الأدلة الرقمية وإثبات الجرائم السيبرانية
ما بين التأصيل والتأويل

أ.د. عدنان إبراهيم الحجار، د. فايز خضر بشير

جامعة الإسراء

الملخص:

لقد أسهم رقي المجتمعات وتقدمها في شتى المجالات إلى ظهور نمط جديد من الجريمة ارتبط بالتطور التقني والمعلوماتي المعقد والسريع، والذي أطلق عليه عدة مسميات مثل: الجريمة السيبرانية، أو الجريمة المعلوماتية، أو الجريمة الالكترونية، ونظراً لأن إثبات الجريمة يتطلب دليلًا جنائيًا يبني عليه القاضي حكمه، فقد ظهر ما يسمى بالأدلة الرقمية، ولعل هذه الدراسة تحقق أهدافها من خلال بيان ماهية هذا النوع من الجرائم، وبيان ماهية الأدلة التي تثبتها، ومحاولة إبراز حضور هذه الأدلة أو غيابها في مواد القوانين والتشريعات المحلية والعالمية، أظهرت نتائج الدراسة وجود ثغرات وفراغ تشريعي يعتري الدليل الرقمي، ووجود نقص وضعف في التعامل مع الواقع التقني الذي فرض نفسه في كافة مناحي الحياة، بما فيها الحياة القانونية والقضائية، بالإضافة إلى عدم وجود اتفاق في تعريف المصطلحات المتعلقة بهذا النوع من الجرائم، وقد أوصت الدراسة بعدد من التوصيات كان أهمها ضرورة العمل على نشر التوعية الالكترونية بين العاملين في السلك القانوني، وتدريب الكوادر الفنية على تقنيات البحث الجنائي الرقمي، بالإضافة إلى تعزيز عمل القضاء في إصدار أحكام وقوانين وتشريعات تستند إلى الدليل الجنائي الرقمي.

كلمات مفتاحية: الدليل الرقمي – الجريمة السيبرانية.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

Abstract

The advancement and progress of societies in various areas have contributed to the emergence of a new pattern of crime that has been associated with Complex and rapid technical and information evolution. This has been called several names like cyber-crime, information crime, or electronic crime. Since proof of the crime requires criminal evidence on which the judge will base his sentence, so-called digital evidence has emerged. This study may achieve its objectives by showing what this type of crime is, indicating what is the evidence to prove, and the attempt to reflect the presence or absence of such evidence in the articles of local and international laws and legislation. The results of the study showed gaps and a legislative vacuum in the digital directory. The results of the study also showed a lack and weakness in dealing with the self-imposed technical reality in all aspects of life, including legal and judicial life. In addition, there is no consensus in the definition of terms for this type of crime. The most important recommendations of this study were the need to promote electronic awareness among legal professionals. The study also recommended training technical personnel in digital criminal research techniques. In addition, the study recommended strengthening the work of the judiciary in issuing judgments, laws, and legislation based on the Digital Criminal Guide.

Keywords: digital guide, cyber-crime

إشكالية الدراسة:

أحدث التطور التقني الهائل والسريع العديد من التغيرات في شتى المجالات، ومن الطبيعي أن يصاحب تلك التغيرات مخاطر وتهديدات قد تصل أحياناً إلى حد الكارثة، مما ألقى على عاتق العاملين في مجال مكافحة الجريمة عبئاً ثقيلاً يفوق القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث والإثبات الجنائي التقليدية، ولقد أصبحت عملية الإثبات الجنائي للجرائم المستحدثة، والتي تسمى الجرائم التخيلية أو السيبرانية (Cybercrimes) (البشرى، ب.ت، ص 99)، أو جرائم تقنية المعلومات، ترتكز على الدليل الجنائي المستمد من أجهزة الحاسوب، ووسائل الاتصال الحديثة، والذي يعرف بالدليل الرقمي، باعتباره الوسيلة الرئيسة لإثبات هذا النوع من الجرائم، لذا فإن الإثبات الجنائي بالأدلة الرقمية يعد من أبرز تطورات العصر الحديث، تلك التطورات التي جاءت لتواكب الثورة العلمية والتقنية، والتي تطور معها الفكر الإجرامي.

وتشكل الجرائم المعلوماتية تحدياً خطيراً للمواطن، ورجل الأمن، ورجل القضاء، لما تُحدث من مخاطر وتهديدات للجانب الاقتصادي، والجانب الأمني، وحيث إن مرتكب هذا النوع من الجرائم يتميز بقدرٍ عالٍ من العلم، والثقافة، والحرفية، للدرجة التي لا يمكن مواجهته، أو كشفه، أو التحقيق معه، أو محاكمته وفقاً للفكر الأمني والقضائي التقليدي، وقواعد الإثبات الجنائي التقليدية، لذا كان من الضروري استحداث طرائق وأساليب خاصة قوامها العلم والمعرفة والحرفية (فرغلي والمسماري، 2007 ، ص 3).

وعند دراستنا لهذا الموضوع واجهتنا مجموعة من الصعوبات أهمها قلة المراجع والدراسات السابقة، بالإضافة إلى انقسام علماء وأهل الفقه حول توصيف طبيعة هذه الجرائم بين من أعطى لها الوصف الخاص والمحدد، وبين من أعطى لها الوصف العام.

وترتيباً على ذلك، سنحاول في هذه الدراسة التطرق إلى دور الأدلة الجنائية الرقمية في الإثبات الجنائي للجريمة الالكترونية – والتي تسمى الجريمة السيبرانية، أو جريمة تقنية المعلومات – وذلك من خلال الإجابة عن التساؤل الرئيس التالي:

ما مدى حجية الأدلة الرقمية في إثبات الجريمة السيبرانية؟

ويتفرع من هذا التساؤل عدة تساؤلات فرعية وهي:

1. ما الدليل الرقمي من حيث المفهوم والتعريف والخصائص؟
2. ما أساليب التعامل مع الدليل الرقمي؟
3. ما الجريمة السيبرانية من حيث المفهوم والتعريف والوصف؟
4. ما صور ارتكاب الجريمة السيبرانية؟

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

5. ما الطبيعة القانونية للدليل الرقمي في ضوء التشريعات والقوانين الدولية والمحلية؟
6. ما تحديات ومشكلات مكافحة الجريمة السيبرانية؟
7. ما دور القاضي الجنائي في ظل غياب النص العقابي للجريمة السيبرانية؟

أهداف الدراسة:

1. التعرف إلى ماهية الدليل الرقمي.
2. الكشف عن ماهية الجريمة السيبرانية.
3. التعرف إلى الدليل الرقمي في ظل القوانين والتشريعات العربية والعالمية.
4. تحديد تحديات ومشكلات مكافحة الجريمة السيبرانية.
5. التعرف إلى دور القاضي الجنائي في ظل غياب النص العقابي للجريمة السيبرانية.

أهمية الدراسة:

تكمن أهمية الدراسة فيما يأتي:

1. تسليط الضوء على نوع جديد ومستحدث من الأدلة الجنائية الذي انتشر في ظل استخدام تقنية المعلومات في الأنشطة المشروعة وغير المشروعة.
2. قد تسهم الدراسة في التعريف بمكانة الأدلة الجنائية كوسيلة إثبات في الجرائم السيبرانية، والتي كادت أن تبلغ حجيتها قوة بصمات الأصابع والبصمة الوراثية DNA.
3. دعوة السلطات التشريعية وأهل الفقه لدراسة وتقنين وبيان القواعد والأسس المتصلة بالجريمة المعلوماتية والأدلة الجنائية الرقمية.

منهج الدراسة:

المنهج الوصفي التحليلي كونه الوسيلة المنهجية المثلى لتحقيق أغراض الدراسة، حيث تتضح سماته من خلال وصف وتحديد وتحليل بعض المفاهيم التي تقوم عليها الدراسة من الناحيتين الفنية والقانونية.

ومن أجل الإجابة عن التساؤلات السابقة تم تقسيم الدراسة إلى ثلاثة مباحث، اشتمل الأول على مفاهيم وتعريفات، واشتمل الثاني على تأصيل وتأويل الأدلة الرقمية في ظل التشريعات والقوانين، واشتمل الثالث على محددات وتحديات الإثبات الجنائي الرقمي.

المبحث الأول: مفاهيم وتعريفات

أحدثت الثورة المعلوماتية الحديثة العديد من المفاهيم والمصطلحات القانونية الجديدة، لا سيما في القانون الجنائي، لذا تناولنا في هذا المبحث المفاهيم والتعريفات الخاصة بالجرائم

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

التي تحدث عبر أجهزة الحاسوب، والشبكة العنكبوتية، حيث تناول المطلب الأول ماهية الدليل الرقمي، وتناول المطلب الثاني ماهية الجريمة السيبرانية (المعلوماتية).

المطلب الأول/ ماهية الدليل الرقمي.

من المعلوم أن الحديث عن ماهية الشيء يعني البحث في مفهومه، وتعريفه، والخصائص التي يتميز بها عن غيره، لذا وجب علينا توضيح مفهوم الدليل الرقمي من خلال التطرق إلى تعريفه لغوياً واصطلاحياً، وبيان خصائصه وأساليب التعامل معه، حيث تناول الفرع الأول من هذا المطلب تعريف الدليل الرقمي، والفرع الثاني خصائص الدليل الرقمي، والفرع الثالث وسائل التعامل مع الدليل الرقمي.

الفرع الأول: تعريف الدليل الرقمي.

الدليل لغة هو ما يستدل به، والدليل هو الدال أيضاً، وقد دله على الطريق أي أرشده، والاسم الدال بتشديد اللام، وفلان يدل فلاناً أي يثق به، فالدليل في اللغة هو ما يستدل به، والجمع أدلة ودلالات. والدليل اصطلاحاً هو ما يلزم من العلم به علم شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني فيما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة (البشرى، ب. ت. ص 104).

أما الدليل قانوناً فهو إقامة البينة والبرهان والحجة على شخص أمام القضاء، ووفقاً لأحكام القانون على واقعة قانونية متنازع عليها بين الخصوم (حمو وعلاء وعبدالله، 2015، ص 32).

وحيث إن الدليل الرقمي نوع من أنواع الأدلة الجنائية، لذا ينطبق عليه خصائص الأدلة الجنائية وشروطها واستخداماتها؛ إلا أنها تتميز عنها بخصائص نوعية لا تتوفر في غيرها من الأدلة الجنائية التقليدية(البشرى، ب.ت.، ص 109)، وإن كانت متشابهة في الغاية إلا أنها مختلفة في المضمون، حيث إن المقصود بالدليل الرقمي هو ذلك الدليل الذي يتم الحصول عليه من الأجهزة الالكترونية، ويكون في شكل نبضات كهربائية أو مغناطيسية يتم تحليلها، وينتج عنها نصوص، أو صور، أو أشكال يتم ربطها بالجريمة، والجاني، والمجني عليه، وكل ذلك بطرق لا تتعارض وأحكام القانون (عبد الحميد، 2000، ص 108).

وهناك العديد من التعريفات للأدلة الجنائية الرقمية حيث يعرفها كيسي (Casey) بأنها كافة البيانات الرقمية التي يمكن من خلالها إثبات وقوع جريمة، أو إثبات وجود علاقة بين الجريمة ومرتكبها، أو بين الجريمة والمتضرر منها (Eoghan Casey ,2000, P.260)، كما وتعرف بأنها الأدلة المأخوذة من أجهزة الحاسوب، وتكون على شكل مجالات أو نبضات مغناطيسية وكهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

تكنولوجيا المعلومات، وهي مكونات رقمية لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة، أو الصور، أو الأصوات، أو الأشكال والرسوم، وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون وتطبيقه (عبد الحميد، 2000، ص 88).

من التعريفات السابقة للدليل الرقمي علينا أن نميز ما بين الأثر المادي الملموس (الفيزيائي)، وما بين الأثر الالكتروني (الرقمي) لبيانات الحواسيب، فالآثار المادية تكون موجودة في القرص الصلب على شكل كهرومغناطيسي، أو موجودة بشكل مؤقت في ترانزستورات الذاكرة المؤقتة، أو موجودة في الأطياف الكهرومغناطيسية في الكوابل، ولا يمكن رؤيتها، أما الأدلة الالكترونية فهي عبارة عن تفسير لهذه الآثار الفيزيائية بواسطة أدوات وبرمجيات خاصة(حمو وعلاء وعبدالله، 2015، ص 11).

الفرع الثاني: خصائص الدليل الرقمي.

حيث إن بنية الدليل الرقمي هي بنية افتراضية، ونظراً لتمايز الدليل الالكتروني على الدليل التقليدي، فإن هناك العديد من الخصائص التي ينفرد بها بسبب طبيعته المغايرة، أبرزها أنه غير ملموس، وغير مادي، ولا يمكن إدراكه بالحواس العادية، وإنما يتطلب لفهمه وإدراكه الاستعانة بالأجهزة الالكترونية، كما أنه دليل يمكن نسخة بصورة مطابقة للأصل لأكثر من مرة بالقيمة العلمية نفسها، والقوة في الإثبات نفسها، كما يمكن محوها وإرجاعها بسهولة، وبالتالي يصعب التخلص من الدليل الالكتروني بصورة نهائية (مرجع سابق، ص 33). وحيث إنه دليل مبني على أسس علمية، فإن تحرير محضر يتناول دليلًا علميًا يعني ضرورة توافر مسلك علمي في تحريره. ويمكن القول بأنه أيضًا دليل متنوع ومتطور، ويصعب التخلص منه ولو كان ذلك باستخدام أقوى أدوات الإلغاء Delete، أو الحذف Erase إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب (بن يونس، 2006، ص ص 7–10).

الفرع الثالث: وسائل التعامل مع الدليل الرقمي.

تعتبر عملية الحصول على الأدلة الجنائية الرقمية أمراً صعب الوصول إليه، لما يتطلب من مهارة وخبرة في مجال التقنية الرقمية، إضافةً إلى تطور وتعدد صور وأشكال الجريمة السيبرانية، وهناك وسائل للحصول على الدليل الرقمي منها وسائل مادية، وأخرى إجرائية، فالوسائل المادية هي تلك الأدوات الفنية والبرامج ذات الطبيعة التقنية التي يمكن من خلال استخدامها إثبات وقوع الجريمة، وتحديد شخصية مرتكبها، أما الوسائل الإجرائية فهي تلك الإجراءات المحددة قانونًا، والتي تستعمل أثناء تنفيذ طرق التحقيق التي تثبت وقوع الجريمة، ويتم ذلك من خلال استخدام تقنيات وبرامج الكترونية مختلفة، تماشيًا مع إرادة المشرع في مكافحة الجرائم المعلوماتية (عبد المطلب، 2015، ص ص 14 – 18).

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

ويعتبر التفتيش من الوسائل الإجرائية التي تستهدف ضبط أشياء مادية تتعلق بالجريمة، وتفيد في كشف ملابساتها، ولكن ذلك لا ينسجم مع طبيعة الدليل الرقمي، التي تكون على صورة مكونات مادية تتمثل في وحدات الإدخال (لوحة المفاتيح، والفأرة،...الخ)، ووحدات الإخراج (الشاشة، والطابعة،...الخ)، أو تكون على صورة مكونات معنوية تتمثل في البرامج والأساليب المتعلقة بتشغيل وحدة معالجة البيانات (مرجع سابق، ص 25).

المطلب الثاني/ ماهية الجريمة السيبرانية.

تتميز النظم المعلوماتية بالدقة والسرعة في معالجة البيانات وتخزينها، وهذا أدى بطبيعة الحال إلى إحداث تطور كبير في جميع مناحي الحياة، وقد أدى هذا التطور إلى ظهور الجريمة السيبرانية التي تسببت في العديد من الاعتداءات على الحياة الخاصة للأفراد، علاوة على أنها أحدثت خسائر كبيرة لاقتصاد الدول، وفي هذا المطلب سنتعرف على مفهوم وتعريف ووصف الجريمة السيبرانية، وصور ارتكابها.

الفرع الأول: وصف الجريمة السيبرانية والتعريف بها

إن أهم ما يلاحظ على ظاهرة الجريمة السيبرانية هو عدم وجود مصطلح معين ومتفق عليه للدلالة عليها، فهناك من يطلق عليها جريمة الاختلاس المعلوماتي، أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة الالكترونية (قنديل، 2015، ص 24)، وهناك من يسميها جرائم تقنية المعلومات، أو الجرائم السيبرانية، وهذا بسبب ارتباطها بالحاسب الآلي، ولما لها من طبيعة خاصة تميزها عن غيرها من الجرائم التقليدية.

وقد جاءت توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة المنعقد في فينا سنة 2000م بتعريف للجريمة السيبرانية او الالكترونية بأنها «جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية،» وبالرجوع إلى قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية نجد أن المشرع الفلسطيني لم يضع تعريفا للجريمة السيبرانية أو الإلكترونية، تاركا المجال مفتوحا للاجتهاد الفقهي، حيث لم يستقر الفقه القانوني على مفهوم محدد للجرائم السيبرانية بوصفها من الجرائم المستحدثة التي ما تزال في مهد البحث والدراسة، فمن تطرق للبحث في هذا النوع من الجرائم اعتمد مفاهيم واستخدم أساليب ومناهج تناسب وتلائم المجال الذي تنتمي إليه دراسته، لذلك تعددت التعريفات تبعاً للمعايير والمنطلقات المستندة إليها، يعرف مكتب تقييم التقنية بالولايات المتحدة الأمريكية الجرائم السيبرانية بأنها « الجرائم التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دوراً رئيسًا» (ابراهيم، 2008، ص 23).

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وهناك من عرَّف الجريمة السيبرانية بأنها السلوك غير المشروع والذي يعاقب عليه القانون، والصادر عن إرادة جرمية ومحله معطيات الحاسوب (المومني، 2000، ص 25)، وهناك من عرَّفها بأنها كل سلوك – إيجابياً كان أم سلبياً – يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت (مرجع سابق، ص 49).

مما سبق يتبين لنا أن تعريف الجريمة السيبرانية يتراوح ما بين الجرائم التي ترتكب من خلال استخدام الحاسوب، وما بين التي ترتكب بالمعدات التقنية، وهي ممارسات تمارس ضد الفرد أو الجماعة بهدف إلحاق الأذى بالمجني عليه، سواء كان الأذى مادياً أو معنوياً[1].

الفرع الثاني: صور ارتكاب الجريمة السيبرانية

تحتاج الجريمة السيبرانية لارتكابها إلى توافر شبكة المعلومات الدولية(الانترنت)، ووجود مجرم يوظف خبرته أو قدرته في التعامل مع الشبكة للقيام بجريمته دون الحاجة إلى سفك دماء، أو ممارسة عنف وإيذاء، أو بذل مجهود عضلي كما في جرائم القتل، أو الاختطاف، ودون الحاجة أيضاً إلى كسر أو خلع، كما في جرائم السرقة التقليدية، فالجريمة السيبرانية جريمة هادئة (soft crime)، ولا تحتاج إلى عنف، وتتم عادة بتعاون أكثر من شخص لارتكابها، وغالباً ما يشترك في إخراجها شخص متخصص في تقنيات الحاسوب والإنترنت، وآخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه (مرجع سابق، ص 57، 58).

وقد ورد في الاتفاقية الأوروبية لعام 2001 تقسيم جرائم الحاسوب والانترنت إلى (مركز هردو، 2018، ص 8):

1. الجرائم التي تستهدف عناصر المعطيات والنظم.
2. الجرائم المرتبطة بالكمبيوتر» التزوير والاحتيال».
3. الجرائم المرتبطة بالمحتوى» الأفعال الإباحية والأخلاقية».
4. الجرائم المرتبطة بحقوق المؤلف والحقوق المجاورة.

المبحث الثاني: الأدلة الرقمية في ظل التشريعات والقوانين تأصيلاً وتأويلاً

تسعى الدول للحد من الجريمة السيبرانية من خلال فرض سياسات دولية وعقوبات كبيرة على مرتكبيها، وتفعيل أحدث التقنيات والوسائل للكشف عن هوية الفاعلين، وكذلك نشر التوعية في المجتمعات حول الجرائم الالكترونية وخطرها، وتعريف الأفراد بكيفية الحفاظ

1. أصدرت دولة فلسطين قرارًا بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية، ويتكون من (57) مادة موضحًا فيه التعريفات والمصطلحات القانونية والعلمية الخاصة بالجريمة السيبرانية، سيما المادة رقم (1) منه.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

على معلوماتهم وخصوصياتهم، وتوجيه التشريعات والقوانين وتحديثها بما يتماشى مع التطورات لفرض قوانين جديدة فيما يستجد من هذه الجرائم (مرجع سابق، ص 18).

ولا شك أن للقاضي – في القوانين الوضعية – سلطة تقدير الأدلة، واستنباط القرائن، وما تحمله من دلالات، شرط أن يكون الدليل مرتبطاً بالواقعة، وثابتاً بيقين، ومنسجماً مع التسلسل المنطقي للأحداث. وينسحب هذا القول على الدليل الجنائي الرقمي كونه أحد أقسام الأدلة المادية العلمية، بل أكثر منها حجية في الإثبات، لأنها جاءت وفق قواعد علمية وحسابية لا تقبل الشك أو التأويل (Amadt and Plaza,1994, p 18).

أما في الفقه الجنائي الإسلامي؛ فإن الأدلة الجنائية الرقمية تنتمي إلى باب القرائن، وذلك لأنها من أقوى الأدلة المادية، وأكثرها علمية(البشرى، ب. ت. ، 129)، ويرى جمهور الفقهاء جواز الاعتماد على القرائن في الإثبات.

وسنتطرق في المطلب الأول من هذا المبحث إلى حجية الدليل الجنائي الرقمي الناشئ عن التفتيش، وفي المطلب الثاني سنبحث عن مكانة الأدلة الرقمية في التشريعات الدولية، وفي المطلب الثالث عن مكانة الأدلة الرقمية في التشريعات الوطنية العربية.

المطلب الأول/ حجية الدليل الرقمي الناشئ عن التفتيش.

كما هو معلوم بأن التفتيش ما هو إلا وسيلة إجرائية تستهدف ضبط أشياء مادية تتعلق بالجريمة، وتفيد في كشف حقيقتها؛ إلا أن ذلك لا يتوافق مع الطبيعة غير المادية للدليل الجنائي الرقمي(هروال، 2007، 223).

وحسب ابو حجيلة فإن هناك خلافاً فقهياً حول موضوع تفتيش أجهزة الحاسوب، حيث إن القواعد العامة تفترض وجود شيء مادي ليقع عليه التفتيش، وهناك جانباً من الفقه لا يعتبر الحاسوب شيئاً مادياً يصح أن تنطبق عليه قواعد التفتيش، وذهب جانب آخر إلى اعتبار أن التفتيش بقواعده ينطبق على الحاسوب، لأن البحث عن دليل في الحاسوب يعني بالضرورة أن هذا الدليل يشغل حيزاً في ذاكرة الحاسوب، وبالتالي يمكن القياس عليه، لكن وبغض النظر عن تلك الاتجاهات فإن العبرة تكمن في مكان وجود الحاسوب، وبالتالي فإن الأجهزة الإلكترونية تأخذ حكم المكان الذي توجد فيه (أبو حجيلة مشار إليه في حمو وعلاء وعبدالله، 2015، ص 32).

وقد عالجت معظم التشريعات الحديثة المتعلقة بالجرائم الالكترونية هذه المسألة صراحة، ومن هذه التشريعات قرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية حيث نصت المادة (32) منه على «1– للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة...»

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

شريطة أن يكون أمر التفتيش مسببًا ومحددًا، فإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة يتعين على مأموري الضبط القضائي في هذه الحالة تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها وفقا للمادة المذكورة آنفًا، والتي أجازت كذلك لوكيل النائب العام أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات والمعلومات، على أن يكون مأمور الضبط القضائي مؤهلًا للتعامل مع الطبيعة الخاصة للجرائم الالكترونية.

كما أجازت المادة (33) من قرار بقانون للنيابة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الالكترونية، أو أي معلومات ذات صلة بالجريمة، أو أي وسيلة من وسائل تكنولوجيا المعلومات من الممكن أن تساعد في كشف الحقيقة، كما أجازت المادة (34) من قرار بقانون لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الالكترونية، وتسجيلها والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يومًا قابلة للتجديد لمرة واحدة بناء على توافر دلال جدية.

ومن الجدير بالذكر أن المشرع الفلسطيني اعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية من أدلة الإثبات وفقا للمادة (38) من ذات القرار بقانون، كما ظهرت في السنوات الأخيرة العديد من التشريعات الوطنية التي تهدف إلى تنظيم وتطوير البنية الأساسية القانونية لتطبيق المعاملات الالكترونية مع إرساء مبادئ قانونية للقواعد والمعايير المتعلقة بتوثيق وسلامة المراسلات والسجلات الالكترونية، والتي تتمثل أساسًا في الاعتراف بحجية الملفات ذات المدلول التقني مثل الملفات المخزنة الكترونياً، ومستخرجات الحاسوب، والبيانات المسترجعة من نظم الميكروفيلم، والميكروفيش، والإقرار بحجية التوقيع الالكتروني، ومعادلته بالتوقيع اليدوي باعتباره دليلا للإثبات، والتخلي بالتدريج عن أية قيود تحد من الإثبات في البيئة التقنية، ومنها في فلسطين القرار بقانون رقم (15) لسنة 2017م بشأن المعاملات الالكترونية، وقانون المعاملات الالكتروني الأردني رقم 15 لسنة 2015، وقانون التوقيع الالكتروني المصري رقم 15 لسنة 2004، حيث اتفقت نصوص هذه القوانين على إعطاء المحررات الالكترونية حجية كاملة في الإثبات إذا استوفت الشروط القانونية.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وحتى يتمكن المحقق الجنائي من إقناع القاضي بالدليل الجنائي الرقمي لا بد أن يراعي – عند عرض هذا الدليل – المنهجية التالية (lexander Geschonneck مشار إليه في حمو وعلاء وعبد الله، 2015، ص 40):

* القبول: أي استخدام الأدوات والآليات المعروفة، والتي سبق استخدامها، ولكن إذا أراد المحقق استخدام أدوات غير معروفة، فإن عليه أن يقدم التبرير المناسب والمقنع لاستخدام تلك الأدوات.
* المصداقية: وهي مدى قبول آلية العمل للصمود والمصداقية أمام أي استفسار.
* التكرار: أي إمكانية اتباع نفس الخطوات من محقق آخر، والحصول على نفس النتائج.
* سلامة الدليل: أي إمكانية حفظ الدليل، وتتبع الخطوات التي استعملت للحصول عليه.
* السبب والمسبب: أي قدرة المنهجية على الربط بين الأشخاص والآثار والنتائج التي تم الوصول إليها من خلال التحقيق.
* التوثيق: أي لا بد أن تراعي المنهجية توثيق جميع خطوات العمل بالتفصيل.

وعليه فإنه يمكن القول بحجية الدليل الرقمي الناشئ عن التفتيش طالما أنه تم الحصول عليه بطرق مشروعة، وطالما أن القاضي اقتنع به بشكل لا يحتمل الشك، شريطة تطبيق القواعد العامة في اعتماد أي دليل رقمي مهما كان الدليل الرقمي حديثا، ومهما كانت تلك القواعد قديمة وتقليدية (مرجع سابق، ص 40).

المطلب الثاني/ الأدلة الرقمية في التشريعات الغربية.

من الطبيعي أن البحث في الأدلة الجنائية الرقمية يتطلب تسليط الضوء على الإطار القانوني له، وبيان وجهة نظر المشرع منه، وتعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الالكتروني. ولقد أدركت العديد من الدول الأخطار المتسارعة لتقنية المعلومات على الحق في الخصوصية، الأمر الذي دفع البعض منها إلى حماية هذا الحق في الدساتير الخاصة بها.

ومن أبرز المجموعات والمنظمات الدولية التي عملت في موضع جرائم شبكة الانترنت مجموعة الدول الثماني G8، والأمم المتحدة ومنظماتها، والاتحاد الدولي للاتصالات، ومجلس أوروبا(مركز هردو، 2018، ص 27).

وعلى صعيد الدول الأوروبية فقد سن المشرع الفرنسي قانون رقم 19–88 لسنة 1988 وضمنه قانون العقوبات الفرنسي في المادة 462 وجرم فيه مجرد الولوج إلى نظام المعالجة

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الآلية، أو البقاء فيه بطريق غير مشروع بعقوبة الحبس أو الغرامة، وخضع هذا القانون لتعديلات سنة 1993 لتحقيق مزيد من الأبعاد الردعية. وسن المشرع البريطاني قانون إساءة استخدام الحاسوب لسنة 1990، وقد شهدت التجربة البريطانية تميزاً من حيث محتوى التنظيم أو الحلول التشريعية المقررة. أيضًا عدل المشرع النرويجي قانون العقوبات عام 1985، وجرم الوصول غير المصرح به عن طريق تخطي الحماية إلى البيانات المخزنة أو المنقولة بالوسائل الالكترونية أو الفنية الأخرى. أما القانون السويسري بشأن الجريمة المعلوماتية فقد شمل نصوصًا تعاقب على الحصول دون تصريح على بيانات مخزنة الكترونيًا، أو على البرامج بقصد الإثراء على نحو غير مشروع، وعلى التوصل إلى نظم الحاسوب وإتلاف المعطيات (مرجع سابق، ص 21، 22).

كما نصت الفقرة الرابعة من المادة 18 من الدستور الإسباني أن « القانون هو الذي يحدد البيانات التي تخضع للمعالجة الالكترونية، وذلك لضمان الكرامة والحصانة الشخصية والأسرية للمواطنين في ممارسة حقوقهم» (المومني، 2000، ص 183).

المطلب الثالث/ الأدلة الرقمية في التشريعات الوطنية العربية.

تسعى الدول والحكومات العربية إلى الحد من الجرائم السيبرانية عبر توجيه التشريعات والقوانين وتحديثها بما يتوافق مع التطورات التقنية، وهنا نستعرض بعض القوانين والتشريعات في عدد من الدول العربية والتي اهتمت بمكافحة الجريمة السيبرانية.

لم يورد قانون أصول المحاكمات الجزائية الأردني رقم 9 لسنة 1961م نصًا صريحًا بقبول الدليل الرقمي، ولكن بالرجوع إلى المادة 2/147 منه نجد أنها تنص على أن البينة تقام في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية، مما يدلل على جواز الأخذ بالدليل أيا كان، شرط استخلاصه بطريق مشروع، وأن يرتاح له ضمير القاضي، مما يعزز توجه المشرع الأردني الأخذ بالدليل العلمي الرقمي (العدوان، 2018، ص 66).

وينص قانون الجزاء العماني الصادر بالمرسوم السلطاني رقم 2018/7 على أنه» يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر، ولا تزيد عن سنتين، وبغرامة مائة ريال، إلى خمسمائة ريال، أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسوب في ارتكاب أحد الأفعال الآتية: انتهاك خصوصيات الغير، أو التعدي على حقهم في الاحتفاظ بخصوصياتهم وتزوير البيانات، أو الوثائق مبرمجة أي كانت شكلها (المومني، 2000، ص 185).

وقد جرم المشرع الجزائري الأفعال الماسة بنظام المعالجة الآلية للمعطيات، أو ما سميت بالغش المعلوماتي بموجب القسم السابع مكرر من قانون العقوبات، فقد عاقب بالحبس من

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

ثلاثة أشهر إلى سنة وبغرامة من 50 ألف إلى 100 ألف دينار جزائري، في حال إدخال – بطريق الغش – معطيات فنية المعالجة أو نفس العقوبة على المحاولة، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، أما إذا ترتب عنها تخريب نظام اشتغال المنظومة تكون العقوبة من 6 أشهر إلى سنتين حبس، والغرامة من 50 ألف إلى 150 ألف دينار جزائري، وتعاقب المادة 394 مكرر على المساس بمنظومة معلوماتية بالإدخال، الإزالة، أو التعديل بطريق الغش بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500 الف إلى 2 مليون دينار جزائري، في حين نصت المادة 394 مكرر 2 على عقوبة الحبس من شهرين إلى 3 سنوات وبغرامة من مليون إلى 5 مليون دينار جزائري لكل من يقوم عمداً وبطريق الغش بتصميم أو بحث أو تجميع أو توفير نشر الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية وافشاء أو نشر المعطيات (مركز هردو، 2018، ص 19).

وبالاطلاع على المادة 12 من قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010 الأردني نجد أنها نصت على أصول وقواعد معينة تتعلق بالتفتيش، وهي ضرورة الحصول على إذن من المدعي العام أو من المحكمة المختصة عند التفتيش، وكذلك أصول تتعلق بإجراء الضبط من موظفي الضابطة العدلية، وتنظيم محضر بكل الإجراءات وتقديمه إلى المدعي العام (حمو وعلاء وعبدالله، 2015، ص 50).

وينص القانون على معاقبة كل من أرسل أو نشر عن طريق نظام معلومات، أو الشبكة المعلوماتية قصداً كل ما هو مسموع، أو مقروء، أو مرئي، يتضمن أعمالاً إباحية تتعلق بالاستغلال الجنسي لمن لم يكمل الثامنة عشرة، أو توجيهه لارتكاب جريمة بالحبس لمدة لا تقل عن سنتين، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد عن خمسة آلاف دينار (مركز هردو، 2018، ص 20).

ونصت المادة 19 من قانون البينات الفلسطيني رقم 4 لسنة 2001 على ما يلي[2]:" 1- تكون للرسائل الموقع عليها قيمة السند العرفي من حيث الإثبات ما لم يثبت موقعها أنه لم يرسلها، ولم يكلف أحداً بإرسالها. 2- تكون للبرقيات ومكاتبات التلكس والفاكس والبريد الإلكتروني هذه القوة أيضاً إذا كان أصلها المودع في مكتب التصدير موقعاً عليها من مرسلها، وتعتبر البرقيات مطابقة لأصلها حتى يقوم الدليل على عكس ذلك".

وأيضاً نصت المادة 1 من القرار بقانون رقم 9 لسنة 2007 بشأن مكافحة غسل الأموال[3]، حيث تم ذكر أن السندات القانونية الالكترونية والرقمية تعتبر من الأموال، فلو أثبت وجود سندات الكترونية تدل على الاشتباه بوقوع جريمة غسل الأموال، وتم إثبات ذلك

2. قانون البينات الفلسطيني رقم 4 لسنة 2001 – صدر في غزة بتاريخ 2001/5/12م.

3 قرار بقانون رقم (9) لسنة 2007م بشأن مكافحة غسل الأموال – صدر في رام الله بتاريخ 2007/10/25م.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

بتلك السندات، فإن الحكم هنا يكون قد استند إلى دليل الكتروني (حمو وعلاء وعبدالله، 2015، ص 36).

وقد أكد المشرع الفلسطيني على حجية الدليل الالكتروني في الاثبات بموجب أحكام المادة (37) من قرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية، والتي نصت على «يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الالكترونية أو البيانات والمعلومات الالكترونية من أدلة الاثبات» كما اعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول اخرى من أدلة الاثبات طالما أن الحصول عليها قد تم وفقا للإجراءات القانونية والقضائية للتعاون الدولي وفقا للمادة (38) من ذات القرار بقانون بالنص على : « تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي".

المبحث الثالث: محددات وتحديات الإثبات الجنائي الرقمي.

لقد باتت جرائم الحاسوب ظاهرة عالمية يصعب التحقيق فيها والحكم عليها، أو التنبؤ بها، وذلك لعدم توافر شهود أو أدلة مادية في كثير من الحالات، علاوة على أن تقنيات الحاسوب في تطور كبير لم يواكبها تعريفات واضحة ومحددة، وتشريعات قانونية مناسبة (منصور، 2011، ص 149). فالأمور لا تستقيم ما لم تكن الأجهزة القضائية ملمة بالجوانب الفنية والعلمية للجرائم الرقمية، وكذلك التعاطي القانوني مع مشكلة الاختصاص المرتبطة بطبيعة هذا النوع من الجرائم، وعليه فإن الإثبات الجنائي للأدلة الرقمية يواجه تحديات تشريعية والتي منها (ابراهيم، 2008، ص 83):

1. في مجال قانون العقوبات: تقاعس المشرع في كثير من الدول، وبخاصة الدول العربية عن تدارك النقص الذي يعتري التشريعات العقابية في مجال الجريمة السيبرانية، وترك أمر معالجتها للنصوص التقليدية، مما أوجد فراغاً تشريعياً، ولتجاوز هذه المشكلة لجأ بعض الفقهاء إلى الاجتهاد في تفسير النصوص القانونية العقابية التقليدية، إلا أن ذلك لم يحل المشكلة، الأمر الذي أدى من بعض الدول إلى استصدار قوانين خاصة بهذا النوع من الجرائم.
2. في مجال قانون الإجراءات الجزائية: إن الخلاف الفقهي الذي نشأ حول مدى خضوع المكونات المعنوية لإجراءات المعاينة والتفتيش والضبط في ظل القواعد التقليدية، يترتب عليه الإضرار بعملية التحقيق والطعن في مشروعية الإجراءات.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

3. في المجال الفني: لا تختلف إجراءات التحقيق في جرائم تقنية المعلومات – من حيث المراحل الفنية – عن الجرائم التقليدية، إلا أن طبيعة وخصائص وسمات هذا النوع من الجرائم هو الذي يختلف، بما تتميز به من سرعة التخفي، وسرعة التطور في الأساليب، وعدم اعترافها بالحدود الجغرافية بين الدول، وصعوبة إثباتها، وعدم وجود آثار مادية ملموسة يمكن أن تقود إلى الجاني، علاوة إلى إمكانية أخذ التدابير الوقائية من قبل الجاني باستخدام الترميز والتشفير للبيانات.

من أجل ما سبق قمنا بتقسيم هذا المبحث إلى ثلاثة مطالب، تناول المطلب الأول الضوابط القانونية المقيدة للقاضي عند تفسير النص العقابي، وتناول المطلب الثاني تحديات ومشكلات مكافحة الجريمة السيبرانية، وتناول المطلب الثالث دور القاضي الجنائي في ظل غياب النص العقابي للجريمة السيبرانية.

المطلب الأول/ الضوابط القانونية المقيدة للقاضي عند تفسير النص العقابي.

تختلف سلطة القاضي الجنائي في تقدير أدلة الإثبات من دولة إلى أخرى حسب ما تعمل به كل دولة من أنظمة الاثبات، حيث يوجد نظامان أحدهما مقيد(قانوني)، والآخر حر(مطلق)، ويعتبر نظام الإثبات القانوني من أقدم أنظمة الإثبات الجنائية (عبد المطلب، 2015، ص 58 –59)، حيث يتقيد القاضي في حكمه بالبراءة أو الإدانة بالأدلة التي حددها المشرع، دون إعمال القناعة الشخصية بصحة الأدلة، إذ يقوم اقتناع المشرع مقام اقتناع القاضي، وبالتالي فإن اليقين القانوني يقوم أساساً على افتراض صحة الدليل بغض النظر عن حقيقة الواقع، أو اختلاف ظروف الدعوى (نصر الدين مبروك – مشار إليه في المرجع السابق– ص59)، وعلى الرغم من أن هذا النظام يقيد القاضي، ويضعه في قالب جامد للإثبات، ويقحم المشرع في أمور لا صلة له بها؛ إلا أنه لا يزال يطبق في بعض التشريعات الجنائية مثل التشريع الإنجليزي والتشريع الأمريكي، وبمراجعة قانون البوليس والإثبات الجنائي الإنجليزي نجد أن الأدلة الناتجة عن الحاسب الآلي لا تُقبل كدليل إلا إذا استكملت اختبارات الثقة المنصوص عليها في المادة 69 بحيث أن عدم قبول هذا النوع من الأدلة يعود إما لسبب معقول يدعو إلى الاعتقاد بأن هذا الدليل غير دقيق، أو أن بياناته غير سليمة، وإما أن الحاسب الآلي لا يعمل بكفاءة وبصورة سليمة، أو أنه تم استخدام جهاز الحاسب الآلي بشكل غير مصرح، وبالتالي عدم قبول الأدلة الناتجة عن هذا الاستعمال (هلالي، 2004، ص 728). بالإضافة إلى عدم قيام الخبير المكلف بفحص الحاسب الآلي بإحداث أي تغيير في البيانات الموجودة في الجهاز، وإذا اضطر لذلك – ولو إجراء تغيير بسيط – يجب أن يقدم تفسيراً مقنعاً لهذا التغيير (Association of Chief Police Officers 2011. P6).

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

أما المشرع الأمريكي فقد ذكر في قانون الإثبات الصادر في ولاية كاليفورنيا عام 1983م بأن النسخ المستخرجة من البيانات التي يحتويها جهاز الحاسب الآلي تكون مقبولة بوصفها أفضل وأنسب الأدلة المتاحة لإثبات هذه البيانات (الطوالبة، 2004، ص 197).

أما نظام الإثبات الآخر وهو النظام الحر (المطلق)، فلم يحدد القانون فيه طرقًا معينةً للإثبات، حيث أنه منح للخصوم الحرية التامة في اختيار الأدلة التي يرونها تؤدي إلى تكوين قناعة القاضي، إلا أن حرية القاضي في الاقتناع ليست مطلقة، ويجب على القاضي أن يكون حكمه مسبباً (بوالطمين، 2018، ص 21)، ولكن هذا النظام لم يسلم من العيوب، فهو لا يحقق الاستقرار في المعاملات لاختلاف الأدلة وتقديرها من قاضٍ إلى آخر، الأمر الذي يؤدي إلى اختلاف المبادئ وتعارضها (الشبكات المشار إليه في المرجع السابق، ص22).

ولتفادي مساوئ كلا النظامين المقيد والحر ظهر نظاماً ثالثاً يجمع بينهما، وهو نظام الإثبات المختلط أو المذهب المختلط، وهو المذهب الذي يجمع بين الإثبات الحر، وبين الإثبات المقيد، فيكون حراً في المسائل الجنائية، وله أن يلتمس الحقيقة من أي دليل يقدم إليه، ثم يتقيد بعض الشيء في المسائل التجارية مع بقائه حراً في الأصل، أما في المسائل المدنية فمقيد إلى حد كبير بطرق محددة للإثبات قد تضيق وقد تتسع وفقا للظروف والملابسات، وهذا المذهب هو خير المذاهب التي قيلت في الإثبات حيث جمع بين ثبات التعامل بما احتوى عليه من قيود، وبين اقتراب الحقيقة الواقعية من الحقيقة القضائية بما أفسح فيه للقاضي من حرية التقدير4، وقد أخذت بهذا النظام أغلب التشريعات الدولية مثل القانون الفرنسي، والقانون البلجيكي، والقانون الإيطالي، وكذلك التشريعات العربية مثل القانون المصري، والأردني، واللبناني (بوالطمين، 2018، ص 23).

وبالرجوع الى المادة (206) من قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001 والتي نصت على « إقامة البينة في الدعاوى الجزائية بجميع طرق الاثبات: 1- تقام البينة في الدعاوى الجزائية بجميع طرق الاثبات إلا إذا نص القانون على طريقة معينة للإثبات ...» وهذا يعني أن الاثبات بالأدلة الالكترونية جائز في الدعاوى الجزائية طالما لم ينص القانون على طريقة معينة للإثبات وطالما اقتنع القاضي بالدليل، أما القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الالكترونية الفلسطيني فقد عالج المسألة بشكل صريح، اذ اعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات (المادة 37).

4. السنهوري، عبد الرزاق (2010)، الوسيط في شرح القانون المدني، الجزء الثاني، نظرية الالتزام بوجه عام، الاثبات، آثار الالتزام، تحديث وتنقيح/ أحمد المراغي، دار الشروق، القاهرة ، ص26 وما بعدها.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

ومن الجدير بالذكر أن التعاون القانوني والقضائي فيما بين الدول من الضرورات اللازمة لمواجهة الجرائم الالكترونية باعتبارها جريمة عابرة للحدود، واتساقاً مع النصوص والجهود الدولية فقد نصت المادة (38) من القرار بقانون على " تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تم وفقاً للإجراءات القانونية والقضائية للتعاون الدولي"

المطلب الثاني/ تحديات ومشكلات مكافحة الجريمة السيبرانية.

تتسم جرائم الحاسوب بصعوبة اكتشافها وإثباتها، فالجريمة المعلوماتية تتم في بيئة أو إطار لا علاقة له بالأوراق أو المستندات، بل تتم بواسطة الحاسب الآلي، أو الشبكة العنكبوتية، ويمكن للجاني عن طريق نبضات الكترونية غير مرئية العبث في بيانات الحاسب الآلي أو برامجه في وقت قياسي قد يكون جزء من الثانية، وهذه البيانات أو المعلومات يمكن محوها أيضاً في زمن قياسي قبل أن تصل يد العدالة إليها، سيما وأن عملية الضبط لا تتم سوى بمعرفة خبير فني أو متخصص (حجازي، ب. ت. ص 24).

ومن المعوقات المتعلقة بإثبات الجرائم المعلوماتية ما يلي (منصور، 2011، ص ص 191-194):

1. انعدام الدليل المادي حيث إن الأدلة الرقمية ما هي إلا بيانات غير مرئية، ومسجلة الكترونياً ومرمزة، ولا تترك أي أثر عند التعديل أو التلاعب فيها، مما يحول دون كشف شخصية الجاني.
2. سهولة محو الدليل، أو تدميره في فترة زمنية يسيرة.
3. صعوبة الوصول إلى الدليل حيث إن استخدام تقنيات التشفير يعد أحد العقبات الكبرى التي تعيق التحري والتحقيق والملاحقة للبيانات الرقمية.
4. مكان ارتكاب الجريمة حيث أن ارتكاب جريمة الحاسب الآلي عادة ما تتم عن بعد، مما يضاعف من صعوبة كشفها، أو ملاحقتها.

أما المعوقات المتعلقة بالجهات المتضررة فمنها ما يلي (ابراهيم، 2010، ص 67 – 69):

1. عدم إدراك خطورة الجرائم السيبرانية من قبل المسئولين بالمؤسسات.
2. إغفال جانب التوعية لإرشاد المستخدمين إلى خطورة الجرائم المعلوماتية.
3. منافسة شركات البرمجة نحو تبسيط الإجراءات، وتسهيل استخدام البرامج والأجهزة وملحقاتها، وذلك على حساب الجانب الأمني.
4. الإحجام عن الإبلاغ عن الجرائم التقنية بسبب عدم رغبة الجهات المتضررة في

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الظهور بمظهر مشين أمام الآخرين، أو خوفاً من الحرمان من خدمات معينة تتعلق بالنظام المعلوماتي.

وهناك معوقات تتعلق بجهات التحقيق تعود إلى شخصية المحقق، وعدم متابعة المستجدات في مجال الجرائم المعلوماتية، ونقص المهارة الفنية المطلوبة (الغافري، ب. ت. ص 409).

كما أن هناك مشكلات وتحديات تتعلق بإجراءات الحصول على الدليل الالكتروني، منها تعذر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلاً بحاسبات أخرى، وتصادم التفتيش عن الأدلة مع الحق في الخصوصية المعلوماتية، وقد يتجاوز النظام المعلوماتي المشتبه به إلى أنظمة أخرى مرتبطة (ابراهيم، 2010، ص ص 75 – 77).

المطلب الثالث/ دور القاضي الجنائي في ظل غياب النص العقابي للجريمة السيبرانية.

من المعلوم أن النيابة العامة تتولى أعمال التحقيق الخاصة بالجرائم، وعند الوصول إلى الأدلة الكافية لإدانة المتهم يتم إصدار قرار ولائحة اتهام لإجراء محاكمة المتهم أصولاً، وهو ما يعرف بمرحلة التحقيق النهائي، حيث يقدم وكيل النيابة الأدلة التي جمعها، ويعرضها على محكمة الموضوع لتصل بدورها إلى إدانة المتهم، أو إعلان براءته، أما في الجرائم السيبرانية؛ فإن القاضي يواجه صعوبة في فهم التقنية الخاصة المستخدمة لارتكاب تلك الجرائم، وبخاصة عند غياب النص العقابي، وكذلك في اكتشاف واستخلاص النية الإجرامية.

إن الأخذ بالدليل الرقمي يعود إلى قناعة القاضي الوجدانية بهذا الدليل، وله في ذلك التأكد من سلامته، وصحة وسلامة إجراءات الحصول عليه، فإن طرحه القاضي من عداد البينة واستبعده، عليه أن يسبب قراره، ويؤيده بأسباب عدم الأخذ به بما جاء لديه في أوراق الدعوى (أبو حجيلة المشار إليه في حمو وعلاء عبد الله، 2015، ص54).

ويمكن الإشارة إلى أنه إذا ما تم الحصول على الدليل الرقمي بطريقة مشروعة، ومن قبل أشخاص مختصين فنياً وعلمياً، فإنه يتمتع من حيث قوته الإثباتية بقيمة قد تصل إلى درجة اليقين، شأنه في ذلك شأن البصمات، والأدلة البيولوجية، ويكون بينة قانونية مقبولة، وعلى الرغم من ذلك فإن مجرد تقديم الدليل الإلكتروني يعطي للمحكمة الصلاحية المطلقة في تقدير هذا الدليل، ويدخل ذلك ضمن الصلاحية التقديرية للقاضي، وفي جميع الأحوال إن من حق قاضي الموضوع – إن لم يتمكن من البث في أمر الدليل الرقمي – أن ينتدب خبيراً آخراً لتقديم رأيه في الدليل المطروح، وتكون مهمة الخبير في هذه الحالة مساعدة

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وتقديم المشورة للمحكمة من الناحية الفنية فقط، والتي لا دراية أو اختصاص للقاضي أو المحكمة بها، وفي النتيجة فإن خلاصة عمل الخبير التي ترد في تقريره تخضع لتقدير القاضي وقناعته (مرجع سابق، ص 54).

الخاتمة

تطرقت الدراسة إلى الأدلة الرقمية ودورها في الإثبات الجنائي، حيث قدم الباحثان عرضاً مركزاً تناولا فيه مفهوم الأدلة الجنائية الرقمية، ومفهوم الجريمة السيبرانية، أو الجريمة الالكترونية، ومن خلال ما تقدم عرضه تبين لنا أن الدليل الجنائي الرقمي يتميز بأنه دليل علمي ذو طبيعة تقنية يتم الحصول عليه بطرق وأساليب غير تقليدية، وبالتالي وجب التعامل معه من خلال استحداث قواعد إجرائية تتماشى مع خصوصية الجريمة السيبرانية، في ظل عجز القواعد الإجرائية التقليدية في التعامل معها، وعلى العموم يمكن القول بأنه مهما كانت قيمة الدليل الجنائي الرقمي العلمية والفنية في الإثبات إلا أن سلطة القاضي التقديرية لازمة حتى تجعل الحقيقة العلمية حقيقة قضائية.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

نتائج وتوصيات:

من خلال دراسة الأدلة الرقمية ومدى حجيتها في التشريعات الدولية والعربية من الناحيتين القانونية والفنية، فقد تبين لنا أن حجية الأدلة الجنائية في مجال الإثبات الجنائي مقيدة بمجموعة من الشروط المتعلقة بإجراءات التحقيق المخصصة لاستخلاص الأدلة الرقمية بحيث يفرض على سلطات التحقيق الحصول عليها بطرق مشروعة، وأن القاضي الجنائي يتمتع بالدور الإيجابي في تقدير القيمة القانونية للأدلة الرقمية مثلها مثل باقي الأدلة، وأن هناك ثغرات وفراغ تشريعي يعتري الدليل الرقمي، وكذلك نقص وضعف في التعامل مع الواقع التقني الذي فرض نفسه في كافة مناحي الحياة، بما فيها الحياة القانونية والقضائية، بالإضافة إلى عدم وجود اتفاق في تعريف المصطلحات المتعلقة بالجريمة المعلوماتية، وبناءً على ما سبق فإننا نوصي بالآتي:

1. نشر التوعية الالكترونية بين العاملين في السلك القانوني.
2. تدريب الكوادر الفنية على تقنيات البحث الجنائي الرقمي.
3. سن قوانين موضوعية وإجرائية ومحايدة للتصدي للأشكال الجديدة والمستحدثة من الجريمة السيبرانية.
4. تنظيم وتعزيز القوانين التي تنظم العملية الالكترونية.
5. تشجيع التعاون والتنسيق بين أجهزة إنفاذ القانون والسلطات القضائية.
6. تعزيز عمل القضاء في إصدار أحكام تستند إلى الدليل الالكتروني.
7. وضع معايير قياسية عند إنشاء المواقع الالكترونية، تتضمن أنظمة أمان وحماية ضد الجرائم السيبرانية.
8. رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي الجرائم السيبرانية.

وفي الختام فإننا ندعو أساتذة العلوم الإنسانية والاجتماعية وفقهاء القانون، وعلماء التقنية المعلوماتية، إلى إعداد الأبحاث والدراسات ذات العلاقة، والتي تمكن القضاء من مواجهة التحدي القائم والمتطور من قبل الجريمة السيبرانية.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

المراجع العربية:

- إبراهيم، خالد ممدوح،(2010)، فن التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الفكر الجامعي، الاسكندرية.
- ابراهيم، راشد بشير،(2008)، التحقيق الجنائي في جرائم تقنية المعلومات دراسة تطبيقية على إمارة أبو ظبي، ط1 ، مركز الإمارات للدراسات والبحوث الاستراتيجية،.
- البشرى محمد الأمين،(ب.ت)، الأدلة الجنائية الرقمية: مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17 ، العدد 33.
- بن يونس، عمر محمد،(2006)، ندوة الدليل الرقمي، جامعة الدول العربية، المنظمة العربية للتنمية الإدارية.
- بوالطمين، إلهام،(2018)، الإثبات الجنائي في مجال الجرائم الإلكترونية، رسالة ماجستير في الحقوق، جامعة العربي بن مهيدي، أم البواقي، الجزائر.
- حجازي عبد الفتاح بيومي،(ب.ت)، القانون الجنائي والتزوير في جرائم الحاسوب والانترنت، دار الكتب القانونية، المحلة الكبرى، مصر.
- حمو، أحمد وعواد، علاء وعبد الله، ولاء،(2015)، الأدلة الالكترونية الجوانب القانونية والتقنية، معهد الحقوق جامعة بيرزيت وهيئة مكافحة الفساد، فلسطين.
- سده، إياد عطا،(2009)، مدى حجية المحررات الالكترونية في الإثبات دراسة مقارنة، رسالة ماجستير، جامعة النجاح، فلسطين.
- السنهوري، عبد الرزاق (2010)، الوسيط في شرح القانون المدني، الجزء الثاني، نظرية الالتزام بوجه عام، الاثبات، آثار الالتزام، تحديث وتنقيح/ أحمد المراغي، دار الشروق، القاهرة.
- الطوالبة، علي حسن،(2004)، التفتيش الجنائي على نظم الحاسوب والانترنت (دراسة مقارنة)، ط1 ، عالم الكتب الحديث، الأردن.
- عبد الحميد، ممدوح،(2000)، البحث والتحقيق الجنائي الرقمي في جرائم الحاسوب والإنترنت، القاهرة، دار الكتب القانونية.
- عبد المطلب، طاهري،(2015)، الإثبات الجنائي بالأدلة الرقمية، رسالة ماجستير، كلية الحقوق، جامعة المسيلة، الجزائر.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

- العدوان، ممدوح حسن والسلامات، نادر عبد الحليم،(2018)، مشروعية وحجية الدليل المستخلص من التفتيش الالكتروني في التشريع الجزائي الأردني، دراسات علوم الشريعة والقانون، المجلد 45 ، عدد 4 ، ملحق 2.
- الغافري، حسين بن سعيد،(ب.ت)، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، جامعة عين شمس.
- فرغلي، عبد الناصر محمد والمسماري، محمد عبيد ،(2007)، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض.
- قنديل، أشرف عبد القادر،(2015)، الاثبات الجنائي في الجريمة الالكترونية، دار الجامعة العربية، مصر.
- مبروك، نصر الدين،(2003)، محاضرات في الإثبات الجنائي، دار هومة للطباعة والنشر والتوزيع، الجزائر.
- مركز هردو لدعم التعبير الرقمي،(2018)، التنظيم القانوني والجرائم الالكترونية ما بين أمن المعلومات وتقييد الحريات، القاهرة.
- منصور، الشحات إبراهيم،(2011)، الجرائم الالكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن، ط1، دار الفكر الجامعي، الاسكندرية.
- المومني، نهلا عبد القادر،(2000)، الجرائم المعلوماتية، ط1، دار الثقافة والنشر والتوزيع، عمان.
- هروال، نبيلة هبة،(2007)، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، ط1، دار الفكر الجامعي، مصر.
- هلالي، أحمد عبد اللاه،(2004)، حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)، مؤتمر القانون والكمبيوتر والانترنت – المجلد الثاني – ط3 – جامعة الإمارات العربية المتحدة.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-005 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

المراجع الأجنبية:

- Amadt, B. L. and Plaza, E. Case, (1994), Based Reasoning: Foundational Issues, Methodological Variations, and system Approaches , Alcom, Artificial intelligence Communications ,7(1).
- Association of Chief Police Officers (of England, Wales, Northern Ireland) (2011) , Good Practice for Computer Based Electronic Evedence, Version 5.
- Eoghan Casey(2000), Digital Evidence and Computer Crime , London: Academic Press.

https://journal.pass.ps « DOI: 10.36554/1796-006-001-006 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854