورقية تُسجل عليها المعلومات باستخدام الطابعات أو الرسمات، بما في ذلك طباعة الرسومات بدرجات وضوح مختلفة. النوع الثاني يتضمن مخرجات إلكترونية، مثل الأشرطة المغناطيسية والأوراق المغناطيسية، التي تُستخدم في تخزين المعلومات بدلًا من الوثائق الورقية.

أما النوع الثالث فيتضمن مخرجات مرئية يتم عرضها عبر شاشة الحاسوب، حيث يُعرض تلقائيا البيانات المعالجة آليا بواسطة الحاسوب.

يمكن تقسيم الدليل الرقمي إلى نوعين رئيسيين كدليل إثبات من عدمه: الأدلة التي أُعدت لتكون وسيلة إثبات، مثل السجلات التي تم إنشاؤها بشكل آلي أو جزء منها تم إدخاله بشكل يدوي، وأخر تم إنشاؤه بواسطة الآلة. وهناك أيضًا أدلة لم تكن مصممة لتكون وسيلة إثبات، حيث يتم إنشاؤها دون إرادة الفرد، وقد تتركها الجريمة دون قصد من الجاني.

1/2-2. أنواع الأدلة الرقمية:

تعددت أنواع الأدلة الرقمية بشكل كبير، مما فتح أمام المحققين فرصًا واسعة لاستخدامها في فهم السياق وبناء حالات تحقيق قوية. يعتبر فهم كيفية جمع وتحليل هذه الأدلة أمرًا حيويًا لتحقيق العدالة والكشف عن الحقائق الكامنة خلف الجرائم والأنشطة غير القانونية.

تظهر الأدلة الرقمية تنوعًا كبيرًا فيما يتعلق بالأنواع والتقسيمات، حيث لا تقتصر على واجهة واحدة فقط. يتم توفير الأدلة الرقمية عبر نظام إلكتروني حاسوبي، حيث يمكن أن يكون هذا النظام حاسوبًا آليًا أو وسيطًا إلكترونيًا آخر.

في سياق الجرائم الإلكترونية، تحدث الأفعال الإجرامية في بيئة غير مادية، حيث يتم استخدام أنظمة المعالجة الآلية. يمكن للمتسبب في هذه الجرائم التلاعب ببيانات الحاسوب وبرامجه في فترة زمنية قصيرة، وبالتالي يمكنه مسحها وتدميرها بسرعة، مما يؤدي إلى ظهور أدلة إثبات إلكترونية مختلفة.

تم تقسيم الأدلة الرقمية إلى قسمين، حيث يتمثل القسم الأول في تلك التي أُعدت لتكون وسيلة إثبات، بينما يشمل القسم الثاني تلك التي لم تعد صالحة كوسيلة.

1/1/2-2. أدلة أعدت لتكون دليل رقمي:

وفقًا لهذا التصنيف، تنقسم الأدلة الجنائية الرقمية إلى نوعين رئيسيين:

1- المعلومات والبيانات التي يتم إنشاؤها تلقائيًا بواسطة الحاسب الآلي:

يشمل هذا النوع من الأدلة جميع المعلومات والبيانات التي تُنتج تلقائيًا عبر الحاسب الآلي أو الأجهزة الإلكترونية الأخرى، دون تدخل مباشر من المستخدم[1]. وتتضمن هذه الأدلة السجلات الناتجة عن العمليات الآلية، مثل فواتير البطاقات البنكية التي تُصدر تلقائيًا وتحتوي على تفاصيل المعاملات المالية[2].

(1) - عبد الناصر محمد محمود فرغلي ،محمد عيد سيف سعيد المسماري ،الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية" دراسة مقارنة تطبيقية ، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف، الرياض في الفترة من 12-14\11\2007 ص 14.

(2) - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، مرجع سابق، ص234

بالإضافة إلى ذلك، تشمل الأدلة الجنائية الرقمية سجلات النظام، مثل سجلات الدخول والخروج، والسجلات الزمنية للتفاعلات بين المستخدمين والأجهزة، والبيانات التي يتم جمعها بواسطة أجهزة الاستشعار أو أنظمة الأمان. تُعتبر هذه المعلومات ذات أهمية كبيرة في التحقيقات الجنائية الرقمية، لأنها توثق كيفية استخدام الأنظمة والتطبيقات، مما قد يساعد في تحديد الأفراد المتورطين أو توضيح مجريات الأحداث

2- المعلومات والبيانات ذات الطبيعة المختلطة:

يتضمن هذا النوع من الأدلة البيانات التي يتم إدخال جزء منها يدويًا، بينما يتم إنشاء الجزء الآخر بواسطة الحاسب الآلي. على سبيل المثال، برنامج Excel حيث تُدخل البيانات يدويًا ويقوم الحاسب بمعالجتها تلقائيًا.

تكمن أهمية هذين النوعين من الأدلة في أنهما قد أُعدّا سلفًا ليُستخدما كوسائل لإثبات بعض الحقائق المتعلقة بالوقائع محل التحقيق. لذلك، من الضروري الحفاظ على هذه المعلومات والبيانات الرقمية لضمان إمكانية الاعتماد عليها كأدلة مستقبلية، مما يقلل من احتمالية فقدانها ويسهل الوصول إليها عند الحاجة [1].

2/1/2-2. أدلة لم تعد لتكون دليل رقمي:

هذا النوع من الأدلة الجنائية الرقمية يتكون بشكل تلقائي دون إرادة المستخدم أو رغبته في وجودها[2]. وتتجسد هذه الأدلة في الآثار التي يتركها المستخدم أثناء استخدامه للحاسب الآلي أو الإنترنت[3]،، حيث تتضمن جميع الأنشطة التي يقوم بها، بما في ذلك الرسائل المرسلة والمستقبلة.

من أمثلة هذه الأدلة: سجلات الدخول (Log Files) والبيانات المخزنة في ملفات النسخ الاحتياطي (Backup)، مثل تاريخ ووقت تحميل أو إرسال الملفات. كذلك، تشمل بيانات الكوكيز (Cookies) [4]التي تُسجل أثناء حدوث أخطاء في النظام[5]، بالإضافة إلى الأنشطة على وسائل التواصل الاجتماعي، مثل التعليقات والمشاركات، التي تُعد جزءًا من الأدلة الرقمية.

تُجمع هذه الأدلة حتى بعد مرور فترة زمنية باستخدام تقنيات وأدوات متخصصة في تحليل البيانات الجنائية (Digital Forensics Tools). رغم أن هذه العملية قد تكون معقدة وصعبة، إلا أن هناك تقنيات متقدمة مثل تحليل البيانات الضخمة (Big Data Analytics) التي تُسهم في تصفية وتحليل كميات هائلة من البيانات بسرعة.

تُعد هذه الأدلة ذات أهمية خاصة لأنها قد تحتوي على معلومات قيمة تُساعد في كشف الجريمة وتحديد مرتكبها. على سبيل المثال، يمكن استخدام سجلات الدخول لتحديد توقيت الأنشطة المشبوهة أو لتتبع حركة البيانات المرتبطة بالاختراقات الأمنية. كما أن ملفات النسخ الاحتياطي قد تكشف عن التعديلات التي أُجريت على الملفات، مما يساعد في إثبات الوقائع في القضايا القانونية.

اننا نرى على الرغم من التقسيمات السابقة للأدلة الرقمية وفقًا لمكان وجودها أو طريقة الحصول عليها، فإن هذه التقسيمات تُعد شكلية. فالقيمة القانونية للأدلة الرقمية أمام القضاء تعتمد بشكل أساسي على شرعية الإجراءات المستخدمة في جمعها ومدى قناعة القاضي بمصداقيتها.

2/2-2 خصائص الدليل الرقمي:

الدليل الرقمي يتميز بميزات تقنية تجعله سهل الوصول إليه وفعال في تقديم المعلومات. يُعد متاحًا على مدار الساعة، مما يسمح للمستخدمين بالوصول إليه بسهولة وسرعة، ويمكن تحديث محتواه بانتظام ليكون دقيقًا ومحدثًا. كما يتيح الوصول إليه بسهولة عبر الإنترنت أو الهواتف المحمولة، ويتميز بواجهة سهلة الاستخدام وإمكانية التفاعل مع المحتوى. يحرص على حماية بيانات المستخدمين ويسهل لهم حذف معلوماتهم بسلاسة.

1/2/2-2. **الدليل الرقمي دليل علمي ذو طبيعة تقنية:**

يُعَدُّ الدليل الرقمي دليلًا علميًا، حيث يتألف من معلومات إلكترونية غير ملموسة، تستمد من طبيعة تقنية المعلومات المُبنية على المفاهيم العلمية في مجال علوم الحاسوب وأدواته[6]. وتترتب على هذه الخاصية عدة نتائج:

1- للوصول إلى الدليل الرقمي وفهم مضمونه يتوجب استخدام أساليب علمية[1].

(1) - نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص 129.

(2) - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، مرجع سابق، ص234.

(3) - ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنيت، دار الكتب القانون،2006، ص95.

(4) - Linda Volonino and Reynaldo Anazaldua, Computer Forensics For Dummies, Wiley Publishing, United States of America, 2008, p 85.

(5) - The Technical Working Group for Electronic Crime Scene Investigation, Electronic Crime Scene Investigation, the national institute of justice, the United States of America, 2001, p 11.

(6) - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة ، الإسكندرية، 2010، ص 61.

2- ينطبق على الدليل الرقمي مبادئ وقواعد علمية مماثلة لتلك التي تسود الدليل العلمي. إذا كان الدليل العلمي ملتزمًا بمبدأ توافقه مع الحقيقة بموجب قاعدة "إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، فإن الدليل الرقمي يجب أن يلتزم بنفس المبادئ للحفاظ على قيمته وموثوقيته[2].

3- ينبغي أن تقوم عملية الاحتفاظ بالدليل الرقمي على أسس علمية[3].

4- يجب على القاضي أن يكون لديه المعرفة العلمية الكافية ليميز بين الجوانب القانونية والعلمية، وليحدد ما إذا كانت القضية تتطلب استشارة خبراء تقنيين متخصصين أم لا[4].

يُعَد الدليل الرقمي دليلًا تقنيًا، حيث يستند إلى مصادر في بيئة تقنية متنوعة، تتضمن وسائل تكنولوجيا المعلومات والاتصالات المتنوعة، مثل أجهزة الحواسيب الشخصية، والخوادم، والمضيفات، والهواتف النقالة، والشبكات.

2-2/2/2. الدليل الرقمي متنوع ومتطور ذو طبيعة ثنائيه:

الدليل الرقمي يشمل كافة أنواع البيانات التي يمكن تداولها رقميًا وترتبط بالجريمة والضحية[5]. يتكون من أرقام ثنائية (0 و1) تشمل نصوصًا وصورًا وصوتيات وفيديوهات[6]. بفضل الطبيعة المتطورة للفضاء الإلكتروني، يتوسع الدليل الرقمي باستمرار ليشمل مظاهر جديدة، مما يجعله أداة قوية للإدانة أو البراءة. يعتمد تكوين هذه البيانات الرقمية على النبضات والذبذبات المستمرة التي تعالجها الأجهزة المختلفة.

3- استخلاص الأدلة الرقمية ومشكلات التعامل معها

تمهيد وتقسيم:

بسبب خطورة الجريمة الإلكترونية وطبيعة بياناتها الرقمية، يصعب على الجاني القيام بأفعال جرمية دون ترك آثار، مما يجعلها صعبة الاكتشاف والاثبات. تتسبب هذه الصعوبة في مشاكل إجرائية أثناء التحقيق وأمام القضاء، حيث لا يمكن تطبيق الإجراءات التقليدية على الجرائم الإلكترونية الجديدة. لحل هذه المشاكل، وضع المشرع قواعد إجرائية خاصة بجمع الأدلة الرقمية التي يمكن من خلالها إثبات الجريمة أو براءة المتهم. يتضمن ذلك استخدام إجراءات استثنائية لاستنباط واستخلاص الأدلة الرقمية، مما يمكن القضاء من التعامل مع الصعوبات الفريدة التي تطرأ أثناء التحقيق في جرائم الحوسبة الإلكترونية.

ولذلك سنتناول في هذا المطلب استخلاص الأدلة الرقمية ومشكلات التعامل معها في الاقسام التاليين:

3-1. استخلاص الأدلة الرقمية

عملية استخلاص الأدلة الرقمية تستهدف جمع المعلومات والبيانات الرقمية من مصادر مختلفة، مثل الأجهزة الإلكترونية والخوادم وشبكات الاتصالات ووسائل التواصل الاجتماعي وأنظمة الحواسيب الأخرى. يهدف هذا النوع من الاستخلاص إلى استخراج معلومات تكون ذات قيمة في سياق التحقيقات القانونية أو التحليلية. في السياق القانوني، يتم استخدام الأدلة الرقمية لدعم قضايا مثل الجرائم الإلكترونية والاحتيال وانتهاكات الأمن والتزوير الإلكتروني، بالإضافة إلى القرصنة الرقمية. تعتمد عملية استخلاص الأدلة الرقمية على تقنيات تحليلية متقدمة لفهم البيانات وكشف الأنماط والاتجاهات وتقديم تفسيرات دقيقة.

تواجه هذه العملية تحديات مثل حجم البيانات الكبير ومسائل الخصوصية والأمان للبيانات الشخصية، إلى جانب ضرورة التكيف مع التطورات التكنولوجية المستمرة. في النهاية، يعد استخلاص الأدلة الرقمية جزءًا حيويًا في التحقيقات والعمليات القانونية في العصر الرقمي، حيث يساهم في كشف الحقائق وتحقيق العدالة بشكل شامل. **ولذلك سنتناول في هذا الفرع استخلاص الأدلة الرقمية كالتالي: .**

3-1/1. الوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية:

تقوم الوسائل الإجرائية الحديثة في جمع الأدلة الجنائية الرقمية بتطبيق مجموعة من الإجراءات لاستخراج الأدلة الرقمية ذات الصلة بتحقيق الجرائم[7].. تتنوع هذه الإجراءات بين أنماط ثابتة ومحددة مسبقًا، وأخرى قد تتغير أو تتعدد وفقًا للظروف الفردية لكل قضية. هدف هذه الوسائل هو تقديم دليل على وقوع الجريمة وتحديد هوية الجاني باستخدام تقنيات وبرامج إلكترونية متعددة. يتم تنفيذ هذه

(1) - حازم محمد حنفي ، الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، الطبعة الأولى،2017، ص16.

(2) - عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه في القانون الجنائي، كلية الحقد جامعة عين شمس، 2004 ، ص977.

(3)- فيصل عايش عيد المطيري، الوعاء القانوني للدليل التقني في إطار إثبات الجريمة الإلكترونية، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق، جامعة عين شمس، 2019، ص 128.

(4) - سامح أحمد بلتاجي، موسى الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة مقدمة لنيل درجة دكتوراه ، كلية الحقوق جامعة الإسكندرية 2010، ص378.

(5) - أميرة محمود بدوي الفقي، الإثبات الجنائي للجرائم المرتكبة عبر الإنترنت، رسالة مقدمة لنيل درجة دكتوراه، جامعة عين شمس 2013، ص 145.

(6) - فيصل عايش عيد المطيري، مرجع سابق، ص130.

(7) - ثنيان ناصر آل ثنيان ، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة مقدمة لنيل درجة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية ،2012، ص77.

الوسائل والإجراءات وفقًا للتشريعات واللوائح المعمول بها[1]، مع مراعاة إرادة المشرع في مكافحة الجرائم المعلوماتية، وحتى في مواجهة الجرائم التقليدية التي تتطلب استخدام هذه التقنيات والوسائل الحديثة.

3-1/1/1. برنامج اذن التفتيش(computer scorch warrant program) :

هو برنامج قاعدة بيانات يتيح إدخال جميع المعلومات الضرورية المطلوبة لترقيم الأدلة وتسجيل البيانات الخاصة بها. يستطيع هذا البرنامج إصدار إيصالات لاستلام الأدلة والبحث في قوائم الأدلة المحفوظة لتحديد موقع دليل معين أو تحديد ظروف ضبط هذا الدليل[2].

3-1/1/2. قرص بدء تشغيل الكمبيوتر(Bootable Diskette):

هو وسيلة يمكن للمحقق من خلالها تشغيل الكمبيوتر، خاصةً إذا كان نظام التشغيل محميًا بكلمة مرور، ويتطلب وجود برنامج "مضاعفة المساحة" (DoubleSpace) على القرص. قد يشير استخدام المتهم لهذا البرنامج إلى نية زيادة مساحة القرص الصلب[3].

3-1/1/3. برنامج معالجة الملفات(X tree pro Gold):

وهو برنامج يمكن المحقق من العثور على الملفات في اي مكان على الشبكة او على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم او الاقراص المرنة المضغوطة او يستخدم لقراءة البرامج في صورتها الاصلية، كما يمكن من البحث عن كلمات معينة او عن اسماء ملفات او غيرها.

3-1/1/4. برنامج النسخ(Lap Link) :

هذا البرنامج يمكن تشغيله من أقراص مرنة، ويسمح بنسخ البيانات من جهاز الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر، سواءً عبر منفذ التوازي (Parallel Port) أو منفذ التوالي (Serial Port). يعد هذا البرنامج أداة مفيدة للحصول على نسخة من البيانات قبل أي محاولة لتدميرها من قبل المتهم.[4].

3-1/1/5. **برامج كشف الدسك(AMA Disk, View Disk) :**

من خلال هذا البرنامج، يمكن الحصول على محتويات القرص المرن بغض النظر عن أساليب تهيئته. يتوفر البرنامج بنسختين، نسخة عامة متاحة للأفراد، ونسخة خاصة مخصصة للاستخدام من قبل الشرطة.

3-1/1/6. برامج اتصالات مثل(LAN tactic) :

البرنامج الذي يمكن تشغيله من أقراص مرنة يسمح للمحقق بربط جهازه بجهاز المتهم لنقل المعلومات إلى جهاز النسخ الاحتياطي، ثم إلى القرص الصلب[5]. جمع الأدلة الرقمية يمكن أن يكون تحديًا بسبب امتزاج المعلومات الجنائية بالمعلومات العادية، مما يعرض خصوصية المستخدمين الأبرياء للخطر. لذا، يقوم بعض مشغلي الأنظمة بعدم إفشاء السجلات إلا للمتورطين في قضايا قانونية، بناءً على أوامر قضائية.

3-1/2-1. صلاحيات الإجراءات التقليدية في جمع الأدلة الرقمية:

رغم التشابه بين التحقيق في الجرائم الإلكترونية والجرائم الأخرى من حيث الإجراءات الأساسية كالمعاينة والتفتيش والاستماع إلى الشهود، إلا أن الجرائم الإلكترونية تتميز بخصائص خاصة تتطلب تطوير أساليب التحقيق. يتعين على المحققين التكيف مع هذه الخصوصية من خلال الرجوع إلى سجلات مثل كتيبات أجهزة الحاسوب وملفات تخزين العمليات. وقد أدى ذلك إلى إنشاء فرق متخصصة في تقنيات المعلومات لمواجهة التحديات الجديدة. رغم التغيرات، تبقى الإجراءات التقليدية مثل المعاينة والتفتيش والحصول على الأدلة أساسًا في التحقيقات الجنائية.

3-1/1/2. المعاينة والتفتيش وضبط الأدلة الجنائية الرقمية

من الناحية الإجرائية، تشكل الإجراءات التقليدية مثل المعاينة والتفتيش أساس عمل أجهزة البحث والتحقيق. يهدف ذلك إلى الحصول على الأدلة الجنائية التي تثبت وقوع الجريمة، وضبط المتورطين بها لتقديمهم للمحاكمة. وسنتناول كل واحدة على النحو التالي:-

(1) - ثنيان ناصر آل ثنيان، مرجع سابق، ص78.
(2) - ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي مجلة كلية الحقوق جامعة النهرين، العراق، المجلد 18 ، العدد 2 ، 2016،ص202.
(3) - حسين طاهر داود، جرائم نظم المعلومات، اكاديمية نايف العربية للعلوم الامنية الرياض،2000،ص 287.
(4) - حسين طاهر داود، مرجع سابق، ص 288 وما بعدها.
(5) - ممدوح عبد الحميد، جرائم الكمبيوتر عبر الانترنت، إصدارات مكتبة الحقوق والشارقة، الامارات، 2000 ص 35 وما بعدها.

3-2-1/1/2-1. المعاينة:

"هي مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها بها الجاني"[1]، إذن تعتبر المعاينة وسيلة مهمة جدًّا لتكوين الفكرة الأولى عن كيفية ارتكاب الجريمة، بالإضافة إلى أنها تعد من أهم مصادر الأدلة الجنائية المادية ،ولكن هل يمكن أن نتصور القيام بإجراء معاينة في الجريمة المعلوماتية ؟.

أ- صلاحية المعاينة في كشف وضبط الدليل الجنائي الرقمي:

يعتقد البعض أن دور المعاينة يتضاءل في الكشف عن الجرائم الإلكترونية، وذلك لأن الجرائم التقليدية عادةً ما تحدث في مواقع تترك آثارًا مادية، مما يوفر فرصًا للجهات المعنية لفهم وتحليل الحدث وكشف غموضه. بالمقابل، في الجرائم الإلكترونية، يقل دور المعاينة بسبب نقص الآثار المادية، فضلًا عن إمكانية التلاعب عن بُعد بالأدلة الرقمية وتدميرها. وللتغلب على هذا التحدي، ينبغي على الفنيين المسؤولين عن المعاينة التعامل مع مسرح الجريمة المعلوماتية على أنه نوعان:

1. **المادي (المسرح التقليدي):** يتضمن جميع المكونات المادية لجهاز الحاسب الآلي، وقد يحتوي على آثار مادية مثل بصمات الجاني أو وسائط التخزين الرقمية أو مستندات ورقية[2].
2. **المسرح الافتراضي (الرقمي):** يقع في العالم الرقمي لجهاز الحاسب الآلي ويحتوي على جميع المعلومات والبيانات الرقمية المخزنة فيه، والتي قد تكون مفيدة في التحقيق.

ب- إجراءات المعاينة في العالم الافتراضي:

لضمان فعالية المعاينة في مسرح الجريمة المعلوماتية في الكشف عن ملابسات الجريمة، ينبغي مراعاة العديد من الإجراءات والخطوات الفنية، بعضها يجب أن يتم قبل إجراء المعاينة، وبعضها بعده[3].

1- الإجراءات والخطوات الفنية المتخذة قبل القيام بإجراء المعاينة:

عادة ما تكون هذه الإجراءات والخطوات تحضرية، غرضها تهيئة الوسائل البشرية والمادية للقيام بإجراء المعاينة، ويتم ذلك بإعداد خطة عمل تحتوي على إعداد شامل للأدوات المستعملة في المعاينة، وتقسيم المهام بين الفنيين القائمين على هذا الإجراء، بالإضافة إلى توفير معلومات مسبقة عن مكان الجريمة وعن نوع وعدد الأجهزة المراد معاينتها، وذلك لتحديد إمكانيات التعامل معها فنيًّا من حيث الضبط والتأمين وحفظ المعلومات، وتأمين التيار الكهربائي تجنبًا لتلفها ، كما أنه يجب في هذا المرحلة توفير الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل وفك التشفير.

2- الإجراءات والخطوات الفنية المتخذة أثناء القيام بإجراء المعاينة:

بعد القيام بالإجراءات التحضيرية التي سبق ذكرها، يقوم الفنيون القائمون على إجراء المعاينة بتصوير جهاز الحاسب الآلي وكافة مكوناته المادية ، مع التركيز على تصوير الخلفية له ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة زيادة على ذلك، القيام بملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل ملحقات الحاسب الآلي، وأيضا التحفظ على محتويات سلة المهملات من الاوراق الملقاة أو الممزقة، وكذا الشرائط والأقراص المضغوطة وفحصها[4].

بعد ذلك يتم البحث في جهاز الحاسب الآلي بعد تشغيله عن الآثار الرقمية التي خلفها المستخدم، وذلك باستعمال كافة الوسائل التقنية كالدخول إلى السجلات والملفات، وفي هذه المرحلة يجب تعطيل حركة الاتصالات السلكية واللاسلكية بشبكة الإنترنت تجنبًا لتلف الدليل الجنائي الرقمي أو التلاعب به وتخريبه عمدًا عن بعد، وفي حالة ضبط معلومات أو بيانات رقمية، يجب مراعاة قواعد تحريز الأدلة الجنائية الرقمية، والتي تتطلب تخزينها عناية فائقة للدعائم مادية وفحصها واستعمالها لاحقا.

3-2-1/1/2-2. التفتيش:

يعتبر التفتيش من بين الإجراءات التحقيقية الرئيسية التي تسهم في كشف الحقيقة، حيث غالبًا ما تؤدي إلى توفر أدلة مادية تدعم توجيه الاتهام للمشتبه به، فيعرف التفتيش بصفة عامة بأنه: " بحث في الخصوصية الشخصية يعد دليلًا هامًا في كشف الجرائم، أو هو البحث عن الدليل" [5]، وعرف أيضا بأنه: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون

(1) - خالد ممدوح ابراهيم، الجرائم المعلوماتية، مرجع سابق، ص 149.
(2) - عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص314.
(3) - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة) مقارنة)، الطبعة الأولى، دار الفكر الجامعي، مصر ، 2007،ص217.
(4) - خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية مصر، ط1، 2009، ص 173.
(5) - عبد الله أوهايبة، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، الطبعة الرابعة، دار هومة، الجزائر، 2013،ص266.

للتفتيش سند من القانون" [1]، إذن يتضح أن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط أشياء مادية تتعلق بالجريمة، وتفيد في كشف حقيقتها، إلا أن ذلك يتنافر مع الطبيعة غير المادية للدليل الجنائي الرقمي[2] .

1- مدى خضوع أنظمة الحاسب الآلي للتفتيش:

والتفتيش واحد من الأنظمة الإجرائية إن لم يكن أهمها، وتختص به سلطة التحقيق، وقد أجاز مرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية لمأمور الضبط القضائي تفتيش المتهم، وقد نصت المادة (52) على أنه: "لمأمور الضبط القضائي أن يفتش المتهم في الأحوال التي يجوز فيها قانونًا القبض عليه، ويجرى تفتيش المتهم بالبحث عما يكون بجسمه أو ملابسه أو أمتعته من آثار أو أشياء تتعلق بالجريمة أو تكون لازمة التحقيق فيها"، وقد أحسن المشرع الإماراتي صنعًا بوضع كلمة "أشياء "بنص المادة حتى تشمل ما يستحدث من أدوات ووسائل اتصال جديدة وتقنيات حديثة تمثل أدلة أو تحتوي عليها وتدل على الجريمة ومرتكبها مثل أجهزة الحاسوب والأقراص الصلبة والأسطوانات والديسكات وبرمجيات الاختراق وتحليل الشفرات وكلمات المرور وغيرها من البيانات والمعلومات المخزنة على الحاسوب. ويشترط بالتفتيش لغرض الحصول على الأدلة الرقمية أن يكون بصدد جريمة معلوماتية وقعت فعلًا[3] ، فلا يصح أن يكون التفتيش بهدف ضبط جريمة مستقبلية وكذلك لا يجوز التفتيش دون إذن من النيابة في غير حالات التلبس، وهذا ما نصت عليه أحكام المادة (54) مرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية بأنه: " لا يجوز لمأمور الضبط القضائي تفتيش منزل المتهم بغير إذن كتابي من النيابة العامة ما لم تكن الجريمة متلبس بها وتتوفر أمارات قوية على أن المتهم يخفي ففي منزله أشياء أو أوراق تفيد كشف الحقيقة، ويتم تفتيش منزل المتهم وضبط الأشياء والأوراق على النحو المبين بهذا القانون، كما يتم البحث عن الأشياء والأوراق المطلوب ضبطها في جميع أجزاء المنزل وملحقاته ومحتوياته"، ومعنى هذا أنه ولإضفاء المشروعية[4]،على الدليل الرقمي يجب أن يكون قد وجد في التفتيش بشكل مشروع، أي أنه إما نتيجة التفتيش بإذن من النيابة أو كان التفتيش في حالة التلبس أثناء التفتيش عن جريمة أخرى، فحينها يقوم رجل الضبط بالجريمة أو ظهر الدليل الرقمي عرضًا الجنائي بضبط الدليل، ويمكن أن يطول التفتيش ذات المتهم أو أحد المتواجدين بمحل التفتيش، إذ يمكن إخفاء ذاكرة محمولة أو جهاز تخزين خارجي أو اسطوانة أو هاتف أو أية أداة يشتبه باحتوائها على بيانات قد تحتوي على أدلة رقمية تدين المتهم، وقد نصت المادة (57) من المرسوم بقانون في سبيل ذلك على أنه: "إذا قامت أثناء تفتيش منزل المتهم قرائن قوية ضده أو ضد شخص موجود فيه على أنه يخفي معه شيئا يفيد في كشف الحقيقة جاز لمأمور الضبط القضائي أن يفتشه".

أما في جمهورية العراق فإنه و بالرجوع إلى القواعد العامة في قانون أصول المحاكمات الجزائية فإننا لا نرى أن مسألة تفتيش المكونات المادية للحاسب الآلي تمثل عقبة تعترض التفتيش في جرائم الإنترنت ذلك أن المادة (74) من القانون المذكور قد أجازت لقاضي التحقيق "إذا تراءى له وجود أشياء أو أوراق تفيد التحقيق لدى شخص ...." وبذلك فالمادة تجيز تفتيش مكونات الحاسب الآلي المادية كونها تدخل تحت حكم هذه المادة، أما فيما يتعلق بالمكونات المنطقية فأرى أنها لا تدخل تحت حكم المادة المذكورة لذا أقترح تعديل نص المادة المذكورة وذلك بإضافة (معطيات إلكترونية) لنص المادة (74) وبذلك يصبح النص" إذا تراءى لقاضي التحقيق وجود أشياء أو معطيات إلكترونية أو أوراق تفيد التحقيق...

نرى أنه يمكن الاعتماد على الأدلة الرقمية لإثبات وقوع الجريمة، سواء تم تقديمها بصيغة رقمية أو ورقية. في هذا السياق، يمكن استخدام الأدلة الرقمية، بغض النظر عن الشكل الذي تُقدم به—إلكترونيًا أو ورقيًا لأغراض التحقيق الجنائي وإثبات الجريمة المزعومة. وقد أقر المشرع العراقي هذا الرأي في مشروع قانون جرائم المعلوماتية لعام 2011، حيث سمح بتقديم الأدلة الرقمية أمام المحكمة على شكل نسخ إلكترونية أو ورقية.

وقد قضت محكمة جنح الحلة بإدانة المتهم (خ. ج) بعد ان قام بأرسال رساله الى هاتف المشتكية (أ .م) تتضمن عبارات لاأخلاقية ثم توالت الرسائل بعد ذلك حتى بلغت 18 عشر رسالة حيث امر القاضي بإحضار عائديه الرقم من قبل شركة زين وتفريغ الرسائل المرسلة من قبل الرقم العائد للمتهم بعد ان قام بأرسال رسائل من شانها ازعاج المجنى عليها (س.ع) والاخذ بها كدليل ضد المتهم.

2- مدى خضوع شبكات الحاسب الآلي للتفتيش:

لا شك أن الطبيعة التقنية الرقمية قد زادت من التحديات التي تواجه القائمين على التفتيش والضبط في الجرائم المعلوماتية. فقد تتوزع البيانات التي تحتوي على أدلة عبر شبكات الحاسب الآلي في مواقع قد تكون بعيدة عن المكان الفعلي الذي يتم فيه التفتيش. كما يمكن أن

(1) - خالد ممدوح إبراهيم، الجرائم المعلوماتية ، مرجع سابق،ص182.
(2) - خالد عباد الحلبي، مرجع سابق ، ص157.
(3) - أحمد عبد اللاه هلالي: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2006 م، ص73.
(4) - علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004م،ص184.

يكون الموقع الفعلي للبيانات والمعلومات ضمن الاختصاص القضائي لدولة أخرى، مما يُعقِّد من عملية التفتيش وضبط الأدلة الجنائية الرقمية[1]:

استنادًا إلى ذلك، يمكن تمييز احتمالين في تفتيش شبكات الحاسب الآلي:

الصورة الأولى: تتعلق بتفتيش المكونات المادية لجهاز الحاسب الآلي. تشمل هذه المكونات مجموعة من الوحدات المتصلة التي تعمل كنظام متكامل، مثل وحدات الإدخال (كالفأرة ولوحة المفاتيح) ووحدات الإخراج (كشاشة الحاسب الآلي والطابعة) ووحدة الذاكرة[2]. في هذه الحالة، لا تواجه فرق التفتيش صعوبات في المعاينة، نظرًا لعدم وجود تعارض بين تفتيش المكونات المادية لجهاز الحاسب الآلي ومفهوم التفتيش التقليدي، إذ إنه يمثل بحثًا عن الأدلة المادية. كل ما يتطلبه التفتيش في هذه الحالة هو الالتزام بالقواعد القانونية المتعلقة بالتفتيش[3].

الصورة الثانية : تتعلق بتفتيش المكونات المعنوية لجهاز الحاسب الآلي، وهي عبارة عن مجموعة من البرامج والأساليب المرتبطة بتشغيل وحدة معالجة البيانات. تنقسم هذه المكونات إلى كيانات أساسية تضم البرامج الضرورية لتشغيل جهاز الحاسب الآلي، وكيانات تطبيقية تتيح للمستخدم تنفيذ مهام معينة. وقد أثار هذا النوع من التفتيش جدلًا فقهيًا حول إمكانية تفتيش المكونات المعنوية. حيث اعتبر بعض الفقهاء أن الهدف من التفتيش، وهو ضبط الأدلة المادية، يمتد ليشمل جميع المعلومات والبيانات الرقمية بصورها المختلفة. ومن جهة أخرى، يرى البعض الآخر أن المفهوم المادي لا ينطبق على البيانات غير المحسوسة (المعنوية) لجهاز الحاسب الآلي، مما يستدعي ضرورة النص صراحة على أن تفتيش الحاسب الآلي يجب أن يشمل البيانات المعالجة من خلاله أو بياناته [4].

3-2/1/2. الشهادة والخبرة

تُعَدّ الشهادة والخبرة جزءًا أساسيًا من إجراءات التحقيق، حيث تؤديان دورًا محوريًا في جمع الأدلة المتعلقة بالجريمة. سنستعرض في الفقرة الأولى مفهوم الشهادة، وفي الفقرة الثانية سنتناول أهمية الخبرة التقنية في العالم الرقمي.

3-2/1/2-1. الشهادة:

عرف بعض الفقهاء الشهادة بأنها: "إخبار الشخص عما رآه أو سمعه بنفسه أو أدركه بالحواس". وفي سياق الجرائم الإلكترونية[5]، يتم تعريف الشاهد بأنه "الشخص المتخصص الذي يمتلك خبرة في المعلوماتية وتخصص دقيق في علم الحاسب الآلي"، حيث يُطلق على هذا النوع من الشهود "الشاهد المعلوماتي" لتمييزه عن الشاهد التقليدي. تشمل فئات الشهود في الجرائم الإلكترونية ما يلي[6].

المسؤول عن تشغيل الحاسب الآلي :يتولى هذا الشخص مسؤولية تشغيل الأنظمة الحاسوبية بفاعلية، ويجب أن يتمتع بخبرة كافية في استخدام الحاسب، بالإضافة إلى معرفة بقواعد كتابة البيانات وبرمجة الأنظمة[7].

1. **المبرمجون** :ينقسم هؤلاء على فئتين:
   - الفئة الأولى: تخطط لبرامج التطبيقات وتحدد السمات المطلوبة للنظام.
   - الفئة الثانية: مسؤولة عن تخطيط برامج النظم، واختيار، وتعديل، وتصحيح البرامج الداخلية.
2. **مهندسو الصيانة والاتصالات** :يقومون بأعمال صيانة تقنيات الحاسوب ومكوناته، وكذلك الشبكات المرتبطة بها.
3. **المحللون** : يتولون تحليل بيانات نظم معينة إلى وحدات مفصلة، ويقومون بتتبع البيانات داخل النظام.
4. **مدراء النظم** : هم المعنيون بإدارة النظم الإلكترونية.
5. **طاقم عمليات البيانات** : يتعاملون مع البيانات التي يمكن قراءتها بواسطة الحاسوب.
6. **مهندس الصيانة الإلكترونية** : يضمن صيانة الجهاز الأصلي وتأكد من عمله بكفاءة.

يتعين على الشاهد المعلوماتي في الجرائم الإلكترونية تقديم المعلومات الأساسية التي تسهم في كشف الجريمة، وتثار هنا مسألة مهمة: هل يُلزَم الشاهد بطباعة الملفات أو الإفصاح عن كلمات المرور؟

هناك رأيان متباينان:

الرأي الأول :يؤكد على عدم التزام الشاهد، وفقًا للالتزامات التقليدية، بطباعة ملفات البيانات أو الإفصاح عن كلمات المرور، مشيرًا إلى الفقه الألماني الذي يستند إلى فكرة أن الالتزام بالشهادة لا يشمل ذلك[8].

(1) - عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق،ص378.
(2) - بكرى بوسف بكرى ،التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، مصر،2011، ص 67.
(3) - خالد عياد الحلبي، مرجع سابق، ص158.
(4) - خالد ممدوح إبراهيم، الجرائم المعلوماتية ،مرجع سابق،ص197.
(5) - مراد فلاك، آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية، مجلة الفكر القانوني و السياسي، العدد 5 المجلد 2019،ص216.
(6) - عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي(دراسة مقارنة)، مرجع سابق، ص80.
(7) - فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق جمعة عين شمس، مصر،2012،ص447.
(8) - فهد عبد الله العبيد العازمي، مرجع سابق، ص 448 ما بعدها.

الرأي الثاني :يرى أن الشاهد ملزم بطباعة الملفات وكلمات المرور، مستندًا إلى الفقه الفرنسي الذي يؤكد على ضرورة الالتزام بتقديم الشهادة[1].

3-2/1/2-2. الخبرة:

تُعَدّ الخبرة الوسيلة التي من خلالها تتمكن النيابة العامة أو القضاء من تفسير الأدلة بشكل فني باستخدام المعلومات العلمية. فهي ليست دليلًا مستقلًا، بل هي تقييم فني للأدلة الموجودة. ما يميز الخبرة هو الرأي الفني للخبير في تقييم الأدلة، ويتطلب معرفة علمية أو فنية لا تتوفر لدى المحقق أو القاضي[2].

تظهر تساؤلات حول إمكانية الاعتماد على الخبرة في التحقيقات الخاصة بجرائم الإنترنت، خاصةً مع التحديات الناتجة عن حداثة العالم الرقمي. ومع ذلك، من الضروري التأكيد على أهمية الاعتماد على الخبرة التقنية المتاحة.

تتعدد أنواع الخبرة التقنية، وأبرزها[3]:

1. **الخبرة الخاصة** :تنشأ من رغبة المؤسسات في تحقيق فرص تنافسية، حيث تسعى الشركات الكبرى إلى توظيف الأشخاص المتميزين في مجال تكنولوجيا المعلومات[4].
2. **المؤسسات التعليمية** :تمثل مصدر دعم شامل لمواجهة الجرائم الرقمية، مثل جامعة ستانفورد ومعهد ماساتشوستس للتكنولوجيا، حيث يقومون بتطوير معرفة لمواجهة التحديات الإلكترونية. [5].
3. **مأمور الضبط القضائي** :بدأت بعض الدول، مثل الولايات المتحدة، في إنشاء أجهزة متخصصة لمواجهة الجرائم الإلكترونية، مع إنشاء المعامل الإقليمية الخاصة بالتحقيقات الرقمية.

يجب على الخبير التقني استخدام الأساليب العلمية خلال عمله، دون أن تتمكن المحكمة من رفض هذه الطرق إلا لأسباب منطقية.

هناك أسلوبان لعمل الخبير التقني.

1. **تجميع المواقع التي تمثل جرائم** :مثل التهديد أو النصب، ثم تحليلها لمعرفة طريقة إعدادها البرمجي[6].
2. **تجميع البيانات التي لا تشكل جريمة** :ولكنها قد تؤدي إلى أفعال جنائية، مثل المواقع التي تقدم معلومات حول كيفية زراعة المخدرات أو صنع القنابل[7].

كما يحق للخبير الاطلاع على شهادات الجناة، حيث يمكن أن تكون هناك عناصر مساعدة في فهم أسلوب ارتكاب الجريمة، وقد شهد الكونغرس الأمريكي شهادات من هاكرز بارزين لتسليط الضوء على كيفية ارتكاب الاختراقات.

3-2. مشكلات التعامل بالأدلة الرقمية:

المشكلات في مكافحة الجريمة الرقمية تتجاوز الحدود الوطنية، حيث يصعب توحيد التشريعات الوطنية والتعاون الدولي. والتعقيدات في تحديد الجهات المختصة والتأخير في العمليات التحقيقية يزيدان من فرص وقوع الجرائم الرقمية. ينبغي إيجاد توازن بين الأمان السيبراني وحقوق الأفراد.

استنادًا إلى ذلك سنعرض في هذا الفرع مشكلات التعامل بالأدلة الرقمية بشكل مفصل ضمن القسمين التاليين:

3-2-1. مشكلات الأدلة الرقمية على المستوى الداخلي:

3-2-1/1. مشكلات المتعلقة بالدليل ذاته:

الدليل الرقمي يعد جزءًا أساسيًا من بنية التكنولوجيا الحديثة، ومع ذلك، يواجه العديد من الصعوبات والمشكلات[8]، من بين هذه المشكلات، وسأتناول أهمها فيما يلي:

المشكلة الأولى: هذه المشكلة تتمثل في صعوبة تحديد هوية الجاني في الجرائم الرقمية وارتباطه بالبيانات المستخدمة كدليل. من الصعب تحديد العلاقة بين الأدلة الرقمية والشخص الذي ارتكب الجريمة، خاصةً عندما يتم ارتكاب الجريمة باستخدام أجهزة حاسوب في أماكن عامة حيث يمكن للآخرين استخدام نفس الأجهزة. يُعقد الأمر أكثر عندما يتعلق الأمر بأجهزة الحواسيب الشخصية، حيث يُمكن

(1) - محمد، عادل ريان، جرائم الحاسوب وأمن البيانات، مجلة العربي، العدد ،440 يوليو ،2002 وزارة الإعلام الكويتية،ص58.
(2) - سامي جلال فقي حسين، الأدلة المتصلة من الحاسب وحجيتها في الاثبات، دار الكتب القانونية، 2012 ، ص114.
(3) - سامي جلال ففي حسين، مرجع سابق ، ص115.
(4) - مراد فلاك، مرجع سابق، ص 214.
(5) - محمد عبد الباسط عبد العزيز حبيب، آليات الحصول على الأدلة الجنائية الرقمية كوسيلة إثبات في الجرائم، بحث مقبول النشر في مجلة الباحث القانونية، العدد 48، نوفمبر2022،ص569.
(6) - سامي جلال فقي حسين، مرجع سابق، ص115.
(7) - محمد عبد الباسط عبد العزيز حبيب، مرجع سابق، ص572.
(8) - عمر السعيد رمضان، مبادئ قانون الاجراءات الجنائية، الجزء الأول، ودار النهضة العربية والقاهرة، ص278.

للمتهم ادعاء أن شخصًا آخر استخدم جهازه لارتكاب الجريمة. لا يعد استخدام عنوان بروتوكول الإنترنت دليلًا حاسمًا على هوية الجاني، وقد يكون الجهاز أو العنوان مسروقًا أو مزورًا.

لتجاوز هذه الصعوبات، يتعين على جهات التحقيق البحث عن أدلة مادية مثل الاعترافات أو الشهادات التي تُساعد في تأكيد هوية الجاني وربطه بارتكاب الجريمة. يجب أن يتم التحقق من الأدلة الرقمية وتقديم الأدلة التقليدية بشكل متزامن، والاعتماد على كل منها لتحقيق العدالة[1].

الأمثلة الواقعية لما تقدم [2]. تقدمت الشرطة بتهمة لشخص متهم بشن هجوم إلكتروني على موقع إنترنت لميناء هيوستن في الولايات المتحدة في 20 سبتمبر 2001. تسبب الهجوم في تعطيل العمليات في الميناء، مما أدى إلى توقف الشحن والتفريغ. أثناء المحاكمة أقر المتهم بأنه جزء من جماعة قامت باختراق أجهزة حاسب أصدقائه لاختبار أمانها، لكنه نفى بشدة مسؤوليته عن الهجوم على موقع الميناء. زعم أن جهازه تم اختراقه بواسطة برنامج حصان طروادة دون علمه، واستخدم لتنفيذ الهجوم دون موافقته.

المحكمة طلبت فحصًا فنيًا لجهازه، حيث لم يتم العثور على أي دليل على وجود برنامج حصان طروادة. بالرغم من ذلك، استندت الدفاع إلى خصائص البرنامج، والتي تتضمن قدرته على محو آثار وجوده بعد فترة من الزمن. بناءً على ذلك، قررت هيئة المحلفين براءة المتهم من التهم الموجهة إليه[3].

هذه الحادثة ليست الوحيدة التي استندت فيها المحاكم البريطانية إلى وجود برنامج حصان طروادة كدفاع في قضايا جنائية. في يوليو 2003، تمت تبرئة شخص آخر من تهمة حيازة صور فاضحة للأطفال، بعدما اكتشف الخبراء وجود برامج حصان طروادة على جهاز حاسبه، واستند الدفاع إلى احتمالية أن يكون تم تحميل الصور دون علمه بسبب هذه البرامج[4].

نرى أنه في الحالات التي تفتقر فيها الدلائل الرقمية، يمكن اللجوء إلى وسائل إثبات تقليدية مثل شهادات الشهود أو القرائن الأخرى لتحديد هوية الجاني وتأكيد تورطه في الجريمة.

المشكلة الثانية: مع تعقيد شبكة الإنترنت التي لا تلتزم بحدود جغرافية تقليدية، يصبح تحديد موقع الجاني في جرائم الإنترنت أمرًا صعبًا. يظهر القضاء الإلكتروني كعالم منفصل لا يتأثر بالحدود الجغرافية التقليدية، مما يجعل تحديد موقع الجاني ذو أهمية بالغة في سياق جرائم الإنترنت.

من المهم أن يلتزم القضاء الوطني بقواعد الاختصاص القضائي والتعاون الدولي في مكافحة الجرائم الإلكترونية. يجب على السلطات القضائية مراعاة حقوق المتهمين وشروط التفتيش عند جمع الأدلة، وضمان قانونية تقديم الأدلة أثناء المحاكمة.

عند ارتكاب الجريمة خارج حدود دولة معينة، يجب على السلطات القضائية احترام القوانين الدولية والقيود المفروضة على التحقيق عبر الحدود. من الأمثلة الواقعية، في عام 2001، قام روسيان بشن هجمات إلكترونية على بنوك أمريكية، وبفضل التحقيقات تم استدراجهما إلى الولايات المتحدة ومحاكمتهما[5]. وفي حالات أخرى، مثل حالة فيروس "Love bug" عام 2000، كان تحديد الجاني صعبًا بسبب عدم وجود قوانين لجرائم الإنترنت في الفلبين، مما حال دون محاكمته بتهم الإتلاف.

ومن الأمثلة الواضحة لتلك الحالة في 4 مايو عام 2000، تم نشر فيروس إلكتروني يُعرف باسم "Love bug" عبر رسائل البريد الإلكتروني، مما أسفر عن هجوم على حوالي 45 مليون جهاز حاسوب في عشرين دولة حول العالم. سبب هذا الهجوم تدمير البيانات والمعلومات الشخصية، وتسبب في أضرار قدرت بحوالي 2 بليون دولار.

قام مكتب التحقيقات الفيدرالية الأمريكي بتتبع مصدر الفيروس، وتبين أنه تم نشره من دولة الفلبين، وكان وراء هذا الفعل طالب دراسات في علوم الحاسب الآلي. على الرغم من ذلك، فشلت جهود المكتب في ملاحقة الجاني قضائيًا وتقديمه للمحاكمة، نظرًا لعدم وجود قوانين لجرائم الإنترنت في الفلبين آنذاك.

تم محاكمة الجاني محليًا بتهمة السرقة والنصب، حيث كان الهدف من الفيروس الحصول على الأرقام السرية لبطاقات الائتمان واستخدامها في شراء بعض السلع. وعلى الرغم من ذلك، لم تتم معاقبته على اختراق وإتلاف أجهزة وشبكات الحاسوب حول العالم، ولم

(1) - شادي محمد عدره، الحماية الجنائية للمعلومات الشخصية الكتاب الثاني، الأحكام الإجرائية، المركز العربي للنشر والتوزيع، ط1، 2023، ص221.

(2)- Susan W. Brenner, Brian Carrier, and Jef Henninger, The Trojan Horse Defense in Cybercrime Cases, Santa Clara High Ttechnology Law Journal, Volume 21, Issue 1, 2004, Available online on 19/12/2023 at the following website: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1370 &context=chtlj

(3) - The Editors of Encyclopedia Britannica, "Trojan horse", Available online on 19/12/2023 at the following website: https://www.britannica.com/topic/Trojan-horse

(4)- Susan W. Brenner, Brian Carrier, and Jef Henninger, The Trojan Horse Defense in Cybercrime Cases, op. cit., p. 7

(5) - شادي محمد عدره، مرجع سابق، ص223.

تستطع السلطات الأمريكية طلب محاكمته بتهمة إتلاف أنظمة التشغيل في الولايات المتحدة الأمريكية، بسبب عدم تصنيف الفعل كجريمة وفقًا لقوانين الفلبين في ذلك الوقت[1].

المشكلة الثالثة: تتعلق هذه المشكلة بصعوبة تحليل البيانات المستمدة من الدليل الرقمي:

تتعلق هذه المشكلة بضخامة حجم المعلومات التي يتعين على جهة التحقيق أو الخبير تحليلها، سواء كانت مخزنة في أجهزة الحاسوب الخاصة بالمتهم أو ذات صلة بمكان الحادث. عندما يقوم رجال الشرطة أو سلطات التحقيق بتفريغ تلك البيانات، يصبح الأمر معقدًا للغاية حتى في حال استعانتهم بخبير[2]. وتزداد هذه الصعوبة مع تقدم تلك الوسائل التكنولوجية وزيادة قدرتها على تخزين المعلومات بأشكالها المتنوعة.

بالإضافة إلى ذلك، تنبع من هذه المشكلة مسألة تكلفة الحصول على الدليل الرقمي، حيث تتطلب هذه العملية تحميل كلفة باهظة، خاصةً في الأنظمة القانونية التي تسمح بالاعتماد على شركات متخصصة في فحص البيانات الإلكترونية لإنتاج الدليل الرقمي[3]. تتناسب تكلفة الحصول على هذا الدليل بشكل كبير مع مستوى كفاءة وتخصص الخبير، بالإضافة إلى حجم البيانات الإلكترونية التي يتعين فحصها.

على سبيل المثال، في الولايات المتحدة الأمريكية، وصلت الرسوم التي فُرضت على خبير في إحدى القضايا إلى خمسين ألف دولار، بعد أن قام بمراجعة ثلاثين مليون صفحة رقمية على أحد أجهزة الحاسوب.

المشكلة الرابعة: تتعلق هذه المشكلة بسهولة التلاعب في الدليل الرقمي: تتعلق هذه المشكلة بسهولة التلاعب في الدليل الرقمي نظرًا لطبيعته، حيث يتم تسجيل البيانات على وسائل تقنية المعلومات، مما يسهل على الجاني مسحها أو تعديلها في لحظات قليلة. وعلى الرغم من ذلك[4]، يظل من الصعب للغاية التخلص من الدليل الرقمي أو حتى حذفه بشكل نهائي من الوسيلة، حتى في حال استخدام خاصية حذف الملفات المتاحة في أنظمة تشغيل تلك الوسيلة. يمكن استعادة جميع البيانات والملفات التي قام الجاني بحذفها باستخدام برامج متخصصة، مما يجعل عملية الحذف غير فعالة.

3-2-1/2. صعوبات مصدرها نقص الخبرة الفنية لدى سلطات العدالة:

نقص الخبرة الفنية في سلطات الاستدلال والتحقيق والمحاكمة يشكل عقبة رئيسية في الحصول على الدليل الرقمي وحفظه، مما يؤثر بشكل كبير على قدرتهم على إثبات جرائم تقنية المعلومات[5]. يتطلب التعامل مع هذه الجرائم وأدلتها الرقمية مستوى عالٍ من الخبرة في تقنية المعلومات والاتصالات، وتقنيات جمع الأدلة والتحقيق في بيئة الاتصالات والمعلوماتية[6].

قد تفشل أجهزة إنفاذ القانون في فهم أهمية هذه الجرائم بسبب قلة خبرتها وتدريبها، مما يؤدي إلى عدم بذل الجهود الكافية لكشفها وضبط مرتكبيها[7]. بعض الصعوبات تشمل تدمير الدليل الرقمي بسبب الخطأ في التعامل معه، وصعوبة استخراج الدليل بسبب استخدام تقنيات حماية المعلومات مثل التشفير وكلمات السر.

للتغلب على هذه الصعوبات، يجب على العاملين في مجال مكافحة جرائم تقنية المعلومات أن يكونوا مؤهلين ومدربين بشكل مستمر في مجال تقنية المعلومات، بما في ذلك تكوين الأنظمة والبرامج واستخراج الدليل الرقمي. يجب عليهم أيضًا فهم شبكة الإنترنت وكيفية استخدامها في ارتكاب جرائم تقنية المعلومات، وتحديد الجهاز المتصل بها لتحديد الجاني [8]. تلك المتطلبات مهمة خاصة مع وجود مجرمين محترفين يتمتعون بمستوى عالٍ من المعرفة والخبرة في البيئة الإلكترونية[9].

---

(1) - محمد عبد الفتاح عبد المقصود علي، القواعد الإجرائية للجرائم التي تقع عبر شبكة الإنترنيت، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة طنطا، 2015، ص175.

(2) - ايمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي دراسة مقارنة، رسالة مقدمة لنيل درجة الدكتوراه، كلية الدراسات العليا، أكاديمية الشرطة،2003، ص392.

(3) - شادي محمد عدره، مرجع سابق، ص225.

(4) - القاضي رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الطبعة الثانية الإسكندرية 2018، ص65.

(5) - محمد ممدوح بدير، مكافحة الجريمة المعلوماتية الطبيعية الاول الانترنت والاستدلال كوسيلة لإنبات الجريمة المرتكبة عبر الإنترنت، دراسة مقارنة، الطبعة الأولى، مركز الدراسات العربة للنشر والتوزيع، الجيزة 2019، ص 171.

(6) - حاتم أحمد محمد، دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، دراسة مقارنة. رسالة مقدمة لنيل دكتوراه، كلية الحقوق جامعة عين شمس، 2017، ص 511.

(7) - محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة جرائم نظم الاتصالات والمعلومات دراسة مقارنة في التشريع المصري والفرنسي والأمريكي والاتفاقيات الدولية والإقليمية، الكتاب الثاني المكتب الجامعي الحديث، الإسكندرية 2018، ص306.

(8) -جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، أجهزة الرادار - الحاسبات الآلية البصمة الوراثية، دراسة مقارنة، دار النهضة العربية، 2002، ص 117.

(9) - طه السيد أحمد الرشيدي، مدى المواجهة التشريعية لجرائم المعلومات في النظام الجزائي المصري والسعودي، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، 2016، ص 30.

3-2-2. مشكلات الأدلة الرقمية على المستوى الدولي:

إذا كان التعاون الدولي يشكل العنصر الأساسي والركيزة الأولى في التصدي للجرائم المعلوماتية، نظرًا لارتباطها غالبًا بأماكن متعددة حول العالم واستخدام تقنيات حديثة، فإن هذا التعاون يواجه صعوبات وعقبات عدة، ولتجاوز هذه الصعوبات والقضاء عليها، يتعين بذل المزيد من الجهود واتخاذ إجراءات فعّالة.

3-2-1/2. القصور التشريعي للدول والتعارض بين مصالحها:

اختلاف الأنظمة القانونية بين الدول يعد عائقًا كبيرًا يحول دون التعاون الفعّال في مجال مكافحة الجرائم المعلوماتية. ينبع هذا الاختلاف من تعقيدات في تطبيق القوانين وتنفيذها على أرض الواقع، مما يؤدي إلى عدم وضوح تعريفات الجرائم المعلوماتية وغياب أنظمة قانونية موحدة لمواجهتها، وبالتالي يصعّب التعاون الدولي في هذا المجال[1].

عند استعراض الأنظمة القانونية في العديد من الدول لمواجهة الصعوبات المتعلقة بالجرائم المعلوماتية، يظهر عدم وجود اتفاق عام بين الدول حول تجريم أنماط معينة من سوء استخدام نظم المعلومات والإنترنت. فما قد يكون مسموحًا في نظام قانوني معين قد يُعد جريمة في نظام آخر، وذلك بسبب اختلاف البيئات والعادات والتقاليد والديانات والثقافات بين المجتمعات[2].

التنوع في التعاريف والمفاهيم القانونية المتعلقة بالجرائم المعلوماتية ينعكس سلبًا على إجراءات التعاون الدولي. عدم التوافق على تحديد جميع الجرائم المعلوماتية التي تشكل تهديدًا لأمن واقتصاد الدول يؤثر سلبًا على صانعي القرار في مختلف المجالات، خاصة السياسية والاقتصادية[3]. كما يعوق القصور التشريعي الداخلي للدول وضع نظام قانوني خاص بالجرائم المعلوماتية، مما يعيق التعاون الدولي في مواجهتها. التعارض في المصالح الدولية يضع عقبات أمام سبل التعاون، حيث تولي كل دولة اهتماماتها أولوية حتى لو تعارضت مع مصلحة دولة أخرى، مما يؤثر على قدرة الدول على التعاون في مجال العدالة الجنائية وتنفيذ القوانين[4].

3-2-2/2. تنوع واختلاف النظم القانونية الإجرائية:

بسبب تنوع واختلاف الأنظمة القانونية الإجرائية، يصبح من الواضح أن الأساليب المستخدمة في التحقيق والمحاكمة، والتي قد تثبت فاعليتها في إحدى الدول، قد تكون غير فعالة أو غير مقبولة في دولة أخرى. على سبيل المثال، قد تمنع بعض الدول ممارسة الرصد الإلكتروني والتسليم المراقب[5] ، والإجراءات السرية، وغيرها من الأساليب ذات الصلة. إذا تم اعتبار طريقة ما لجمع الأدلة أو التحقيق قانونية في إحدى الدول، قد تكون هذه الطريقة غير قانونية في دولة أخرى. وبالتالي، قد تشعر الدولة الأولى بخيبة الأمل بسبب عدم قدرة سلطات إنفاذ القانون في الدولة الثانية على استخدامها كأداة فعالة. بالإضافة إلى ذلك، قد لا تسمح السلطات القضائية في الدولة الثانية باستخدام أي دليل، حتى وإن كان قد تم الحصول عليه بشكل قانوني في اختصاص قضائي. يظهر هذا الواقع عدم وجود تنسيق بين الدول المختلفة فيما يتعلق بالإجراءات الجنائية المتبعة لمكافحة جرائم المعلومات، سواء كان ذلك يتعلق بأعمال الاستدلال، التحقيق، أو المحاكمة[6].

3-2-3/2. تنازع الاختصاص القضائي الدولي:

الاختصاص القضائي هو سلطة القضاء للنظر في القضايا واتخاذ القرارات بموجب القوانين المعمول بها. في سياق الجرائم المعلوماتية، يمكن أن تحدث تحديات كبيرة بسبب طبيعة هذه الجرائم التي تتجاوز الحدود الوطنية وتتعلق بشبكات عالمية. يُعد تحديد الاختصاص القضائي في هذه الحالات أمرًا معقدًا، حيث يمكن أن تنشأ صراعات بين الدول بشأن مكان محاكمة المتهم وتطبيق العقوبات[7].

-(1) سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة مقدمة لنيل درجة دكتوراه، كلية حقوق جامعة الإسكندرية،2010م ،ص538.

(2) - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة،2002 م، ص 102 \ مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الطبعة الأولى، 2006 م، ص 142 وما بعدها.

(3) - هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، الطبعة الأولى، 2006،ص529.

(4) - هشام عبد العزيز مبارك، مرجع السابق، ص536.

(5) - وهي وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يقوم مراقب إلكتروني، يتمثل في مأمور ضبط قضائي ذي كفاءة تقنية عالية، تتماشى مع نوع الجريمة التي يتعامل معها، مستخدماً في ذلك التقنية الإلكترونية وعبر شبكة الإنترنت، كأن يراقب أحد الهكرة ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه، أو يقوم بإعداد صندوق بريد إلكتروني مستنسخ لمراقبة المشتبه فيه عند إرساله أو استقباله لصور داعرة للأطفال عبر الإنترنت، ينظر: د. مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب والوثائق القومية المصرية، 2004 م، ص 4.

(6) - حسين بن سعيد الغافري، السياسية الجنائية في مواجهة جرائم الإنترنت، رسالة مقدمة لنيل درجة دكتوراه ، كلية الحقوق، جامعة عين شمس، 2007 م،ص550 وما بعدها.

(7) - محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، 1988م، ص 823.

تتنوع تلك الصعوبات بين تنازعات الاختصاص الإيجابي والسلبي. في التنازع الإيجابي، يُطالب متهم بالمحاكمة في أكثر من دولة، بينما في التنازع السلبي، يمكن أن ترفض الدولتان محاكمة المتهم بناءً على عدم وجود اختصاص[1]..

تعتبر الحالات المعقدة، مثل الجرائم المعلوماتية التي تؤثر على دول متعددة، تحديًا خاصًّا للقانون الدولي. يجب أن تتعاون الدول معًا لوضع إجراءات وآليات لمواجهة هذه الصعوبات، مما يتطلب تبادل المعلومات والتعاون القضائي الدولي بشكل فعّال.

بما أن الجرائم المعلوماتية تزداد تعقيدًا وتأثيرًا على الساحة الدولية، فإنه من الضروري وجود إطار قانوني دولي يوضح الاختصاص القضائي ويساهم في التعاون بين الدول لمكافحة هذه الجرائم بفعالية وعدالة.

3-2-2/4. صعوبات الخاصة بالإنابة القضائية الدولية:

من صعوبات والمشكلات التي تواجه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية والتي تتعلق بالإنابة القضائية الدولية، يبرز ما يُعرف بإشكالية فكرة السيادة وإشكالية البطء في الإجراءات.

أولا: إشكالية فكرة السيادة:

فكرة السيادة تعني أن الدولة هي السلطة العليا في إدارة شؤونها الداخلية والخارجية، وتمتلك الاختصاصات الكاملة دون تدخل من جهات خارجية، وتتمتع بالاستقلالية التامة في اتخاذ القرارات وتطبيقها[2].

عندما يُرتكب فرد جريمة معلوماتية في دولة ما وتحاكمه في دولة أخرى، يتطلب التعاون القضائي بين الدول بحثًا عن الأدلة التي تثبت الجريمة أو تبرئ منها في البلد الأصلي للحادث. ورغم أهمية هذا التعاون، إلا أنه قد يواجه صعوبات بسبب مفهوم السيادة الوطنية، حيث تفضل الدول الاعتماد على نظمها القضائية الوطنية لحل النزاعات[3]. بالتالي، يمكن أن يكون التوازن بين التعاون القضائي ومفهوم السيادة تحديًا في مكافحة الجرائم العابرة للحدود[4].

ثانيًا: إشكالية البطء في إجراءات الإنابة:

يتطلب الحصول على طلبات الإنابة القضائية في إطار الإجراءات القانونية الدولية إجراءات تسليم بواسطة القنوات الدبلوماسية، وغالبًا ما يتسبب هذا النهج في بطء وتعقيد العملية. يتعارض هذا التباطؤ مع الطبيعة السريعة للعمل عبر الإنترنت، مما يضعف جهود التعاون الدولي في مجال مكافحة الجرائم الإلكترونية. بالإضافة إلى ذلك، يُعد التأخر في الرد أيضًا من بين الصعوبات، حيث غالبًا ما تتأخر الدولة المستلمة للطلب في الرد عليه، سواء بسبب نقص الموظفين المسؤولين، أو بسبب الصعوبات اللغوية، أو بسبب الفروقات في الإجراءات التي تعيق الاستجابة، وهناك أسباب أخرى كذلك.[5].

وهذا ما وضحته المادة 44 من قانون الإمارات الاتحادي رقم (39) لسنة 2006 في شأن التعاون القضائي الدولي في المسائل الجنائية والتي نصت على " يقدم طلب المساعدة القضائية من السلطة المختصة في الجهة القضائية الأجنبية إلى السلطة المركزية بالدولة بالطريق الدبلوماسي.وتقوم السلطة المركزية بعد دراسة طلب المساعدة القضائية والتأكد من استيفائه شروطه الشكلية بإحالته إلى السلطة القضائية المختصة لاتخاذ اللازم بشأنه" .

وأيضًا، بينت المادة 353 من قانون أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 آلية استخدام الإنابة القضائية حيث نصت على "إذا رغبت إحدى الدول الأجنبية في اتخاذ إجراء من إجراءات التحقيق في جريمة ما بواسطة السلطات القضائية في العراق فعليها أن ترسل طلبًا بذلك بالطرق الدبلوماسية إلى وزارة العدل ويجب أن يكون الطلب مصحوبًا بيان وافٍ عن ظروف الجريمة وأدلة الاتهام فيها والنصوص القانونية المنطبقة عليها وتحديد دقيق للإجراء المطلوب اتخاذه".

4-. الخاتمة

لا شك أن استخدام الدليل الرقمي كأداة للإثبات في المسائل الجزائية هو موضوع مهم يتطلب الاهتمام، حيث يتزايد أهميته نتيجة للتطورات المستمرة في هذا المجال. تعتبر أدوات استخلاص الدليل الرقمي من أجهزة الحاسوب الآلي جزءًا لا يتجزأ من هذا التطور. على الرغم من تقدم الدليل الرقمي وارتفاع قيمته العلمية والتقنية في الإثبات، إلا أن دوره لا يكتمل إلا بوجود سلطة تقديرية قضائية تستطيع تنقية الدليل الرقمي من أي أخطاء أو محاولات للتلاعب. هذا يؤكد على أهمية السلطة التقديرية في تحويل الحقيقة العلمية إلى حقيقة قانونية. الباحثة اختارت تحليل آليات الحصول على الأدلة الرقمية واستخدامها كوسائل إثبات في الجرائم الإلكترونية في تشريعات

(1) - جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002 م،ص42.
(2) - محمد سامي عبد الحميد، محمد السعيد الرقاق، التنظيم الدولي، دار المطبوعات الجامعية، الإسكندرية، 2002م، ص 153.
(3) - أمين عبد الرحمن محمود عباس، الإنابة القضائية في مجال الاجراءات الجزائية، دار الفكر الجامعي، الإسكندرية، 2000م،ص188.
(4) - عبد الرحيم صدقي، التعاون الدولي الجنائي، بحث مقبول النشر في المجلة المصرية للقانون الدولي، عدد 40 عام 1980م، ص 1.
(5) - حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة ، رسالة مقدمة لنيل درجة دكتوراه، حقوق ، جامعة عين شمس، 2007م،ص553

دولة الإمارات العربية المتحدة وجمهورية العراق، خاصةً أن التشريع الجنائي لم يناقش بشكل محدد قواعد الإثبات بالدليل الرقمي. ونتيجة لذلك، قامت بتوظيف القواعد العامة للإثبات وبالمرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية وأصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971 غيرها من القوانين ذات الصلة كأساس لتنظيم استخدام الدليل الرقمي في الدراسة بأكملها.

وقد خرجت الباحثة بجملة من النتائج والتوصيات، التي قد تشكل فائدة قانونية وتشريعية نستعرضها على النحو الآتي:

4-1. استنتاج البحث:

1. إن الإثبات يشكل أساسًا حيويًا لعمليات التحقيق القانونية، حيث يبدأ الأمر بوقوع الجريمة ويستمر حتى تقديم القضية إلى المحكمة. وبموجب القوانين، لا يمكن للنيابة تقديم القضية إلى المحكمة ما لم يكن لديها السندات والأدلة اللازمة والمقبولة قانونًا.
2. تطور الجريمة ليشمل الواقع الإلكتروني قد أدى إلى ظهور أدلة جديدة تسمى الدليل الرقمي. هذه الأدلة أصبحت مقبولة ومعترف بها بشكل رسمي وفي إطار تشريعي في الإثبات العام بدولة الإمارات والعراق.
3. الدليل الرقمي هو مجموعة من البيانات المخزنة بشكل كهرومغناطيسي على الأقراص الصلبة في أجهزة الحاسوب أو على شبكات المعلومات. يتم استخراج هذا الدليل بواسطة إجراءات فنية معينة تحكمها إجراءات قانونية، بهدف ترجمة هذه البيانات وتقديمها كدليل إثبات لنفي أو إثبات فعل معين ينسب إلى صاحبه.
4. من خلال البحث، تبين أن الطبيعة القانونية للأدلة الرقمية في التشريع العراقي تعتبر قرينة قضائية تُستخدم للاستدلال على الجريمة المرتكبة. ومع ذلك، لا يمكن اعتبار هذه القرينة دليلًا قاطعًا في القضايا الجزائية، نظرًا لإمكانية التلاعب بها من خلال أفعال مادية ترتبط بجريمة التلاعب بالمعلومات الرقمية، مثل الإدخال أو التعديل أو الحذف، مما قد يعيق الوصول إلى الحقيقة.
5. يجب أن يكون الدليل الرقمي موثوقًا به، ويتم الحصول عليه بطرق قانونية، ويُقدم للمحكمة بالشكل الذي تم جمعه عليه، دون تغيير أو تحريف خلال فترة الحفظ، وذلك نظرًا لتطورات التكنولوجيا في مجال المعلوماتية.
6. دور الدليل الرقمي ليس مقتصرًا على إثبات الجرائم المعلوماتية فحسب، بل قد يُستخدم أحيانًا لإثبات جرائم أخرى تشمل استخدام الحاسوب كوسيلة لارتكابها.
7. يجب أن يكون دليل الإثبات وخصوصًا الدليل الرقمي مشروعًا لضمان توافر حجيته القانونية، وتظهر مشروعيته في قسمين. الأول يتعلق بوجود الدليل الإلكتروني نفسه، بينما الثاني يتمثل في مشروعية استخلاصه وتحقيقه.
8. اختلاف الأنظمة القانونية بين الدول يعد تحديًا كبيرًا يعترض الطريق أمام التعاون الدولي في مجال مكافحة الجرائم المعلوماتية. ينجم هذا الاختلاف عن صعوبات في تطبيق القانون ومشاكل عملية، كما أنه يتسبب في عدم وضوح تعريفات الجرائم المعلوماتية وفي قصور الأنظمة التشريعية عن وضع نظام قانوني مخصص لتلك الجرائم. هذا الوضع يجعل التعاون الدولي أمرًا صعبًا وغير فعال.

4-2. المقترحات:

وبعد ان تعرضنا لأبرز الاستنتاجات التي توصلت اليها الباحثة توصي ب:

1- إعداد قانون مختص بتنظيم وإثبات الأدلة الرقمية، وتنظيم عمليات استخراجها من الأنظمة الرقمية بواسطة أدوات مشروعة، وتحديد الجهات المسؤولة عن تنفيذ هذا القانون، بالإضافة إلى تحديد الشروط الضرورية للحصول على الدليل الرقمي.

2- ندعو المشرع العراقي إلى إعادة النظر في قانون أصول المحاكمات الجزائية، حيث إن نصوص هذا القانون صُممت للتعامل مع الإجراءات المتعلقة بالجرائم والأدلة التقليدية التي لا تواجه تحديات كبيرة في إثباتها أو التحقق من صحتها. ومع ظهور أدلة ذات طبيعة مختلفة، وهي الأدلة الرقمية، أصبحت هذه الأدلة عرضة للتلاعب بمختلف أشكاله.

3- إدراج مفردات قانونية تركز على دراسة المجال الرقمي أو الإلكتروني بشقيه الموضوعي والإجرائي، بهدف تأهيل كوادر متخصصة تلعب دورًا فاعلًا في المجالين القضائي والفني.

4- نوصي بالانتقال إلى استخدام بروتوكول الإنترنت IPv6 بدلًا من الإصدار السابق IPv4، مع التركيز على تعزيز الأمان لعناوين IP لحمايتها من التزييف أو الاختراق، حيث تعتبر هذه العناوين أداة حيوية في الإثبات.

5- ينبغي فحص كل ما يتم وضعه في سلة المهملات على الجهاز وجمع البصمات التي قد تكون دليلًا على المتهم، بالإضافة إلى ضرورة الاحتفاظ بجميع الوثائق المتعلقة بالنشاطات الداخلية والخارجية التي قد تكون لها علاقة بالجريمة.

6- تعزيز التعاون والتنسيق بين السلطات القضائية وشركات الاتصالات المزودة بخدمات الاتصالات السلكية واللاسلكية وشبكة الإنترنت، من خلال تقديم جميع المعلومات ذات الصلة التي تسهم في التحقيقات.

7- تدريب الخبراء المحققين وتوجيه القضاة حول كيفية التعامل مع الأدلة الرقمية للحد من الجرائم الإلكترونية يعد أمرًا ضروريًا.

5-. المراجع

5-1. الكتب العامة:

- أمين عبد الرحمن محمود عباس، الإنابة القضائية في مجال الاجراءات الجزائية، دار الفكر الجامعي، الإسكندرية، 2000.
- أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، ج1، دار النشر بالمركز العربي للدراسات الأمنية والتدريب، السعودية،1993.
- محمد بن يعقوب الفيروز آبادي ، القاموس المحيط ، ج 1، 2010.
- محمد سامي عبد الحميد، محمد السعيد الرقاق، التنظيم الدولي، دار المطبوعات الجامعية، الإسكندرية، 2002.
- هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، الطبعة الأولى، 2006.

5-2. الكتب الخاصة:

- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، أجهزة الرادار - الحاسبات الآلية البصمة الوراثية، دراسة مقارنة، دار النهضة العربية، 2002.
- جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، 2002
- حازم محمد حنفي ،الدليل الإلكتروني ودوره في المجال الجنائي، دار النهضة العربية، الطبعة الأولى،2017.
- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، ط1، دار الثقافة للنشر والتوزيع الأردن،2011.
- القاضي رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية دراسة تحليلية مقارنة، المكتب الجامعي الحديث، الطبعة الثانية الإسكندرية 2018.
- شادي محمد عدره، الحماية الجنائية للمعلومات الشخصية الكتاب الثاني، الأحكام الإجرائية، المركز العربي للنشر والتوزيع، ط1، 2023.
- طه السيد أحمد الرشيدي، مدى المواجهة التشريعية لجرائم المعلومات في النظام الجزائي المصري والسعودي، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، 2016.
- عمر السعيد رمضان، مبادئ قانون الاجراءات الجنائية، الجزء الأول، ودار النهضة العربية والقاهرة.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة،2002 م، ص 102 \ مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الطبعة الأولى، 2006 .
- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة ، الإسكندرية، 2010.
- محمد علي سويلم، شرح قانون جرائم تقنية المعلومات (القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات) دراسة مقارنة، دار المطبوعات الجامعية، الطبعة الأولى، الإسكندرية، 2019.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنيت، دار الكتب القانون،2006.
- ممدوح عبد الحميد، جرائم الكمبيوتر عبر الانترنت، إصدارات مكتبة الحقوق والشارقة، الامارات، 2000.
- محمد ممدوح بدير، مكافحة الجريمة المعلوماتية الطبيعية الاول الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت، دراسة مقارنة، الطبعة الأولى، مركز الدراسات العربة للنشر والتوزيع، الجيزة 2019.
- محمود محمد محمود جابر، الأحكام الإجرائية للجرائم الناشئة عن استخدام الهواتف النقالة جرائم نظم الاتصالات والمعلومات دراسة مقارنة في التشريع المصري والفرنسي والأمريكي والاتفاقيات الدولية والإقليمية، الكتاب الثاني المكتب الجامعي الحديث، الإسكندرية 2018.
- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة بين المراقبة الأمنية التقليدية والإلكترونية، دار الكتب والوثائق القومية المصرية، 2004 م.

5-3. الرسائل والأبحاث والندوات العلمية:

- أميرة محمود بدوي الفقي، الإثبات الجنائي للجرائم المرتكبة عبر الإنترنت، رسالة مقدمة لنيل درجة دكتوراه، جامعة عين شمس 2013.
- ايمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي دراسة مقارنة، رسالة مقدمة لنيل درجة الدكتوراه، كلية الدراسات العليا، أكاديمية الشرطة،2003.
- ثنيان ناصر آل ثنيان ، إثبات الجريمة الإلكترونية (دراسة تأصيلية تطبيقية)، رسالة مقدمة لنيل درجة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية ،2012.
- حاتم أحمد محمد ، دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، دراسة مقارنة. رسالة مقدمة لنيل دكتوراه، كلية الحقوق جامعة عين شمس، 2017.
- حارث عاصم داود، المخاطر الأمنية في بروتوكول الإنترنت الإصدار السادس IPv6، المجلة العربية الدولية للمعلوماتية، المجلد الثاني، العدد الرابع، جامعة نايف العربية للعلوم الأمنية، السعودية، 2013.
- حسين طاهر داود، جرائم نظم المعلومات، اكاديمية نايف العربية للعلوم الامنية الرياض،2000.

- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة ، رسالة مقدمة لنيل درجة دكتوراه، حقوق ، جامعة عين شمس، 2007.
- عبد الرحيم صدقي، التعاون الدولي الجنائي، بحث مقبول النشر في المجلة المصرية للقانون الدولي، عدد 40 عام 1980.
- خالد عايد جاسم العنزي الجرائم الإلكترونية وتأثيرها على الاقتصاد القومي، دراسة مقارنة، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق جامعة القاهرة 2018.
- خالد عايد جاسم العنزي الجرائم الإلكترونية وتأثيرها على الاقتصاد القومي، دراسة مقارنة، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق جامعة القاهرة 2018.
- سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الإنترنت، رسالة مقدمة لنيل درجة دكتوراه، كلية حقوق جامعة الإسكندرية،2010.
- سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة مقدمة لنيل درجة الماجستير، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية،2003.
- سمير شبلاق، حجية الدليل الرقمي في الكشف عن الجريمة، رسالة مقدمة لنيل درجة ماجستير كلية الحقوق والعلوم السياسية، جامعة سعيدة، جزائر، 2020.
- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، رسالة دكتوراه في القانون الجنائي، كلية الحقد جامعة عين شمس، 2004.
- عبد الناصر محمد محمود فرغلي ،محمد عيد سيف سعيد المسماري ،الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية" دراسة مقارنة تطبيقية ، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي جامعة نايف، الرياض في الفترة من 12-14\11\2007.
- طاهري عبد المطلب ، الإثبات الجنائي بالأدلة الرقمية، رسالة لنيل درجة ماجستير، كلية الحقوق جامعة مسلية، جزائر،2015 .
- فيصل عايش عيد المطيري، الوعاء القانوني للدليل التقني في إطار إثبات الجريمة الإلكترونية، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق، جامعة عين شمس، 2019.
- محمد عبد الفتاح عبد المقصود علي، القواعد الإجرائية للجرائم التي تقع عبر شبكة الإنترنيت، رسالة مقدمة لنيل درجة الدكتوراه، كلية الحقوق، جامعة طنطا، 2015.
- ميسون خلف حمد الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي مجلة كلية الحقوق جامعة النهرين، العراق، المجلد 18 ، العدد 2 ، 2016.
- محمد فوزي إبراهيم حسن، دور مأمور الضبط القضائي في الحصول على الدليل الإلكتروني، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد (66) ، الجزء الأول، أغسطس 2018.
- يوسف سعيد محمد الكلباني، الحماية الجزائية للبيانات الإلكترونية في التشريعين العماني والمصري دراسة مقارنة، رسالة مقدمة لنيل درجة دكتوراه، كلية الحقوق، جامعة عين شمس 2016.

5-4. الكتب الإنجليزية:

- Debra Littlejohn Shinder. Scene of the Cyber Crime (Computer forensic Handbook) Publishing by Syngress (Ine), United states of America, 2002.
- Susan W. Brenner, Brian Carrier, and Jef Henninger, The Trojan Horse Defense in Cybercrime Cases, op. cit.

5-5. الأبحاث الإنجليزية:

- The Editors of Encyclopedia Britannica, "Trojan horse", Available online on 19/12/2023 at the following website: https://www.britannica.com/topic/Trojan-horse
- الدليل الصادر عن الاتحاد الدولي للاتصالات و الخاص بفهم الجرائم الإلكترونية:
- UNDERSTANDING CYBERCRIME AGUIDE FOR DEVELOPING COUNTRIES, Draft April 2009, International Telecommunication Union Cybercrime, Legislation Resources

5-6. التشريعات والقوانين:

- مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات.
- قانون الإمارات الاتحادي رقم (39) لسنة 2006 في شأن التعاون القضائي الدولي في المسائل الجنائية.
- أصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971.