حجية المواقع الإلكترونية في إثبات الجريمة الإلكترونية

(دراسة تحليلية مقارنة)

The Authority of Websites in Proving Cybercrime
(An Analytical Comparative Study)

أ. منار أحمد عطا ريان

الجامعة العربية الأمريكية، (فلسطين)

Manar_tarifi99@hotmail.com

DOI: https://doi.org/10.70411/MJLS.4.1.2026226

تاريخ الاستلام: 2025-04-01 تاريخ المراجعة: 2025-08-11 تاريخ القبول: 2025-08-13

الملخص

شهد العالم تطورًا كبيرًا ونقلة نوعية في كيفية التواصل فيما بين البشر، إذ عمل هذا التطور الهائل على تقريب المسافات والذي أفضى إلى ظهور العديد من المشكلات، والتي أصبحت تشكل عائقًا أمام تحقيق أهداف التطور والتقدم، ومن هذه المشكلات الجرائم الإلكترونية؛ حيث شهدت الجرائم الإلكترونية انتشارًا كبيرًا في الواقع البشري نتيجة للتطور الحاصل في وسائل التواصل الاجتماعي، والإقبال المتزايد على تلك المواقع. حاولنا في هذه الدراسة تبيان حجية الموقع الإلكتروني في إثبات الجريمة الإلكترونية من خلال مبحثين، ناقشنا في الأول: مفهوم الدليل الرقمي الناتج عن المواقع الإلكترونية وإجراءاته، من خلال تبيان مفهوم الموقع الإلكتروني كوسيلة إثبات رقمية، وبحث الإجراءات الخاصة بالأدلّة الرقمية المتحصلة من الموقع الإلكتروني، وتناولنا في المبحث الثاني: طرق استخلاص أدلّة الإثبات الرقمية المتحصلة من الموقع الإلكتروني، عن طريق بحث القيمة القانونية للأدلّة الرقمية المتحصلة من الموقع الإلكتروني في إثبات الجرائم الإلكترونية، ودراسة آليات ضبط الأدلّة الرقمية الناتجة من الموقع الإلكتروني.

وهذا البحث يسلّط الضوء على الموقع الإلكتروني وحجيته في الجريمة الإلكترونية، من خلال بيان ماهية الموقع الإلكتروني والتعرض لوسائل ثبوت الجريمة، مستعرضين أهم الحلول الوقائية والتشريعية المقترحة، وتوصلنا لنتائج وتوصيات في نهاية البحث، ومن خلال الاعتماد المتزايد على التكنولوجيا في جميع مجالات الحياة، تصاعدت ظاهرة الجرائم الإلكترونية في الوطن العربي، لتصبح من أخطر التحديات التي تهدد الأمن الفردي والمجتمعي، وتتميز هذه الجرائم بأنها تتجاوز الحدود الجغرافية، وتستهدف الأفراد، والمؤسسات، وحتى الحكومات، باستخدام أدوات رقمية متطورة وأساليب خفية يصعب تعقبها.

الكلمات المفتاحية: الموقع الإلكتروني، القانون، الدليل الإلكتروني، الإثبات، القاضي الجزائي.

Abstract

The world has witnessed significant development and a qualitative shift in the way people communicate with each other. This tremendous development has shortened distances, leading to the emergence of many problems that have become an obstacle to achieving the goals of development and progress. Among these problems is cybercrime. Cybercrime has witnessed a significant spread in human reality as a result of the development of social media and the increasing demand for these sites.

In this study, we attempted to demonstrate the validity of websites as evidence in proving cybercrimes through two sections. In the first section, we discussed the concept of digital evidence derived from websites and its procedure, clarifying how websites function as a means of digital proof and examining the procedures for digital evidence obtained from websites. In the second section, we addressed methods for extracting digital evidence obtained from websites by examining its legal value in proving cybercrimes and studying the mechanisms for controlling and verifying this type of evidence.

This research sheds light on the website and its significance in cybercrime by explaining its nature, examining the means of proving the crime, and reviewing the most important proposed preventive and legislative solutions. Conclusions and recommendations are at the end of the research. Through the increasing reliance on technology in all areas of life, the phenomenon of cybercrime has escalated in the Arab world, becoming one of the most dangerous challenges threatening both individual and societal security. These crimes transcend geographical borders, targeting individuals, institutions, and even governments, using sophisticated digital tools and stealthy methods that are difficult to track.

Keywords: Website, digital evidence, crime, proof, judge**.**

المقدمة

استخدام الحواسيب والشبكات الإلكترونية أنتج منافع متعددة، سواء أكانت في مجالات البحث العلمي وتوثيق المعلومات وتخزينها أم الحصول على معلومات تيسيرًا لأعمال القطاعين الخاص والعام، وما لبث الأمر إلا إنّ تحولت هذه المنفعة إلى سيف ذي حدين؛ أحدثت تغيرات جذرية ونوعية بمختلف مناحي الحياة، وذلك في نهاية القرن العشرين من خلال استغلال هذه التقنيات المتطورة في ارتكاب العديد من الجرائم، سواء أكان على الصعيد الوطني أم الدولي محدثًا آثارًا سلبية ومباشرة وخطيرة.

وتستمد هذه الجرائم طبيعتها الخاصة من قدرة الشبكة المعلوماتية على نقل وتبادل المعلومات العامة والخاصة في آن واحد، وهذا كله جاء نتيجة لتطور العالم الافتراضي الذي أصبح جزءًا من حياة الإنسان والذي رافقه وجود الحواسيب والإنترنت والتطور التكنولوجي الهائل، والتعامل مع هذه التقنيات المتطورة سواء أكان في القطاع العام أم الخاص. ففي وقتنا الحاضر أصبحت الدول تعتمد على حوسبة وأتمتة أعمالها ونشاطاتها واتصالاتها وتنظيم إدارتها والإشراف على حسن سير أعمالها من خلال نظام إلكتروني، وأصبحت هذه التكنولوجيا المتمثلة بالحواسيب والشبكة العالمية جزءًا من الحياة اليومية للأفراد ونشاطه الاجتماعي وتعامله، حيث إنّه لا يمكن الاستغناء عنها لتسهيل وتسيير الحياة بشكل عام.

ونظرًا لتميز الجريمة الإلكترونية بطبيعة خاصة أصبحت هنالك ضرورة لوجود تشريع خاص بها، لاتصالها ببيانات وكلمات ورموز وأرقام، سواء أكان من حيث تجميعها وتخزينها وتجهيزها أم استرجاعها وتصحيحها وتعديلها ومحوها وطباعتها ونسخها، فهي تتم من خلال المعالجة الآلية للبيانات لهدف الحصول على المعلومات المرجوة، ومن خلال الطبيعة الخاصة للجريمة الإلكترونية والتي تميزها عن الجريمة التقليدية من حيث طريقة التحقيق بها، وتحليلها وربطها والحصول على الدليل الرقمي الذي هو أهم دليل لاكتشافها ومتابعتها من خبراء تكنولوجيا المعلومات، فهي تمتاز بطبيعة مزدوجة ما بين الحصول على الدليل وتحليله واتصاله بالنص القانوني، فالجريمة الإلكترونية بحاجة إلى إجراءات خاصة لمتابعتها بشكل يتلاءم ويتماشى مع التقنيات المستخدمة والمستحدثة لارتكابها، والتحري عن النظام القانوني الملائم لطبيعة هذه الجرائم ليتوافق والخصوصية التي تتميز بها.

كما أن عدم وجود هيئات قضائية متخصصة في مجال الجرائم الإلكترونية يضعنا أمام معادلة غير متكافئة، طرفها الأول: الجهات القضائية بنقص خبراتها في مجال مواكبة التطور الإلكتروني والمعلوماتي في ارتكاب الجرائم الإلكترونية، والطرف الآخر: هم قراصنة ومجرمون يتمتعون بمهارات وخبرات فنية عالية يواكبون كل جديد في العالم الإلكتروني والمعلوماتي.

إشكالية البحث

نظرًا لما تؤديه المواقع الإلكترونية من دور فاعل في قانون الجرائم الإلكترونية وتعديلاته، وما تثيره من إشكالات في القانون الجنائي الذي يقتضي ضرورة التعرض للمشكلات الموضوعية والإجرائية التي يثيرها هذا النوع المستحدث من الجرائم، وعليه يمكن طرح مشكلة البحث في التساؤل الرئيس الآتي: **ما هو النظام القانوني للمواقع الإلكترونية من حيث الجريمة الإلكترونية؟** وهذا ما نريد أن نستعرضه في هذه الدراسة.

أسئلة البحث

تثير هذه الدراسة تساؤلًا رئيسًا، وهو: **ما هي حجية الموقع الإلكتروني في إثبات الجريمة الإلكترونية؟** وتتفرع عن هذا التساؤل جملة تساؤلات تتمثل في الآتي:

1. ما هي الطبيعة القانونية لقواعد الإثبات الجنائي في الجريمة الإلكترونية؟
2. هل نظَّم القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته الأحكام العامة للإثبات الجنائي بالمقارنة مع التشريعات العربية؟
3. هل يُعد الدليل الناتج عن المواقع الإلكترونية من أدلّة الإثبات الجنائي في الجرائم الإلكترونية؟

أهمية البحث

تنبع أهمية الدراسة في المسائل القانونية الآتية:

1. هناك حاجة ماسة للدراسات والبحوث التي تهتم بتنمية الوعي بالجرائم الإلكترونية كأحد القضايا الحديثة لدي أفراد المجتمع من منظور طريقة العمل مع المجتمع مما يعطي أهمية خاصة لتناول هذا النوع من القضايا.
2. الجرائم الإلكترونية موضوع ينال اهتمامًا عالميًا في ظل العولمة، ويتضمن جرائم عديدة بدءًا من اختراق المواقع الإلكترونية (القرصنة) والتجسس وسرقة البيانات وتزويرها فهو موضوع زاد انتشاره في السنوات القليلة الماضية مما يستوجب دراسته.
3. تزويد الباحثين بمفهوم الجريمة الإلكترونية ومخاطرها يعد أمرًا على قدر كبير من الأهمية، أما أهمية الدراسة من الناحية العملية، فتكمن في أنها تأتِي في سياق جملة من الانتهاكات التي تقترفها بعض جهات إنفاذ القانون في تطبيق نصوص القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته في مجال جمعها للأدلّة الإلكترونية.

نطاق البحث

يتحدد نطاق دراستنا لحجية الموقع الإلكتروني في إثبات الجريمة الإلكترونية في القانون الفلسطيني والقوانين المقارنة، وتقييم الواقع الحالي لتطبيقها، والاستفادة من التجربة العربية في مكافحة الجريمة المعلوماتية.

منهجية البحث

تم استخدام المنهج الوصفي التحليلي الذي تناول حجية الموقع الإلكتروني في إثبات الجريمة الإلكترونية وفق نصوص القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، ووصفهًا وصفًا دقيقًا، وتحليل أحكامها وواقع الممارسة الفلسطينية بشأنها.

بالإضافة إلى المنهج المقارن الذي تمت من خلاله مقارنة تلك النصوص مع أحكام قانون الجرائم الإلكترونية كلما اقتضى المقام ذلك، لهدف الوصول إلى تحليل نقاط الضعف في القانون الفلسطيني، أو النقص ومعالجة مشكلة الدراسة.

خطة البحث

تمّ تقسيم الدراسة إلى مبحثين؛ واشتمل كل مبحث على مطلبين؛ تناول المبحث الأول **تحديد مفهوم المواقع الإلكترونية**، وتناول المبحث الثاني **طرق استخلاص أدلّة الإثبات من الموقع الإلكتروني**.

المبحث الأول

تحديد مفهوم المواقع الإلكترونية

يتحتم على القائمين بإنفاذ القانون الإلمام الدائم بالتقنية العلمية المتطورة، وتطبيقًا لذلك جاءت وسائل الإثبات الرقمية؛ لتكون نتاجًا للتطور الحاصل في جميع المجالات العلمية والتقنية، حيث يصح القول إنّها انعكاس لما بلغه العلمُ واكتسبته الخبرة، ولها من الممارسات القضائية ما يشهد لها بالدور المهم والفعال في عملية الإثبات.

وفي هذا الشأن تم تقسيم هذا المبحث إلى مطلبين، تناول المطلب الأول التعريف بالموقع الإلكتروني، وخُصص المطلب الثاني للحديث في الإجراءات الخاصة بالأدلّة الرقمية للموقع الإلكتروني.

المطلب الأول

تعريف الموقع الإلكتروني

يعرف الموقع الإلكتروني بأنه مساحة يتم تخصيصها على شبكة الإنترنت تحتوي كثيرًا من المعلومات وتقدم العديد من الخدمات التفاعلية للمستخدم، وكل موقع إلكتروني مقسم إلى عدة صفحات مع وجود صفحة رئيسة للموقع (Home Page)، وكل صفحة في الموقع عبارة عن نسق خاص أو نظام معين[1]، وتدخل الأدلّة المتحصلة من الموقع الإلكتروني في عداد وسائل الإثبات الرقمية. فيما عرفت المادة الأولى: من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته الموقع الإلكتروني بأنه: "**مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد**".

يرى الباحثان أن تعدد مفاهيم الدليل الرقمي والتباسه بمفهوم الدليل الإلكتروني، يعد من الأمور التي لا بد من الوقوف عندها ومناقشتها؛ تمهيدًا لتحديد فيما إذا كانت الأدلّة المتحصلة من الموقع الإلكتروني أدلّة رقمية أم إلكترونية.

وانطلاقًا مما تقدم تمّ تقسيم هذا المطلب إلى فرعين، تناول الفرع الأول ماهية وسائل الإثبات الرقمية، وتناول الفرع الثاني خصائص المواقع الإلكترونية.

[1]. ربحي مصطفى عليان، وسائل الاتصال وتكنولوجيا التعليم، ط 2، دار صفاء للنشر والتوزيع، عمان، (2003)، ص127.

الفرع الأول

ماهية وسائل الإثبات الرقمية

لا بد لنا بدايةً أن نعرف ماذا يقصد بمصطلح (الرقمية)؟، إذ تبين من خلال المراجعة أن المصطلح مترجم من كلمة (Digital) باللغة الإنجليزية، وقد عرفها قاموس كامبردج أنها: "تسجيل أو تخزين المعلومات كسلسلة من الأرقام (0،1) من خلال إظهار أو إخفاء الإشارة"[1]، ويسمى هذان الرقمان (0،1) بالأرقام الثنائية أو بالنظام الثنائي، وهي الصيغة التي تسجل فيها البيانات كافة من حروف ورموز وأشكال وغيرها داخل الحاسوب، حيث يطلق على الواحد أو الصفر بالـ (بايت، Bit)، وبعبارة أخرى تحويل المعلومات إلى أرقام؛ لكي يتم تخزينها في جهاز الحاسوب، مثال على ذلك: الرقم 65 يمثل الحرف (A)، ويمثل الرقم 66 الحرف (B)، فيرمز للرقم 65 بهذا الشكل (01000001) والرقم 66 يرمز له (01000010)، ويمثل أمر المسافة أو الفراغ (Space) بين كلمتين الرقم 32 ويرمز له (00100000)، وهكذا تتحول الأرقام إلى معلومات يمكن تخزينها في جهاز الحاسوب أو ما شابه ذلك، من خلال النظام الثنائي الذي يعد كشِيفرة تترجم جميع المعلومات وتخزنها[2].

أما الأدلّة الرقمية فتعد من الناحية النظرية كأي دليل آخر، فهي عبارة عن معلومات تجمع لإيجاد العلاقة السببية بين الوقائع والأشخاص لإثبات المسؤولية القانونية[3]. وقد عرفها قانون الشرطة والأدلّة الجنائية في المملكة المتحدة بأنها: "جميع المعلومات الموجودة على جهاز الحاسوب"[4]. ويُلاحظ أن هذا التعريف، قد حصر الأدلّة الرقمية في جهاز الحاسوب، في حين عرفتها المجموعة العلمية للعمل بالأدلّة الرقمية (Scientific Working Group Digital Evidence–SWGDE) المكونة من دائرة مختبرات الجريمة الفيدرالية في واشنطن في العام 1998 على أنها: "أية معلومات ذات قيمة إثباتية يتم تخزينها في شكل ثنائي– وفي وقت لاحق تغير المصطلح من "ثنائي" إلى "رقمي"–. وتشمل هذه الأدلّة، أدلّة أجهزة

---

[1] Cambridge Dictionary https://dictionary.cambridge.org/dictionary/english/digital.

[2] أسامة المناعسة جلال الزعبي، جرائم تقنية المعلومات، دراسة مقارنة، ط1، دار الثقافة للنشر والتوزيع، عمان، (2014)، ص 290. جيتس، بيل المعلوماتية بعد الإنترنت– طريق المستقبل، ترجمة عبد السلام رضوان، مجلة عالم المعرفة، العدد 231، الكويت، (1998)، ص40–46.

[3] Goodison, Sean E. and Others (2015), Digital Evidence and the U.S. Criminal Justice System, RAND Corporation, US, P.2.

[4] Gercke, Marco (2012), Understanding cybercrime: Phenomena, challenges and legal response, ITU publication, Switzerland – Geneva, P.227.

الحاسوب، الفيديو الرقمي، والصوت الرقمي، وأجهزة الفاكس الرقمية، والهواتف المحمولة، والمواقع الإلكترونية وغيرها"[1]، ويُلاحظ أن هذا التعريف جاء أوسع من سابقه.

وهنالك من يعرفها بأنها: "معلومات وبيانات ذات قيمة للتحقيق، يتم تخزينها على جهاز إلكتروني، أو استلامها، أو إرسالها بوساطة جهاز إلكتروني، ويتم الحصول عليها من خلال الحجز على الأجهزة الإلكترونية وتأمين بياناتها للفحص"[2]. وقد عرفها آخرون بأنها "البيانات الرقمية التي يمكن أن تثبت ارتكاب جريمة ما، وتعزز الصلة بين الجريمة وضحاياها، أو بين الجريمة ومرتكبها، ومن بين الأمثلة على هذه الأدلّة هي البيانات الموجودة في ذاكرة الحاسوب أو القرص الصلب أو الهاتف المحمول"[3].

وفي الصدد نفسه قد تطرح تساؤلات منها: وبما أنه كانت هنالك مسميات كالأدلّة الإلكترونية أو أدلّة الحاسوب، فهل يقصد بهذه الأدلّة المعنى ذاته المتجسد في الأدلّة الرقمية؟ وهل يدخل الدليل الناتج عن المواقع الإلكترونية في إطار الأدلّة الإلكترونية أم الرقمية؟

وللإجابة عن الأسئلة السابقة، يمكن القول: إنّ دليل الحاسوب يعرف أحيانًا بالدليل الإلكتروني، والأدلّة الإلكترونية تشمل الأدلّة التي يتم إنشاؤها وإنتاجها بوساطة الحاسوب، ومخرجاته، والأدلّة المستندة إليه، والأدلّة المرتبطة به، وجميع البيانات والمستندات الإلكترونية، وبشكل عام يمكن أن تشمل الأدلّة الإلكترونية أي بيانات يتم إنشاؤها أو تخزينها في شكل رقمي باستعمال جهاز الحاسوب[4]، وفضلًا عما سبق تعرف الأدلّة الرقمية بأنها: "عبارة عن معلومات مرسلة أو مخزنة كبيانات رقمية يمكن أن يستعملها أحد أطراف الدعوى، وقد تكون هذه الأدلّة على شكل صور فوتوغرافية، أو صور الأقمار الاصطناعية، أو فيديو، أو تسجيل صوتي، أو بريد إلكتروني، أو تكون على شكل موقع إلكتروني، أو أحد مواقع التواصل الاجتماعي، مثل: (Facebookأو Twitter)" [5].

---

[1] Whitcomb, Carrie Morgan (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vo1.1, no pages number

[2] Dutelle, Airc W (2017), An Introduction to crime scene Investigation, thired Edition, Jones & Bartleff learning, USA, P.374.

[3] Carrier, Brian and Spafford Eugene H. (2003), Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vo1.2, P.6.

[4] Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin, P.1.

[5] Ashouri, Aida and Others (2013), An Overview of the Use of digital Evidence in International Criminal Courts, Working Paper, Salzburg Workshop on Cyber Investigation, P.1.

ويرى الباحثان أنه يصح القول: إنّ الأدلّة الرقمية هي أوسع نطاقًا من الأدلّة الإلكترونية، إذ إنّها تشتمل فضلًا عن الأخيرة على ما ذكر في تعريف الأدلّة الرقمية المذكورة آنفاً بما فيها المواقع الإلكترونية.

ويتضح مما تقدم، أنه لم يكن هناك اتفاق على تعريف موحد، سواء أكان ما تعلق بالأدلّة الإلكترونية أم بالأدلّة الرقمية، وخصوصًا بعد المحاولة التي جرت في المؤتمر الذي عقد في مدريد في 14 كانون الأول 2006 من قِبَل الجمعية الأوروبية لخبراء الطاقة (Associated European Energy Consultant–AEEC)، بشأن مشروع قبول الأدلّة الإلكترونية في إجراءات المحاكم، إذ لم يستطع هذا المشروع التوصل إلى تعريف موحد للأدلّة الإلكترونية أو الرقمية، وعلى الرغم من ذلك لا يُعدّ هذا التعريف ضروريًا في الإجراءات القانونية؛ لأنّ معظم السلطات القضائية في أغلب الدول تتعامل مع الأدلّة الإلكترونية أو الرقمية كشكل من أشكال المستند، ويقصد بهذا الأخير: "أيّ شيء يسجل بأيّ شكل كان، ويكون مُسْتَوفيًا لشروط المقبولية"[1].

يتفق الباحثان على ما ذهبت إليه المحكمة الجنائية الدولية لرواندا في تعريفها (المستند) على نطاق واسع في قضية المدعي العام ضد (ألفرد موسما) (Alfred Musema) إذ قالت: "يقصد بالمستند أيّ شيء يتم تسجيل المعلومات فيه، من أيّ وصف كان". وهذا التعريف واسع بما يكفي ليشمل فضلًا عن الوثائق الخطية: الخرائط والرسومات، والخطط والرسوم البيانية، والسجلات الحاسوبية، والمواقع الإلكترونية، والسجلات الكهرومغناطيسية، والسجلات الرقمية، وقواعد البيانات والمسارات الصوتية، والأشرطة الصوتية، وأشرطة الفيديو، والشرائح والصور الفوتوغرافية، وصور الأقمار الاصطناعية[2].

ونستنتج مما تقدم، أن وسائل الإثبات الرقمية، ما هي إلا امتداد واستمرار للأدلّة الخطية أو الكتابية؛ لكن بوجهٍ متطور، لذا من المفترض أن تستجيب المحاكم الوطنية بشكل جيد ومستمر لما يطرأ من تطورات في جميع المجالات، من أجل توضيح ذلك لأغراض العدالة.

[1] Mason, Stephan (2008), International Electronic Evidence, British Institute of International and Comparative law, London, P.xxxiv.

[2] Prosecutor v. Alfred Musema (2000), ICTR, Trial Chamber I, Case No. ICTR-96-13-T, 27,parper 53, P.24.

الفرع الثاني

خصائص المواقع الإلكترونية

نعرض في هذا الفرع بإيجاز أهم ما يميز الأدلّة الرقمية عن الأدلّة التقليدية، وذلك على النحو الآتي:

أ. يمكن للمتخصصين في المجال الرقمي أن يستعيدوا الملفات ورسائل البريد ومعلومات المواقع الإلكترونية المفقودة أو المحذوفة، والعثور على المعلومات المخفية منها بالاعتماد على برامج إلكترونية معدة لهذا الغرض[1].

ب. للأدلّة الرقمية مجال أوسع في الإثبات لتعدد وانتشار أدواتها، وقد تتعامل مع معلومات حساسة وأكثر شخصية من الأدلّة التقليدية[2].

ج. يمكن عمل نسخ احتياطية للأدلّة الرقمية مطابقة للأصل، وتكون لها القيمة الإثباتية ذاتها، وهو الأمر الذي لا يتوافر في الأدلّة التقليدية، وهذا ما يشكل ضمانة مهمة للحفاظ على الدليل ضد التلف أو التغيير أو الفقد[3].

د. لا يُعد الدليل الرقمي دليلًا ماديًا، فهو غير ملموس بطبيعته، حتى وإن استخرج في شكل مادي فإنه لا يفقد صفته؛ وهذا لأن عملية الاستخراج لا تعدو أن تكون عملية نقل من الطبيعة الرقمية غير الملموسة (Software) إلى الهيئة الصلبة أو الملموسة (Hardware) التي يمكن أن يستدل بها على معلومة معينة[4]، فالدليل الرقمي لا يمكن إدراكه بالحواس العادية؛ وإنما يتطلب الاستعانة بخبراء وأجهزة كالحاسوب، وأدوات خاصة كالطابعة والكاميرا الرقمية وغيرها، وقد يتطلب بعض البرامج الحاسوبية المعقدة[5].

---

[1] Grobler, Marthie (2012), The Need for Digital Evidence Standardisation, International Journal of Digital Crime and Forensics, 4(2), p.2.

[2] Goodison, Sean E. and Others, op.cit, P.3

[3] عبد الناصر محمد فرغلي محمود، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية،(د. ط)، جامعة نايف العربية للعلوم الأمنية، الرياض،(2007)،ص15.

[4] تقرير صادر عن مركز (هردو) لدعم التعبير الرقمي الجريمة الإلكترونية، وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، (2014)، ص23.

[5] ميسون خلف الحمداني، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، بحث منشور في مجلة الحقوق، العدد 18، جامعة النهرين، بغداد، (2016)، ص200.

هـ. الطبيعة الثنائية للدليل الرقمي، وهو ما يتم القيام به من عملية اختزال للمعلومات والبيانات كالصوت أو الصور أو النصوص وتحويلها إلى رموز ثنائية، كما أوضحنا ذلك آنفًا[1].

و. تُعد الأدلّة الرقمية ذات طبيعة متطورة ديناميكية، فهي تنتقل بسرعة فائقة عبر شبكات الاتصال أو برامج معدة لهذا الغرض، ويمكنها رصد تحركات الأشخاص، وتحليلها وتسجيل المعلومات عنها، فضلًا عن تسجيل عادات وسلوكيات الفرد وأموره الشخصية، لذا فقد تجد المحكمة وأطراف الدعوى ضالتها عند الاستعانة بالأدلّة الرقمية ذات الصلة بالجاني، أو بالواقعة الإجرامية محل نظر المحكمة[2].

المطلب الثاني

الإجراءات الخاصة بالأدلّة الرقمية المتحصلة من الموقع الإلكتروني

بما أن وسائل الإثبات الرقمية المتحصلة من الموقع الإلكتروني هي ذات طبيعة خاصة تميزها عن باقي الأدلّة الأخرى؛ لذا لا بد من أن تكون لها إجراءات خاصة تُهيئ لها الأساس الذي تستند عليه، من هنا فقد تناولنا هذه الإجراءات من خلال تقسيم هذا المطلب إلى فرعين، وتقسيمه إلى فرعين، تناول الفرع الأول وسائل الإثبات الناجمة عن الموقع الإلكتروني، وتناول الفرع الثاني قيمة أدلّة الإثبات المتحصلة عن الموقع الإلكتروني.

الفرع الأول

وسائل الإثبات الناجمة عن الموقع الإلكتروني

هنالك أربعة مبادئ أساسية للأدلّة الرقمية صادرة عن رابطة كبار ضباط الشرطة في المملكة المتحدة (Association of Chief Police Officers – ACPO) ويمكن الاسترشاد بها عند إعمال وسائل الإثبات الرقمية المتحصلة من الموقع الإلكتروني[3] وغيرها من الأدلّة الناتجة بأية وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو البيانات والمعلومات الإلكترونية.

---

[1]. عبد المطلب طاهري، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، (2014-2015)، ص9.

[2]. بسام ليدية، الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، الجزائر، (2017-2018)، ص14.

[3]. Aljneibi, Khaled Ali (2014), The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PHD Thesis, Bangor University, Wales, UK, P.103

1. لا يجوز لأية سلطة من سلطات إنفاذ القانون تغيير البيانات الموجودة في جهاز الحاسوب، أو أية وسائط تخزين يمكن الاعتماد عليها في إجراءات التقاضي.
2. يجب أن يكون الشخص الذي يتعامل مع الأدلّة الموجودة في جهاز الحاسوب أو وسائط التخزين شخصًا متخصصًا وقادرًا على تقييمها، ويجب أن يقدم أسبابًا تبين أهمية الوصول والحصول على تلك الأدلّة، وما يترتب عليها من نتائج ذات صلة بالتحقيق.
3. يجب إنشاء سجل لتوثيق كل ما جمع من الأدلّة الرقمية، وما جرى من عمليات في سبيل جمعها، وذلك من أجل تدقيقها والحفاظ عليها.
4. يتحمل القائم بالتحقيق المسؤولية الكاملة عن ضمان تطبيق القانون وهذه المبادئ خصوصًا[1].

إن هذه المبادئ تُعد تدابير أساسية يجب ألا تنتهك، وينبغي على المحققين المتخصصين في الأدلّة الرقمية وضعها دائمًا بعين الاهتمام، ومع ذلك قد تؤدي بعض طرق الحصول على الأدلّة الرقمية إلى الإضرار بالبيانات الرقمية الأصلية على الرغم من أنها تمّت بصورة سليمة، مما يؤدي إلى انتهاك المبدأ الأول المذكور آنفًا، في هذه الحالة يمكن التغاضي عن هذا الانتهاك إذا كان ضروريًا للتوصل إلى كشف الحقيقة، مع التأكد من تحقق باقي المبادئ[2].

ويجب على المحقق المتخصص اتخاذ الاحتياطات كافة اللازمة لتخزين وحفظ الأدلّة الرقمية المتحصلة من الموقع الإلكتروني، والتعامل معها بحذر؛ للمحافظة على ما تحتوي من بيانات، بمعنى أنّه يجب أن تكون هذه البيانات محمية مؤمنة بصورة جيدة؛ لكي يتم استعمالها كأدلّة[3]، من خلال إزالة كل ما يؤثر على سلامتها فور استلامها والمحافظة عليها بعد تخزينها بعيدًا عن المجالات المغناطيسية، وختمها وترقيمها وعمل نسخ احتياطية كلما أمكن ذلك، واستعمال النسخ الاحتياطية أولًا بدلًا من النسخ الأصلية[4].

[1] Wilkinson, Sue, Association of Chief Police Officers (ACPO), Good Practice Guide for Computer-Based Electronic Evidence, published by 7safe, Official release version 4.0, United Kingdom, no date of issue, P.4.

[2] Casey, Eoghan (2011), Digital evidence and computer crime – Forensic Science, computer and the Internet, Published by Elsevier Inc, USA, P.232.

[3] Dutelle, Airc W. (2014), An Introduction to crime scene Investigation, second Edition, Jones & Bartleff learning, USA, P.412.

[4] Petit, Robert and Warren, Maria and Akerson, David (2012), Prosecution Mass Atrocities Lessons from the International Tribunals, open society Foundation, Bangkok – Thailand, P.137.

الفرع الثاني

قيمة أدلّة الإثبات المتحصلة عن الموقع الإلكتروني

إن أهمية وسائل الإثبات الرقمية المتحصلة من الموقع الإلكتروني تنطلق من كونها مستحدثة ومتطورة، خصوصًا إذا كانت الواقعة محل الإثبات خارجة عن الإدراك البشري المجرد، زيادة على الدقة التي تتمتع بها في نقل المعلومة، إذا توافرت شروطها القانونية والعلمية.

ومع ذلك لا يمكن عد وسائل الإثبات الرقمية المتحصلة من الموقع الإلكتروني محصنة ضد الخطأ، فهي تعتمد على دقة وسلامة الأجهزة المستخدمة، وعلى درجة كفاءة المتخصص القائم عليها، وهي لا تخلو من العيوب، فقد تكون عملية تحديد مصدر المعلومات المتحصلة عن طريق الموقع الإلكتروني أمرًا يصعب التحقق منه، مقارنة بالشاهد الذي يرى المجرم بأم عينه، أو يسمع الصوت بأذنه، فضلًا عن ذلك من المحتمل أن يتم إصدار المعلومات عن طريق برنامج إلكتروني أو إنسان آلي (Robot)، وهذا ما يجعل عملية الإثبات تحتاج إلى إسناد أو دعم من أدلّة أخرى، كأن تكون شهادة أو خبرة، أو تكون وسيلة إثبات رقمية أخرى[1].

ومن أكثر التحديات هي تلك الناشئة عن محو آثار الجريمة أو تعقب مرتكبها، وهنا تكمن الصعوبة، ففي الغالب يقوم المجرم الإلكتروني بمحو آثار الجريمة (الماديات) من خلال إتلاف الموقع أو البرامج أو التضليل مما يصعب التحقيق، وكذلك قيام شركات خاصة ببرمجة وتنفيذ تلك المواقع، وقد تكون في مناطق غير تابعة لسيطرة الدولة الفعلية أو القانونية، خصوصًا إذا كان الموقع يعمل وفقًا لبرنامج روبوت (إنسان آلي). أو أن يكون الجناة والضحايا من ولايات قضائية مختلفة، وصعوبة تعقب البيانات في "السحابة" وهي البيانات التي يتم نقلها باستمرار من خادم إلى آخر، وتتنقل داخل عدة بلدان أو تصل إليها في أي وقت، وقد تظهر البيانات الموجودة في "السحابة" لأسباب تتعلق بالأمان والتوافر؛ وبالتالي يمكن العثور عليها في مواقع متعددة داخل بلد واحد أو في عدة بلدان، لدرجة أن مزود الخدمة "الحوسبة السحابية" قد لا يعرف بالضبط مكان البيانات المطلوبة[2].

ختامًا، يطرح الباحثان تساؤلًا جوهريًا متصلًا بموضوع الدراسة وهو: ما القيمة التي يمكن أن تضيفها أدلّة الإثبات الرقمية المتحصلة من الموقع الإلكتروني؟ للإجابة عن هذا التساؤل، يمكن القول بأن مهمة أدلّة الإثبات الرقمية المتحصلة من الموقع الإلكتروني تبدأ في تأكيد هُوية المسؤول عن هذه الجرائم

[1] Outerbridge, David and Siller, Ezra, The Admissibility of Electronic Evidence, Torys LLP, Toronto.
[2] INTERPOL (2011), European Working Party on Information Technology Crime (EWPITC) Project on cloud computing.

الإلكترونية، ودرجة مساهمته، والظروف التي رافقت ارتكاب الجرائم، وبعبارة أخرى البحث عن مكنونات الجريمة، والكشف عن الإرادة الآثمة في ارتكابها؛ حيث تسهم هذه الأدلّة في تحديد الجزاءات التي يمكن أن تفرضها المحاكم بناءً على مستوى القصد الجرمي (Mens Rea) فضلًا عن شدة الأضرار التي لحقت أو عاصرت ارتكاب الجريمة.

المبحث الثاني

طرق استخلاص أدلّة الإثبات من الموقع الإلكتروني

إن وسائل وإجراءات جمع الأدلّة الجنائية لإثبات الجرائم قد وردت في مواد قانون الإجراءات الجزائية رقم (3) لسنة 2001[1] وتعديلاته[2]؛ ولأجل ذلك يعمل المحقق الجنائي على استخدام الطرق المشروعة؛ لجمع وتحليل ما توفر لديه من الأدلّة التي يرى أنها ملائمة للكشف عن حقيقة الجريمة، فيجوز له أن يباشر أي إجراء يرى فيه فائدة للإثبات[3].

كما أن استخلاص الدليل الرقمي في الجرائم الإلكترونية الناجمة عن الاستخدام غير المشروع لتقنية الحاسوب والإنترنت من أجل الاعتداء على الحقوق التي يحميها القانون، قد يخلق عدة صعوبات عملية بالنظر إلى خصوصيته التقنية المتطورة وطبيعته الرقمية، بالإضافة إلى الفضاء الواسع والمتاح الذي ترتكب فيه الجريمة، فإن هذه الميزات تجعل من إمكانية إخفاء ومحو آثار الجريمة ممكنة.

لذلك تم البحث في الوسائل الممكنة والمتاحة لاستخلاص الأدلّة الرقمية المتحصلة من الموقع الإلكتروني في إثبات الجرائم الإلكترونية التي تمثل ضربًا من ضروب الذكاء الإجرامي الجديد، التي باتت تتخذ أنماطًا جديدة لا يجدي معها اتِّباع الإجراءات التقليدية، لما تثيره طبيعتها غير المادية من إشكالات وما تؤديه التقنية الحديثة من دور في ارتكابها، وما توفره لها من مسرح غالبًا ما يكون أقل إظهارًا للأدلّة محل التحقيق، وذلك لوقوعها في عالم افتراضي وبأدلّة غير ملموسة، وتُعد مسألة جمع الأدلّة من المسائل الأساسية في تكوين الجريمة وإعادة ملامحها وكيفيات حدوثها.

وفي هذا الشأن قسمنا هذا المبحث إلى مطلبين، الأول: ناقشنا فيه القيمة القانونية للأدلّة الرقمية المتحصلة من الموقع الإلكتروني، والثاني: خصصناه لدراسة آليات ضبط الأدلّة الرقمية للمواقع الإلكترونية.

---

[1]. منشور على الصفحة (94) من عدد الوقائع الفلسطينية رقم (38) بتاريخ: 2001/09/05.

[2]. القرار بقانون رقم (17) لسنة 2014 بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001، والقرار بقانون رقم (13) لسنة 2018 بشأن تعديل القرار بقانون رقم (17) لسنة 2014 م بشأن تعديل قانون الإجراءات الجزائية رقم (3) لسنة 2001.

[3]. مفتلح بوبكر مطردي، الجريمة الإلكترونية والتغلب على تحدياتها، مؤتمر رؤساء المحاكم العليا في الدول العربية، السودان، (2012)، ص52.

المطلب الأول

القيمة القانونية للأدلّة الرقمية المتحصلة من الموقع الإلكتروني

إن مجرد وجود دليل جنائي يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، حيث إنّه يجب أن تكون لهذا الدليل قيمة قانونية، وهذه القيمة للدليل الجنائي تتوقف على مسألتين رئيستين، الأولى: المشروعية، والثانية: اليقينية في دلالته على الوقائع المراد إثباتها[1]، مما يوجب إبراز أهم الأسس التي يستند إليها الدليل حتى يكون مشروعًا، وإلى أية درجة من اليقين يجب أن يحققها. وعليه فقد كان لزامًا علينا أن نبين حجية الأدلّة الرقمية للموقع الإلكتروني في الفرع الأول، ونستعرض شرعية الأدلّة الرقمية المتحصلة من الموقع الإلكتروني أمام القاضي الجزائي في الفرع الثاني.

الفرع الأول

حجية الأدلّة الرقمية للموقع الإلكتروني

لما كان الدليل الرقمي بشكل عام والدليل الرقمي المتحصل من الموقع الإلكتروني على وجه الخصوص يختلفان في إثبات الجرائم الإلكترونية عن الأدلّة التقليدية، فقد كان لزامًا علينا وقبل أن نبدأ ببسط بحثنا بشأن شرعية الأدلّة الرقمية المتحصلة من الموقع الإلكتروني أن نسعى لدراسة مدى حجية هذه الأدلّة أمام القاضي الجزائي.

فقد اختلفت الآراء حول مسألة مدى إمكانية الأخذ بالدليل الجنائي الرقمي على إطلاقه، أو أنه يعتمد نسبيًا؛ بمعنى: هل القاضي حر في الأخذ بما يشاء من الأدلّة الرقمية؟ أم أنه مقيد فيما قيده المشرع بالنص عن هذه الأدلّة؟ فما يسري على الدليل الرقمي بشكل عام يسري على الدليل الرقمي المتحصل من الموقع الإلكتروني في إثبات الجرائم الإلكترونية؛ وذلك نظرًا لوجود عدة اختلافات بين النظم الإجرائية للإثبات الجنائي، فمنها ما يأخذ بنظام الإثبات الحر، ومنها ما يأخذ بنظام الإثبات المقيد، ومنها ما يأخذ بالنظامين معًا، وهنا حاولنا الإشارة إلى هذه الأنظمة الإجرائية باختصار على النحو الآتي:

1. **الحجية في نظام الإثبات المقيد:** يقوم نظام الإثبات المقيد على مبدأ أساسي في أن المشرع الجنائي يحدد سلفًا الوسائل والطرق التي يعتمدها في إقامة الدليل الجنائي على مرتكبي الجرائم، فوفقًا لهذا الاتجاه فإن المشرع هو الذي يحدد الأدلّة التي يجوز للقاضي اللجوء إليها ويقدر قيمتها الاقناعية؛ بحيث يقتصر دور القاضي في هذا النظام على مجرد فحص الدليل والتأكد من

[1] محمد حماد الهيتي، التحقيق الجنائي والأدلة الجرمية، ط 1، دار المناهج للنشر والتوزيع، عمان، (2010)، ص22 وما بعدها.

توافر الشروط التي حددها القانون، فلا سبيل للاستناد إلى دليل لم ينص عليه القانون صراحة ضمن أدلّة الإثبات، كما لا دور للقاضي في تقدير القيمة الاستدلالية للدليل، حيث إنّ القانون يقيد القاضي بقائمة الأدلّة التي حددت قيمتها الإثباتية[1].

2. **الحجية في نظام الإثبات الحر:** يسود نظام الإثبات الحر في القوانين الإجرائية اللاتينية؛ بحيث يتمتع القاضي بموجب هذا النظام بالحرية المطلقة في إثبات الوقائع المعروضة عليه، ولا يُلزمه القانون بأدلّة معينة للاستناد إليها في تكوين قناعته الشخصية، وإن حجية الدليل الرقمي المتحصل من الموقع الإلكتروني لا تثير أية صعوبات متعلقة بمدى حرية تقديم الأدلّة لإثبات الجرائم الإلكترونية، ولا بمدى حرية القاضي الجنائي في تقدير هذه الأدلّة ذات الطبيعة الخاصة، بوصفها أدلّة إثبات في المواد الجنائية أم لا؛ بل إن العنصر الأساسي وفق هذا المذهب هو مدى حرية قاضي الموضوع في تقدير هذه الأدلّة، ومدى قبول هذه الأدلّة، كدليل قائم بذاته، وكافٍ لإثبات الإدانة أو البراءة[2].

ويرى الباحثان أن القاضي في هذا النظام يتمتع بدور إيجابي في مجال الإثبات، وبالمقابل تقييد دور المشرع، وعليه فإنه في هذا الاتجاه لا تثور مشكلة مشروعية الدليل الرقمي بشكل عام؛ والدليل الرقمي المتحصل من الموقع الإلكتروني في إثبات الجرائم الإلكترونية بشكل خاص، من حيث الوجود على وصف أن المشرع لم يعهد إليه مهمة تحديد قائمة أدلّة الإثبات، فمسألة قبول الأدلّة لا ينال منها سوى مدى اقتناع القاضي بها.

ولما كانت المحررات أحد الأدلة التي قد يلجأ إليها القاضي في الإثبات، فهي تخضع كغيرها من الأدلّة لتقدير المحكمة، إلا إذا كان الإثبات متعلقًا بمواد غير جنائية، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيد بطريق الإثبات المحددة في ذلك الفرع من القانون، مثال ذلك: حق الملكية في جريمة السرقة، والعقود التي تثبت التصرف في الحق في جريمة خيانة الأمانة، أو صفة التاجر في جريمة التفالس بالتدليس[3].

3. **الحجية في نظام الإثبات المختلط:** يقوم النظام المختلط على أساس الجمع بين خصائص النظام المختلط ونظام الإثبات الحر؛ حيث يعتمد أساسًا على أن القانون يحدد أدلّة معينة لإثبات وقائع

---

1. عبد الإله أحمد هلالي، حجية المخرجات الكمبيوترية، ط1، دار النهضة العربية، القاهرة، (1997)، ص22.
2. عبد الإله أحمد الهلالي المرجع السابق، ص23.
3. مأمون سلامة– الإجراءات الجنائية في التشريع الليبي– ج، ط2– منشورات المكتبة الجامعة–،2000، ص151.

دون بعضها الآخر، وقد يحدد قبول الدليل بشروط معينة في بعض الحالات، كما يعطي للقاضي الحرية في تقدير الأدلّة القانونية على غرار القانون الفلسطيني، فقد نصت المادة (1/206) من قانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته على أنه". تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات، إلا إذا نص القانون على طريقة معينة للإثبات.." [1].

[1]. وفي ذلك تقول محكمة النقض الفلسطينية بأنه: "أما عن أسباب الطعن في مجملها نجد أنها بنيت على أن المحكمة أخطأت في تطبيق القانون وعدم بناء حكمها على الخبرة الفنية. ولما كانت البينة من طرق الإثبات الجزائي في الدعوى أن المادة 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001 تفيد ((1/206 تقام البينة في الدعاوى الجزائية بجميع طرق الإثبات إلا إذا نص القانون على طريقة معينة للإثبات)). خاصة وأن الأدلة في الدعوى الجزائية تخضع لمبدأ القناعة الوجدانية للمحكمة، ومحكمة الاستئناف كمحكمة موضوع لها صلاحية وزن البينة حيث إن القاعدة في الأحكام الجزائية وجوب اشتمالها على الأدلة والأسباب الموجبة للتجريم؛ أي استظهار أركان الجريمة وعناصرها وفقًا للتعريف الذي نص عليه القانون، ولمحكمة الموضوع الصلاحية في الأخذ بما تقتنع به من البينة المقدمة والخبرة من عداد البينات وهي مسألة موضوعية يترخص قاضي الموضوع بتقديرها وما دام أن محكمة الموضوع لم ترى جدوى بإحداث خبرة خلاف من ثم سماع شهادته كخبير في الدعوى وهو موظف البنك بكر العمري فإنها تكون قد استعملت خيارها في هذه المسألة ما دام أنها ثبتت حكمها على الوقائع الثابتة في الدعوى والمستمدة من الأدلة المقدمة إليها والتي عالجت هذه الواقعة محكمة الاستئناف أيضًا كما أن هذا لم يكن مدار طعن أمام محكمة الاستئناف مما يجعل من هذه الأسباب أسبابًا جديدة لا يستقيم طرحها أمام محكمة النقض مما يستوجب ردها"، حكم محكمة النقض الفلسطينية المنعقدة في رام الله في الدعوى الجزائية رقم 77 لسنة 2016 بتاريخ 2016/04/04. وقضت محكمة النقض الفلسطينية في حكم آخر بأنه: "ترى هذه المحكمة أن المحكمة الاستئنافية حينما عدلت حكم محكمة أول درجة وأدانت الطاعن بالتهمة الأولى المسندة إليه قد أعملت وظيفتها الأساسية وهي إعادة النظر في الحكم المستأنف من الناحيتين القانونية والموضوعية وأعملت صلاحيتها في الرقابة على محكمة أول درجة في تقدير الشهود وأنزلت صحيح حكم القانون والسوابق القضائية بالنسبة للبينة التي ساقتها النيابة العامة ذلك أنه من المقرر قانونًا في المواد الجزائية جواز إثباتها بطرق الإثبات المقررة كافة ما لم ينص القانون على غير ذلك (م 206 من قانون الإجراءات الجزائية رقم 3 لسنة 2001) وأن من ضمن هذه الطرق حسبما نصت عليه المواد106، 108، 109 من قانون البينات رقم 4 لسنة 2001 القرائن القضائية كما أن ما استقر عليه قضاء هذه المحكمة من أن البينة الظرفية كافية لإثبات التهمة قبل فاعلها الأمر الذي يكون معه النعي على الحكم المطعون فيه بمخالفته للقانون على غير أساس متعينًا رفضه أما عن النعي على الحكم بإجحافه بحقوق الطاعن فإن هذا النعي مردود كذلك؛ لكون هذا السبب ليس من الأسباب الموجبة للطعن بالنقض طبقًا لنص المادة 251 من قانون الإجراءات الجنائية الأمر الذي يتعين معه رفض الطعن"، حكم محكمة النقض الفلسطينية المنعقدة في غزة في الدعوى الجزائية رقم 205 لسنة 2003 بتاريخ 2005/10/25.

الفرع الثاني

شرعية الأدلّة الرقمية المتحصلة من الموقع الإلكتروني أمام القاضي الجزائي

لحسن تطبيق مبدأ الشرعية الجنائية على الجرائم يتوجب على القاضي احترام مبدأ الشرعية الإجرائية، أو ما يعرف بشرعية الدليل الجنائي، فلا يسوغ له بناء حكمه على دليل جنائي غير شرعي، أو تحصل عليه المحقق بطرق غير شرعية، حتى يكتسي الدليل القضائي الحجية في إسناد واقعة الاتهام إلى المتهم أو نفيها عنه.

وانطلاقًا من مبدأ ضرورة أن يكون القضاء نزيهًا؛ فإنه يتوجب عليه أن يبني أحكامه وقراراته على أدلّة مشروعة، حيث يشترط في الدليل الجنائي عمومًا لقبوله كدليل إثبات أن يتم الحصول عليه بطرق مشروعة، وذلك يقتضي أن تكون الجهة المتخصصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون. كما أن الحديث عن مدى مشروعية الدليل الرقمي عمومًا والدليل الرقمي المتحصل من الموقع الإلكتروني في إثبات الجرائم الإلكترونية على وجه الخصوص يجرّنا حتمًا إلى لحديث عن مدى مشروعية طرق ووسائل الحصول عليه، مثل اللجوء إلى ممارسة إجراءات التفتيش في مختلف الوسائط التقنية الرقمية والوسط الافتراضي، الذي استعملت فيه الجريمة الإلكترونية، بالإضافة إلى أن هذا الإجراء ينبغي أن يمارس من سلطة التحقيق المتخصصة، وهي النيابة العامة[1].

ويرى الباحثان أن مجرد الحصول على الدليل الرقمي وتقديمه أمام القضاء لا يكفي لاعتماده كدليل للإدانة، إذ إنّ الطبيعة الفنية الخاصة لهذا الأخير يمكن العبث بمضمونها على نحو يحرف الحقيقة، فضلًا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على الدليل للوصول إلى الحقيقة عالية في مثل هذا النوع من الأدلّة، ولذلك تثور فكرة الشك في مصداقيتها كأدلّة إثبات جنائي.

وفي ظل النظم القانونية التي تعتمد النظام اللاتيني فإن للقاضي السلطة الواسعة في تقييم الدليل من حيث قيمته الدليلية، فله أن يقبل بالدليل أو أن يرفضه، وهو يعتمد في ذلك على مدى اقتناعه الشخصي، وبذلك يكون للقاضي في هذا النظام أن يستعمل سلطته في تقرير الدليل؛ بحيث تمتد لتشمل الأدلّة العلمية؛ لأنّ هذه الأخيرة لها قيمتها الاستدلالية في الإثبات، قد تصل إلى درجة اليقين كالأدلّة العلمية.

فالدليل الرقمي عمومًا والدليل الرقمي المتحصل من الموقع الإلكتروني في إثبات الجرائم الإلكترونية على وجه الخصوص– من حيث تدليله على الوقائع– تتوفر فيه شروط اليقين، مما لا يمكن قبول ممارسة

---

[1]. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، ط4، المجلد الأول، دار النهضة العربية، القاهرة، (1981)، ص506.

القاضي لسلطته في التأكد من ثبوت تلك الوقائع أو نفيها، ولكن هذا لا يناقض القول بأن هذا الدليل موضع شك من حيث سلامته والعبث به، وصحة الإجراءات المتبعة للحصول عليه، بحيث يمكن أن يثار الشك في سلامة الدليل الرقمي لسببين اثنين[1]، نذكرهما فيما يلي:

1. إمكانية العبث بالدليل على نحو يصبح مخالفًا للحقيقة، ومن ثمّ يكون هذا الدليل معبرًا عن واقعة معينة صنعت أساسًا لأجل التعبير عنها خلافًا للحقيقة، وذلك دون أن يكون لغير الخبراء في هذا المجال إدراك هذا التحريف أو التدمير الذي لحق بتلك الأدلّة.
2. كما أن احتمال حدوث الخطأ الفني في جمع وتحليل الدليل الرقمي ممكن جدًا، بالنظر إلى الأجهزة المعقدة التي تستعمل في ارتكاب الجريمة.

المطلب الثاني

آليات ضبط الأدلّة الرقمية للمواقع الإلكترونية

إن ضبط الدليل الرقمي بما في ذلك المتحصل من الموقع الإلكتروني من شأنه أن يُكوِن نظرة واضحة عن الجريمة الإلكترونية، ويمنح إمكانية تقديم هذا الدليل أمام القضاء لإثبات التهم الموجهة إلى مرتكبي الجرائم. كما أن عملية ضبط هذا الدليل من شأنها أن تضفي الصفة الشرعية للملاحقة الجزائية أمام القضاء؛ الأمر الذي يستدعي لغايات هذا البحث بيان مفهوم ضبط الأدلّة الرقمية المتحصلة من الموقع الإلكتروني في الفرع الأول، وإظهار آليات التعامل مع الأدلّة الرقمية المتحصلة من الموقع الإلكتروني في الفرع الثاني.

الفرع الأول

مفهوم ضبط الأدلّة الرقمية المتحصلة من الموقع الإلكتروني

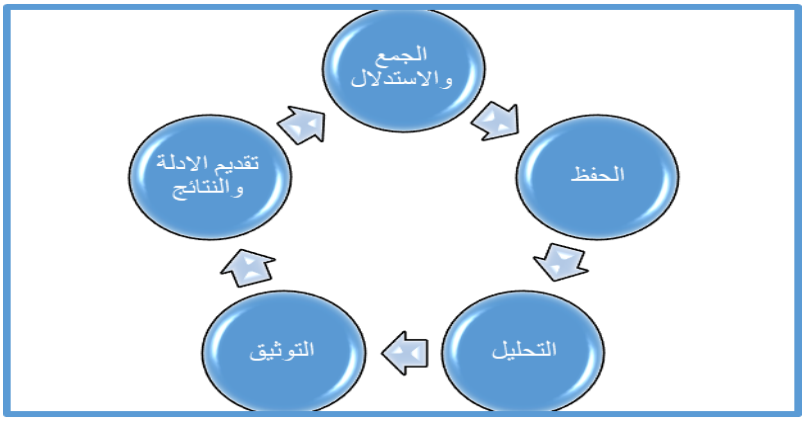
إن سلسلة حيازة الدليل (Chain of Custody)[2] ما هي إلا وسيلة تبين من حصل على الأدلّة، وأين ومتى تم الحصول على هذه الأدلّة، ومن قام بتأمين الأدلّة والتعامل معها، والشكل الآتي يوضح مراحل الحياة وفترتها التي يمر بها الدليل الرقمي[3]:

---

[1]. عبد الإله أحمد المرجع السابق، ص43.

[2]. International Bar Association (2016), Evidence Matters in ICC Trials, The Global Voice of Legal Profession, United Kingdom, P.19-20.

[3]. مقابلة مع الأستاذ علاء التميمي/ رئيس النيابة العامة، رام الله، بتاريخ 2022/01/05.



1. **الجمع والاستدلال:** ويمكن تسمية هذه المرحلة البحث والضبط، وتتم هذه المرحلة من خلال ضباط مدربين للقيام بهذه المهمة، ومن المهم أيضًا عند القيام بهذه المهمة مراعاة عدة أمور في أثناء التواجد في مسرح الجريمة الإلكترونية:
   - تأمين المشهد ماديًا وإلكترونيًا.
   - فصل اتصالات البيانات الخارجية.
   - تحديد الأجهزة والبيانات التي نود حفظها.
   - يمكن أن تتضمن أي شكل من أشكال البيانات، أو الأجهزة الإلكترونية، مثل: ملفات محملة من موقع إلكتروني، ورسائل البريد الإلكتروني، وأنشطة الإنترنت، وأجهزة الكمبيوتر الشخصية، وأجهزة الكمبيوتر المحمولة، ومحركات الأقراص الثابتة، والهواتف المحمولة، وأجهزة المساعد الرقمي الشخصي، والكاميرات الرقمية.
2. **حفظ الدليل الرقمي:** في هذه المرحلة يتم عزل الأدلّة الرقمية وحمايتها تمامًا كما وجدت دون تغيير، حيث يمكن تحليلها لاحقًا، ومن المهم اتخاذ تدابير وقائية مهمة من أجل الحفاظ على الدليل الرقمي[1]:
   - اتخاذ جميع التدابير اللازمة لتجنب تغيير الأدلّة أو إتلافها.
   - النقل إلى خزانة الأدلّة إن أمكن.
   - إنتاج نسخة طبق الأصل من القرص الصلب (صورة) وأحيانًا في مسرح الجريمة إن كان هذا ضروريًا.

[1] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1، المكتب الجامعي الحديث، بغداد، (2012)، ص 54.

3. **التحليل:** يتم في هذه المرحلة تحليل الأدلّة الرقمية والعمل على النسخ المطابقة التي تم الحصول عليها من خلال الأدلّة الرقمية، ومن المهم في هذه المرحلة التعامل مع العديد من الأمور والملفات، ومنها:
   - استكشاف واستخراج كل الملفات.
   - استعادة كل (أو ما يمكن استعادته) من الملفات المحذوفة.
   - الكشف عن محتويات الملفات المخفية، وكذلك الملفات المؤقتة منها المستخدمة في كل من برامج التطبيق ونظام التشغيل.
   - الوصول إلى محتويات الملفات المحمية والمشفرة.
   - العثور على الملفات التي تم استخدامها للجريمة.
4. **التوثيق وتقديم الأدلّة:** وتُعد هذه المرحلة هي المرحلة النهائية للتعامل مع الدليل الرقمي؛ حيث يتم خلال هذه المرحلة العمل على:
   - كتابة تقرير رسمي نهائي (يذكر الخبير ما فعله وما وجده).
   - توفير ملفات صور النظام.
   - بيان الأدلّة المستخرجة.
   - وجود تقارير أدوات التحليل الرقمي المستخدمة للتحليل.
   - تقديم النتائج والشهادة عليها.

الفرع الثاني

آليات التعامل مع الأدلّة الرقمية المتحصلة من الموقع الإلكتروني

لما كان الضبط بحسب الأصل لا يرد إلا على الأشياء المادية، فليس هناك صعوبة في ضبط أدلّة الجريمة الواقعة على المكونات المادية للحاسوب كرفع البصمات مثلًا، وكذلك لا صعوبة أيضًا في ضبط الدعامة المادية للبرامج أو الوسائل المستخدمة في إتلاف البرامج؛ ولكن في ضبط بيانات الحاسوب أو الموقع الإلكتروني، ولعدم وجود أيّ دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شيفرات المرور أو ترميز البيانات؛ فلا بد أن يتم اتِّباع قواعد فنية لحماية

البيانات وتجنيبها خطر الإتلاف[1]، مما دفع المشرع الفلسطيني[2] إلى توسيع صلاحيات سلطة التحقيق في ضبط ما يحتويه الحاسوب من بيانات دون إخطار مسبق بعملية التفتيش والضبط.

فالمادتان (32) و(33) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته تمنح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، ودون أمر من المحكمة المتخصصة، بتفتيش وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية، والتحفظ على كامل نظام المعلومات، أو أية وسيلة من وسائل تكنولوجيا المعلومات من شأنها أن تساعد على كشف الحقيقة، ودون حضور المتهم أو حائز الأجهزة لإجراءات التفتيش والضبط، ودون تحديد لمدة أمر التفتيش في النص المذكور.

ونعتقد بأن هذا الاتجاه قد ينتقص من ضمانات المتهم في مرحلة التحقيق؛ حيث ينبغي أن تتم تلك الإجراءات بناء على طلب من النيابة العامة، وقرار من المحكمة المتخصصة، وأن تتم في حضور المتهم أو حائز الأجهزة، وضمان توقيعه على محضر التفتيش، وأن يكون القرار الصادر عن المحكمة المتخصصة بالتفتيش محددًا زمنيًا، وذلك حفاظًا على ضمانات المتهم في مرحلة التحقيق الابتدائي، وانسجامًا مع الاتفاقيات والمعايير الدولية على هذا الصعيد[3].

---

1. أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، ط1، دار الجامعة الجديدة للنشر، الإسكندرية، (2018)، ص 149.
2. المادتان (32) و(33) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته.
3. وهذا ما أكد عليه المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في تقريره المقدم إلى مجلس حقوق الإنسان في العام 2013 وثيقة رقم (A/HRC/23/40) في بند "الاستنتاجات والتوصيات" التي خرج بها التقرير وتحديدًا في البند (81) على أنه "ينبغي على الدول أن تنظر إلى مراقبة الاتصالات ووسائل تكنولوجيا المعلومات كعمل تطفلي بدرجة كبيرة ربما يتعارض مع الحق في حرية التعبير والحق في الخصوصية ويهدد دعائم المجتمع الديمقراطي. ويجب على التشريعات أن تنص على وجوب ألا تقوم الدولة بالمراقبة إلا في ظروف استثنائية جدًا، وأن يكون ذلك حصرًا تحت إشراف سلطة قضائية مستقلة، ويجب أن يتضمن القانون ضمانات واضحة عن طبيعة التدابير الممكنة، ونطاقها ومدتها الزمنية والأسس اللازمة للأمر بها، ونوع الانتصاف الذي تتضمنه التشريعات الوطنية". وهذا ما أكدت عليه أيضًا المبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات للعام 2014 وذلك في المبدأ السادس الذي شدد على أن القرارات المتعلقة بمراقبة الاتصالات يجب أن تضطلع بها سلطة قضائية كفؤة نزيهة ومستقلة منفصلة عن الجهات التي تضطلع بمراقبة الاتصالات، علمًا بأن تفتيش وسائل تكنولوجيا المعلومات يندرج في تعريف "مراقبة الاتصالات" بموجب تلك المبادئ الدولية.

فقواعد الإثبات الجنائية التقليدية المعمول بها لا تصلح لإثبات الجرائم الإلكترونية بشكل مباشر؛ بل يحتاج ذلك إلى جهات إنفاذ قانون متخصصة وقضاة ووكلاء نيابة متخصصين في الشأن ذاته. وحتى يصبح الدليل الرقمي بشكل عام_ وذلك المتحصل من الموقع الإلكتروني على وجه الخصوص_ دليلًا يعتمد عليه في كشف أثر الجريمة الإلكترونية وتتبعه، تقوم جهات إنفاذ القانون المتخصصة بمكافحة الجرائم الإلكترونية باستخدام برامج الكشف والتتبع[1]، واتخاذ إجراءات التفتيش الإلكتروني التي تشكل في مجملها وسائل لضبط أدلّة يمكن التحرز عليها وضبطها والاستعانة بأهل الفن والدراسة والخبرة؛ لمعرفة أماكن تخزين المعلومات وإجراءات إرسالها، ويبقى الحذر مطلوبًا في هذا النوع من الجرائم؛ وذلك من خلال خلق آلية متطورة لا يكلفها إلا التعاون الدولي وتبادل الخبرات والممارسات الفضلى في هذا المجال.

مما حدا بالمشرع الفلسطيني وعلى غرار قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 للنص في المادة (37) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته على أنه: "يُعد الدليل الناتج بأية وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية، من أدلّة الإثبات"[2]، فيما نصت المادة (38) من القانون ذاته على أنه: "يُعد الدليل الناتج بأية وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية من أدلّة الإثبات"[3]. وقد تميز المشرع الفلسطيني بهذه النصوص والتي لم يرد لها نظير في قانون الجرائم الإلكترونية الأردني رقم (24) لسنة 2015 وتعديلاته. كونها عُدّت بشكل صريح الأدلّة

[1] Law Reform Commission (2009), Documentary and Electronic Evidence, First Published, Dublin, P.1.

[2] نصت المادة (11) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 على أنه: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة، أو المعدات، أو الوسائط، أو الدعامات الإلكترونية، أو من النظام المعلوماتي، أو من برامج الحاسب، أو من أية وسيلة لتقنية المعلومات، ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة في اللائحة التنفيذية لهذا القانون".

[3] نصت المادة (4) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018 على أنه: "تعمل السلطات المصرية المتخصصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها، على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن".

الناتجة بأية وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية من أدلّة الإثبات الجنائي.

الخاتمة

وفي نهاية هذه الدراسة البحثية التي هي إبراز لأهم النتائج التي توصلت إليها، وبيان لأهم المقترحات التي يمكن التوصية بها، فقد توصلت هذه الدراسة إلى عدد من النتائج والتوصيات، والتي يمكن إجمال أهمها فيما يأتي:

أولاً: النتائج

1. الأدلّة الرقمية هي عبارة عن معلومات مرسلة أو مخزنة كبيانات رقمية يمكن أن يستعملها أحد أطراف الدعوى، وقد تكون هذه الأدلّة على شكل صور فوتوغرافية، أو صور الأقمار الاصطناعية، أو فيديو، أو تسجيل صوتي، أو بريد إلكتروني، أو أن تكون على شكل موقع إلكتروني.
2. من الثابت أن المواقع الإلكترونية تجعل من الصعوبة بمكان الحصول عليها؛ إلا إنّ التقنيات العلمية الحديثة أدّت دورها الفاعل في إمكانية ضبط وتوثيق هذه الأدلّة، وإمكانية استرجاعها بعد محوها وإظهارها بعد إخفائها.
3. وصف مبدأ حرية الإثبات الجنائي أساسًا لقبول الدليل الرقمي بشكل عام، وتلك المتحصلة من المواقع الإلكترونية على وجه الخصوص في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته.
4. لم يفرد القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، تنظيمًا قانونيًا خاصًا يعالج كل المسائل ذات الصلة بالدليل الرقمي.
5. الدليل الرقمي أصبح حجة يُعتد بها في إثبات الجرائم الإلكترونية متى كان سالمًا من العوارض؛ إذ إنّ عدم الأخذ به يؤدي إلى ضياع الحقوق، وإفلات المجرم من العقاب، إذ أوضحت الدراسة بأن الأدلّة الرقمية لها حجية بشرط اتِّباع الإجراءات الصحيحة في استخلاصها في مرحلة جمع الاستدلالات والتحقيق الابتدائي، ويتبع ذلك خضوعها للتدقيق والمناقشة أمام القاضي حتى يُكوّن قناعته، ويبني عليها حكمه؛ إذا كانت كافية ومشروعة، وتساندت مع باقي الأدلّة.

ثانياً: التوصيات

1. نوصي المشرع الفلسطيني بإعادة النظر في المادتين (32) و(33) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية وتعديلاته، والتي تمنح الصلاحية للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي، ودون أمر من المحكمة المتخصصة، بتفتيش وسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية، والتحفظ على كامل نظام المعلومات أو أية وسيلة من وسائل تكنولوجيا المعلومات.
2. نتمنى على المشرع الفلسطيني الاهتمام بجانب التعاون القضائي الدولي؛ لغايات تيسير جمع الأدلّة الإلكترونية، والسعي لإيجاد تنظيم قانوني خاص للتعاون المباشر مع مقدم خدمة الإنترنت؛ حيث تمتاز الجرائم الإلكترونية بأنها لا تعترف بالحدود الجغرافية بين الدول؛ وذلك بسبب انتشار شبكات الإنترنت بين دول العالم، فهي جرائم تنتشر بين الدول بوساطة تلك الشبكات فمن المتصور ارتكاب جريمة في دولة ما والضحية في دولة أخرى، ويكون الدليل في دولة ثالثة، مما يتطلب مزيدًا من تكريس التعاون الدولي والقضائي.
3. نقترح على المشرع إقرار نصوص تعالج كل المسائل ذات الصلة بالدليل الرقمي، بحيث تبين بشكل واضح آليات ضبطه، وشروط قبوله في الإثبات، وحجيته سواء أكان في إثبات وقوع جريمة إلكترونية بوسيلة إلكترونية، أم في وقوع جريمة تقليدية بوسيلة إلكترونية.
4. نوصي جهات إنفاذ القانون بالالتزام بالقانون الأساسي المعدل لسنة 2003 فيما يتعلق بأي تدخلات في الحياة الخاصة للإنسان، لا سيما المواد (10، 11، 17، 32)، وأن يمنحوه الأفضلية في التطبيق على القوانين الأخرى التي تتعارض معه تطبيقًا لقاعدة هرمية التشريعات.

بيان تضارب المصالح

يقر جميع المؤلفين أنه ليس لديهم أي تضارب في المصالح.

قائمة المصادر والمراجع

أولًا: القوانين

1. قانون الإجراءات الجزائية رقم (3) لسنة 2001 وتعديلاته.
2. قانون الجرائم الإلكترونية الأردني رقم (24) لسنة 2015م.
3. قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018م.
4. القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية الفلسطيني وتعديلاته.

ثانيًا: الكتب الفقهية

1. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، ط4، المجلد الأول، دار النهضة العربية، القاهرة، 1981.
2. ربحي مصطفى عليان، وسائل الاتصال وتكنولوجيا التعليم، ط 2، دار صفاء للنشر والتوزيع، عمان، 2003.
3. علي عدنان الفيل، إجراءات التحري وجمع الأدلّة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1، المكتب الجامعي الحديث، بغداد، 2012.
4. أشرف عبد القادر قنديل، الوسائل الإلكترونية ودورها في الإثبات الجنائي، دراسة مقارنة، ط1، دار الجامعة الجديدة للنشر، الإسكندرية، 2018.
5. عبد الناصر محمود، محمد فرغلي المسماري، محمد عبيد سيف سعيد، الإثبات الجنائي بالأدلّة الرقمية من الناحيتين القانونية والفنية، (د. ط)، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.
6. أسامة المناعسة، جلال الزعبي، جرائم تقنية المعلومات، دراسة مقارنة، ط1، دار الثقافة للنشر والتوزيع، عمان، 2014.
7. عبد الإله أحمد هلالي، حجية المخرجات الكمبيوترية، ط1، دار النهضة العربية، القاهرة، 1997.
8. محمد حماد الهيتي، التحقيق الجنائي والأدلّة الجرمية، ط 1، دار المناهج للنشر والتوزيع، عمان، 2010.

ثالثًا: الرسائل الجامعية

1. بسام ليدية، الدليل الرقمي في الإثبات الجنائي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة- بجاية، الجزائر، 2017-2018.

2. طاهري عبد المطلب، الإثبات الجنائي بالأدلّة الرقمية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر، 2014-2015.

رابعًا: البحوث

1. بيل جيتس، المعلوماتية بعد الإنترنت– طريق المستقبل، ترجمة عبد السلام رضوان، مجلة عالم المعرفة، العدد 231، الكويت، 1998.
2. ميسون خلف الحمداني، مشروعية الأدلّة الإلكترونية في الإثبات الجنائي، بحث منشور في مجلة الحقوق، العدد 18، جامعة النهرين، بغداد، 2016.

خامسًا: المؤتمرات والتقارير

1. تقرير صادر عن مركز (هردو) لدعم التعبير الرقمي، الجريمة الإلكترونية، وحجية الدليل الرقمي في الإثبات الجنائي، القاهرة، 2014.
2. مفتلح بوبكر مطردي، الجريمة الإلكترونية والتغلب على تحدياتها، مؤتمر رؤساء المحاكم العليا في الدول العربية، السودان، 2012.

سادساً: المراجع الأجنبية

1. Aljneibi, Khaled Ali, The Regulation of Electronic Evidence in the United Arab Emirates: Current Limitations and Proposals for Reform, PHD Thesis, Bangor University, Wales, UK. 2014
2. Ashouri, Aida and Others, An Overview of the Use of digital Evidence in International Criminal Courts, Working Paper, Salzburg Workshop on Cyber Investigation. 2013
3. Cambridge Dictionary:
4. Carrier, Brian and Spafford Eugene H., Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vo1.2. 2003
5. Casey, Eoghan, Digital evidence and computer crime – Forensic Science, computer and the Internet, Published by Elsevier Inc, USA. 2011
6. Dutelle, Airc W, An Introduction to crime scene Investigation, thired Edition, Jones & Bartleff learning, USA. 2017
7. Dutelle, Airc W., An Introduction to crime scene Investigation, second Edition, Jones & Bartleff learning, USA. 2014
8. Gercke, Marco, Understanding cybercrime: Phenomena, challenges and legal response, ITU publication, Switzerland – Geneva. 2012
9. Goodison, Sean E. and Others, Digital Evidence and the U.S. Criminal Justice System, RAND Corporation, U.S. 2015.
10. Grobler, Marthie, The Need for Digital Evidence Standardisation, International Journal of Digital Crime and Forensics, 4(2). 2012
11. https://dictionary.cambridge.org/dictionary/english/digital.
12. International Bar Association, Evidence Matters in ICC Trials, The Global Voice of Legal Profession, United Kingdom. 2016

13. INTERPOL, European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing. 2011
14. Law Reform Commission, Documentary and Electronic Evidence, First Published, Dublin. 2009
15. Mason, Stephan, International Electronic Evidence, British Institute of International and Comparative law, London. 2008
16. Outerbridge, David and Siller, Ezra, The Admissibility of Electronic Evidence, Torys LLP, Toronto.
17. Petit, Robert and Warren, Maria and Akerson, David (2012), Prosecution Mass Atrocities Lessons from the International Tribunals, open society Foundation, Bangkok – Thailand.
18. Whitcomb, Carrie Morgan (2002), An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vo1.1.
19. Wilkinson, Sue, Association of Chief Police Officers (ACPO), Good Practice Guide for Computer-Based Electronic Evidence, published by 7safe, Official release version 4.0, United Kingdom.