

مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

الدليل الرقمي وأثره على الدعوى الجنائية

The Digital Evidence and its Impact on the Criminal Case

يس حسن محمد عثمان^{*1}

¹ الأستاذ المساعد - جامعة نيلالا - كلية القانون والشرعية - قسم القانون العام

E-mail: yasseinhassan@yahoo.com

تاريخ النشر: 2020/09/01

تاريخ القبول: 2020/08/11

تاريخ ارسال المقال: 2020/07/27

^{*} المؤلف المرسل

المستخلص

الهدف من هذه الدراسة هو معرفة مفهوم الدليل الرقمي ومدى تأثيره على الدعوى الجنائية بنفيها أو إثباتها، وهذا الدليل الرقمي يتمثل في مجموعة من البيانات الرقمية والأجهزة الإلكترونية التي إستخدامها المكرز عند إرتكابه للجريمة. كذلك من ضمن أهداف هذه الدراسة معرفة التحديات التي تواجه كيفية الحصول على الدليل الرقمي وإستخلاصه وتحليله. لذلك تعتبر طبيعة الدليل الرقمي ووزنه وحجته وكيفية إستخدامه في إثبات أو نفي الدعوى الجنائية كلها من تحديات هذه الدراسة. إستخدم الباحث قواعد المنهج الوصفي والتحليلي للوصول إلى أهداف الدراسة والآثار القانونية التي ينتجها الدليل الرقمي في الدعوى الجنائية هذا بالإضافة إلى التعرف على مصادر الدليل الرقمي والطرق الفنية المتبعة في إستخلاصه وتقديمه كوسيلة إثبات جنائي. في هذه الدراسة توصل الباحث إلى عدة نتائج بجانب بعض المقترحات التي نراها تساعد في تعضيد بينة الدليل الرقمي بإعتباره بيئة قاطعة غير قابلة لإثبات العكس في إثبات الجريمة وتحقيق العدالة الجنائية، بالإضافة إلى بعض الإشكالات التي تواجه إستخلاص الدليل الرقمي وصعوبة معرفته بالطرق العادية التي يعرف بها أدلة الإثبات العادية. علاوة على ذلك الدراسة تناولت الجانب العملي الخاص بعملية إستخلاص الدليل الرقمي بواسطة خبراء مختصين في مجال الأدلة الإلكترونية والإجراءات القانونية المتعلقة بها منذ بدء التحريات وأثناء سير الدعوى الجنائية وحتى مرحلة إصدار الحكم.

كلمات مفتاحية: الدليل الرقمي، إلكتروني، خصائص، حجية، أثر، مصادر الدليل الرقمي.

Abstract

This study aims to know the concept of the digital evidence and its impact on the criminal case by proving or exiling. This digital evidence centralizes in the following group: Digital data and electronic hardware that which was use by the criminal (hackers) when he commits the crime. to find out ways of the obtainment of the digital evidence, and the challenges facing how to obtain and analyze the digital evidence. Therefore, the natsure of the digital evidence and its value, dependability and how it can be used to prove or deny a ciriminal case. A descriptive analytical method has been used to conduct the study and the legal impacts produced by the digital evidence in the criminal case, in addition to identifying the sources of digital evidence and the technical methods used in it, extracting, analizing and presenting it as a criminal proof device. The study conculed with some findings several proposals and propositions we see that it will promte the digital evidence us conclusive evidence that is not capable of proving the opposite in proving a crime and achieving criminal justness, beside that the study also conculed some of the difficulty and the challenges of the criminal procedures that wich knowing it through the ordinary ways of proving. Moreover the study also contains the technical proceedings during the criminal case in a manner that is appropriate for it from the beginning of the investigation till judement time.

Key words: Digital Evidence, Electronic, Characteristics, Authentic, Impact, Sources.

مقدمة

التطور المضطرد الذي يصاحب أسلوب وأنواع الجرائم الإلكترونية أدى إلى إجبار القانونيين والأجهزة الأمنية والشرطية والإدارات المختصة بأمن المعلومات في القطاعات الحكومية والخاصة إلى الإهتمام وتتبع هذه القضايا والتحري فيها بشكل خاص بغرض الوصول إلى الدليل الرقمي القاطع الذي يمكن إستخدامه أثناء إجراءات الدعوى الجنائية لإثبات الجريمة، كما أن إعتداد الدليل الرقمي كوسيلة إثبات لبعض أنواع الجرائم تؤثر إيجاباً أو سلباً في الدعوى الجنائية إما بالإثبات أو النفي. وعلى الرغم من ذلك نجد أن مفهوم الدليل الرقمي وإستخدامه كدليل إثبات ووزنه القانوني أحدث جدلاً قانونياً في بعض الأنظمة التشريعية خاصة في تشريعات الدول التي تطبق نظام الإثبات المقيّد.

مصطلح الدليل بصورة عامة لا يخرج من أنه البيّنة التي تسند بها الوقائع على مرتكب الجريمة هذا وفق التعريف التقليدي للدليل، أما مفهوم الدليل الرقمي وتعريفاته وأنواعه ونطاقه وإستخدامه وموضوعاته يختلف عن المفهوم العام التقليدي للدليل العادي. هذا الاختلاف لا يشكل فرقاً جوهرياً في أنظمة الإثبات المتبعة والمتفق عليها لأن الدليل الرقمي هو واحد من أنواع أدلة الإثبات المتطورة التي تنتمي إلى أدلة الإثبات المألوفة.

مشكلة الدراسة: المشكلة الأساسية للدراسة تكمن في ماهية الدليل الإلكتروني وكيفية إستخلاصه ومدى وزنه وهل يصلح الدليل الرقمي لإثبات كافة أنواع الجرائم؟

أهداف الدراسة: تهدف الدراسة إلى معرفة مفهوم الدليل الرقمي كوسيلة إثبات حديثة، وكذلك معرفة مصادره وحجته في إثبات الجريمة والآثار القانونية التي ينتجها الدليل الرقمي في الدعوى الجنائية.

منهج البحث: إعتد الباحث على المنهج الوصفي التحليلي لدراسة مفهوم الدليل الرقمي وأثره على الدعوى الجنائية، هذا فضلاً عن المنهج التطبيقي وذلك للإستعراض الموجز لبعض التشريعات مثل السودان، أمريكا و مصر كنماذج لموضوع الدراسة ولتأكيد فرضية تأثير الدليل الرقمي على الدعوى الجنائية.

هيكل الدراسة: يتكون هيكل الدراسة من ثلاثة مباحث وذلك على النحو الآتي:

المبحث الأول: مفهوم الدليل الرقمي وأنواعه وخصائصه

المطلب الأول: تعريف الدليل الرقمي (Digital Evidence):

المطلب الثاني: أنواع الدليل الرقمي

المطلب الثالث: خصائص الدليل الرقمي

المبحث الثاني: حجية الدليل الرقمي وأثره على الدعوى الجنائية

المطلب الأول: حجية الدليل الرقمي في التشريع السوداني

المطلب الثاني: حجية الدليل الرقمي في التشريع الأمريكي

المطلب الثالث: حجية الدليل الرقمي في التشريع المصري

المطلب الرابع: حجية الدليل الرقمي في التشريع التركي

المبحث الثالث: مصادر وطرق الحصول على الدليل الرقمي

المطلب الأول: مصادر الحصول على الدليل الرقمي

المطلب الثاني: الأجهزة الواجب فحصها للحصول على الدليل الرقمي

المبحث الأول: مفهوم الدليل الرقمي

يعتبر الدليل الرقمي كوسيلة من وسائل الإثبات غير العادية، ويرجع ذلك لسبب الطبيعة الفنية والتقنية للجرائم المعلوماتية عند ارتكابها خاصة الجرائم السرية، كما أن محاولة الجاني لطمس الدليل المادي للجريمة يزيد من صعوبة إثبات الجريمة وهذا ما يؤدي إلى إستخدام نوع جديد من البيّنات لمجابهة الفعل الإجرامي عُرفت بإسم الدليل الرقمي أو الدليل الإلكتروني. حيث أصبحت المحاكم تأخذ بهذا الدليل ليس فقط في القضايا ذات الطبيعة الإلكترونية بل حتى في القضايا العادية وبعض الجرائم التقليدية خاصة في حالات المسح والحوسبة الإلكترونية وتحديد وفحص مسرح الجريمة.

نجد بعض النظم القانونية المقارنة والدولية الحديثة تعتمد بصورة كبيرة في إثبات الجريمة على الأدلة الرقمية (الإلكترونية) خاصة السرقات أو السطو على المصارف أو جرائم الإرهاب وغسل الأموال حيث تعتمد المحكمة على الدليل المستخلص من عملية تسجيل الأحداث عبر الكاميرات الإلكترونية الحائطية أو التي توضع على سقف الأمكنة. ومن هنا جاء الحاجة إلى إستخدام دليل يثبت تلك الجرائم ويحد من الخطورة والقرصنة الإجرامية فظهر الدليل الرقمي مع تطور الجريمة الإلكترونية¹.

المطلب الأول: تعريف الدليل الرقمي (Electronic Evidence):

يُعرّف الدليل الرقمي بأنه: البيّنات أو الدليل الذي يجد له أساساً في العالم الافتراضي ويتم عبره معرفة الجريمة أولاً ومن ثم التوصل إلى الجاني. أيضاً هنالك تعريف آخر يشير إلى أن الدليل الرقمي هو مجموعة من الوقائع المثبتة أو المسندة كدليل إلكتروني "الأرقام أو الرموز أو الأقراص الإلكترونية" والذي يؤدي إلى اقناع قاضي الموضوع بشبوت ارتكاب شخص ما لجريمة ما عبر الإنترنت أو عبر إستخدامه للحاسوب أو أي جهاز إلكتروني آخر². كذلك من ضمن تعريفات الدليل الرقمي (الدليل الإلكتروني) وهو تعريف في غاية البساطة حيث عرف البعض الدليل الرقمي بأنه: هو الدليل المأخوذ من أجهزة الكمبيوتر المستخدمة في ارتكاب الجريمة³.

يُستخلص من التعريفات السابقة أن الدليل الرقمي هو عبارة عن معلومات أو بيانات، أرقام أو رموز إلكترونية سواء كانت من صنع الإنسان أو تم إستخلاصها من الحاسوب وبشكل يمكن قراءته أو تفسيره من أشخاص لديهم مهارات عالية عادة في تشكيل المعلومات بمساعدة من برامج الكمبيوتر. هنا يميل الباحث إلى التعريف الثاني ويضيف على ذلك: أن كل ما هو مستخرج أو متحصل عليه كوسيلة أو أداة إثبات من الأجهزة الإلكترونية كالحاسوب والهاتف الجوال أو مافي حكمهما من الأجهزة الإلكترونية يعتبر دليل إلكتروني⁴. كذلك

للدليل الإلكتروني عدة أنواع كلها تعتبر أدلة إثبات إلكتروني مهما كانت مصدرها ومتى ما تم استخدام أيٍّ منها فإنها تؤثر على الدعوى الجنائية.

المطلب الثاني: أنواع الدليل الرقمي:

عادة يقسم الدليل الرقمي إلى ثلاث مجموعات وهي على النحو التالي:

أولاً: السجلات المحفوظة في الكمبيوتر: وهي الوثائق المحفوظة أو المخزنة في الكمبيوتر مثل البريد الإلكتروني وملفات برامج معالجة الكلمات وغيرها.

ثانياً: السجلات التي تم إنشاؤها بواسطة الكمبيوتر مثل سجلات الهاتف وفواتير أجهزة السحب الآلي (ATM) والكارت الإلكتروني الذكي⁵.

ثالثاً: السجلات التي تمت حفظها عن طريق إدخالها أو جزء منها تم إنشاؤها بواسطة الكمبيوتر أو عليها: مثل أوراق العمل المالية التي تحتوي على مدخلات تمت معالجتها إلى برامج أو أوراق رسمية للتعامل باستخدام بعض برامج الحاسب الآلي مثل (excel) ومن ثم تمت معالجتها من خلال البرامج بإجراء العمليات الحسابية عليها.

هذه التقسيمات السابقة ما هي إلى تفسيراً لمصادر الدليل الرقمي وكيفية إستنتاجه وقد يكون هناك أنواع أخرى للدليل الإلكتروني لأن المعلوم أن الجريمة الإلكترونية هي جريمة متطورة بتطور علم التقنية والحاسوب وبالتالي تضطرد معها تطور الجريمة وهذا ما يلزم معه تطور الدليل الرقمي لمجاراة هذا التقدم وإلا فشلنا في إثبات الجريمة المعلوماتية. أما وفقاً لوزارة العدل الأمريكية قسمت الدليل الرقمي إلى ثلاثة مجموعات وهي:

1. السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الإنترنت.

2. السجلات التي تم إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الآلي ATM.

3. السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب، ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيها إلى برامج أوراق العمل مثل Excel ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها⁶.

عليه نستطيع أن نقول أن أي معلومات سواء كانت من صنع الإنسان أو تم إستخلاصها وتسجيلها عبر الحاسوب وما في حكمه وبشكل يمكن قراءته أو تفسيره من أشخاص لديهم مهارات في إعادة تشكيل المعلومات بمساعدة من الكمبيوتر يعتبر دليلاً إلكترونياً يمكن إستخدامه في مرحلة التحريات والمحكمة ويخضع للوزن بواسطة قاضي الموضوع.

الدليل الرقمي وفق أقسامه يمكن إستخدام أي منه في إثبات أي جريمة، بمعنى آخر أن إستخدام الدليل الرقمي لا ينحصر فقط في الجرائم المعلوماتية بل يمكن إستخدام تلك الرموز والأرقام التي تعتبر بينات كوسيلة

إثبات ليس فقط في المجال الجنائي بل حتى في المسائل المدنية له دور كبير في تقرير حقوق الخصوم والفصل العادل في الدعاوى المدنية خاصة في نزاعات العقود الإلكترونية، وبالتالي الدليل الرقمي بكافة أنواعه يساعد كثيراً في تحقيق العدالة.

المطلب الثالث: خصائص الدليل الرقمي:

على قرار خصائص ومميزات الجريمة المعلوماتية والجرم المعلوماتي أيضاً يتميز الدليل الرقمي بعدة خصائص ينفرد بها عن الدليل التقليدي وهي:

أولاً: الدليل الرقمي دليل علمي:

يقصد بذلك أن الدليل الرقمي هو عبارة عن بيئة تقنية علمية لتنشأ فيها المعلومات "طبيعة تقنية علمية بحتة"، لذلك فإن ما ينطبق على الدليل العلمي من حيث الصفة التقنية ينطبق على الدليل الرقمي. إلى جانب ذلك الدليل العلمي يخضع لقاعدة لزوم تتجاوب معه الحقيقة كاملةً وفقاً للقاعدة القانونية المستمدة من الفقه القضائي المقارن (أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة)، فإذا كان الدليل العلمي له منطقته الذي يجب ألا يخرج منه وهو عدم تعارضه مع القاعدة العلمية السليمة، فإن الدليل الرقمي أيضاً كذلك له ذات الطبيعة⁷.

ثانياً: الدليل الرقمي ذات طبيعة تقنية:

الدليل الرقمي ليس كالدليل المادي المرئي الذي يمكن إستخلاصه بمجرد الإطلاع أو النظر إليه كما هو الحال في الأدلة المادية بل هو دليل لا يفصح عن مجرم معين عادة بقدر ما يشير ويثبت وجود جريمة بصورة قاطعة، هذه الصفة تكمن في جرائم الإنترنت مثل الجرائم التي ترتكب على البريد الإلكتروني حيث يصعب على جهات التحري تحديد مصدر المرسل ومكان الجاني. عليه نستطيع القول بأن لا وجود لدليل رقمي خارج البيئة التقنية أو مصادر البيانات الرقمية⁸.

ثالثاً: الدليل الرقمي متنوع ومتطور:

التطور المضطرد الذي يشهده عالمنا اليوم في مجال التكنولوجيا يتحتم معه تطور الدليل الرقمي من حيث التعدد والتنوع. لذلك في المقابل تحتاج البرامج الإلكترونية أيضاً لحماية تقنية قبل الحماية القانونية، وهذا ما تقوم بها كبرى المواقع الإلكترونية العالمية بإحاطة البيانات المخزنة على صفحاتها بسياسات من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها⁹. على الرغم من ذلك فإن الجريمة الإلكترونية متطورة ومنشرة بصورة مخيفة وكبيرة جداً مضاهية بتطور الجريمة التقليدية. من جانب آخر يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يساعد في إثبات الجريمة أو القبض عليه وتجرمه، لأنه يقوم بتشفير الموقع بعد ارتكابه جرمه¹⁰.

رابعاً: صعوبة التخلص من الدليل الرقمي:

تُعتبر صعوبة التخلص من الدليل الرقمي أحد أهم خصائص الدليل الرقمي على الإطلاق بل إنه يمكن اعتبارها ميزة يتمتع بها الدليل الرقمي عن غيرها من الأدلة الجنائية الأخرى، لأن الدليل الرقمي في كثير من الحالات لا يمكن إتلافه أو تدميره أو التخلص منه بأي طريقة خاصة الرموز والأحرف والأرقام. الأدلة التقليدية التي يعرفها القانون تجد قوتها أمام القضاء في مسألة التشريع في كيفية الحصول عليها ومدى مشروعيتها، فبصمات الأصابع (finger print) مثلاً يمكن أن تكون محل إشكال خاصة إذا طالت المدة بين وقت ارتكاب الجريمة وبين الحصول عليها، وكذلك الشهادة إذا مضى عليها مدة من الزمن فإن مسألة الاستعانة بها تخضع لتحقيق متواصل بحيث يجب التعرف على مدى قدرة الشاهد على التذكر والعوامل المؤثرة في الذاكرة وما إذا كان يتمتع بمستوى ذاكرة مقبولة وفق نظرية ذاكرة الرجل العادي التي يعرفها القانون¹¹، أيضاً سهولة التخلص من بصمات الأصابع بمسحها من موضعها أو لمجرد تعرضها للأتربة والظروف البيئية القاسية. أما بالنسبة للشهود نجد في بعض الدول يتم التخلص منهم بقتلهم أو تهديدهم أو إقصائهم لكي لا يدلوا بالشهادة¹². لذلك أصبح مسألة حماية الشهود (protection witnesses) من القضايا ذات الإهتمام الكبير الذي يتولاه المدعى العام منذ مرحلة جمع الأدلة وحتى ما بعد إنقضاء العقوبة. يمكن التخلص من الأوراق والأشرطة أو الأقراص المسجلة إذا حملت في ذاتها إقرارات بإرتكاب شخص ما جريمة وذلك بتمزيقها وحرقها بإعتبارها أدلة تقليدية، هذا بعكس الدليل الرقمي الذي يكون التخلص من في غاية الصعوبة لأنه عبارة عن بيانات وأرقام ورموز مسجلة ومخزنة على الوسائط الإلكترونية.

المبحث الثاني: حجية الدليل الرقمي وأثره على الدعوى الجنائية

يثير حكم مخرجات الحاسب الآلي في مجال الإثبات مسألتين هامتين هما، مدى إستيفاء هذه المخرجات لمطلوبات الدليل العادي ومدى حجيتها في مجال الإثبات الجنائي لأن الهدف من جمع البينات هو إفراز دليل صحيح يستند عليه القاضي في إصدار أحكامه. لذلك نتناول حجية الدليل الرقمي في التشريع السوداني ومن ثم نتطرق إلى مدى حجية الدليل الرقمي في التشريع الأمريكي كنموذج مثالي للنظام الأنجلوسكسوني. كما نتناول تلك الحجية في التشريع المصري كمثال لحجية الدليل الرقمي في بعض الأنظمة القانونية اللاتينية المخالطة.

الجدير بالذكر أن أثر الدليل الرقمي على الدعوى الجنائية مرتبطة بمدى مقبولية الدليل الرقمي وقوة حجيته في التشريع المعني، لذلك نستطيع أن نقول أن للدليل الإلكتروني أثر كبير في إثبات الدعوى الجنائية أو نفيها خاصة إذا كان الدليل صحيحاً أو سليماً. لكن التشريعات الوطنية مختلفة في تحديد نظم الإثبات المتعارف عليها دولياً (نظام الإثبات المقيّد والنظام الحر والنظام المختلط)، ولما كان لكل دولة الحق في إتباع نظام معين لم يكن هنالك ما يعرف بالدليل الرقمي بل هناك تحوط في النظام الحر بإعتماد كل أنواع أدلة الإثبات الموجودة والمستحدثة لذلك يعتبر الدليل الرقمي دليلاً مستحدثاً. وللقول بتأثير الدليل الرقمي على الدعوى الجنائية هذا الأثر متوقف على مدى مقبولية ووزن الدليل الرقمي نفسه في كل تشريع، ويكون ذلك التأثير جلياً في مرحلة سير النطق بالحكم خاصة عند إعتماد قاضي الموضوع على البيئة الإلكترونية أو إستبعادها، بالتأكيد إما أن يثبت الحق لصاحبه إن

وجد أو ينفيه إذا لم يوجد وبالتالي هنا يظهر أثر الدليل الرقمي على الدعوى الجنائية وتكون بيّنة قاطعة. أما بالنسبة للتشريعات الوطنية التي لم تأخذ بنظام الدليل الرقمي فلا أثر للدليل الإلكتروني على الدعوى الجنائية على الرغم من قوة حجيتها¹³، لذلك سوف نستعرض في المطالب القادمة حجية الدليل الرقمي في بعض ن التشريعات الوطنية كنماذج وأمثلة لأثر الدليل الرقمي على الدعوى الجنائية¹⁴.

المطلب الأول: حجية الدليل الرقمي في التشريع السوداني:

لم ينص قانون الإثبات السوداني صراحةً على الدليل الرقمي وحجيته كدليل إثبات وذلك لعدة أسباب أهمها التشريع الإلكتروني تشريع حديث في السودان حيث أصدر المشرع السوداني قانون جرائم المعلوماتية في العام 2007م، كما أن أنظمة الإثبات المتبعة في النظام القانوني السوداني بالنسبة للجريمة المعلوماتية لم تشهد التحديث على الرغم من تعديل قانون جرائم المعلوماتية في العام 2018م. قانون الإثبات السوداني نص على إتباع نظام الإثبات المقيّد في بعض الجرائم "جرائم الحدود" وكذلك إمكانية الأخذ بنظام الإثبات الحرّ في بعض الجرائم أو الأخذ بنظام الإثبات المختلط وهنا يدخل لنا الدليل الرقمي كوسيلة إثبات حرّ يمكن للمحكمة تقييمه والإستناد إليه في إصدار الحكم¹⁵.

كذلك التشريع السوداني لم ينص صراحةً على الدليل الرقمي كما لم يرفضه لكن يُستحسن النص صراحةً على الدليل الرقمي في مجال الإثبات الجنائي لمواكبة التطورات التي حدثت في التشريعات الدولية ومجاراةً لتطور الجريمة الإلكترونية أو منع الإشتباه في ضعف وعدم حجية الدليل الرقمي وكذلك الحد من الدفع بالبطلان للدليل الإلكتروني. على الرغم من أن المشرع السوداني لم ينص صراحةً على قواعد وأحكام الدليل الرقمي نستطيع أن نقول يمكن الأخذ بالدليل الرقمي وإستخدامه في كافة مراحل الدعوى الجنائية وذلك لأن القضاء السوداني لم يأخذ بنظام إثبات موحد بل يمكن تطبيق أنظمة الإثبات الثلاثة السابقة "المحدد، الحر والمختلط" في الدعوى الجنائية، وبما أن نظام الإثبات الحرّ يقبل بكل وسيلة صحيحة أو سالمة نجد أن الدليل الرقمي يعتبر واحدة من تلك الوسائل، لكن على ذات النهج يحق للطرف الآخر في الدعوى الجنائية الطعن بعدم حجية الدليل الرقمي، وهذا الأمر يؤثر على سير إجراءات الدعوى الجنائية بالتعطيل أو التأخير لذلك وكما أشرنا سابقاً نؤكد ضرورة النص صراحة في التشريع الوطني على الدليل الرقمي كوسيلة لإثبات الجريمة حتى لا يتم التوسع في طرق دحض (disprove)¹⁶.

المطلب الثاني: حجية الدليل الرقمي في التشريع الأمريكي:

المشرع الأمريكي أفلح في حسم حجية الدليل الرقمي بالنص عليه صراحة في القوانين الخاصة بالولايات المتحدة الأمريكية. يُعتبر النظام الأمريكي في إثبات الجرائم الإلكترونية من أكثر الأنظمة تطوراً في الأخذ بالحجة القاطعة للدليل الإلكتروني، وتتبعه في ذلك بريطانيا وتركيا وفرنسا وبعض الدول المتطورة. نظام الإثبات في التشريع الأمريكي يعتمد على الدليل الرقمي بصورة أساسية في كافة المجالات الجنائية والمدنية وحتى الشرعية كذلك. هذا الإعتماد الكبير والحجية القاطعة للدليل الإلكتروني في النظام القانوني الأمريكي جعل درجة إثبات الجريمة وفق

الدليل الرقمي محل نقد كبير وذلك بأن للدليل الإلكتروني عيوب أيضاً كما له من مزايا. من أكثر عيوب الدليل الرقمي مسألة تصنيع الدليل (الدبلجة أو البينة المختلفة) ومن أمثلته إدخال الدليل أو برمجته في حاسوب الغير لإثبات الجريمة عليه.

نص قانون الحاسب الآلي لسنة 1984م الصادر في ولاية أيوا (iowa) على أن مخرجات الحاسب الآلي تكون مقبولة بوصفها أدلة إثبات بالنسبة لبرامج وبيانات الحاسب الآلي المخزنة بداخله¹⁷.

في المقابل نجد قانون الإثبات الصادر سنة 1983م في ولاية كاليفورنيا نص على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب الآلي تكون مقبولة بوصفها أفضل الأدلة المتاحة في مجال الإثبات.

وعلى ذات النهج أكد القضاء الأمريكي في أحكامه وسوابقه المختلفة: أن الأدلة الإلكترونية المتحصل عليها من أجهزة الحاسب الآلي يجب أن تكون مقبولة كأدلة إثبات، طالما أن الكمبيوتر المستمد منه سليم ووظائفه سليمة. يتضح مما سبق أن المعلومات والبيانات التي يحتويها الحاسب الآلي لها حجيتها في الإثبات الجنائي لتلك الأنظمة حيثما أمكن الحصول عليها بطريقة مشروعة دون إنتهاك حرمة الحياة الخاصة للأفراد.

المطلب الثالث: حجية الدليل الرقمي في التشريع المصري:

المشرع المصري لم ينأى بنفسه بعيداً عن ما صار عليه المشرع السوداني وبالتالي لم يحسم بعد مسألة حجية الدليل الرقمي. حيث إنتهج المشرع المصري أسلوب أو مدرسة الفقه أو التشريعات اللاتينية التي يتزعمها القانون الفرنسي والقوانين الأخرى التي تأثرت به، كالقانون الإيطالي والأسباني فيما يتعلق بقضايا جرائم المعلوماتية، بل ترك المشرع حرية الإثبات لأطراف الخصومة في أن يقدموا ما يرونه مناسباً لإقناع القاضي، وللقاضي أن يقوم بتقييم الدليل المقدم وفق منهج الإثبات الحر ومن ثم إصدار الحكم وفق صحيح القانون.

المطلب الرابع: حجية الدليل الرقمي في التشريع التركي:

يأخذ التشريع التركي بنظام الإثبات الحر، بحيث يستطيع الخصوم في الدعوى إثبات دعوهم بكل وسائل الإثبات والأدلة المقدمة بما في ذلك الدليل الرقمي ويشترط في تلك الأدلة الجنائية أن تقبل بنسبة كبيرة لا تدع معها مجالاً للطعن أو الشك. والجدير بالذكر أن قانون الإثبات التركي يتبع لفروع القانون الخاص لأن التشريع التركي ترك مسألة إتباع نظام أو دليل معين لإثبات الحق للخصوم وليس لنظام الدولة وبالتالي أصبح الأمر مدنياً. هذا النظام يُعتبر إمتداداً للقانون الفرنسي الذي يُعتبر بدوره أم القوانين اللاتينية. لكن من جهة أخرى أيضاً هناك وجه شبه كبير بين التشريع التركي الأمريكي في إثبات الجرائم الإلكترونية لأن القانون التركي أيضاً يعطى الدليل الرقمي الحجة القاطعة متى ثبت للمحكمة صحته وسلامته من أي عيب أو شك بأنه دليل مصطنع. الآن القضاء في تركيا يعتمد على الدليل الرقمي بصورة أساسية في كافة المجالات الجنائية والمدنية الشرعية، لكن مع ذلك يستطيع الخصم في الدعوى إثبات عيب الدليل الرقمي بأنه مصطنع (مدبلج) وهذا يعني أن حجية الدليل الرقمي وقوته في التشريع التركي أمر مفتوح يخضع لوزن المحكمة للبيّنات المقدمة بواسطة الخصوم.

هناك ثمة أسئلة تحتاج إلى إجابة واضحة لإزالة الغموض أو الشكوك حول صحة وقوة وحجية الدليل الرقمي وأثره على الدعوى الجنائية وهي:

1. هل تعتبر الصورة الرقمية دليل إثبات قاطع أم تحتاج إلى تعضيد؟

خصوصية الدليل الرقمي وما يحتاجه من خبرة فنية عالية لجمع وإستخلاص المعلومات الإلكترونية المدخلة أو المثبتة بمسرح الجريمة (الأجهزة والأدوات الإلكترونية المستخدمة) مثل تحليل ال CD أو الفيديو وتأكيد صحتها بعدم إجراء أي تعديلات جوهرية عليها هذا ما يثبت الدعوى الجنائية¹⁸. فالصورة الرقمية إذا كانت ثابتة (Still Image) أو متحركة (Vide Photo) فهي مجرد إظهار للحقائق الظاهرة حول الجريمة إما أن تثبت أو تنفي الجريمة، وقد تكون هذه الصور في شكل ورقي مرئي بإعتباره صور أصلية أو مطبوعة ومقدمة للمحكمة¹⁹.

2. هل يُعتبر شريط الفيديو دليل أساسي؟

بذات الكيفية التي إعتمدت بها إستخلاص الصورة الرقمية للصورة الثابتة وإعتمادها كدليل إثبات أصلي أيضاً شريط الفيديو الأول يعتبر دليل أساسي ويمكن نسخ عدة أشرطة أخرى وتكون لها ذات الحجية والقوة الإثباتية ونفس الأثر على الرغم من أن الأشرطة المنسوخة قد لا تكون بذات الجودة من حيث وضوح الصور بسبب العوامل الطبيعية كالضوضاء المصاحب لعملية النقل وهذا مايجوز الشريط المنسوخ إلى إدخال بعض الإشارات حتى لا يحدث تلف طبيعي ينتج عن التخزين أو مرور بعض الوقت الذي يتعرض له الشريط الأصلي أو المنسوخ ولا تعتبر تلك العملية تصنيع أو إنتاج دليل²⁰.

المبحث الثالث: مصادر وطرق الحصول على الدليل الرقمي:

لمواجهة التحديات التي تواجه الدليل الرقمي ولقبول الوسائط الإلكترونية كدليل إثبات فإن دراسة الجانب القانوني للجريمة والدليل الرقمي يُعتبر من أولويات التشريع ولا ينبغي أن ينفصل القانون عن هذا التطور التكنولوجي والفني²¹. الدليل الرقمي حتي ينتج أثره في الدعوى الجنائية يجب معرفة مصدره وضرورة سلامته من أي عيب (الغش، التقليد أو التزوير فيه) وهذا لا يتأتى إلا بمعرفة مصدره والوثوق فيه. كذلك المحكمة حتى تطمئن على سلامة الإجراءات التي إتخذت في كيفية الحصول على الدليل الرقمي تبحث أولاً في مصدره لبث الثقة في أحكامها لذا مصدر الدليل الرقمي هو أمر في غاية الأهمية لضمان خلو الأحكام من العيوب وتحقيق العدالة²².

للحصول على الدليل الرقمي هنالك طرق تقنية تتبع في فحص الأدوات والآلات الإلكترونية تحتاج إلى كفاءة ودقة عالية جداً لا يستطيع الشخص العادي معرفتها كما أن الشخص التقني الذي يقوم بإستخراج الدليل أو تجميعه يقع عليه عبء تحليل الرموز والبيانات المتحصله عليه من تلك المصادر. كما أن هذه المصادر توضح البرامج المستخدمة في جمع الأدلة والأنظمة الواجب فحصها للحصول على الدليل الرقمي، لذلك سوف نتناول مصادر الحصول على الدليل الرقمي في مطلب أول، ومطلب ثاني نوضح فيه الأجهزة الواجب فحصها بغرض الحصول على الدليل الرقمي.

المطلب الأول: مصادر الحصول على الدليل الرقمي:

الحصول على الدليل الرقمي يكمن في الطريقة التي إرتكبت بها الجريمة وتنحصر تلك الأدلة في المتهم (المشتبه به)، المجني عليه (المضروب)، ومقدم خدمة الإنترنت وهذه المصادر وتوابعها تعتبر مسرح الجريمة الإلكترونية، هذا التطور العلمي والتقني قد يسفر عن أنواع جديدة من الأدلة وهذه المصادر سوف نتناولها على سبيل المثال فقط ليس الحصر وهي تتمثل في:

الكمبيوتر الخاص بالمتهم المشتبه فيه:

فحص جهاز كمبيوتر المتهم المشتبه فيه وخاصة وحدة التخزين الدائمة القرص الصلب (hard disk) والوحدات الفرعية الملحقة وتشتمل على القرص المرن وأقراص الليزر أو أي وحدة تخزين أخرى من الممكن إستعمالها مثل جهاز (flash memory) كل تلك الأجهزة يمكن فحصها وبيان الطريقة التي قام بها المتهم في إرتكاب الجريمة.

الكمبيوتر الخاص بالمجني عليه:

لا شك أن حاسوب المجني عليه هو المصدر الرئيسي الذي يكشف لنا الجريمة وتوضح لنا العمليات التي قام بها المتهم في إرتكاب الجريمة، والمجني عليه قد يكون شخص طبيعي أو مؤسسة خاصة أو عامة أو مؤسسة مالية أو هيئة حكومية أو غيرها وبالتالي فإن فحص تلك الأجهزة الخاصة بهم يقود إلى معرفة المجرم الذي قام بإرتكاب الجريمة وهذا بدوره يؤدي إلى تسهيل عملية القبض عليه.

مقدم خدمة الإنترنت:

يمكن الإستعانة أيضاً في الكشف على الأدلة الإلكترونية بعدة جهات أخرى مثل مقدم خدمة الإنترنت شركة ياهو (yahoo) أو جوجل (google) فإن نظام تلك الشركات يتم فيها تسجيل البيانات الخاصة بعملائها ومن ثم يمكن اللجوء إليهم للتعرف على هوية المجرم المشتبه فيه، وكذا البريد الإلكتروني على شبكة الإنترنت، حيث يمكن التعرف على البيانات الشخصية ومنه يمكن تحديد هوية المشتبه فيه عن طريق صندوق الرسائل الواردة إليه أو المرسلة منه وبالتالي يمكن تحديد مكانه وموقعه وذلك من خلال إرشيف المجموعات البريدية²³.

المطلب الثاني: الأجهزة الواجب فحصها للحصول على الدليل الرقمي:

للحصول على الدليل الرقمي يجب فحص مكونات الحاسوب بالإضافة إلى فحص نظام الإتصال بالإنترنت. فحص مكونات الحاسوب يكون على القطع الصلبة (hard ware) والقطع المرنة أو البرمجيات (software)، وهناك عنصر ثالث يتوزع بين البرمجيات والقطع الصلبة وهو عنصر المعلوماتية²⁴. ولو نظرنا إلى متطلبات المحاكمة العادلة نجد أنها تستلزم أن يكون الفحص مادياً، ومعنوياً للإرتباط القائم في شكل طبيعي بين مكونات أو ملحقات الحاسوب كوحدة متكاملة، وذلك حتى يتوافر للمتهم ضمانات المحاكمة العادلة من عدم تجزئة الدليل. ومن الأجهزة الواجبة فحصها هي:

1) القرص الصلب:

يُعد القرص الصلب المحتوى الذي يضم في داخله مجموعة البيانات الرقمية ذات الطابع الثنائي "تقني، علمي مرئي وغير مرئي"، والتي تتميز بعدم تشابهاها فيما بينها على الرغم من وحدة الرقم الثنائي، بحيث يمكن أن يُجرى فحص كلي أو جزئي للقرص الصلب²⁵.

(2) نظام ذاكرة التخزين:

يُعتبر نظام ذاكرة التخزين من مزايا تشغيل الحاسوب، وكلما كان نظام التشغيل متطوراً كان نظام ذاكرة التخزين أكثر دقةً.

تُعرف ذاكرة التخزين بأنها قدرة الحاسوب على الاحتفاظ في ذاكرته بنسخة كاملة مما إطلع عليه عضو الإنترنت أثناء إبحاره عبر العالم الافتراضي. لذا فإن فحص نظام التخزين في الذاكرة يعد من الإجراءات الهامة عند القيام بفحص نظام الحاسب الآلي لمعرفة ما تم زيارته عبر الإنترنت وتعتبر هذه الذاكرة جزءاً من مسرح الجريمة المعلوماتية.

(3) الطابعة:

يمكن فحص الطابعات خاصة الحديثة منها إذ تتضمن الطابعات الحديثة ميزة تخزين منطقية لمجموع الصفحات التي تم إستخراجها من الحاسوب، حتي في الحالة التي يكون الملف قد تم إلغائه من الأمر المطلوب تنفيذه عبر جهاز الحاسوب.

(4) لوحة المفاتيح:

يمكن أن تكون لوحة المفاتيح keyboard محلاً للفحص بواسطة خبراء تكنولوجيا المعلومات في المعامل الجنائية، حيث تعتبر لوحة المفاتيح الحديثة كثيراً ما يتم إستخدامها كملقم أو خادم وهمي من قبل المكرز، وفي هذه الحالة يكون التعامل معها كأداة أو وسيلة مساعدة في إرتكاب الجريمة، وفي كثير من الأحيان يُخلف الجاني بصمته على اللوحة وبالتالي يمكن إعتبار لوحة المفاتيح دليل يساعد في إبراز حقيقة الواقعة الإجرامية.

الخاتمة

الدليل الرقمي بإعتباره وسيلة إثبات حديثة أثار جدلاً قانونياً واسعاً من حيث المفهوم والتعريف وقوة حجته في الإثبات، إضافة إلى ذلك تباين أنظمة الإثبات المعاصرة خاصة لدى بعض الدول التي تطبق نظام الإثبات المقيّد الذي يترتب عليه أحياناً هدم بعض الحقوق القانونية التي نصت عليها التشريعات الوطنية المنظمة للجريمة المعلوماتية. أيضاً تشريعات جرائم المعلوماتية تعتبر قوانين حديثة لم يمضى على سنّها فترة طويلة في بعض الدول لذلك يشوبها بعض النقص في الإجراءات المتبعة وكيفية جمع الدليل الرقمي المتعلق بالجريمة ولعل ذلك يكون بسبب الحداثة وغياب السوابق القضائية التي تشكل مصدراً مهماً لقواعد قانون الجريمة المعلوماتية. لكن بمرور الزمن وتراكم القضايا الإلكترونية قد يظهر ذلك الدور الذي تلعبه تلك السوابق القضائية في التشريع الجنائي الإلكتروني. نختم دراستنا لموضوع الدليل الرقمي وأثره على الدعوى الجنائية بالنتائج والتوصيات الآتية:

أولاً: النتائج:

1. لم يكن هنالك تعريف موحد للدليل الإلكتروني إلا أن جميع تلك التعريفات تشير إلى مفهوم جامع للدليل الإلكتروني وهو: الدليل التقني المتحصل عليها عن طريق فني معين من البيئة الإلكترونية.
2. للدليل الإلكتروني طبيعة فنية عالية لا يمكن الحصول عليه وتحليله إلا بواسطة خبير تقني.
3. التطور المضطرد للجريمة الإلكترونية وخصائصها وخصائص الهكرز هي من أكبر التحديات التي تواجه الدليل الرقمي، حيث يصعب مجاراتها منذ الوهلة الأولى وعامل الزمن يشكل عبء كبير جداً في الحد من خطورة الجريمة وآثارها وقد يهدر معه الدليل.
4. غياب التقنين الموحد وإغفال بعض التشريعات الوطنية للأحكام المتعلقة بحجية الدليل الرقمي يضعف كثيراً من وزنه في الدعوى الجنائية وقد ينتج عنه إهدار الحقوق.
5. للدليل الإلكتروني حجية قاطعة في التشريعات التي تطبق نظام الإثبات الحر مثل أمريكا كما يصلح هذا الدليل لإثبات جميع الدعاوى، بينما تتضاعف تلك الحجية في تشريعات الدول التي تطبق النظام المختلط كالسودان، قد تكون بيئة تحتاج إلى تعضيد، بينما قد تنعدم تلك الحجية في تشريعات الدول التي تطبق نظام الإثبات المقيّد كالسعودية خاصة في جرائم الحدود.
6. الدليل الرقمي تثبت الجريمة على الجاني ويُعتبر بيّنة قاطعة لكن بذات القدر يجوز الإنتقاص منه ونقضه كما يجوز إستخدامه كبيّنة عكسية لنفي الجريمة، وبالتالي هي بيّنة مستقلة بذاتها.
7. للدليل الإلكتروني خاصية متفردة وهي؛ أنه يحمي نفسه بنفسه حيث يصعب جداً التخلص منه أو التلاعب به من حيث مصدره.

ثانياً: المقترحات:

1. هنالك ضرورة لتقنين مسألة الدليل الرقمي والأحكام المتعلقة بها ومدى قوته الإثباتية وأثره على الدعوى الجنائية على مستوى التشريعات الوطنية.
2. العمل على التدريب المتقدم للتقنيين المختصين في مجال الأدلة الإلكترونية وذلك لمواكبة تطور الجريمة الإلكترونية ووسائل الحد منها وتطوير الدليل الرقمي.
3. إعتتماد الدليل الرقمي السليم المستخلص بواسطة الخبراء الفنيين كدليل إثبات قاطع في التشريعات التي تطبق نظام الإثبات المقيّد.
4. ضرورة إجراء التحري والمحاكمة في الدعاوى الجنائية ذات الطبيعة الإلكترونية بواسطة متحرين وقضاة ومحامين إن أمكن مختصين أو مؤهلين "مدرين" في المجال الإلكتروني.
5. إيجاد حماية أكثر فاعلية للدليل الإلكتروني والروابط الإلكترونية أو الشبكية بحيث يستحيل معها التخلص من الدليل أو تدميره.
6. تقنين حماية الدليل الرقمي عن طريق تجريم إتلاف الدليل الرقمي أو إبادته بنصوص قانونية منفصلة في قانون جرائم المعلوماتية.

7. كذلك نوصي باستخدام الدليل الرقمي لكافة أنواع الجرائم مع مراعاة نظرية تحول الجريمة.

المراجع والمصادر

أولاً: الكتب المتخصصة:

1. بابكر الشيخ، إنعكاسات العولمة على الجوانب القانونية والتشريعية، ط1، الخرطوم، السودان، 2007م.
2. حسن طاهر داؤد، جرائم نظم المعلومات، ط 1، الرياض، السعودية، 2000م.
3. عزة علي محمد الحسن، الجرائم المعلوماتية في القانون السوداني، الزيتونة للطباعة، إيداع 2009/11م.
4. علي حسن طوالة، حقوق منتجي ومستخدم الإنترنت في مواجهة الإجراءات الجنائية، ط1، جامعة اليرموك، السعودية، 2004م.
5. علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، جامعة الإسكندرية، العدد 24، مصر، 1992.
6. علي عبدالقادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، ط 1، جامعة الإمارات العربية المتحدة، الإمارات، مايو 2000م.

ثانياً: الرسائل العلمية:

1. زكريا أحمد عمار، حماية الشبكات الرئيسة من الاختراق والبرامج الضارة، رسالة ماجستير في تقانة المعلومات، جامعة النيلين، كلية الدراسات العليا، السودان، 2011م.
2. عبدالله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، دراسة تأصيلية مقارنة، رسالة ماجستير في قسم العدالة الجنائية، جامعة نايف العربية للعلوم الإنسانية، كلية الدراسات العليا، السعودية، 2010م.

ثالثاً: المقالات:

1. عارف خليل أبو عيد، جرائم الإنترنت، دراسة مقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3، الإمارات، 2008م.
 2. عمر بن عبدالمجيد مصبح، بصمة الصوت وأثرها في الإثبات الجنائي، مجلة البحوث الأمنية، العدد 52، يوليو 2012.
 3. عمر محمد بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، موسعة التشريعات العربية، 2003م.
 4. محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1423-1424هـ.
- رابعاً: الملتقيات العلمية:

1. عبدالناصر محمد محمود فرغلي - محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر الأول العربي لعلوم الأدلة الجنائية والطب الشرعي، الرياض، السعودية، (12-14-11/2007م).

خامساً: المراجع الأجنبية:

1. Bell, B.L. A Special-purpose Architecture for the Design of Educational Software, Tech. Rep. No. 70, Evanston, IL: Northwestern University, The Institute for the Learning Sciences, 1996, p 55.
2. Carter, D. L. and Katz, A.J, "Cyber crime: An Emerging Challenge for Law Enforcement" FBI Law Enforcement Bulletin, (1996), available on the World Wide Web (<http://www.fbi.gov/leb/dec961.txt>), arrival date: 10.06.2020..
3. Casey, E. "Using Case-Based Reasoning and Cognitive Apprenticeship to Tech Criminal Profiling and Internet Crime Investigation", Knowledge Solutions, available on the World Wide Web (http://www.corpus-delicti.com/case_based.html), (1997, arrival date: 15.06.2020.

سادساً: التشريعات الوطنية:

1. قانون الإثبات السوداني لسنة 1994م.
 2. قانون الإثبات ولاية كاليفورنيا سنة 1983م.
 3. قانون الحاسب الآلي لسنة 1984م الصادر في ولاية أيوا (iowa).
 4. قانون جرائم المعلوماتية لسنة 2007م المعدل لسنة 2018
- الهوامش:

1 . Bell, B.L. A Special-purpose Architecture for the Design of Educational Software, Tech. Rep. No. 70, Evanston, IL: Northwestern University, The Institute for the Learning Sciences, 1996, p 55.

2 Carter, D. L. and Katz, A.J, "Cyber crime: An Emerging Challenge for Law Enforcement" FBI Law Enforcement Bulletin, (1996), available on the World Wide Web (<http://www.fbi.gov/leb/dec961.txt>), arrival date: 10.06.2020.

- ³ عبدالناصر محمد محمود فرغلي - محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، المؤتمر الأول العربي لعلوم الأدلة الجنائية والطب الشرعي، الرياض، السعودية، (12-14/11/2007م)، ص 12-14.
- ⁴ عمر بن عبدالمجيد مصبح، بصمة الصوت وأثرها في الإثبات الجنائي، مجلة البحوث الأمنية، العدد 52، يوليو 2012، ص 25-47.
- ⁵ بابكر الشيخ، انعكاسات العولمة على الجوانب القانونية والتشريعية، ط1، الخرطوم، السودان، 2007م، ص 20-30.
- ⁶ عبدالناصر محمد محمود فرغلي - محمد عبيد سيف سعيد المسماري، نفس المرجع، ص 14.
- ⁷ محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، أكاديمية نايف العربية للعلوم الأمنية، السعودية، 1423-1424هـ، ص 72-159.
- ⁸ علي عبدالقادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، ط 1، جامعة الإمارات العربية المتحدة، الإمارات، 2000م، ص 32-52.
- ⁹ علي عبدالقادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، جامعة الإسكندرية، العدد 24، مصر، 1992، ص 30-41.
- ¹⁰ حسن طاهر داؤد، جرائم نظم المعلومات، ط 1، الرياض، السعودية، 2000م، ص 23-29.
- ¹¹ نفس المرجع، ص 29.
- ¹² محسن بن سليمان الخليفة، مرجع سابق، ص 72-159.
- ¹³ حسن طاهر داؤد، مرجع سابق، ص 83-93.
- ¹⁴ عمر بن عبدالمجيد مصبح، مرجع سابق، ص 30-35.
- ¹⁵ عمر محمد بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، موسعة التشريعات العربية، 2003م، ص 49-67.
- ¹⁶ عزة علي محمد الحسن، الجرائم المعلوماتية في القانون السوداني، الزيتونة للطباعة، الخرطوم، السودان، 2009م، ص 45.
- ¹⁷ Casey, E. (1997) "Using Case-Based Reasoning and Cognitive Apprenticeship to Tech Criminal Profiling and Internet Crime Investigation", Knowledge Solutions, available on the World Wide Web (http://www.corpus-delicti.com/case_based.html), arrival date: 15.06.2020.
- ¹⁸ تعمل وكالة المباحث الجنائية الفيدرالية الأمريكية FBI بالقيام بتصوير الإلكتروني وذلك بناءً على طلب أجهزة الشرطة الأمريكية بغرض تحقيق العدالة الجنائية، حيث تجمع وتستخلص المعلومات المثبتة على الأقراص الإلكترونية وتقوم بتحليلها وتمد المحاكم الجنائية بها.
- ¹⁹ عمر بن عبدالمجيد مصبح، مرجع سابق، ص 25-47.
- ²⁰ عبدالله بن ناصر بن أحمد العمري، الحماية الجنائية للبريد الإلكتروني، دراسة تأصيلية مقارنة، رسالة ماجستير في قسم العدالة الجنائية، جامعة نايف العربية للعلوم الإنسانية، كلية الدراسات العليا، السعودية، 2010م، ص 55، 148-150.
- ²¹ علي حسن طوالة، حقوق منتجي ومستخدم الإنترنت في مواجهة الإجراءات الجنائية، ط 1، جامعة الزمرك، السعودية، 2004م، ص 25-46.
- ²² عارف خليل أبو عيد، جرائم الانترنت، دراسة مقارنة، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد 3، الإمارات، 2008م، بدون ص.
- ²³ عبدالله بن ناصر بن أحمد العمري، مرجع سابق، ص 117-128.
- ²⁴ حسن طاهر داؤد، مرجع سابق، ص 152-176.
- ²⁵ زكريا أحمد عمار، حماية الشبكات الرئيسة من الاختراق والبرامج الضارة، رسالة ماجستير في تقانة المعلومات، جامعة النيلين، كلية الدراسات العليا، السودان، 2011م، ص 52-78.