Journal of Economic, Administrative and Legal Sciences (JEALS) • Vol 7, Sup Issue 10 (2023) • P: 53 - 37
https://journals.ajsrp.com/index.php/jeals
ISSN: 2522-3372 (Online) • ISSN: 2522-3372 (Print)

The validity of electronic evidence in Omani law

Mr. Hamad Salem Hamad Al-Alawi

College of Legal, Economic and Social Sciences | Ibn Zohr University | Kingdom of Morocco

Received: 03/09/2023

Revised: 14/09/2023

Accepted: 28/09/2023

Published: 30/10/2023

* Corresponding author: hsh133@hotmail.com

Citation: Al-Alawi, H. S. (2023). The validity of electronic evidence in Omani law. *Journal of Economic, Administrative and Legal Sciences, 7*(10S), 37 – 53. https://doi.org/10.26389/AJSRP.L030923

Abstract: This study aimed to identify the authenticity of electronic evidence in the Omani Law and the role of the Omani legislation regards the way of dealing with electronic evidence as evidence of proof. To achieve the objective of this study, the descriptive analytical legal approach was used.

The results showed that, despite the difficulties encountered by the concerned authorities in the field of criminal proof, the Omani legislator was able to keep up with civilizational progress by enacting laws to regulate electronic evidence. Moreover, the legislation cared about electronic evidence and regulated the way of obtaining it given its importance for criminal proof. The research came up with various recommendations; most notably that it is required to qualify a specialized cadre of judicial officers and electronic crime cases officers by providing courses and practical programs in information technology and methods of getting evidence to be protected from being lost. The recommendations also emphasized the importance of international collaboration in criminal affairs, especially in terms of electronic crimes and collecting electronic evidence.

Keywords: Electronic Evidence – Omani legislator – Criminal Evidence.

حجية الأدلة الإلكترونية في القانون العماني

أ. حمد بن سالم بن حمد العلوي

كلية العلوم القانونية والاقتصادية والاجتماعية | جامعة ابن زهر | المملكة المغربية

المستخلص: هدفت الدراسة إلى التعرف على مدى حجية الأدلة الالكترونية في القانون العماني، ودور التشريع العماني في كيفية التعامل مع الدليل الإلكتروني كدليل للإثبات، ومن أجل تحقيق هدف البحث الرئيس، فقد تم استخدام المنهج القانوني الوصفي التحليلي.

وتوصل البحث إلى أن المشرع العماني استطاع مواكبة التقدم الحضاري من خلال تطوير القوانين التي تنظم الأدلة الإلكترونية بالرغم من الصعوبات التي تواجهها السلطات في مجال الإثبات الجنائي، كما أن التشريعات اهتمت بالدليل الإلكتروني ونظمت كيفية الحصول عليه نظراً لأهمية في الإثبات الجنائي، وتوصل البحث إلى جملة من التوصيات من أهمها تأهيل كادر متخصص من مأموري الضبط القضائي والقائمين على قضايا الجرائم الإلكترونية بدورات وبرامج عملية في تقنية المعلومات وكيفية استخراج والحصول على الدليل الإلكتروني لحمايته من الضياع، والتأكيد على أهمية التعاون الدولي في المجال الجنائي وخاصة فيما يتعلق بالجرائم الإلكترونية وجمع الأدلة الالكترونية.

الكلمات المفتاحية: الدليل الإلكتروني – المشرع العماني – الإثبات الجنائي.

المقدمة:

لم تسلم طرق الإثبات من التأثيرات الناتجة عن ثورة المعلومات والتكنولوجيا، ذلك أن التوافق المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي يتولد منها، أدى إلى استحداث نوعاً جديداً من الأدلة يتماشى مع طبيعة جرائم تقنية المعلومات، وهو ما يعرف بالدليل الرقمي أو الدليل الإلكتروني، أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواسب وشبكة الانترنت، ومع التطور السريع في التقنيات أصبح المجرمون يستخدمون الوسائل التقنية المتطورة لتنفيذ أعمالهم الإجرامية، وهذا يؤكد ضرورة التعرف على الأدلة المنبثقة عن هذه الوسائل، ومن أهم الأدلة العلمية التي أصبحت تهتم بها الجهات المعنية المكلفة بالبحث والتحقيق والمحاكمة الدليل الإلكتروني، وهذا الأخير يطرح مجموعة من التساؤلات والإشكالات سواء على مستوى طبيعته أو تحصيله أو على مستوى مشروعيته.

ويلاحظ أن الدليل الإلكتروني لا يتعلق فقط بجرائم تقنية المعلومات، فقد تكون الجريمة عادية مثل القتل أو التهريب أو السرقة وغيرها لكن الدليل الذي يدين المجرمين هو دليل رقمي والبيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح مفردة أو مجتمعة لكي تكون دليلاً للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل، حيث يرتبط الدليل عموماً بفكرتي الشرعية والحقيقة، فهو الوسيلة الوحيدة للوصول إلى الحقيقة المراد إثباتها أمام القضاء.

أهمية الدراسة:

تبرز أهمية الدراسة في كونها تتناول أحد أهم العوامل التي يتم فيها إثبات الجرائم المادية وتحديد المسؤولية الجزائية، وبالتالي يتوقف عليها الحكم على المتهم بالجريمة من عدمه، فالدليل هو وسيلة لإظهار الحقيقة وهو حجر الأساس في ثبوت الواقعة من عدمه، حيث أنه جاء مصاحباً للتطور التكنولوجي لتقنية المعلومات والاتصالات، وتبرز أهمية الموضوع في أنه أصبح لزاماً على أجهزة العدالة أن تتعامل مع الدليل الإلكتروني كدليل مستحدث في مجال الإثبات الجنائي، مما يتحتم على الجهات المعنية مواكبة للتطور التكنولوجيا من جهة ومكافحة الجريمة الإلكترونية من جهة أخرى، كما تظهر أهمية الدراسة في أنها تساهم في إثراء المكتبة العربية المتخصصة في هذا المجال، إذ أنها من الدراسات القليلة التي تناولت الدليل الإلكتروني وبالتالي معرفة مدى مواكبة الجهات المعنية للتطور الحاصل في تكنولوجيا المعلومات.

أهداف الدراسة:

- التعرف على الدليل الإلكتروني وخصائصه.
- معرفة الشروط الواجب توافرها للحصول على الدليل الإلكتروني.
- التعرف على إجراءات وإشكاليات جمع الأدلة الإلكترونية .
- المساهمة في إثراء المكتبة العربية فيما يتعلق بموضوع الدليل الإلكتروني كأداة لكشف الجريمة ومرتكبيها وتقديمهم للعدالة.

إشكالية الدراسة وتساؤلاتها:

تدور إشكالية الدراسة وتساؤلاتها حول مدى حجية الأدلة الالكترونية في القانون العماني، ذلك أن هذا الموضوع يثير اشكالية حقيقية متعلقة بالأدلة الالكترونية واثباتها وحجيتها القانونية في القانون العماني، حيث أن الدليل الإلكتروني من الأدلة التي يصعب الحصول عليها إلا بخطوات معقدة، وما يثيره من مشكلات عند قبوله كدليل في الإثبات الجنائي.

فالحصول على الدليل الإلكتروني يشكل صعوبة بالغة على مأموري الضبط القضائي في الوصول لمرتكب الجريمة، وأعضاء سلطة التحقيق في إجراءات وأعمال التحقيق في الجرائم وإثباتها من قبلهم، ولدى القضاء كذلك من حيث قبول وتقدير الأدلة .

منهج الدراسة:

اتبعت الدراسة المهج الوصفي التحليلي من خلال عرض الاتجاهات الفقهية والتطرق إلى بعض النصوص القانونية وتحليلها والوقوف على أوجه الضعف والقصور بها إن وجدت، مع بيان الرأي القانوني إذا دعت الحاجة إلى ذلك .

نطاق الدراسة:

ينحصر نطاق الدراسة حول طبيعة الدليل الإلكتروني وخصائصه والتحديات التي تواجه الاستدلال والإثبات، والتحديات الإجرائية في الضبط والتفتيش في القانون العماني .

هيكل الدراسة:

تحتوي الدراسة على مبحثين رئيسيين، يحتوي كل مبحث على مطلبين على النحو التالي: -

المبحث الأول: ماهية الدليل الإلكتروني.

المطلب الأول: تعريف الدليل الإلكتروني وخصائصه.

المطلب الثاني: القواعد الإجرائية للدليل الإلكتروني.

المبحث الثاني: إجراءات وإشكاليات جمع الأدلة الإلكترونية.

المطلب الأول: إجراءات جمع الأدلة الإلكترونية .

المطلب الثاني: إشكاليات جمع الأدلة الإلكترونية .

صعوبات الدراسة:

الصعوبات التي واجهت الدراسة تتركز في قلة الدراسات والمراجع العلمية التي تناولت الدليل الإلكتروني بصفة خاصة، بالإضافة إلى ندرة الأحكام القضائية التي تناولت كيفية الحصول على الدليل الإلكتروني، حيث أن القوانين الخاصة بالجرائم الإلكترونية حديثة النشأة.

المبحث الأول: ماهية الدليل الإلكتروني

يرتبط الدليل عموماً بفكرتي الشرعية والحقيقة، فمن جهة يعتبر الدليل الوسيلة الوحيدة للوصول إلى الحقيقة المراد إثباتها أمام القضاء، ومن جهة أخرى يجب أن يتميز هذا الدليل بكونه مشروعاً أي تم الحصول عليه وفق ما يقتضيه القانون، وإذا كان الحصول على الدليل يجب أن يجسد فكرة الانضباط لروح القانون فإن هناك مجموعة من الأفراد قد يتلاعبون بالأدلة التي قد تثبت إدانتهم فتضيع حقوق الضحايا وتندثر الأدلة ولا يحصلون جراء ذلك على حقوقهم.

وتتشارك الأدلة الإلكترونية مع الأشكال التقليدية للأدلة في بعض الخصائص ولكنها تمتلك أيضاً بعض الخصائص تميزها عن غيرها من الأدلة، كما أن البيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية وتصلح منفردة أو مجتمعة لكي تكون دليلاً للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص تميزه عن الدليل الجنائي التقليدي.

المطلب الأول: تعريف الدليل الإلكتروني وخصائصه

1. تعريف الدليل الإلكتروني

الدليل في اللغة هو: " المرشد وما يتم به الإرشاد وما يستدل به، والدليل هو الدال أيضاً والجمع أدلة أو دلالات "(الرازي، 1981، ص 209)، وورد في مختار الصحاح أن الدليل ما يستدل به وقد دله على الطريق أي أرشده، والدليل اصطلاحاً هو ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة، ويعرف الدليل اصطلاحاً بأنه: " توصل العقل إلى التصديق المفترض العلمي والمنطقي بما كان يشك بصحته بمعنى التوصل إلى معرفة الحقيقة " (المعمري، 2018، ص 192).

وقام العديد من الباحثين بتعريف الدليل الإلكتروني أو الدليل الرقمي من الناحية القانونية وكانت معظم هذه التعريفات منسجمه مع بعضها من حيث المضمون والدلالة وإن اختلفت في النص والطريقة، ومن هذه التعريفات للدليل الإلكتروني بأنه: " البيانات الرقمية المخزنة في الأجهزة الحاسبية أو المنظومات المعلوماتية أو المنقولة بواسطتها والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية"(فتح الله، 2015، ص 420)، كما تم تعريفه على أنه: " الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء" (عبدالمطلب، ممدوح عبدالحميد، 2006، ص 88).

ويتبين لنا من خلال التعريفات السابقة بأن الدليل الرقمي يختلف كثيراً عن نظيرة المادي، فهو لا يرتبط بالضرورة بمسرح الجريمة بل يستخلص من الوسيلة التي يشتغل بها النظام المعلوماتي، فهو يوجد حتى قبل حصول الواقعة الإجرامية في النظام الإلكتروني، ولكن هذا لا يفسر سهولة الحصول عليه أو الاحتجاج به في أي وقت، ذلك أن ما سبق ينقلب كعائق حقيقي أمام جهات التحقيق والقاضي الجنائي.

وينقسم الدليل الرقمي إلى نوعين هما، النوع الأول: أدلة أعدت لتكون وسيلة إثبات وهي تشمل السجلات التي يتم إنشاؤها تلقائياً بواسطة الأجهزة الإلكترونية كأدلة رقمية دون تدخل الإنسان ومنها سجلات الهاتف وفواتير أجهزة الحاسب الآلي، وهناك أدلة رقمية تم حفظها عن طريق إدخالها في جهاز الحاسب الآلي كالبيانات والمعلومات التي تم إدخالها وثم معالجتها عن طريق برامج معده لذلك، النوع الثاني: أدلة لم تعد لتكون وسيلة إثبات ونشأت دون إرادة الشخص، ويعد هذا النوع من الأدلة من الآثار التي يتركها الجاني دون أن يعلم بذلك ودون أن يكون راغباً في وجودها، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة العنكبوتية التي تمت من خلال الآلة أو المعلومات العالمية، ومن أمثلة هذا النوع البصمة الإلكترونية حيث ينشأ هذا الدليل عند استخدام الحاسب الآلي أو شبكة الإنترنت من سجلات أو بيانات تم تسجيلها عند إرسال أو استقبال الرسائل أو المكالمات سواء عن طريق جهاز الحاسب الآلي أو الشبكة العنكبوتية، وبصورة عامة قد تكون الأدلة الرقمية مخرجات ورقية يتم استخراجها من جهاز الحاسوب، أو مخرجات غير ورقية كالأشرطة أو الأقراص أو عرض البيانات على شاشة الحاسوب، فإذا ما تم تحصيل هذه الأدلة بصورة غير مشروعة فإنه سيكون باطلاً وبالتالي لا يمكن الاعتماد عليه في الإثبات (الزعابي، 2014).

2. الحجية القانونية للأدلة الإلكترونية

اختلفت الآراء حول مسألة مشروعية الدليل الإلكتروني وحول مدى إمكانية الأخذ به على إطلاقه أو أن يعتمد نسبياً، كما اختلفت نظم الإجراءات الجنائية وتنوعت تبعاً لاختلاف الأوضاع الاجتماعية والسياسية للشعوب، وهذه الأوضاع فرضت على التشريعات الجنائية أن تنتهج نظاماً إجرائياً معيناً من أجل العمل على إثبات الجريمة، فمنها ما يأخذ بالنظام الحر ومنها ما يجعل الدليل مقيداً بنصوص قانونية على سبيل الحصر ومنها ما يأخذ بالنظامين معاً.

ويتمتع القاضي في نظام الإثبات الحر بالحرية المطلقة في إثبات الوقائع المعروضة عليه ولا يلزمه القانون بأدلة معينة للاستناد عليها في تكوين قناعته الشخصية، وإن حجية الأدلة الإلكترونية لا تثير أي إشكالية متعلقة بمدى حرية تقديم الأدلة لإثبات جرائم الحاسوب، ولا بمدى حرية القاضي الجنائي في تقدير هذه الأدلة ذات الطبيعة الخاصة باعتبارها أدلة إثبات في المواد الجنائية أم لا، فالأساس الذي يقوم عليه نظام الإثبات الحر هو اقتناع القاضي بالأدلة المعروضة عليه، ويقصد بذلك ما يبذله القاضي من جهد عقلي أثناء نظر الدعوى انتهاء إلى الوصول إلى الحقيقة بالحكم الذي يصدره، وعليه يمكن القول أن اقتناع القاضي هو البديل لنظام الأدلة القانونية وهو تقدير مسبب لعناصر الإثبات في الدعوى(الرقيشي، 2008).

إلا أن حرية الاختيار والتقدير للقاضي وفق قناعته لا تعني أنها على إطلاقها، فليس له أن يدخل تخميناته وتصوراته الشخصية ضمن أدلة الإثبات التي يبني عليها حكمه أو يحلها محل الأدلة المقدمة، ويعاب على هذا النظام أنه يعزز الثقة في التعامل، فالتقدير في مسائل الإثبات يختلف من قاضي إلى آخر، وهذا الاختلاف يعرض المتقاضين للمفاجئات فلا يكونوا على بينه من أن الأدلة المقدمة من شأنها إقناع القاضي أم لا .

أما بالنسبة لنظام الإثبات المقيد فيتمثل في أن المشرع الجنائي يعد سلفاً الوسائل ومختلف الطرق التي يعتمدها في إقامة الدليل الجنائي على مرتكبي الجرائم، وليس للقاضي توظيف قناعته في تقدير الأدلة وتحديدها، كما أن المشرع يحدد القوة القانونية للدليل إذا ما توافرت فيه الشروط والعناصر التي يتطلبها، ويعاب على هذا النظام أنه يقيد سلطة القاضي بأنواع محدده من الأدلة دون النظر لاقتناعه فيها، وما هو معروض أمامه من وقائع وأدلة، وهو ما يعد إغفال لقناعة القاضي في الدعوى.

أما بالنسبة للنظام الثالث في الإثبات فهو النظام المختلط، فهو يجمع إيجابيات النظام الحر والمقيد ويتحاشى سلبياتهما، إذ أنه يتقف مع تحديد طرق الإثبات إلا أنه يمنح القاضي سلطة تقدير الأدلة، ويعد هذا النظام أفضل الأنظمة المعمول بها في الإثبات، لأنه يجمع بين مزايا النظامين السابقين ويتجنب مساوئهما وسلبياتهما(الرقيشي، 2008).

وقد أخذ المشرع العُماني بمذهب الإثبات المختلط، الذي يعد من أهم مميزاته السماح للقاضي في توجيه أطراف الدعوى واستكمال الأدلة الناقصة، والاستيضاح عن النقاط الغامضة في وقائع الدعوى المعروضة أمامه بشرط عدم تعارضها.

3. خصائص الدليل الإلكتروني

أ- الدليل الإلكتروني دليل علمي

يتكون الدليل من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقني متخصص يتعامل معه، وهذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يكون فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني (الرقيشي، 2008).

لذلك فإن الدليل الإلكتروني ذو طبيعة غير مرئية ولعل هذه الطبيعة للأدلة المتحصلة من الوسائل الإلكترونية تلقي بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية، حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه

خاصة في حالات التلاعب في برامج الحاسبات، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة، فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائط التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية كما يطبقها على المعلومات المعنوية.

كما أن من طبيعة الدليل الإلكتروني تعرض ذاكرة الحاسب الآلي للتلف نتيجة العوامل البيئية مثل الحرارة الشديدة أو الرطوبة أو وجود الحقول الكهرومغناطيسية، كما أن أجهزة الحاسب الآلي تتغير بسبب أية استخدامات أخرى سواءً كان ذلك بناء على طلب المستخدم كالحفظ أو النسخ أو يكون ذلك تلقائياً بواسطة نظام تشغيل جهاز الحاسب الآلي.

كما تعني أن خاصية الدليل الإلكتروني دليل علمي أن تكون عملية حفظ الدليل عند ضبطه أو اكتشافه على أساس علمي، فتحرير محضر الضبط أو المعاينة للدليل الإلكتروني لابد أن تكون مختلفة، ففي عملية تحرير محضر يتناول دليلاً علمياً يختلف عنه في تحرير محضر يتناول اعتراف شخص بجريمة قتل أو سرقة عادية أو إيذاء، ويعني ذلك أن تحرير محضر يتناول دليل علمي تكون بضرورة التطرق لأساس علمي في التحرير يتوافق مع الدليل العلمي محل المعاينة (الرقيشي، 2008).

ب- الدليل الإلكتروني دليل تقني

فالدليل الإلكتروني مستوح من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الإلكترونية في العالم الافتراضي، وهذا العالم كامن في الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها، فالأدلة الرقمية ليست مثل الأدلة العادية التقليدية، حيث لا تنتج التقنية سكيناً يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو بصمة اصبع، وإنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان (قنديل، 2015).

كما أن هذا النوع من الأدلة يحتاج إلى متخصصين وذو خبرة عالية للتعامل معها خاصة بعد التقدم الكبير في تكنولوجيا تقنية المعلومات، ذلك أن كل نوع من الأجهزة الإلكترونية والشبكات المعلوماتية وغيرها تتطلب إجراءات خاصة، والتعامل مع تلكم الأجهزة من غير المختصين قد يتلف الأدلة أو يمحوها، لذلك فإنها تحتاج إلى أشخاص مختصين وذو خبرة في التعامل مع الأدلة الإلكترونية .

ويقصد بالتقنية على أنها علم تطبيقي لأدوات ووسائل تم اختراعها من أجل تسهيل حياة الفرد والمجتمع، وهي تقوم على أساس علمي مثلها مثل الدليل الإلكتروني الذي هو كذلك دليل علمي، ويمكن استنتاج أن الدليل الإلكتروني هو دليل تقني استناداً للمصدر الذي جاء منه وهو البيئة الرقمية أو التقنية، مثلما هو دليل علمي استناداً إلى البيئة التي يتواجد بها والتي تم إنشاؤها من قبل مختصين وفنيين على أساس علمي (الرقيشي، 2008).

ج- الدليل الإلكتروني يصعب التخلص منه

وتعد من أهم خصائص الدليل الإلكتروني، بل إنه يمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الإلكتروني عن غيرة من الأدلة التقليدية، حيث يمكن التخلص بسهولة من الأوراق والأشرطة المسجلة والسلاح والأموال المزورة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن أيضاً التخلص من بصمات الأصابع بمسحها من موضعها، بالإضافة إلى أنه يمكن التخلص من الشهود بقتلهم أو تهديدهم بعد الإدلاء بالشهادة، إلا أن الدليل الإلكتروني يصعب التخلص منه .

حيث يلجأ بعض المجرمون إلى حذف البيانات والملفات التي يمكن أن تحتوي أدلة رقمية قد تمثل إدانة للمتهم، وهذا لا يعني أن البيانات قد حذفت بالفعل حتى لو جرى إتلاف التجهيزات فيزيائياً، إذ يمكن في بعض الأحيان عبر استخدام أدوات وبرامج استرجاع البيانات المحذوفة، والطريقة الأكثر استخداماً لحذف الملفات بصورة نهائية هي الكتابة فوقها، حيث يعمد بعض المشتبه بهم إلى كتابة أصفار فوق البيانات القديمة مما يجعل استرجاعها مستحيلاً وتكون أمام حالة طمس الأدلة الرقمية.

بل إن محاولة الجاني لحذف الدليل يعد دليل آخر ضده، حيث أن جهاز الحاسب الآلي يقوم بتسجيل وحفظ المحاولات المستخدمة والأنشطة التي يقوم بها المستخدم بحذف أو إلغاء أو تعديل أي بيانات داخل الجهاز، وعليه فإن نشاط الجاني لحذف الدليل الإلكتروني يمكن استخراجه لاحقاً كدليل إدانة ضده، وكما أن التخلص من الدليل الإلكتروني باستخدام الأدوات المتوفرة في وسيلة التقنية مثل خيارات الحذف أو الإلغاء أو الإزالة لاتعد من العوائق التي تمنع من استرجاع الدليل، فهناك برامج متخصصة من ذات طبيعة الدليل التقني تمكن الجهات القضائية المختصة من الحصول على الدليل المحذوف واسترجاع البيانات الملغاة من الجهاز محل ارتكاب الجريمة.

د- الدليل الإلكتروني قابل للنسخ

الأصل أنه عند إعداد نسخة من محتوى دليل معين لا يكون مثل قوة الأصل في حجية إثباته سواءً في المجال الجنائي أو المدني، كما أن الأدلة التقليدية الأخرى على خلاف الدليل الإلكتروني فإنه لا يمكن الحصول على نسخ من تلك الأدلة لتقديمها كدليل

بديلاً عن الأصل، فالمحرر المزور لابد من مضاهاته مع الأصل عن طريق المستند المزور وليس نسخة منه، إلا أن ذلك يختلف في مجال الأدلة الإلكترونية فهو دليل يمكن استخراج منه نسخ مطابقة للأصل ويكون لتلك النسخة ذات القيمة العلمية للأصل (الرقيشي، 2008).

حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوفر في أنواع الأدلة الأخرى التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق نسخ طبق الأصل من الدليل، وإن نسخ المعلومات الرقمية بصورتها الآلية تعني أنه يمكن إجراء فحص الأدلة الرقمية من قبل المختصين وبالتوازي مع مختلف الاختصاصات ولأسباب مختلفة مع الاحتفاظ بالأصل .

هـ- السعة التخزينية العالية

يمتاز الدليل الإلكتروني بالسعة التخزينية العالية، فنجد أن بعض حافظات الذاكرة الإلكترونية تسع لآلاف من الصور والفيديوهات والمستندات، بل أن بعض منها يمكنه من تخزين عدد كبير من الكتب يوازي مكتبة صغيرة الحجم، ونرى أن التقدم العلمي في هذا المجال يتطور يوماً بعد يوم، حيث أن حافظات الذاكرة تصغر في الحجم وتزداد في سعتها التخزينية .

و- التنوع والتطور

وتعني هذه الخاصية من حيث التنوع أن الدليل الإلكتروني يمكن أن يظهر على هيئات مختلفة، فقد يكون غير مقروء للأشخاص مثلما هو الحال في المراقبة عبر الشبكات أو الخوادم التقنية للشبكات، وقد يكون مقروء ومفهوم للأشخاص مثلما يكون عليه الدليل في صورة وثيقة أو صورة مخزنة في جهاز حاسب آلي أو في البريد الإلكتروني، أما خاصية الدليل الإلكتروني أنه دليل متطور فهي تفيد أنها تستخدم في جرائم مستحدثة، فجريمة النصب مثلاً يمكن ارتكابها بالطرق التقليدية التي تنتج أدلة مادية، وكذلك أصبح مع التقدم التكنولوجي من الممكن ارتكابها باستخدام التقنية سواءً أكانت باستخدام جهاز الحاسب الآلي أو يكون الحاسب الآلي محلاً لارتكاب جريمة النصب (الرقيشي، 2008).

ز- دقة الدليل الإلكتروني

حيث نجد أن الدليل الإلكتروني في بعض الأحيان يرصد معلومات عن الجاني ويحللها في ذات الوقت ويمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فنجد أن الباحث الجنائي يجد غايته بسهوله أيسر من الدليل المادي في بعض الأحيان .

المطلب الثاني: القواعد الإجرائية للدليل الإلكتروني

لا شك أن وجود فئات جديدة من جرائم تقنية المعلومات أوجب على جميع المشاركين في النظام القانوني أن يكونوا على دراية جيدة لأشكال الدليل الإلكترونية، فلا مرية أن التطور العلمي يؤدي إلى تطور الجريمة، ولكي يمكن مواجهة هذه الجريمة فإنه يجب تطوير طرق الحصول على الدليل أو إجراءات الحصول عليه، ولذلك فإن هذه الطرق هي التي تحدد كون الدليل علمياً أو فنياً أو إلكترونياً، وأما الأدلة التي لا تحتاج إلى طرق علمية للحصول عليها كالأدلة القولية فإنها مازالت حتى اليوم هي بذاتها لم تتغير.

وتشترط القوانين للأخذ بالدليل الرقمي واعتباره ذو حجية في عملية الإثبات توافر بعض الشروط في هذا الدليل، ومن أهم هذه الشروط كالتالي: -

1. أن يتم الحصول على الدليل بصورة مشروعة وغير مخالفة للدستور أو للقوانين

إن أهم هدف للدساتير هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير الحديثة نصوصاً تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها(سقف المحيط، 2011)، بحيث يتقيد المشرع بها عند وضع القوانين خاصة الجزائية منها(الطوالبة، 2018)، حيث نص النظام الأساسي للدولة لسلطنة عمان في المادة (33) منه على أن: " للمساكن حرمة، فلا يجوز دخولها بغير إذن أهلها، إلا في الأحوال التي يبينها القانون وبالكيفية المنصوص عليها فيه " .

ونصت كذلك المادة (36) من النظام الأساسي للدولة على أن: " للحياة الخاصة حرمة، وهي مصونه لا تمس. وللمراسلات الإلكترونية بكافة أنواعها والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها، إلا في الأحوال التي يبينها القانون، ووفقاً للإجراءات المحددة فيه "، فهذه النصوص الواردة في النظام الأساسي للدولة وغيرها من النصوص التي تضمن الحقوق والحريات للأفراد تفرض على المشرع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها (المضحكي، 2014).

حيث أن مخالفة القانون في الحصول على الدليل يؤدي إلى بطلان هذه الأدلة، وتتمثل الطرق غير المشروعة في الحصول على الدليل كإكراه المتهم لفك شيفرة أو كلمة سر من أجل الوصول إلى الملفات التي توجد بها البيانات المخزنة، أو التحريض على ارتكاب

الجريمة الإلكترونية أو التجسس المعلوماتي، أو الاستخدام غير المصرح للحاسوب والتنصت والمراقبة الإلكترونية عن بعد في الحصول على الأدلة الرقمية، وتعد من الطرق غير المشروعة أيضاً استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية (الشمري، 2016) .

وكذلك فإن اجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده النظام الأساسي للدولة، وإلا فإن الدليل المستمد بطرق مخالفة للأحكام الأساسية الواردة في النظام الأساسي للدولة يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها .

ولعل مباشرة سلطتي التحري والاستدلال في الجرائم المعلوماتية في التحصل على الأدلة يجب أن تكون مشروعة، أي لا يتم التحصل عليها عن طريق انتهاك الحقوق الأساسية للجاني أو المتهم، وإلا ترتب على ذلك بطلانها، ويجب أن يكون الدليل مشروعاً أي أن يكون الدليل ومضمونة قد تم التحصل عليه وفقاً للإجراءات والقواعد القانونية المنظمة لذلك، والحقوق التي نصت عليها الإعلانات والمواثيق والاتفاقيات الدولية التي تنظم حقوق الإنسان في هذا الشأن .

كما لابد أن يصدر إذن رسمي من الجهة المختصة بالتحقيق للتفتيش والحصول على هذا النوع من الأدلة، ويشترط في الإذن بالتفتيش الصادر بالنسبة للجرائم التي تقع في دائرة أو محيط الوسائل الإلكترونية أن يكون مكتوباً ومحدد التاريخ وموقعاً ممن أصدره، وأن يكون صريحاً في الدلالة على التفويض في مباشرة التفتيش، وأن يتضمن من البيانات ما يحدد نوع الجريمة المطلوب جمع الأدلة عنها، ويجب كذلك تحديد محل التفتيش والذي قد يكون شخصاً أو منزلاً أو شركة خاصة، وتحديد الفترة الزمنية التي يراها المحقق كافيه لتنفيذ الإذن.

وتطبيقاً لذلك فقد أقرت المحكمة العليا بسلطنة عمان في أحد أحكامها على أن: " اقتصار التفتيش على حدود الغرض منه هو مبدأ قانوني هام مقرر لحماية حق الخصوصية، فيجب أن يستهدف الأشياء المتعلقة بالجريمة. لأنه إذا كان التفتيش هو في حقيقته انتهاكاً لخصوصية شخص اقتضته ظروف قانونية معينة فإنه يجب أن يبقى في الحدود التي اقتضت اجراءه. مؤدى ذلك بطلان ما يتم ضبطه خارج نطاق أمر التفتيش مادام لم تتعلق به شبهه معقوله ".

2. يجب أن تكون الأدلة الرقمية يقينية وغير قابلة للشك

لا يكفي أن يتم الحصول على الأدلة الإلكترونية بطريقة مشروعة، وإنما لابد أن تكون الأدلة التي تم استخراجها من الحاسوب أو الإنترنت غير قابلة للشك أو الريبة حتى يتم على أساسها الحكم بالإدانة على المتهم، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين(الطوالبة ، 2018) .

ولكي يستطيع القاضي الجنائي من خلالها الوصول إلى الاقتناع وبشكل جازم ويقيني عن طريق ما يتم عرضه عليه من أدلة رقمية إلكترونية، والمصغرات الفيلمية وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر أو التي كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات، يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية وما ينطبع في ذهنه من تصورات واحتمالات أن يحدد قوتها الاستدلالية وبالتالي يعتبرها دليل على حصول الجريمة الإلكترونية وبعدها يمكن له أن يحكم بالإدانة على المتهم (الزعابي، 2014).

وهذا يستوجب أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه، ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال(قنديل، 2015).

وباستقراء نصوص المشرع العماني حول الإثبات الجنائي يتضح بأنه يأخذ بنظام الإثبات الحر، فمشروعية الدليل الإلكتروني في نظام الإثبات الحر يمكن من خلاله للقاضي ان يأخذ بأي دليل آخر ومنها الدليل الإلكتروني، فهو الأصل في هذا النظام ويبقى مدى اقتناع القاضي بالدليل المعروض عليه في الدعوى سواءً بقبوله أو رده، ومع الإقرار بحرية القاضي الجزائي في الإثبات وفقاً لهذا النظام إلا أنه يجب أن يمارس الحرية وفق منطق سليم وتفكير صحيح، لذا فقد أوجد المشرع العماني بعض الاستثناءات على تلك الحرية التي منحها للقاضي لضمان حسن سير العدالة، وتتمثل تلك الاستثناءات في وجوب ان يستمد القاضي اقتناعه من أدلة صحيحة لها قوتها في الإثبات، وان تكون تلك الادلة طرحت على بساط البحث وأتيحت للمناقشة أثناء المحاكمة، وان يلتزم القاضي بطرق الإثبات الخاصة في المسائل غير الجزائية وبتسبيب حكمه وهي ما تعد قيوداً على حرية القاضي الجزائي في تكوين قناعته (عبيد، 2014) .

3. إمكانية مناقشة الأدلة المتحصلة من الحاسوب أو الإنترنت من قبل الخصوم وأطراف الدعوى

يفترض القانون أن المتهم برئ حتى تثبت إدانته لأن الأصل في الإنسان البراءة وهذا ما نصت عليه أغلب القوانين، لذلك يتطلب افتراض البراءة في المتهم عدم مطالبته بتقديم أي دليل على براءته، ويمكن للمتهم أن يتخذ موقفاً سلبياً تجاه الدعوى أو الشكوى

المقدمة ضده وعلى الادعاء العام تقديم الدليل على ثبوت التهمة المنسوبة إليه، إلا أن ذلك قد يؤدى إلى عرقلة سير المحاكمة وبالتالي من مصلحة الأطراف الكشف عن أي دليل يمكنه أن ينهي القضية (سقف المحيط، 2011).

ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على الأدلة التي تم طرحها في جلسات المحاكمة وخضعت للمناقشة من قبل الخصوم وأطراف الدعوى، وعلى هذا الأساس فإن الأدلة التي تم تحصيلها من الحاسوب أو الإنترنت سواءً كانت مطبوعة أو بيانات تم عرضها على شاشة الحاسوب أو أشرطة أو أقراص ممغنطة وما إلى ذلك من أدلة لابد أن تخضع للمناقشة إذا ما أريد الأخذ بها كأدلة إثبات أمام المحكمة وتعرض في الجلسة أمام القاضي.

فإذا كان القاضي الجنائي يحكم باقتناعه هو وليس باقتناع غيره فإنه يجب عليه أن يعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكن من تكوين اقتناع بقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاضٍ عادل ومجتهد، ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم الإلكترونية استناداً إلى علم شخصي له أو استناداً إلى رأي للغير، إلا أذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناءً عليه يكون متولداً من عقيدته هو وليس من تقرير الخبير وبالتالي يحكم بما تولد لديه من عقيدة.

وهذا ما أقرته المحكمة العليا في سلطنة عمان في أحد أحكامها والذي ينص على أن: " إن المشرع أخذ بمبدأ شفوية المرافعات والتي تعني أن كل دليل يعتمد عليه القاضي في حكمه يجب أن يكون قد طرح شفوياً بالجلسة وجرت بشأنه المناقشة الشفوية، ولا يجوز للمحكمة أن تكتفي بمحاضر التحقيقات، بل يجب عليها أن تستمع إلى أقوال الخصوم وشهادات الشهود وآراء الخبراء وتطرح على بساط البحث كافة أدلة الدعوى لكي تستخلص منها في النهاية ما تبني عليه عقيدتها، فإذا استندت المحكمة إلى شهادة شاهد أو شهود دون أن تسمعهم أو إلى مستند دون أن تبسط تلك الأدلة للبحث بالجلسة فإن حكمها يكون معيباً "(الرقيشي، 2008، ص53).

المبحث الثاني: إجراءات وإشكاليات جمع الأدلة الإلكترونية

غالباً ما يترك الجاني آثاراً مادية في مكان الجريمة عند ارتكابه لجريمته، فمهما حاول محو كل الآثار الناتجة عن الجريمة والتخلص منها إلا أنه في النهاية لابد أن يترك أي أثر نتيجة فعله، وهو حسبما يرى العلماء نتيجة الحالة النفسية والانفعالات التي تصاحب الجاني أثناء ارتكاب الجريمة.

المطلب الأول: إجراءات جمع الأدلة الإلكترونية

لقد شمل التطور الإجراءات القانونية المتخذة في جمع الأدلة وكذلك كيفية الحصول عليها، فعلى مستوى الإجراءات فإن جهات جمع الاستدلالات والتحقيق أصبحت تدرك كيفية التعامل مع الحاسب الآلي وكيفية المحافظة على الأدلة التي تحتويها، وكذلك كيفية التعامل مع الأجهزة الحديثة ووسائل التقنية المختلفة وكيفية استخراج الأدلة منها، أما على مستوى وسائل الحصول على هذه الأدلة فقد أدى التطور إلى توظيف التكنولوجيا الحديثة وإمكانياتها في استخراج الأدلة والحصول عليها لتساهم في مكافحة الجرائم وعملية إثباتها(الرقيشي، 2008).

وتعد أدلة الإثبات في الدعوى الجزائية محور الجريمة من حيث إثبات التهم على المتهم، أو نفيها عنه بإعلان براءة المتهم من الجريمة التي ارتكبها، وتخضع الأدلة الإلكترونية كغيرها من الأدلة الجنائية التقليدية لنفس الإجراءات التي تحكم الأدلة الجنائية، وتعد الأدلة الإلكترونية من الأدلة المستحدثة نظراً لاستخراجها من الجرائم الإلكترونية، والتي تتميز عن الأدلة التقليدية من حيث مكانها والبيئة التي تحكم عمل هذا النوع من الأدلة، وقد أجمع الفقهاء على أن الأدلة الإلكترونية بجميع أنواعها سواءً كانت بيانات أو صور أو تسجيلات أو أفلام تعد من قبل القرائن (البقمي، 2012).

ونظمت التشريعات كيفية الحصول على الأدلة باتخاذ إجراءات تتبع وصولاً للغاية منها وهي إثبات الجريمة المرتكبة وإثبات فاعلها، وهي تستخدم بصفة عامة لجمع الدليل في مختلف الجرائم فتشمل الجرائم التقليدية والجرائم المستحدثة منها إلا أن دور تلك الإجراءات يختلف بينها، ففي الجرائم التقليدية يتعاظم دور هذه الإجراءات ويقل لدى الجرائم المستحدثة (مصطفى، 2010).

فالأدلة الإلكترونية لا تختلف عن الأدلة التقليدية من ناحية أنه يتعين على أحد أطراف الدعوى إدخالها في الإجراءات القانونية، فهي تعكس مجموعة من ظروف ارتكاب الجريمة وتقدم معلومات عن الجريمة كما وقعت بالفعل، كما أنه يجب أن تتوافر الوسائل لإثبات أن الأدلة الإلكترونية لم تتعرض لأية تعديات سواءً بالحذف أو الإضافة أو التعديل أو أي تغييرات أخرى منذ لحظة الحصول عليها (فتح الله، 2019).

لذلك فإنه يبقى للإجراءات التقليدية لجمع الأدلة دور مهم مهما كان دوره في إثبات الجريمة في جمع الدليل الإلكتروني، فتغير طريقة المعاينة والتفتيش لا يعني أنها ليست من الإجراءات التقليدية لجمع الدليل الجنائي، واتباع الإجراءات التي حددها المشرع يجعل

من الدليل المستخرج والمعروض أمام القضاء مشروعاً ويساعد على إثبات الجريمة والوصول إلى الجاني وتقديمه للعدلة لمحاكمته، ويمكن تقسيم الإجراءات التقليدية لجمع الأدلة وفق الآتي: -

1. المعاينة

تعرف المعاينة على أنها: " إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكاناً أو شخصاً أو شيئاً له علاقة بالجريمة، لإثبات حالته والتحفظ على كل ما قد يفيد من الآثار في كشف الحقيقة" (العازمي، 2016، ص266)، وتعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة ومن أهم إجراءات التحقيق على الإطلاق نظراً لما يمكن أن توفره من أدلة إثبات، وتزداد أهميتها أكثر إذا تعلق الأمر بالجرائم الإلكترونية باعتبارها من الجرائم المستحدثة وغير المألوفة بالنظر إلى الطبيعة الخاصة للسلوك الإجرامي فيها، والذي يستوجب ابتكار تقنيات جديدة مناسبة بالمعاينة في هذا المجال(سويلم، 2019).

ولقد تطرق المشرع العماني إلى موضوع المعاينة في قانون الإجراءات الجزائية، حيث نصت المادة (30) منه على أنه: " يقوم مأمورو الضبط القضائي بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات وإجراء المعاينات اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، وعليهم أن يتخذوا جميع الوسائل اللازمة للمحافظة على أدلة الجريمة "، ويستفاد من هذه المادة على أنه عند علم مأمور الضبط القضائي بوجود جريمة فعليه أن يحظر فوراً إلى موقع الجريمة، وأن ينتقل إلى مكان الواقعة للمحافظة عليه وإجراء المعاينة اللازمة، فلا يمكن أن تكون المحافظة على مكان وقوع الجريمة إلا بالانتقال السريع له قبل حدوث أي إتلاف أو تغيير فيه، وهذا ما أكدت عليه المادة (39) من ذات القانون والتي نصت على أن: " على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً لمحل الواقعة ويعاين الآثار المادية للجريمة ويحافظ عليها ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ويسمع أقوال من كان حاضراً أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها، وعليه إخطار الادعاء العام فوراً بانتقاله، وعلى عضو الادعاء العام الانتقال فوراً إلى محل الواقعة بمجرد إخطاره بجناية متلبس بها ".

كما أن إجراء المعاينة يمكن أن يكون من سلطات التحقيق إذا رأت أهمية القيام بهذا الإجراء من أجل التثبت من حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثباته، حيث أتاح ذلك المشرع العماني في قانون الإجراءات الجزائية وذلك بموجب المادة (76) التي تنص على أن: " لعضو الادعاء العام أن ينتقل إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً وكل ما يلزم إثباته "، انتقال عضو الادعاء العام لإجراء المعاينة يكون جوازياً وفق المادة المذكورة، ولكنه يكون وجوبياً في حالة إخطاره من قبل مأمور الضبط القضائي بجناية متلبس بها، وفي هذه الحالة عليه الانتقال فوراً إلى محل الواقعة بمجرد إخطاره وهو ما نصت عليه الفقرة الثانية من المادة (39) من القانون ذاته والتي تم ذكرها سابقاً .

2. التفتيش

يقصد بالتفتيش بأنه: " إجراء من إجراءات التحقيق يقوم به موظف مختص طبقاً للإجراءات القانونية في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة، تحقق وقوعه لإثبات ارتكابها أو نسبتها إلى المتهم "(حجازي، 2007، ص2019)، لذا فهو يعد من أهم إجراءات التحقيق في كشف الحقيقة لأنه غالباً ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم (مصطفى، 2010).

والأصل أن التفتيش هو إجراء من إجراءات التحقيق تختص به سلطة التحقيق بصفة أصلية، إلا أنه استثناءً يمكن لمأموري الضبط القضائي أن يقوموا بهذا الإجراء في حالات حددها قانون الإجراءات الجزائية، ولقد تطرق المشرع العماني لذلك في المادة (36) من قانون الإجراءات الجزائية العماني حيث نصت المادة المذكورة على أن: " إذا رأى أحد مأموري الضبط القضائي عند قيامه بجمع الاستدلالات ضرورة إجراء تفتيش شخص أو مسكن معين، تعين عليه أن يحصل على إذن بذلك من الادعاء العام "، كما نصت المادة (46) من ذات القانون على أن: " لمن يقوم بتنفيذ القبض من مأموري الضبط القضائي أن يفتش المقبوض عليه لتجريده من أية أسلحة أو أشياء قد يستعملها في المقاومة أو في إيذاء نفسه أو غيره وأن يضبطها ويسلمها مع المقبوض عليه إلى الآمر بالقبض ".

كما تنص المادة (77) من ذات القانون أعلاه على أن: " لمأموري الضبط القضائي تفتيش المتهم في الأحوال التي يجوز فيها قانونا القبض عليه، كما يجوز تفتيش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة، ويشمل التفتيش جسمه وملابسه وأمتعته "، ومن تلك النصوص الواردة في القانون نرى أن التفتيش هو إجراء طبيعي يمس حق المتهم في سرية حياته الخاصة، ولا يجوز أن يترتب على حق الدولة في العقاب المساس بسرية الحياة الخاصة بالإفراد إلا وفقاً للإجراءات القانونية الخاصة المنصوص عليها بذلك وفي أضيق الحدود .

كما أن الهدف من التفتيش هو البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها بمحل منح له القانون حرمة خاصة باعتبارها مستودع سر صاحبه، فلا يجوز الاطلاع عليه أو على ما بداخله إلا في الأحوال المنصوص عليها في القانون أو برضاء صاحبه، والغاية من التفتيش هي البحث عن الأشياء المتحصلة بالجريمة الجاري التحقيق بشأنها(عبدالمجيد، 2022) .

والتفتيش في مدلوله القانوني بالنسبة للجرائم المعلوماتية لا يختلف عن مدلوله السائد في فقه الإجراءات الجنائية، ويقصد به إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات، بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبه وتشكل جناية أو جنحة، والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها وتقديمة للمحاكمة (عبدالمجيد، 2022) .

لذلك فإن تفتيش أجهزة ووسائل تقنية المعلومات الحديثة من أخطر المراحل عند اتخاذ الإجراءات الجزائية في الجريمة الإلكترونية وغيرها من الجرائم التي تتضمن دليلاً إلكترونياً، لكون أن محل التفتيش وهو جهاز الحاسب الآلي أو شبكات أو وسائل تقنية المعلومات محل جدل فقهي واسع ومتزايد وخاصة فيما يخص المكونات المعنوية لتلك الأجهزة والوسائل، فهي لا وجود لماديتها إنما هي عبارة عن بيانات ومعلومات رقمية (مصطفى، 2010).

3. الخبرة

للخبراء في الوقت الحاضر دور مهم في عملية التحقيق الجنائي، وذلك لدورهم الفعال في كشف غموض الجرائم، وكذلك استنادهم للوسائل العلمية والفنية في دراسة الآثار التي تتركها الجريمة، ولقد أباحت أغلب التشريعات للمحق من تلقاء نفسه أو بناءً على طلب الخصوم الاستعانة بخبير إذا ما واجهت السلطة المختصة بالتحقيق صعوبة بمسألة ما(يوسف، 2016).

والخبرة هي إجراء يستهدف استخدام قدرات الشخص الفنية أو العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرينة يفيد في معرفة الحقيقة بشأن وقوع الجريمة ونسبتها إلى المتهم، أو تحديد ملامح شخصيته الإجرامية، وبالنظر إلى الطبيعة الخاصة بالجرائم الإلكترونية فإن إماطة اللثام عنها يحتاج إلى خبرة فنية تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر هذه الحاجة في مرحلة التحقيق والمحاكمة نظراً للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء، فالخبرة الفنية في مجال الجريمة الإلكترونية لها أهمية بالغة، حيث لا يستطيع التعامل مع إثبات هذه الجريمة إلا شخص ذو دراية وخبرة متعمقة في مجال الحاسبات وبرامجها والشبكات(عبدالمجيد، 2022) .

4. الشهادة

يقصد بالشهادة بشكل عام أنها: " التعبير عن المضمون الحسي للشاهد بما رآه أو سمعه بنفسه من معلومات عن الغير مطابقة لحقيقة الواقعة التي يشهد عليها في القضاء بعد أداء اليمين ممن تقبل شهادتهم وممن يسمح لهم بها ومن غير الخصوم في الدعوى " (قنديل، 2015، ص173)، ولقد أشار المشرع العماني إلى موضوع الشهادة في عدة مواد من قانون الإجراءات الجزائية، حيث نصت المادة (34) من قانون الإجراءات الجزائية العماني على أن: " لمأموري الضبط القضائي أثناء قيامهم بجمع الاستدلالات أن يسمعوا أقوال من يكون لديهم معلومات عن الجريمة وفاعلها، وأن يسألوا المتهم بها، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة، ولكن لا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يستطاع فيما بعد سماع الشهادة بيمين"، كما نصت المادة (104) على أن: "يسمع عضو الادعاء العام شهادة الشهود الذين يطلب الخصوم سماعهم ما لم ير عدم الفائدة من سماعهم، وله أن يسمع شهادة من يرى لزوم سماعه من الشهود عن الوقائع التي تثبت أو تؤدي إلى ثبوت الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها "، كما نصت المادة (106) على أن: " يكلف عضو الادعاء العام الشهود الذين تقرر سماعهم الحضور بواسطة رجال الشرطة، وله أن يسمع شهادة أي شاهد يحضر من تلقاء نفسه ويثبت ذلك في المحضر".

ولا تقل أهمية الشهادة في الجريمة الإلكترونية عن باقي إجراءات جمع الأدلة الإلكترونية، فهي لا تختلف من حيث ماهيتها عنها في الجرائم التقليدية، والشاهد في الجريمة الإلكترونية هو الشخص صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والشخص الذي تكون لديه المعرفة الكافية والجوهرية بنظام المعالجة الآلية للبيانات، أو لديه معلومات هامة لازمة للدخول في النظام، متى ما كانت مصلحة التحقيق تتطلب التنقيب عن أدلة الجريمة الإلكترونية داخله، ولذلك يطلق على هذا الشخص الشاهد المعلوماتي تميزاً له عن الشاهد التقليدي في سائر أنواع الجرائم الأخرى(يوسف، 2016)، فالشاهد المعلوماتي وفق ذلك المفهوم لابد أن يكون ذا خبرة فنية في مجال الجهاز الإلكتروني.

إن من أهم الصعوبات التي تواجه سلطتي جمع الاستدلالات والتحقيق في الجريمة الإلكترونية عملية إثباتها، ولا يتم إثبات الجريمة إلا بتوافر الأدلة التي تؤكد ذلك، ويرجع ذلك للتطور الكبير والمستمر في وسائل تقنية المعلومات والأجهزة الإلكترونية الحديثة التي تستخدم شبكات الاتصال ونقل البيانات، وهو ما أدى إلى مواكبة ذلك التطور بتطور أساليب وأدوات ارتكاب الجريمة الإلكترونية والتقليدية على السواء، نتيجة الاستخدام السلبي لهذه التكنولوجيا، وهو ما أدى إلى عدم كفاءة الإجراءات التقليدية والصعوبات التي تحيط بهذه الإجراءات عند مواجهة هذا النوع من الجرائم، لذا أصبح من الضروري أن تواكب التشريعات هذا التطور بتطوير إجراءاتها التقليدية لمواجهة الجرائم وخلق قواعد قانونية مستحدثة في هذا المجال، من أجل تيسير عملية جمع الأدلة في الجريمة الإلكترونية وإثباتها(الرقيشي، 2008).

ومن الواضح أن الدليل في الجريمة الإلكترونية يشترك مع الأشكال التقليدية للأدلة في العديد من الخصائص إلا أنها تتميز ببعض من الخصائص الفريدة، ذلك أن الدليل الرقمي لا يتعلق فقط بجرائم تقنية المعلومات بالنظر إلى الطبيعة غير المادية للبيانات والمعلومات المخزنة بشكل إلكتروني والتي من السهل التلاعب بها (فتح الله، 2019). فهي تحتاج إلى نوع جديد من الإجراءات في جمعها يختلف عن طريقة جمع الأدلة التقليدية الأخرى، لذلك تنقسم الإجراءات الحديثة التي تساعد على جمع الأدلة إلى ثلاثة أقسام وهي كالتالي:

1- الإجراءات المتعلقة بنظم التشغيل والبيانات الساكنة

قد تكون المعلومات في حالة سكون داخل الحاسب الآلي، والمعلومات الساكنة داخل الحاسب الآلي أكثر أمناً من تلك المتحركة، لأن الاعتداء على المعلومات الساكنة يتطلب تواجد المعتدي في مركز الحاسب ودخول الحاسب التي توجد به تلك المعلومات مباشرة وهو أمر صعب، لذلك فهي لا تحتاج لحماية مشددة بل إجراءات أمنية محدودة(عبدالمجيد، 2022) .

وتعد الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية التي تم توقيعها في بودابست عاصمة المجر بتاريخ 23 نوفمبر2001م من أولى الاتفاقيات الدولية التي تختص بمكافحة الجرائم الإلكترونية والتي تم ذكرها سابقاً، وقد تضمنت هذه الاتفاقية النص لأول مره على التفرقة بين نوعين من البيانات وهي البيانات المخزنة أو الساكنة، والبيانات المتحركة أو البيانات المتعلقة بخط سير المعلومات، ومن خلال نصوص هذه الاتفاقية نجد أنها نصت على إجراءات جديدة لجمع الأدلة الإلكترونية منها إجراءات ممهده تسبق عملية جمع الأدلة ومنها إجراءات خاصة بجمع الأدلة(الرقيشي، 2008).

فمن أهم ما جاءت به اتفاقية بودابست لمكافحة الجريمة الإلكترونية النص على التحفظ المعجل أو السريع على بيانات الحاسب المخزنة، حيث نصت الفقرة الأولى من المادة (16) على أن: " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من الأمر أو الحصول على الحفظ المعجل لبيانات كومبيوتر محددة، بما في ذلك بيانات الحركة المخزنة بواسطة نظام الكومبيوتر، خاصة في حال وجود أسس للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل".

كما نصت الفقرة الثانية من المادة ذاتها على أن: " في حال تفعيل دولة طرف للفقرة ١ أعلاه عبر توجيه أمر إلى شخص من أجل حفظ بيانات كومبيوتر محددة ومخزنة توجد بحوزته أو تحت سيطرته، تعتمد الدولة الطرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام ذلك الشخص بحفظ بيانات الكمبيوتر المعنية والإبقاء على سلامتها لأطول مدة زمنية ضرورية على ألا تتجاوز تسعين يوماً من أجل تمكين السلطات المختصة من التماس الكشف عنها. ويجوز للدولة الطرف التنصيص على تجديد هذا الأمر لاحقا"، كما نصت الفقرة الثالثة من ذات المادة على أن: " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لإلزام القيّم على حفظ بيانات الكومبيوتر أو أي شخص آخر عهدت له هذه المهمة، بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المنصوص عليها في قانونها الوطني".

كما أن اتفاقية بودابست لمكافحة الجريمة الإلكترونية نصت على إجراء آخر وهو سلطة إصدار الأوامر، حيث جاء ذلك بموجب الفقرة الأولى من المادة (18) من الاتفاقية التي تنص على أن: " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى: أ. أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر .ب. أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته " .

كما أشارت المادة (19) من الاتفاقية على صلاحية تفتيش وضبط بيانات الحاسب الآلي المخزنة ومصادرتها وكذلك إصدار أمر بتقديم البيانات واعتراضها، وكذلك كإجراء من إجراءات جمع الأدلة الإلكترونية في الجريمة الإلكترونية، ويمكن تقسيمها إلى نوعين من الإجراءات، النوع الأول: إجراءات التحفظ وهي إجراءات تهدف إلى الحفاظ على البيانات المخزنة التي ترى الجهة المختصة أن لها أهمية في التحقيق ببقائها في مكانها في الحاسب الآلي أو وسائل التخزين الأخرى ومنع الوصول إليها، أما النوع الثاني: هي إجراءات ضبط وهي الإجراءات التي تقوم بها سلطات التحقيق لأخذ الدليل، سواءً بعمل نسخة طبق الأصل من البيانات المخزنة على الحاسب، أو بأخذ النسخة الأصلية من دعامات التخزين الموجودة على الحاسب الآلي.

إضافة إلى ذلك فلقد تم النص على إجراء آخر وهو الاعتراض على مضمون البيانات ضمن المادة (21) من الاتفاقية، ويقصد بهذا الإجراء مراقبة الاتصالات الإلكترونية أثناء بثها وليست المخزنة على نظام الحاسب الآلي، وقد ميزت الاتفاقية بين نوعين من البيانات هما البيانات المتعلقة بالمرور وخط سير البيانات، وقد ألزمت الاتفاقية هذا النوع من البيانات بالتجميع الفوري وتخزينها كبيانات بشكل دائم، أما النوع الآخر فهي البيانات المتعلقة بمحتوى الاتصال وهي تشمل جميع بيانات الاتصال أو الرسالة أو المعلومة المنقولة عن طريق الاتصال، وهذا النوع هو محل الاعتراض، ورغم مساسه بالحرية الشخصية إلا أن الاتفاقية وضعت لهذا الإجراء شرطاً لازماً وهو أن يكون في الجرائم الخطيرة التي يحددها التشريع الوطني لكل دولة (الرقيشي، 2008).

2- الإجراءات المتعلقة بالبيانات المتحركة في شبكة المعلومات

بما أن هناك معلومات ساكنة تم الحديث عنها، توجد هناك أيضاً معلومات وبيانات في حالة حركة من حاسب إلى آخر فهي تنتقل عبر شبكات الاتصال وذلك عبر شبكة من الشبكات، ولذلك فإن المعلومات المتحركة بعكس المعلومات الساكنة تتعرض لكثير من المخاطر وتحتاج إلى إجراءات أمنية مشددة أكبر من تلك التي تحتاجها المعلومات الساكنة (عبدالمجيد، 2022)، وتتنوع البيانات المتحركة المحفوظة على شبكة المعلومات إلى أنواع مختلفة، حيث تختلف أنواع البيانات هذه في طريقة تكوينها وانتشارها وحركتها على الشبكة العالمية للمعلومات، ويمكن أن نوضح أربعة أمثلة مختلفة توضح طبيعة البيانات المتحركة وهي كالتالي: -

أ- البريد الإلكتروني

وهو يعد من الخدمات المهمة والإيجابية التي قدمتها الثورة المعلوماتية للمجتمعات، فهو يعد شكل من أشكال التواصل الإلكتروني يسمح لمستخدم الشبكة في تبادل الرسائل النصية بدلاً عن استخدام الوسائل التقليدية الورقية، وكأنه صندوق بريدي خاص على شبكة المعلومات حيث يتيح للمستخدم الدخول له وتفقد الرسائل الواردة إليه وإرسال الرسائل إلى أشخاص آخرين، وقد أصبح من أكثر وسائل التواصل شيوعاً واستخداماً عبر الإنترنت، ونظراً لسهولة استخدامه وعدم وجود ضوابط مشددة تحكمه فإن ذلك أدى إلى وجود الاستخدامات السلبية وغير المشروعة للبريد الإلكتروني، مثله مثل باقي الخدمات الأخرى التي تتيحها الشبكة والتقنية المعلوماتية بشكل عام (إبراهيم، 2008).

ومع تزايد التطور المعلوماتي وما يلعبه من دور مهم في مختلف مجالات حياة البشرية، فقد اعترفت التشريعات بحجية المستندات التي تستخدم عبر البريد الإلكتروني شأنها شأن المستندات الورقية، وأصبحت كذلك محلاً لجريمة التزوير كونها مستنداً له حجية في الإثبات ويحمل فكراً ويمكن قراءته وتتمتع بذات الحماية التي تتمتع بها المستندات الورقية، فلا يجوز الاطلاع عليها وعلى ما تحتويه من أسرار إلا وفق الإجراءات والقواعد العامة التي يحددها القانون، بالإضافة إلى أن البريد الإلكتروني يعتبر مصدراً هاماً للأدلة الرقمية حيث يمكن بسهولة معرفة مصدر البريد الإلكتروني وتحديد من أرسل الرسالة، ذلك إن برامج البريد الإلكتروني تخفي المعلومات التقنية عن القارئ، وتوجد هذه المعلومات فيما يسمى ترويسة البريد الإلكتروني (فتح الله، 2019).

ولقد أشار المشرع العماني إلى موضوع المراسلات والبرقيات، ولقد وضع لها حماية خاصة في قانون الإجراءات الجزائية العماني، حيث نصت المادة (90) من القانون المذكور على أن: " لا يجوز ضبط المراسلات والبرقيات أو الاطلاع عليها أو ضبط الجرائد والمطبوعات والطرود أو تسجيل الأحاديث التي تجرى في مكان خاص أو مراقبة الهاتف أو تسجيل المكالمات بغير إذن من الادعاء العام ".

ب- بيانات مواقع التواصل الاجتماعي

مع التقدم التقني الذي صاحب الثورة العلمية وتعدد وسائل الاتصال وانتشار التكنولوجيا الرقمية، جعل هذا الشركات المتخصصة في مجال تقنية المعلومات والاتصالات تتنافس فيما بينها لتستقطب أكبر شريحة من الأعضاء والمشتركين، ومن هنا جاء التنوع والاختلاف في شبكات ومواقع التواصل الاجتماعي لتحقق رغبات متنوعة واستخدامات مختلفة (السيابي، 2018).

وتتنوع هذه المواقع كما أن عددها كبير جداً ومن أشهرها تويتر وإنستجرام وفيس بوك، حيث أن هذه المواقع تتيح للمستخدم أن يرفع إليها ملفات مختلفة كالصور ومقاطع الفيديو والمستندات والروابط ويسمح بانتشارها على شبكة المعلومات لجميع المستخدمين، ويستطيع في المقابل أن يحملها مستخدم آخر ويحصل على نسخة منها ويعيد نشرها بكل سهولة، ووفق هذه الميزات أصبحت هذه المواقع وما تحتويه من معلومات وبيانات أخطر أنواع البيانات المتحركة، فهي تمنح المستخدم أن يكون أداة ومصدر لنشر المعلومة أو مستند وكأنه قناة إعلامية مستقلة (الرقيشي، 2008).

ج- بيانات المواقع المتخصصة لبث المحتوى المرئي

وهي نوع من المواقع الأخرى التي تتيح لمستخدمها برفع ملفاته المصورة على شكل مقاطع مرئية (فيديو)، ورغم تنوعها إلا أن أشهر هذه المواقع على مستوى شبكة المعلومات العالمية هو موقع يوتيوب، وهو موقع يسمح للمستخدم بنشر ما يشاء من المقاطع المرئية المصورة وفق السياسات والشروط التي يسمح بها الموقع، ويستطيع مشاهدة تلك المقاطع كل شخص في العالم، ولم تخلو هذه المواقع من إساءة استخدامها من بعض المجرمين في نشر ما من شأنه زعزعة استقرار البلدان عبر تلفيق المقاطع المصورة، أو الاعتداء على حرمة الحياة الخاصة للأفراد (الرقيشي، 2008).

د- بيانات محفوظة على الشبكة

وتتمثل هذه البيانات والمعلومات عن طريق الخدمات التي تقدمها بعض المواقع كذلك، فمن خلال هذا الموقع يمكن للشخص أن يحتفظ بما يشاء من بيانات وملفات ورفعها في هذا الموقع ويحصل على كلمة مرور خاصة يمتلكها هو فقط، يستطيع من خلالها الدخول والاطلاع على ملفاته وبياناته التي قام بتخزينها متى ما أراد ذلك، مع امكانية إضافة المزيد من الملفات والبيانات كذلك وفق مساحة تخزينية عالية متاحة لكل مستخدم، كما أنه يمكن أن يسمح الموقع للمستخدم أن يشارك هذه الملفات لمن يشاء دون كلمة مرور

ويحدد الأشخاص الذين يمكنهم مشاهدة الملفات، فيمكن من خلال هذه الملفات إدارة محتوى معين بين مجموعة من الأشخاص دون القدرة على الحصول أو الاطلاع عليها من الآخرين دون أذن من المالك لها، وهو ما قد يسيء من استخدامها في إدارة محتويات غير مشروعة أو ملفات محظورة وإيصالها إلى الشخص المقصود دون الخوف من انتشارها عبر شبكة المعلومات(الرقيشي، 2008).

3- إجراءات الحصول على بروتوكول عنوان البريد الإلكتروني

وهو يسمى بعنوان الإنترنت IP وهو اختصار لكلمة Internet protocol، وهو المسؤول عن نقل الملفات عبر شبكة الإنترنت وتوجيهها إلى أهدافها وهو يشبه إلى حد كبير عنوان البريد العادي، حيث يتيح للموجهات والشبكات المعنية نقل الرسالة وهو يوجد بكل جهاز مرتبط بالإنترنت ويتكون من أربعة أجزاء، كل جزء يتكون من أربع خانات فيكون المجموع اثنا عشر خانة كحد أقصى (عبدالمجيد، 2022) .

المطلب الثاني: إشكاليات جمع الأدلة الإلكترونية

إن إجراءات الحصول على الأدلة خصوصاً الإلكترونية منها، هي من المسائل التي تثير عدداً لا يستهان به من الإشكاليات القانونية والفنية في مجال التحقيق في الجرائم الإلكترونية، ونظراً لما تتميز به الجريمة الإلكترونية من طابع خاص فإن سلطات الاستدلال والتحقيق الابتدائي تواجه العديد من الصعوبات والإشكاليات في مجال الإثبات الجنائي للجريمة الإلكترونية، بداية من استخلاص الدليل ووصولاً إلى إثباتها بهذه الأدلة وتقديمها للقضاء.

ويمكن أن نلخص أهم الإشكاليات التي تواجهها سلطات التحقيق في مجال الإثبات الجنائي للجريمة الإلكترونية والتي تتعلق بطبيعة الدليل الإلكتروني في الجرائم الإلكترونية بالصعوبات التالية: -

1. سهولة ارتكاب الجريمة الإلكترونية

فالجريمة الإلكترونية لا تعترف بالحدود الجغرافية للمكان، حيث يتم ارتكابها عادة عن بعد بدون أن يكون الفاعل موجود في مسرح الجريمة، وهو ما يؤدي إلى تباعد المسافة بين الفعل والنتيجة، وهذه المسافة لا تقف عند حدود الدولة الواحدة فيمكن أن ترتكب الجريمة في دولة وتكون نتيجتها في دولة أخرى، وهو ما يضاعف من صعوبة اكتشافها وملاحقتها(الرقيشي، 2008).

كما أن هذه الجرائم لا تحتاج من الفاعل القيام بجهد كبير أو تعرضه لخطر في سبيل ارتكاب الجريمة كما هو الحال في الجرائم التقليدية مثل ارتكاب جريمة سرقة أو خطف، فالمسألة لا تتجاوز حد النقر على الجهاز الإلكتروني من أي مكان لإرسال عبارات سب أو قذف، أو الانتظار لبعض الوقت في مكان جلوسه للبحث عن ثغرات يمكن استغلالها في اختراق موقع إلكتروني.

2. سهولة محو الدليل أو تدميره

من الصعوبات التي تواجه سلطة التحقيق أو الاستدلال في إثبات الجريمة الإلكترونية والوصول إليها سهولة قيام الجاني بتدمير أدلة الإدانة وفي فترة زمنية قصيرة، ولا شك أن إثبات الأمور المادية التي تترك آثاراً ملحوظة يكون سهلاً وميسوراً بعكس إثبات الأمور المعنوية، فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي آثار قد تدل عليه أو تكشف عنه، بحسب أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدارتها إذا ما تم محوها أو تدميرها (المري، 2018).

ويشكل انعدام الدليل المرئي عقبة كبيرة أمام كشف الجرائم، وقد يشكل تشفير البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال عن بعد عقبه كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسوب والإنترنت، وعادة ما يضع الجناة تعليمات أمنية في النظم الحاسوبية التابعة لأجهزتهم تعمل على محو كافة البيانات المخزنة عند اختراقها من قبل شخص غير مرخص له، وهو ما من شأنه التأثير على أدلة الجريمة وصعوبة سلطة التحقيق أو الاستدلال من الوصول إليها واكتشاف الجريمة ومرتكبيها ومعاقبتهم على الجريمة.

3. صعوبة الوصول إلى الدليل

تعد من الصعوبات الكبرى التي تواجه سلطة التحقيق في هذا الأمر، حيث تتمتع البيانات المخزنة إلكترونياً أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لمنع التسلل والوصول غير المشروع إليها، سواءً لتدميرها أو استبدالها أو الاطلاع عليها أو نسخها، كما يمكن للمجرم المعلوماتي زيادة تلك الصعوبة والوصول إلى الأدلة التي تدينه .

فعند ارتكاب الجريمة الإلكترونية ولشدة ذكاء وفطنة أغلب المجرمين يعمد الجاني إلى إعاقة وصول جهات التحقيق إلى الحيز المعنوي المشتمل على الدليل بعدة طرق، حيث يستخدم الجاني بعض التدابير الأمنية ككلمات المرور أو وضع بعض التعليمات الخفية أو تحويلها لرموز لإعاقة قراءتها أو الاطلاع عليها أو ضبطها، أو وضع منظومات حماية تمنع أي دخول غير مشروع للأنظمة والبرمجيات والملفات وبالتالي صعوبة فتحها أو نسخها .

4. الأدلة الإلكترونية أدلة غير مادية تنعدم رؤيتها

يعتبر الدليل الرقمي دليلاً غير ملموس أي أنه ليس دليلاً مادياً فهو عبارة عن مجالات مغناطيسية أو كهربائية، ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات من طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة(الزعابي، 2014)، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة إذا كانت في دولة أخرى، حيث أن هذا الإجراء يتعارض مع سيادة الدول (الطوالبة، 2018).

ويعتبر الدليل الإلكتروني دليل غير مادي أي أنه لا يظهر بصورة مادية كالأدلة التقليدية الأخرى كالأوراق والمستندات والأسلحة وغيرها من الأدلة المتحصل عليها من الجريمة التقليدية، وإنما يتم عن طريق أجهزة إلكترونية تتعامل بنبضات إلكترونية وكهرومغناطيسية تنتج هذه الأدلة، كما أنها لا يمكن رؤيتها بالعين المجردة إذ إنها بيانات مسجلة إلكترونياً بكثافة بالغة وبصورة رموز لا يمكن قراءتها، وإنما تستخدم الأجهزة ذاتها في عرض هذه الأدلة ومحتوياتها كشاشة العرض في الحاسب الآلي .

5. ضخامة تكاليف جمع الأدلة

لا شك أن طبيعة الدليل تنعكس عليه، فالدليل الفني قد يكون مضمونه مسائل غنيه معقده لا يقوى على فهمه الفني غير المختص بعكس الأدلة المادية الأخرى، وإذا كان الدليل الناتج عن الجرائم التي تقع على العمليات الإلكترونية قد تحصل من عمليات فنية معقده عن طريق التلاعب في نبضات وذبذبات إلكترونية وعمليات أخرى غير مرئية، فإن الوصول إليه وفهم مضمونه قد يكون في غاية الصعوبة وذلك ما يجعل الوصول لتلك الأدلة ضخمة التكاليف (المري، 2018).

فالدليل الرقمي ليس أقل مادية من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في حجمها وشكلها ومكان تواجدها غير المعلن، وذلك لأن مصطلح الدليل الرقمي يشمل كافة أنواع وأشكال البيانات الرقمية الممكن تداولها رقمياً، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني.

وفي كثير من الأحيان تجد جهات التحقيق أنفسها مجبرة على تفتيش نظام الحاسب الآلي برمته بحثاً عن الدليل، وهو الأمر الذي يحتاج إلى فحص آلاف الصفحات خصوصاً عندما لا تثبت تلك الصفحات شيئاً، بالإضافة إلى الحالات التي يكون فيها الحاسب الآلي متصلاً بشبكة الاتصالات العالمية فتزداد الصعوبة أكثر فأكثر وترتفع التكاليف، الأمر الذي يتطلب خبرة فنية ومقدرة على معالجة المعلومات والبيانات بصورة يمكن معها تحديد مكان وجود الدليل وأقصر وأيسر السبل لضبطه (المضحكي، 2014).

6. قلة الخبرة وضعف الثقافة بتقنية المعلومات

من البديهي ونحن نتحدث عن جرائم تقع في بيئة الحاسب الآلي أن تكون تلك الجرائم معتمدة بشكل أساسي على تقنية المعلومات ووسائل التكنولوجيا المتطورة والحديثة، الأمر الذي يظهر تطوراً في وسائل ارتكاب الجريمة وفي نوع وطبيعة الدليل وفي طريقة كشفه وضبطه.

فهذه الجريمة لا ترتكب من أناس أو مجرمين عاديين، بل بالعكس فهي جريمة ترتكب من قبل مجرمين أذكياء وذوي إلمام ودراية يمتلكون أدوات المعرفة التقنية والفنية، ويكون توجههم شامل ولا يقتصر على مجال دون آخر حيث توجه جرائمهم للنيل بصورة مباشرة من أجهزة الحاسب الآلي وكل جهاز موصل بالشبكة (البريكي، 2017).

هذه المتغيرات لاشك أنها تتطلب من الجهة المختصة قضائياً أكثر من معرفة عادية وتقليدية بالجرائم الإلكترونية، بحيث لابد من تزويد كل جهة من جهات التحقيق وجمع الاستدلالات بالمعارف الضرورية لمعالجة تلك الجرائم، وخير وسيلة لذلك استحداث إدارات متخصصة تعنى بتلك الجرائم، من حيث ضبطها وجمع أدلتها على غرار دوائر مكافحة المخدرات وتبييض الأموال وغيرها من التقسيمات الأخرى.

7. القضاء المختص بالنظر في الجرائم الإلكترونية

إن من أهم التحديات الإجرائية في اشكاليات جمع الأدلة هو الاختصاص القضائي الذي ينظر في جرائم الكمبيوتر والقانون المعين تطبيقه على الفعل عندما تكون الجريمة خارج حدود الدولة، أو أنها تمر عبر شبكات معلومات وأنظمة خارج الحدود عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهو ما يبرز أهمية امتحان قواعد الاختصاص والقانون الواجب التطبيق (شوقي، يعيش تمام، 2019).

لقد حسم المشرع العماني موضوع الاختصاص القضائي بأن منح القضاء العماني صلاحية نظر الجرائم الإلكترونية المرتكبة في السلطنة وعلى إقليمها بغض النظر عن شخوص الجريمة أو نوعها أو مكان الاعتداء، فأي جريمة ترتكب على إقليم السلطنة فإن الاختصاص ينعقد للقضاء العماني، ومنح أيضاً صلاحية نظر الجرائم التي ترتكب خارج السلطنة إذا كانت تمس أمن السلطنة واستقراره سواء كان مرتكب الجريمة من مواطني السلطنة أو شخص أجنبي، حيث نصت المادة (2) من قانون مكافحة جرائم تقنية المعلومات على

أن: " تسري أحكام هذا القانون على جرائم تقنية المعلومات ولو ارتكبت كلياً أو جزئياً خارج السلطنة متى أضرت بأحد مصالحها أو إذا تحققت النتيجة الإجرامية في إقليمها أو كان يراد لها أن تتحقق فيه ولو لم تتحقق " .

كما بينت المادة (15) من قانون الجزاء العماني المقصود بالأراضي العمانية وجاء فيها على أن: " تسري أحكام هذا القانون على كل جريمة ترتكب في إقليم الدولة، بما يشمله من أراض خاضعة لسيادتها ومياهها الإقليمية، وما يعلوها من فضاء جوي، ويشمل ذلك الجرائم التي ترتكب على متن السفن والطائرات التي تملكها الدولة، أو تحمل علمها، أو تديرها لأي غرض أينما وجدت. وتعد الجريمة مرتكبة في الدولة إذا وقع فيها فعل من الأفعال المكونة لها، أو إذا تحققت نتيجتها، أو كان يراد أن تحقق فيها "، وبناء على ذلك فإن كل جريمة ترتكب في إقليم الدولة سواءً على الأرض أو المياه الإقليمية أو ما يعلوها من فضاء جوي بالإضافة إلى الجرائم التي ترتكب على متن السفن أو الطائرات تعد مرتكبة في الإقليم العماني.

ومع أن المشرع العماني قد أشار إلى أن القاعدة الأساسية في مبدأ الإقليمية أن يتم تطبيق قانون الجزاء على كافة الجرائم التي ترتكب في الإقليم العماني، فلا تفرقه بين مرتكبي هذه الجرائم من حيث جنسيتهم أو طوائفهم أو مهنهم، إلا أن هذه القاعدة ليست مطلقة فهناك استثناءات تعطل أعمال مبدأ الإقليمية وتحول دون سريان قانون الجزاء على بعض الجرائم المرتكبة في إقليم الدولة بسبب الحصانة التي يتمتع بها مرتكبو هذه الجرائم، وقد تكون هذه الحصانة مصدرها قانون الجزاء أو القوانين والتشريعات الداخلية الأخرى، أو قد يكون مصدرها ما تقضي به المعاهدات الدولية أو ما يجري به العرف بين الدول أو مبدأ المعاملة بالمثل.

وتتمثل هذه الاستثناءات في ما أقره قانون الجزاء العماني، حيث نصت المادة رقم (16) من قانون الجزاء على الحالات التي لا تطبق عليها أحكام قانون الجزاء العماني وذلك استثناء من مبدأ الإقليمية، ووفقاً لهذه المادة فإن الاستثناءات تنحصر في الحالات التالية:

أ- الجرائم التي ترتكب على متن السفن والطائرات الأجنبية الموجودة أو المارة بإقليم الدولة .

ب- الجرائم التي يقترفها موظفو السلك الدبلوماسي والقناصل الأجانب، وهم متمتعون بالحصانة التي يخولهم إياها القانون الدولي .

ج- رؤساء الدول الأجنبية .

د- المقرات التمثيلية للدول .

كما أن هناك استثناءات أشار إليها قانون الجزاء العماني، وهي استثناءات مقررة وفقاً لأحكام التشريعات الوطنية وهي كالتالي:

أ- الوضع بالنسبة لرئيس الدولة .

ب- الوضع بالنسبة لأعضاء السلطة التشريعية .

وهناك أيضاً استثناءات مقررة وفقاً لأحكام القانون الدولي وهي كالتالي: -

أ- حصانة رؤساء الدول الأجنبية .

ب- الحصانة الدبلوماسية لأعضاء السلك السياسي والقنصلي .

ج- الحصانة الخاصة بالقوات العسكرية الأجنبية المتواجدة على إقليم الدولة بإذن منها .

ولمواجهة مثل هذه الجريمة مواجهة فعالة يجب تجريم صورها في القوانين الوطنية للمعاقبة عليها، كما يجب أن يكون هناك تعاون دولي كتوقيع الاتفاقيات لمواجهة تلك الجرائم ومشاكلها، من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وايجاد الحلول لمشكلاتها الأساسية.

وتعد مكافحة الجريمة الإلكترونية والحد من انتشارها مسؤولية الحكومات وهي مقياس لرقي المجتمعات، وتتطلب المكافحة آليات وقوانين وتقنيات، فبقدر ما تكون الآليات متطورة بقدر ما تحقق الغايات التي وجدت من أجلها، ويرى الباحث الى أن هناك بعض الحلول أو الآليات القانونية تحد من المعيقات التي تعيق جمع الأدلة الالكترونية ومن أهمها: -

أ- تفعيل دور الأجهزة الوطنية المعنية بمكافحة الجريمة الإلكترونية.

ب- استحداث أقسام متخصصة في مجال جرائم تقنية المعلومات في مراكز الشرطة في مختلف محافظات وولايات السلطنة، كونها أول من يتلقى البلاغ، وضرورة وجود ادعاء عام متخصص.

ج- التدريب والتطوير المستمر للقائمين على مسألة الضبط والتحقيق والمعنيين بجمع الادلة الإلكترونية، وتزويدهم بكل ما هو جديد في عالم التقنيات الحديثة.

د- تأهيل القضاة وتدريبهم ليكونوا قادرين على مناقشة الخصوم بالأدلة الجنائية الإلكترونية.

هـ- التنسيق والتعاون الدولي في النواحي الأمنية والقضائية والقانونية في مجال مكافحة الجرائم الإلكترونية بين الدول.

الخاتمة

من خلال الدراسة تم التوصل إلى أن الدليل الإلكتروني من الأدلة العلمية الحديثة الناتجة عن الجريمة الإلكترونية، كما أن له طبيعة خاصة يختلف بها عن الأدلة الجنائية التقليدية الأخرى، لذا ناقشت الدراسة العديد من المحاور والتي ركزت في مجملها على التعريف بالدليل الإلكتروني، من خلال التطرق إلى أهم الخصائص التي يتميز بها عن الأدلة الجنائية التقليدية الأخرى، إضافة إلى التطرق إلى القواعد الإجرائية التي تحكم الدليل الإلكتروني والتي يجب مواجهة الجريمة بها وتطوير طرق الحصول عليه .

وتناول الباحث في الجزء الأخير من الدراسة إجراءات وإشكاليات جمع الأدلة الإلكترونية، وكيف ان إجراءات جمع الأدلة لها الأثر الكبير في اكتشاف الجاني تقديمة للمحاكمة، كما تم تلخيص أهم الإشكاليات التي تواجهها سلطات التحقيق في مجال الإثبات الجنائي للجريمة الإلكترونية والتي تتعلق بطبيعة الدليل الإلكتروني، وصولاً الى الحلول أو الآليات القانونية للحد من المعيقات التي تعيق جمع الأدلة الالكترونية .

النتائج

1. يتمتع الدليل الالكتروني بمجموعة من الخصائص التي جعلته يتميز عن باقي الأدلة الجنائية .
2. إن تغير أبعاد الجريمة وتميزها بصفات خاصة وأنماط جديدة، يصبح من الضروري أن يتغير تبعاً لذلك أسلوب اكتشافها وطريقة اثباتها، لذا لا يمكن أن تتبع الإجراءات التقليدية لوحدها لمواجهة الجريمة الإلكترونية والحصول على الدليل، حيث أنها لا تكون مجدية في كثير من الأحيان، لما تثيره من إشكاليات نتيجة لطبيعتها غير المادية وما تنتجه من أدلة غير ملموسة .
3. نظراً لأهمية الدليل الإلكتروني في الإثبات الجنائي اهتمت به التشريعات ونظمت كيفية الحصول عليه، باتخاذ إجراءات تتبع وصولاً للغاية منها وهي إثبات الجريمة المرتكبة وإثبات فاعلها وتقديمة للعدالة بناءً على الأدلة التي تم الحصول علها.
4. تفتيش الأجهزة الإلكترونية ووسائل تقنية المعلومات الحديثة والمتطورة للحصول على الدليل الإلكتروني من أخطر المراحل عند اتخاذ الإجراءات الجزائية، لكون محل التفتيش هو جهاز الحاسب الآلي أو الشبكات أو وسائل تقنية المعلومات هو تفتيش للمكونات المعنوية لتلك الوسائل، فلا وجود لمادية الدليل في تلك الوسائل بل هي عبارة عن بيانات ومعلومات رقمية.
5. تواجه سلطات التحقيق العديد من الصعوبات في مجال الإثبات الجنائي من ناحية طبيعة الدليل الإلكتروني، وتتمثل أهمها في أنها أدلة غير مادية تنعدم رؤيتها، إضافة إلى صعوبة الوصول إلى هذه الأدلة، كما أنه يسهل محوها أو تدميرها.

التوصيات

1. تأهيل القضاة وتدريبهم على النظر في القضايا الإلكترونية، ليكونوا قادرين على مناقشة الأدلة الإلكترونية المقدمة في الدعوى مع أطراف الدعوى .
2. إيجاد نصوص قانونية تجرم الأفعال التي تتضمن التخلص من الأدلة الإلكترونية التي يمكن الاستناد عليها لإثبات جريمة معينة وإجراء التحفظ السريع على البيانات، لأن ذلك يجعل المجرم لا يفلت من العقاب إذا ما قام بحذف أو إلغاء الأدلة الإلكترونية التي تدينه.
3. استخراج الأدلة الإلكترونية باحترام كافة الضمانات والحقوق التي يكف لها النظام الأساسي للدولة وكذلك القوانين الأخرى .
4. تأهيل كادر متخصص من مأموري الضبط القضائي والقائمين على قضايا الجرائم الإلكترونية وتقنية المعلومات بدورات وبرامج عملية في تقنية المعلومات وكيفية استخراج والحصول على الدليل الإلكتروني، وتزويدهم بأحدث الأجهزة للقيام بإجراءات الاستدلال في هذه الجرائم وضرورة تدريبهم على كيفية التعامل مع أجهزة الحاسوب والإنترنت لأن دليل سهل تدميره ومحوه في وقت قصير جداً.
5. عدم الاكتفاء بالإجراءات التقليدية لجمع الدليل الالكتروني بحيث يجب أن تصاحبها إجراءات حديثة وهذا من طرف الدول التي لم تنص على الاجراءات الحديثة و اكتفت بالإجراءات التقليدية.
6. التأكيد على أهمية التعاون الدولي في المجال الجنائي وخاصة فيما يتعلق بالجرائم الإلكترونية وجمع الأدلة الالكترونية، وضرورة وضع تشريع دولي خاص بالأدلة الالكترونية لأن الدليل الالكتروني لا يقف عند حدود دولة، باعتبار أن الجرائم الالكترونية من الجرائم العابرة للحدود، مما يحتم أن يكون هذا التعاون لتسهيل إجراءات تحصيل هذا النوع من الأدلة.

المراجع

- إبراهيم، خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008.

- البقمي، ناصر بن محمد، أهمية الأدلة الرقمية في الإثبات الجنائي دراسة وفق الأنظمة السعودية، مجلة الفكر الشرطي، مركز بحوث الشرطة، شرطة الشارقة، المجلد 21، العدد 82، 2012.
- البريكي، ناصر حمد، دور التشريع العماني في مواجهة تحديات التجارة الإلكترونية، دار النهضة العربية، القاهرة، 2017.
- حجازي، عبدالفتاح بيومي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، 2007.
- الرازي، محمد أبوبكر، مختار الصحاح، دار الكتاب العربي، القاهرة، 1981.
- الرقيشي، محمد بن ناصر، الإثبات الجنائي في الجريمة الإلكترونية، رسالة ماجستير، مقدمة لجامعة السلطان قابوس، سلطنة عمان، 2008.
- الزعابي، محمد سالم، الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية، دولة الإمارات العربية المتحدة، 2014.
- سقف المحيط، عادل عزام، جرائم الذم والقدح والتحقير المرتبطة عبر الوسائط الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، 2011.
- سويلم، محمد علي، مكافحة الجرائم الإلكترونية، دار المطبوعات الجامعية، الطبعة الأولى، الإسكندرية، 2019.
- السيابي، حمد بن سعود، وعي الشباب العماني بدور شبكات التواصل الاجتماعي في التوعية بمخاطر الجريمة الإلكترونية ، رسالة ماجستير، مقدمة جامعة السلطان قابوس، 2018.
- الشمري، غانم مرضي، الجرائم المعلوماتية، الدار العلمية الدولية للنشر والتوزيع، عمّان، 2016.
- الطوالبة، علي حسن، أبحاث في جرائم تقنية المعلومات، دار الكتب والدراسات العربية، الإسكندرية، 2018.
- عبدالمجيد، محمود سعد، المجرم المعلوماتي وسلوكياته الإجرامية والأساليب المبتكرة في ارتكابه لجرائمه وسبل مواجهتها، دار المطبوعات الجامعية، الإسكندرية، 2022.
- العازمي، فهد عبدالله العبيد، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016.
- فتح الله، محمود رجب، الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2019.
- قنديل، أشرف عبدالقادر، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015.
- مصطفى، عائشة بن قارة، حجية الدليل الإلكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، 2010.
- المضحكي، حنان مبارك، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت، 2014.
- المعمري، مسعود بن حميد، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة القانون الكويتية العالمية، الكويت، العدد 6، 2018.
- عبدالمطلب، ممدوح عبدالحميد، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والإنترنت، دار الكتب الوطنية، القاهرة، 2006.
- عبيد، مزهر جعفر، شرح قانون الإجراءات الجزائية العماني، الجزء2، أكاديمية السلطان قابوس لعلوم الشرطة، 2014.
- المري، راشد محمد، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، دار النهضة العربية، القاهرة، 2018.
- شوقي، يعيش تمام، الجريمة المعلوماتية، مطبعة الرمال، سكرة، 2019.
- يوسف، أمير فرج، جرائم تقنية المعلومات بدول الخليج العربي والجهود الدولية والمحلية لمكافحة جرائم الإنترنت والحاسوب الإلكترونية في دول الخليج العربي ، دار الكتب والدراسات العربية، الإسكندرية، 2016 .

القوانين: -

- النظام الأساسي للدولة رقم (2021/6).
- قانون الإجراءات الجزائية العماني رقم (99/97).

الاتفاقيات: -

- الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية .