حجية الدليل الرقمي في الإثبات الجنائي في النظام السعودي
دراسة تحليلية مقارنة

فارس بن صالح الفارس (*)
جامعة المجمعة

(قدم للنشر في 1444/6/11هـ، وقبل للنشر في 1444/9/14هـ)

ملخص البحث: أدى تطور تقنية المعلومات إلى ظهور أشكال مستحدثة من الجرائم، اصطلح على تسميتها بالجرائم المعلوماتية، وأصبح من الصعب في الفضاء المعلوماتي على المحققين والمختصين اكتشاف أو إثبات الجريمة؛ لأنها وقعت في بيئة افتراضية غير ملموسة ولا حدود لها، وأصبحت الأدلة التقليدية عاجزة عن إثبات هذه الجرائم ولا يمكنها مجاراتها، ومن ثم يصعب إدانة المتهم.
الأمر الذي أدى إلى إثارة التساؤل عن مدى حجية الدليل الرقمي في إثبات هذه النوعية من الجرائم. تأسيساً على ما تقدم؛ فقد تطرق البحث إلى مفهوم الدليل الرقمي وطريقة الحصول عليه ومبادئ قبول الدليل الرقمي في الإثبات الجنائي، وسلطة المحكمة في قبول وتقدير الأدلة الرقمية. وذلك في إطار تحليلي مقارن بين النظام السعودي والقانون الإماراتي، منتهية بأهم النتائج والتوصيات التي أسفرت عنها الدراسة.

كلمات مفتاحية: الدليل الرقمي-الجرائم المعلوماتية-الإثبات الجزائي-الاقتناع القضائي-المحكمة الجزائية.

*****

The validity of digital evidence in Saudi criminal law: A comparative analytical study

Fares Saleh Al Fares (*)
Majmmah University

(Received 4/1/2023, accepted 5/4/2023)

Abstract: The development of information technology has led to the emergence of new forms of crime, which in the information space are called "information crimes." It has become difficult for investigators and specialists to detect or prove the crime because it occurred in an intangible and limitless virtual environment. Traditional evidence has become incapable of proving these crimes and cannot keep pace with them, making it difficult to convict the perpetrator. This has raised the question of the authoritativeness of digital evidence in proving this type of crime. Based on the aforementioned facts, this research dealt with the concept of digital evidence and how to obtain it, the basic principles of accepting digital evidence in criminal evidence, and the authority of the criminal court in accepting and estimating digital evidence within a comparative analytical framework between the Saudi system and Emirati law. The study concludes with the most important findings and recommendations.

Keywords: Digital evidence-information crimes- criminal proof- Judicial conviction- criminal court.

(*) للمراسلة:

أستاذ مساعد، قسم القانون، كلية إدارة الأعمال، جامعة المجمعة
ص ب: 66رمز بريدي: 11952: مدينة الرياض، محافظة المجمعة.

(*) Corresponding Author:

Assistant Professor Dept law., Faculty College of Business Administration -, Majmaah University, P.O. Box: 66, Code City11952, Kingdom of Saudi Arabia.

DOI: 10.12816/0061517

e-mail: f.alfaris@mu.edu.sa

مقدمة

أدى التطور الهائل في الثورة المعلوماتية التي يشهدها العصر الرقمي إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميتها بالجرائم المعلوماتية. ويتسم مرتكبي هذه الجرائم بالدهاء حيث يلجؤون إلى تخزين المعلومات المتعلقة بنشاطهم الاجرامي في النظم التقنية للدول الأجنبية بواسطة شبكة الإنترنت عن بعد، مع استخدام شفرات سرية لإخفائها عن الأجهزة الأمنية، مما تثار معه إشكالية بشأن الحصول على الأدلة الجزائية لإثبات تلك الجرائم قبل مرتكبيها.

وعلى ضوء ذلك، فإن الطبيعة التقنية لهذه الجرائم نتج عنها ظهور وسيلة إلكترونية تتناسب مع طبيعتها بحيث يكون بمقدور الجهات المختصة فك شفراتها وترجمة نبضاتها إلى معلومات يمكن قراءتها وصالحة كأدلة إثبات تلك الجرائم، ومن ثم نسبتها إلى مرتكبيها، ويطلق على هذه الوسيلة في وقتنا الحالي مسمى الدليل الرقمي والذي أصبحت العديد من الأنظمة القانونية تأخذه كأداة لها حجيتها النظامية في الإثبات متساوية مع الحجية المقررة للدليل المادي.

وهو الأمر الذي يوجد معه وضع جديد، يضمن إخضاع الدليل الرقمي للسلطة التقديرية للمحكمة الجزائية وقناعتها به كدليل إثبات له قيمة نظامية. ومن هذا المنطلق ستركز دراسة موضوع البحث على النظام السعودي بشكل أساسي، دون إغفال-في بعض المواطن-موقف القانون الإماراتي لوجود تقارب وتشابه بينهما فيما يخص إجراءات جمع الأدلة الجزائية الرقمية والمبادئ الأساسية لقبولها أمام القضاء، من أجل الوقوف على حجية الدليل الرقمي في الإثبات الجزائي.

أهمية البحث

تكمن أهمية الدراسة في التعرض لأحد الموضوعات المهمة المستحدثة تحديداً في المجال الجزائي، لاسيما وأن نظام الإثبات السعودي لم يتطرق لتنظيم قواعد خاصة بالإثبات بالدليل الجزائي الرقمي، بعكس الإثبات الجزائي بالأدلة المادية التي تم تنظيمها وأخذت حقها من الدراسة.

بالإضافة إلى محاولة بيان مدى تأثير طبيعة الدليل الرقمي على اقتناع المحكمة الجزائية، باعتبار أن هذا الاقتناع يأتي كوجاء يقي من أي شطط قد ينجم عن استخدام وسيلة علمية حديثة في الإثبات، والتي قد تمس في بعض الأحيان حرمة الحياة الخاصة.

الدراسات السابقة:

موضوع البحث يتسم بالحداثة نظراً لدراسته

في إطار نظام الإثبات السعودي الجديد والأدلة الإجرائية لهذا النظام، ولغاية الشروع في كتابة البحث لم يتمكن الباحث من العثور على أي دراسة ذات صلة مباشرة تناولت موضوع الإثبات بالدليل الجزائي الرقمي وفقاً للنظام السعودي الحالي، فمن الطبيعي ألا تزال الكتابة فيه في بداياتها.

ولغاية الشروع في كتابة البحث، وفي حدود ما تم الاطلاع عليه، لم نجد سوى بعض الدراسات التي تناولت موضوع حجية الدليل الرقمي في الإثبات الجنائي، وتتمثل أهم هذه الدراسات في التالي:

-دراسة وهيبة لعوارم (الدليل الرقمي في مجال الإثبات الجنائي وفقاً للتشريع الجزائري، 2014م):

اقتصرت هذه الدراسة على تناول ماهية الدليل الرقمي وقيمته القانونية في الإثبات الجنائي وفقاً للقوانين الجزائرية، ويكمن الاختلاف في أن دراستنا تناولها هذه الموضوعات وفقاً للأنظمة السعودية والقوانين الإماراتية، كما تتميز دراستنا عنها في تسليط الضوء على إجراءات جمع الدليل الجزائي الرقمي، والمبادئ الأساسية لقبول الدليل الرقمي أمام القضاء الجزائي، وسلطة المحكمة الجزائية في الاقتناع بالدليل الرقمي.

-دراسة فارس بن محمد العبيدي (دور الدليل الرقمي في الاثبات الجنائي في النظام السعودي، 1441هـ،2020م):

وتناول هذه الدراسة ماهية الدليل الرقمي وإجراءات الحصول عليه، وبيان حجية الدليل الرقمي في ضوء نظام الإجراءات الجزائية السعودي الصادر بالمرسوم الملكي رقم (م/2) بتاريخ 1435/1/22هـ، وقانون الإجراءات الجزائية الإماراتي رقم 35 لسنة 1992م، والقيمة القانونية للدليل الرقمي أمام القضاء الجنائي، وتتفق هذه الدراسة مع دراستنا في تناول هذه الموضوعات، إلا أن دراستنا تختلف عنها في أنها تناولتها وفقاً لنظام الإثبات السعودي الحالي، الصادر بالمرسوم ملكي رقم (م/43) وتاريخ 1443/5/26هـ، والقانون الاتحادي الإماراتي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، والمعمول به بتاريخ 2022/1/2م، وغيره من الأنظمة السعودية والقوانين الإماراتية ذات الصلة بموضوع الدراسة، كما تتميز دراستنا عنها في تطرقها للمبادئ الأساسية لقبول الدليل الرقمي أمام القضاء الجزائي.

-دراسة أسامة حسين عبدالعال (حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، 2021م):

اقتصرت هذه الدراسة على تناول ماهية الدليل الرقمي ودوره في الإثبات الجنائي والقيمة

القانونية للدليل الرقمي وفقاً لقانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004، والقانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018، وتختلف دراستنا عنها في تناولها هذه الموضوعات وفقاً للأنظمة السعودية والقوانين الإماراتية، كما تتميز دراستنا عنها في تناولها إجراءات جمع الدليل الجزائي الرقمي، والمبادئ الأساسية لقبول الدليل الرقمي أمام القضاء الجزائي، وسلطة المحكمة الجزائية في الاقتناع بالدليل الرقمي.

-دراسة أحمد عبد السلام (الإثبات بالدليل الرقمي في النظام السعودي، 2022م):

اقتصرت هذه الدراسة على ماهية الدليل الرقمي وأشكاله وحجيته في الإثبات في المسائل المدنية والتجارية في ضوء نظام الإثبات السعودي فحسب، بينما تركز دراستنا على مفهوم الدليل الرقمي وتقسيماته ونطاقه وإجراءات جمعه في المسائل الجنائية، كما تعمقت دراستنا في تناول المبادئ الأساسية لقبوله في الإثبات الجنائي وسلطة المحكمة الجزائية في الاقتناع بالدليل الرقمي وفقاً للعديد من الأنظمة السعودية والقوانين الإماراتية.

إشكالية البحث:

لما كان الأساس في خطورة الجرائم المعلوماتية يكمن في أنها في طبيعتها تجمع بين الذكاء الاصطناعي والذكاء البشرى، مما يجعل إثباتها جنائيا قد يكون في منتهى الصعوبة، كما ترجع الصعوبة كذلك إلى اختلاف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط افتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية.

ولقد أثار هذا النوع من الأدلة الكثير من الجدل والذي يمكن إرجاعه إلى إشكالية رئيسية تتمحور حول مدى حجية الدليل الرقمي في الإثبات الجزائي؟ وذلك مرده قابليته للتعديل في معطياته مما يفتح الباب واسعاً للطعن في مصداقيته.

تساؤلات البحث:

يناقش البحث جملة من التساؤلات حول كيفية ضمان مصداقية الدليل الرقمي في الإثبات الجزائي وأنه يعبر عن الحقيقة ويمكن الاستناد عليه من قبل القضاء، مما يتطلب ذلك الإجابة على التساؤلات التالية:

ما مدى مشروعية الدليل الرقمي في الإثبات، وفيما إذا كان للدليل الرقمي تلك الفعالية والقوة الثبوتية بحيث تؤثر على الاقتناع القضائي للمحكمة الجزائية في إصدار حكمها؟ وما مدى سلطة المحكمة الجزائية في تقدير وقبول الدليل الرقمي؟ وهل يخضع الدليل الرقمي لمبدأ

الاقتناع القضائي، وآليات الأخذ بهذا الدليل في الإثبات وفق النظام الجزائي السعودي؟

أهداف البحث:

تتلخص أهداف البحث فيما يلي:

1. الوقوف على ماهية الدليل الرقمي من حيث مفهومه وتقسيماته ونطاقه.
2. التعرف على مشروعية تحصيل الدليل الرقمي وأثره أمام القضاء الجزائي.
3. بيان الاشتراطات التي حددها النظام للتأكد من صحة وسلامة الدليل الرقمي.
4. التعرف على القوة الثبوتية للدليل الرقمي في ثبوت الدعوى الجزائية.
5. تحديد سلطة المحكمة في تقدير وقبول الدليل الرقمي وصلاحيته للإثبات الجزائي.

منهجية البحث:

يتبع الباحث في هذا البحث المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية المعمول بها النظام السعودي مع نظيره القانون الإماراتي وبعض الاتفاقيات الدولية ذات الصلة بحجية الدليل الرقمي في الإثبات الجزائي، وكذلك تحليل آراء فقهاء القانون المتعلقة بموضوع البحث، مع استخلاص لأهم النتائج والتوصيات التي سيتم التوصل إليها.

خطة البحث:

سوف يُقسم موضوع البحث إلى أربع مباحث على النحو التالي:

المبحث الأول: ماهية الدليل الجزائي الرقمي

المطلب الأول: مفهوم الدليل الرقمي

المطلب الثاني: تقسيمات الدليل الرقمي ونطاقه

المبحث الثاني: إجراءات جمع الدليل الرقمي

المطلب الأول: الإجراءات التقليدية لجمع الدليل الرقمي

المطلب الثاني: الإجراءات التقنية لجمع الدليل الرقمي

المبحث الثالث: سلطة المحكمة المختصة في قبول الدليل الرقمي

المطلب الأول: مشروعية الدليل الرقمي ويقينيته في الإثبات

المطلب الثاني: ضوابط قبول الدليل الرقمي كوسيلة إثبات

المبحث الأول

ماهية الدليل الرقمي

تتركز عملية الإثبات الجزائي في الجرائم المتصلة بالتكنولوجيا الحديثة على الدليل الجزائي الرقمي باعتباره الوسيلة الوحيدة والرئيسة لإثبات تلك الجرائم، وهي محور البحث، لذا سيتناول الباحث في هذا المبحث مفهوم الدليل الرقمي (المطلب الأول) تقسيمات الدليل الجزائي الرقمي ونطاقه (المطلب الثاني).

المطلب الأول

مفهوم الدليل الرقمي

يقتضي الحال لمعرفة مفهوم الدليل الرقمي،

أن يتم التطرق لتعريفه (الفرع الأول) وتحديد خصائصه (الفرع الثاني).

الفرع الأول

تعريف الدليل الجزائي الرقمي

سوف يتناول الباحث في هذا الفرع تعريف الدليل الجزائي الرقمي سواء من الناحية اللغوية أو الاصطلاحية على النحو التالي.

أولاً: التعريف اللغوي

الدليل في اللغة مأخوذ من فعل دلَ بمعنى أشار وأرشد، ويقال دل على الطريق أي أرشد إليه أسم الفاعل من فعل دلَ هو الدال والدلالة تعني الإشارة، وأيضاً بمعنى الإرشاد، وبمعنى السكينة والوقار في الهيئة والمنظر والشمائل والدليل هو ما يستدل به (يعقوب،2004م، ص:179).

أما الجزائي فأصله جزاء: أي المكافأة على الشيء، جزاه به وعليه جزاءً وجازاه مجازاة ً وجزاءً، وقول الحطيئة: من يفعل الخير لا يعدم جوازيه. وقال ابن سيده: قال ابن جني: ظاهر هذا أن تكون جوازية جمع جازٍ أي لا يعدم جزاءً عليه، وجاز أن يجمع جزاءً على جوازٍ لمشابهة اسم الفاعل للمصدر، فكما جمع سيلٌ على سوائل كذلك يجوز أن يكون جوازية جمع جزاءٍ.

واجتزاه: طلب منه الجزاء؛ قال: يجزون بالقرض إذا ما يجتزى، والجازية: الجزاء اسم للمصدر كالعافية: قال أبو الهيثم: الجزاء يكون ثواباً ويكون عقاباً، وخير دليل على هذا قوله تعالى: ((وَجَزَاءُ سَيِّئَةٍ سَيِّئَةٌ مِثْلُهَا)) [1]، وقوله تعالى: ((وَاتَّقُوا يَوْمًا لَا تَجْزِي نَفْسٌ عَنْ نَفْسٍ شَيْئًا)) [2] فالجزاء في هذه الآيات الكريمة يعني القضاء أي جزى هذا الأمر أي قضى (ابن منظور،1999، ص:278).

بينما الرقمي أو الإلكتروني فيعرف بأنه «علم يختص بدراسة حركة وسلوك المسببة للتيار سواء كان ذلك باستخدام الصمامات المفرغة أو المحتوية على غارات أو الصمامات الضوئية أو أشباه المواصلات» (الهادي،1988م، ص:138).

ثانياً: التعريف الاصطلاحي

على الرغم من عدم وجود تعريف عالمي متفق عليه بشأن الدليل الرقمي إلا أن بعض التشريعات الدولية تطرقت إلى تعريف الدليل الرقمي ومن هذه التشريعات نذكر منها الآتي: عرفت المنظمة الدولية لأدلة الحاسوب (IOCE) الدليل الرقمي بأنه» المعلومات ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية»، وعرفت المنظمة الدولية للمواصفات والمقاييس (الأيزو) الأدلة الرقمية بأنها «مجموعة من المعلومات والسياسات المدونة على دعامة مادية بشكل دائم بحيث يسهل

1. سورة الشورى، الآية (40).
2. سورة البقرة، الآية (48).

قراءتها مباشرة من قبل الإنسان أو بالاستعانة بآلة مخصصة لذلك الغرض»(العتيبي،2016م، ص:78).

بينما عرف قانون المعاملات الإلكترونية الاتحادي للولايات المتحدة الأمريكية لعام 1999، المعلومات الرقمية في المادة (10) من القسم الثاني، بأنها» البيانات والنصوص والصور والأصوات والرموز وبرامج الكمبيوتر والبرمجيات وقواعد البيانات أو مشابه ذلك»(حسن،2018م، ص:8).

أما على صعيد التشريع العربي، فنجد أن القانون الاتحادي الإماراتي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، والمعمول به بتاريخ 2022/1/2م، فقد عرف الدليل الرقمي في المادة (1) حيث قد جاءت، على أنه: « أي معلومات إلكترونية لها قوة، أو قيمة ثبوتية مخزنة، أو منقولة، أو مستخرجة، أو مأخوذة من أجهزة الحاسب، أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة».

أما نظام الإثبات السعودي، الصادر بالمرسوم ملكي رقم (م/43) وتاريخ 1443/5/26هـ، فقد عرف الدليل الرقمي في المادة (53) فقد جاءت، بأنه « يعد دليلاً رقمياً كل دليل مستمد من أي بيانات تنشأ أو تصدر أو تسلم أو تحفظ أو تبلغ بوسيلة رقمية، وتكون قابلة للاسترجاع أو الحصول عليها بصورة يمكن فهمها».

من خلال ما تقدم من تعريفات وعلى اختلاف التسميات التي أطلقتها على الدليل الرقمي، يتبين أنها قد أحاطت بجوانب شتى من الدليل الرقمي مع بقاء الجوهر واحداً، فقد أوضحت معنى الدليل وصوره وطبيعة الوسط الذي يستخلص منه على نحو يمكن معه توظيفه في مجال الإثبات الجزائي.

تعددت التعريفات بشأن الدليل الرقمي، وقد استقى الباحث من هذه التعريفات الآتي: فقد عرف جانب من الفقه الدليل الرقمي على أنه» البيانات التي ممكن أن تثبت أن هناك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، والرسوم، والخرائط، الصوت والصورة»(البشري،2004م، ص:233).

ويلاحظ على هذا التعريف أنه قد خلط بين الدليل الرقمي وبرامج الحاسوب الآلي، حيث إنه اعتبر الدليل الرقمي مجرد بيانات يتم إدخالها إلى الحاسوب بغرض إنجاز عملية محددة، وهذا من دون شك ينطبق على وظائف برامج الحاسوب، إذ تؤدي مكونات الحاسوب الصلبة وظائف تشبه شفرة الآلة، أما الدليل الرقمي فهو الأثر الذي يتركه الجاني عقب

ارتكابه للجريمة ويؤدي إلى اكتشافها.

وعرف جانب آخر من الفقه الدليل الرقمي بأنه» الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الصوت والأشكال والرسوم؛ وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون»(إبراهيم،2008م، ص:178).

ويؤخذ على هذا التعريف تضييقه من نطاق الدليل الرقمي حيث إنه حصره بمخرجات الحاسوب الآلي وملحقاته، ولكنها تعد أحد أنواع الدليل الرقمي.

أيضاً عرف رأي آخر في الفقه الدليل الرقمي بأنه» الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات عن طريق إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها وتفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها»(فرغلي،2007م، ص:7).

ويؤخذ على هذا التعريف أنه قد خلط بين الدليل وعملية استخراجه من المصدر، حيث اعتبر المجال الكهربائي أو المغناطيسي قبل فصله عن المصدر لا يسبغ بوصف الدليل إلا إذا تم إخراجه.

وبناء على ما تقدم ومن خلال التعريفات السابقة **نرى أن** الدليل الجزائي الرقمي هو «معلومة مخزنة في وسائل الاتصال الإلكترونية وملحقاتها، أو معلومة مدونة على شبكات الاتصال، يتم جمعها وتحليلها وعرضها باستخدام تطبيقات وتقنيات خاصة، بغرض إثبات ارتكاب الجريمة ونسبتها إلى المتهم أو نفيها عنه».

الفرع الثاني

خصائص الدليل الجزائي الرقمي

للدليل الرقمي خصائص مميزة يستكمل من خلالها الإطار العام لمفهومه، ومن أبرز هذه الخصائص:

أولاً- الدليل الرقمي دليل علمي

يتكون هذا الدليل من المعلومات المحملة أو المنقولة أو المخزونة في الأجهزة ذات الأنظمة الإلكترونية وبالنظر لكون هذه المعلومات غير محسوسة، فإنه يتطلب لإدراكها استخدام الحاسوب الآلي وبرمجيات حاسوبية، فهي تحتاج إلى مجال تقني يتعامل معها، مما يعني هذا أن الدليل الرقمي بصفته دليل معلوماتي يحتاج للبيئة التقنية ليتكون منها، ولما كانت التقنية وليدة العلم فمن ثم يعد ما ينشأ عن التقنية أدلة

علمية (بن يونس،2004م، ص:977).

ثانياً- الدليل الرقمي دليل تقني

يحتاج هذا الدليل إلى بيئة رقمية حيث إنه من طبيعة تقنية المعلومات، ولا تنتج التقنية دليلاً مادياً تقليدياً مثل اعترافاً مكتوباً أو بصمة أصابع، وإنما ما تنتجه التقنية هو نبضات رقمية، ولابد من وجود توافق بين هذا الدليل وبيئته التي نشأ فيها، ولا وجود له خارجها، بمعنى أنه يجب لكي يكون هناك دليل رقمي أن يكون مستنبطاً أو مستجلباً من العالم الافتراضي في أجهزة الحاسوب الآلي والخوادم وشبكات الإنترنت وغيرها من الوسائل التي يتم عبرها تداول الحركة (إبراهيم،2008م، ص:181).

ثالثاً- الدليل الرقمي متطور ومتنوع

1-دليل متطور

الدليل الرقمي متطور بطبيعته مقارنة بالدليل المادي، وأن هذه الطبيعة ناتجة عن بيئته التقنية المتطورة التي ينشأ فيها فالعالم الافتراضي الذي يتواجد فيه الدليل الرقمي يأتي كل دقيقة بجديد ومعها يتطور شكل هذا الدليل (إبراهيم،2008م، ص:183).

2-دليل متنوع

التنوع في الدليل الرقمي له أشكال ومظاهر متعددة ومن ذلك أنه يمكن أن يكون في صورة بيانات غير مقروءة كما هو الشأن حال المراقبة عبر الخوادم وشبكات الإنترنت، وقد يكون الدليل في صورة بيانات يمكن قراءتها مثل التسجيل السمعي والمرئي والتوقيع الإلكتروني أو مرفقات مخزنة في البريد الإلكتروني (فرغلي،2007م، ص:14)، وهذا التنوع للدليل الرقمي مرتبط بالتطور الحاصل في عالم تقنية المعلومات.

رابعاً-الدليل الرقمي قابل للنسخ

يمكن استخراج نسخ متعددة من الدليل الرقمي جميعها تتطابق الأصل ولها ذات القوة الثبوتية[1]، على خلاف الدليل التقليدي الذي لا يتمتع بهذه الخاصية، وهذا يشكل ضمانة لحفظ الدليل من الإتلاف أو التبديل (فرغلي،2007م، ص:15)، ومن ثم هذا يؤدي إلى الحفاظ على الدليل الرقمي في مجال المحررات الرقمية أطول وقت ممكن.

خامساً -الدليل الرقمي ذو سعة تخزينية عالية

يمتاز الدليل الرقمي بقدرته على تخزين كم هائل من البيانات والمحررات الرقمية المخزنة بكثافة في أجهزة الحاسوب الآلي وملحقاته، والتي تم تجميعها وتحليلها باستخدام برامج وتطبيقات لكي نحصل منها على الدليل الرقمي،

1. تنص المادة (1/63) من نظام الإثبات السعودي، على أنه» يكون للمستخرجات من الدليل الرقمي الحجية المقررة للدليل نفسه، وذلك بالقدر الذي تكون فيه المستخرجات مطابقة لسجلها الرقمي»، كما تنص المادة من الأدلة الإجرائية لنظام الإثبات السعودي الصادرة بقرار وزير العدل رقم (921) وتاريخ 1444/3/16هـ، على أنه « عند منازعة الخصم في صحة المستخرج من الدليل الرقمي، فيجب مطابقته على سجله الرقمي».

وخير مثال أجهزة التصوير الرقمية التي يمكنها تخزين آلاف الصور الملتقطة في وقت سابق، ومن خلالها يمكن التعرف على شخصية مرتكب الجريمة وضبطه(فرغلي،2007م:15).

سادساً-الدليل الرقمي دليل تحليلي

يرصد هذا الدليل معلومات عن مرتكب الجريمة ويحللها في الوقت نفسه، حيث يمكن من خلال الدليل الرقمي تسجيل تحركات مرتكب الجريمة وتصرفاته وسلوكياته الرقمية ومعلوماته ونشاطاته الشخصية؛ لذا فإن البحث الجنائي باستخدام الدليل الرقمي قد يجد غايته التي يصبو إليها بشكل أيسر وأسرع مقارنة مع البحث باستخدام الدليل المادي (Alan,1999: p.75).

سابعاً-الدليل الرقمي صعب الخلاص منه

يتميز الدليل الرقمي بصعوبة التخلص منه مقارنة مع الدليل المادي الذي يمكن محوه أو إخفائه بكل سهولة مثل تمزيق الأوراق التي تحمل إقرار أو حرقها، أو مسح بصمات الأصابع من موضعها، أو إخفاء الأدوات المستخدمة في ارتكاب الجريمة، وإذا كان هذا هو الحال بالنسبة للدليل التقليدي، فإن الأمر مختلف بالنسبة للدليل الرقمي حيث يمكن استرجاعه بعد محوه، وإظهاره بعد إخفائه، مما يؤدي إلى صعوبة الخلاص منه ، فمثلاً في حالة حذف البيانات أو الملفات من الحاسوب الآلي فإنه يمكن استعادتها بواسطة برامج حاسوبية معدة لهذا الغرض، كل ذلك يضع صعوبة أمام الجاني عند محاولته إتلاف أدلة الجريمة أو محو آثارها أو طمس معالمها، كما أنه يتم تسجيل تلك المحاولة كدليل إدانة ضد الجاني (الرشودي،2008م، ص:252).

المطلب الثاني

تقسيمات الدليل الرقمي ونطاقه

سوف يتناول الباحث في هذا الفرع تقسيمات الدليل الجزائي الرقمي (الفرع الأول) ثم يبين نطاقه (الفرع الثاني).

الفرع الأول

تقسيمات الدليل الرقمي

يتخذ الدليل الرقمي العديد من الأنواع والأشكال[1]، ولذلك تعددت تقسيماته انطلاقاً من الجهة التي ينظر بها إليه.

أولاً-تقسيم الأدلة الجزائية الرقمية حسب طبيعة الجريمة

قسم البعض (عبد المطلب،2006م، ص:88) الأدلة الرقمية على نحو يتوافق مع تقسيم الجريمة المرتكبة عبر الكمبيوتر، على النحو التالي:

1. تنص المادة (60) من نظام الإثبات السعودي، على أنه» يرجع في مفهوم أنواع الدليل المنصوص عليها في المادة (الرابعة والخمسين) من النظام للأنظمة ذات الصلة، ومنها نظام التعاملات الإلكترونية».

1-الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكاتها

وتعني الأدلة الناتجة عن جرائم الكمبيوتر التي هي عبارة عن سلوك إنساني يشكل فعلاً غير مشروع نظاماً ويقع على أجهزة الكمبيوتر، سواء وقع على المكونات المادية لأجهزة (Hardware)، أو مكونات معنوية (Soft-Ware) أو قواعد بيانات رئيسة (Data Base) [1]. ومثالها جرائم تخريب وسائط التخزين المرنة والصلبة لأجهزة الكمبيوتر وكذلك نشر فيروسات الكمبيوتر (Eoghan,2011: p.19).

2-الأدلة الرقمية الخاصة بالإنترنت

ويقصد بها الأدلة الناجمة عن جرائم الإنترنت، وتقع على آليات نقل البيانات بين مستخدمي شبكة الإنترنت، ومثالها جريمة موقع إلكتروني بطريقة غير مشروعة واستخدام عنوان (IP) زائفة للولوج إلى شبكة الإنترنت (Bri-an,2005: p.23).

3-الأدلة الرقمية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة شبكة الإنترنت

هي الجرائم التي يستخدم فيها الكمبيوتر أو الشبكة العالمية للمعلومات أو ما تعرف باسم (الويب) أو الإنترنت، كوسيلة مساعدة لارتكاب الجريمة، ومثالها جرائم غسل الأموال. هذا ويظل الكمبيوتر محتفظاً بالآثار الرقمية التي يستعان بها في الإرشاد عن مرتكب الجريمة (قنديل،2015م، ص:124).

4-الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات

وتعني الأدلة الناتجة عن الجرائم الواقعة على وثائق أو نصوص موجودة على الشبكة، ومثالها سرقة أرقام البطاقات الائتمانية.

ونرى أن التقسيم السابق يتناسب مع التقسيم الفقهي للجرائم المرتكبة باستخدام الكمبيوتر، إلا أنه لا يتناسب مع مفهوم الرقمية الحديثة، ويرجع ذلك إلى أنه يمكن استخلاص الدليل الجزائي الرقمي ليس فقط من أجهزة الكمبيوتر وشبكاتها، بل يمكن استخلاصه من كافة الأجهزة الرقمية مثل آلات التصوير والهاتف وغيرها، كما أن التمييز بين شبكات الكمبيوتر وبروتوكولات تبادل المعلومات والشبكة العالمية للمعلومات لا جدوى منه، لأن جميعها في الأصل واحد، فاختلاف المصطلحات ليس معناه أن هناك اختلافاً في المدلول.

ثانياً-تقسيم الأدلة الرقمية من حيث إعدادها كوسيلة للإثبات

1-أدلة رقمية معدة كوسيلة إثبات

أ-البيانات أو المعلومات الرقمية التي أنشئت بواسطة الحاسوب الآلي أو جهاز آخر بشكل تلقائي، وتعتبر هذه البيانات أو المعلومات من مخرجات الحاسوب التي لا دخل للمستخدم في

1. انظر نظام الإثبات السعودي، المادة (6/54).

إنشائها مثل فواتير البطاقات المصرفية المعدة آلياً[1].

ب-البيانات أو المعلومات الرقمية التي تم حفظ جزء منها عن طريق الإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسوب الآلي مثل رسائل البريد الإلكتروني[2]، والرسائل المتبادلة عبر منصات التواصل الاجتماعي المتبادلة على الإنترنت (الحلبي،2011م، ص:234). أو البيانات أو المعلومات الرقمية المدخلة والمعالجة من طرف برنامج (Excel).

وهذه الأدلة أعدت مسبقاً بغرض جعلها وسيلة لإثبات بعض الوقائع التي تتضمنها، ولهذا يتم حفظ هذه البيانات أو المعلومات الرقمية منعاً لفقدها وحتى يسهل الرجوع إليها لاحقاً للاحتجاج بها (عبد المطلب،2006م، ص:108). وتجدر الإشارة إلى أن القانون الإماراتي نص في المادة (65) من القانون الاتحادي بشأن مكافحة الشائعات والجرائم الإلكترونية، على أنه» يكون للأدلة المستمدة أو المستخرجة من الأجهزة، أو المعدات، أو الوسائط، أو الدعامات الإلكترونية، أو النظام المعلوماتي، أو برامج الحاسب، أو أي وسيلة لتقنية المعلومات حجية الأدلة الجزائية المادية في الإثبات الجنائي». ويتبين من هذا النص أن ما تضمنه من أدلة تعد أدلة جزائية رقمية وساوى بينها وبين الأدلة المادية العادية من حيث الحجية النظامية في الإثبات الجزائي، ولا يوجد نص نظامي مماثل لهذا النص في النظام السعودي.

2-أدلة رقمية غير معدة كوسيلة إثبات

هذه النوعية من الأدلة الرقمية تسمى البصمة الرقمية (Log Files) وتنشأ نتيجة الآثار التي يتركها مرتكب الجريمة دون إرادة أو رغبة منه في وجوها وتتجسد هذه الأدلة في الآثار المعلوماتية الرقمية التي يتركها مستخدم شبكة الإنترنت بسبب تسجيل المراسلات الصادرة منه أو تلقيها جميعها ويمكن ضبطها باستخدام وسائل تقنية وكافة الاتصالات التي أجراها الفرد خلال الحاسوب الآلي أو عبر شبكة الإنترنت (Back-up Files)[3]. حيث إن هذه الأدلة غير معدة أساساً للحفظ من قبل من صدرت عنه، لكن بمقدور الوسائل الفنية المخصصة لهذا الغرض ضبط تلك الأدلة ولو بعد مرور مدة زمنية من نشوئها (Linda,2008: p.17).

وتكمن أهمية هذه النوعية من الأدلة الرقمية في أنها قد تتضمن أحياناً معلومات تساعد في الكشف عن ملابسات جريمة والجاني.

الفرع الثاني

نطاق الدليل الجزائي الرقمي

تجدر الإشارة إلى أن الدليل الجزائي الرقمي لا

1. انظر نظام الإثبات السعودي، المادة (1/54) والمادة (2/63).
2. انظر نظام الإثبات السعودي، المادة (4/54).
3. انظر نظام الإثبات السعودي، المادة (57).

يقتصر على إثبات الجرائم المعلوماتية فحسب، بل يصلح لإثبات الجرائم التقليدية، وفي هذا الصدد ميز الفقه بين نوعين من الجرائم لتحديد نطاق الدليل الجزائي الرقمي، وهي كالتالي:

أولاً: الجرائم المرتكبة باستخدام الحاسوب الآلي:

في هذه النوعية من الجرائم يستخدم الحاسوب الآلي وشبكة الانترنت كوسيلة مساعدة لارتكابها، مثل استخدام الحاسوب الآلي في جرائم القتل أو غسل الأموال أو تهريب المخدرات، كما قد تستخدم شبكة الانترنت في ارتكاب العديد من الجرائم التقليدية مثل الاستيلاء على أموال البنوك، أو قيادة المنظمات الإرهابية، أو تهديد الأمن الداخلي والخارجي للدولة، أو الاحتيال باستخدام البطاقات المصرفية، وبالرغم من أن هذه الجرائم لا تتصل بالأنظمة المعلوماتية إلا أن ذلك لا يمنع من صلاحية الدليل الرقمي كوسيلة لإثباتها(Debra,2008:p.545).

ثانياً: جرائم الاعتداء على الحاسوب الآلي:

هذه النوعية من الجرائم يكون محلها هو جهاز الحاسوب الآلي نفسه، فإما أن يقع الاعتداء على الكيان المادي للحاسوب، فتعتبر الجريمة في هذه الحالة جريمة تقليدية تلحق بالنوعية الأولى من الجرائم، وإما أن يقع الاعتداء على الكيان المادي للحاسوب، أو على المعلومات الموجودة على شبكة الإنترنت مثل إتلاف هذه البيانات أو تعديلها أو انتهاك حقوق الملكية الفكرية وجرائم القرصنة.

أضف إلى ذلك أن الدليل الرقمي يصلح لإثبات جرائم أخرى، وإن لم تكن من نفس النوعين المذكورين بعاليه، كما في حالة استخدام الحاسوب الآلي للتمهيد لارتكاب جريمة أو إخفاء معالمها، مثل الرسائل التي يبعثها الجاني لشريكه وتحتوي على بيانات عن جريمة يعزمان ارتكابها، فتصلح هذه الرسائل كدليل لإثبات هذه الجريمة عند وقوعها (الصغير،2002م، ص:32)

المبحث الثاني

إجراءات جمع الدليل الرقمي

يتطلب التعامل في مسرح الجريمة الإلكترونية توافر إجراءات معينة لجمع الأدلة الرقمية واستخلاصها وإبراز قيمتها الاستدلالية، واتساقاً مع ذلك سوف يبين الباحث أهم إجراءات جمع الدليل الجزائي الرقمي، وذلك في مطلبين متعاقبين، على أن يتناول الإجراءات التقليدية لجمع الدليل الجزائي الرقمي في (المطلب الأول) ثم يستعرض الإجراءات الحديثة لجمع الدليل الجزائي الرقمي في (المطلب الثاني).

المطلب الأول

الإجراءات التقليدية لجمع الدليل الرقمي

سيتناول الباحث في هذا المطلب المعاينة (الفرع الأول) والتفتيش (الفرع الثاني) وذلك لعلاقتهما

بالدليل الجزائي الرقمي حيث ينما في الغالب عن نتائج مادية ملموسة، وسوف يبين الباحث دور كل إجراء منهما في استنباط الدليل الجزائي الرقمي.

الفرع الأول

المعاينة

للمعاينة أهمية كبيرة في كشف غموض الكثير من الجرائم، وتعرف في علم التحقيق الجزائي بأنها «مشاهدة المكان الذي ارتكبت فيه الجريمة وعمل وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها بها الجاني»(إبراهيم،2009م، ص:149).

وتتطلب المعاينة سرعة الانتقال إلى مكان ارتكاب الجريمة لمباشرتها بغرض إثبات حالتها وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها. وقد نصت على المعاينة في مرحلة التحقيق كل من المادة (79) من نظام الإجراءات الجزائية السعودي الصادر بالمرسوم الملكي رقم (م/2) بتاريخ 1435/1/22هـ، والمادة (71) من قانون الإجراءات الجزائية الإماراتي رقم 35 لسنة 1992م، كما نصت على المعاينة في مرحلة المحاكمة كل من المادة (108) من نظام الإثبات السعودي، والمادة (67) من القانون الاتحادي الإماراتي رقم 10لسنة1992 والمعدل بالقانون رقم 36 لسنة 2006 بشأن قانون الاثبات في المعاملات المدنية والتجارية.

وتتخذ المعاينة في الجرائم المعلوماتية أشكال عديدة، وذلك على حسب نوع الجرائم المرتكبة، كما أن هناك وسائل عامة تتلاءم مع طبيعة النظام المعلوماتي، مثل وسيلة تصوير شاشة الحاسوب الآلي عن طريق برامج متخصصة عن طريق أخذ صورة لما يظهر على الشاشة، وهو ما يعرف ب «طريقة تجميد مخرجات الشاشةFrozen» أو أن يتم ذلك عن طريق حفظ الموقع الإلكتروني باستخدام خاصية الحفظ «Save as» المتوافرة في نظام التشغيل.

وفي سبيل إجراء المعاينة التقنية يتم التعامل مع مسرح الجريمة المعلوماتية على أنه مسرحان هما:

-مسرح تقليدي(مادي): ويشمل المكونات المادية المحسوسة للحاسب الآلي، ويمكن أن يحتوي على بعض الآثار المادية لمرتكب الجريمة مثل بصماته أو بعض متعلقاته الشخصية أو وسائط تخزين رقمية.

-مسرح افتراضي(رقمي): ويقع داخل العالم الافتراضي، ويحتوي على البيانات الرقمية التي توجد داخل الحاسوب الآلي وشبكة الإنترنت، في ذاكرة القرص الصلب الموجود بداخله (Steve,2006:p.37).

وعملية الانتقال إلى المسرح الافتراضي لا يتطلب بالضرورة أن يكون عبر العالم المادي،

وإنما يكون في الغالب عبر العالم الافتراضي، حيث يكون بمقدور المحقق أن يجري المعاينة وهو متواجد في مقر عمله عبر الحاسوب الموضوع في جهة عمله، كما يمكنه إجراء المعاينة عن طريق اللجوء إلى مقر مزود خدمات الإنترنت أو أحد بيوت الخبرة القضائية أو الاستشارية (بن يونس،2004م، ص:895).

الفرع الثاني

التفتيش القضائي

التفتيش هو أحد إجراءات التحقيق المهمة في كشف الحقيقة لأنه في أغلب الأحوال يسفر عن وجود أدلة مادية ترجح نسبة الجريمة إلى مرتكبها، لذلك يعرف التفتيش بأنه «البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها ويجب أن يكون للتفتيش سند من القانون»(إبراهيم،2009م، ص:182).

ولأن إجراء التفتيش من سلطة التحقيق فقد منحت المادة (43) من نظام الإجراءات الجزائية السعودي سلطة تفتيش المتهم لرجل الضبط الجنائي، ويقابلها المادة (51) من قانون الإجراءات الجزائية الإماراتي التي منحت هذه السلطة لمأمور الضبط القضائي.

وبالنظر لكون محل التفتيش مكونات وشبكات الحاسوب الآلي فإنه يثار هنا تساؤل حول مدى قابلية هذا المحل للتفتيش؟ وهو ما سوف يتناوله الباحث على النحو التالي:

أ-تفتيش مكونات للحاسوب الآلي المادية:

المكونات المادية هي عبارة عن مجموعة من الوحدات المتصلة مع بعضها على نحو يجعلها تعمل كمنظومة متكاملة، وتتمثل في وحدات الإدخال مثل الفأرة ولوحة المفاتيح، ووحدات الإخراج مثل وحدة الذاكرة وشاشة الحاسوب الآلي، بالإضافة للطابعة (عبد المطلب،2014م، ص:26).

وبناء على ذلك لن يكون هناك أي صعوبة عند معاينة المكلف بالتفتيش لمسرح الجريمة الواقعة لمكونات الحاسوب الآلي المادية، نظراً لعدم وجود ثمة تعارض بين تفتيش مكون الحاسوب المادي مع المفهوم التقليدي للتفتيش.

ب-تفتيش مكونات الحاسوب الآلي المعنوية:

المكونات المعنوية هي عبارة عن مجموعة برامج وأساليب متصلة بتشغيل وحدة معالجة البيانات، ومقسمة إلى كيانات أساسية تضم البرامج الضرورية لتشغيل واستخدام جهاز الحاسوب الآلي، وكيانات تطبيقية تضم برامج تساعد المستخدم على تنفيذ مهام معينة (عبد المطلب،2014م، ص:25).

وقد ثار خلاف فقهي بشأن مدى جواز تفتيش مكونات الحاسوب الآلي المعنوية، فذهب الرأي الأول في الفقه إلى جواز تفتيش مكونات الحاسوب المعنوية، واستند في ذلك إلى عموم نصوص التفتيش، وذلك من خلال

توسيع تفسير عبارة ضبط «الأشياء» لتشمل مكونات الحاسوب الآلي المادية والمعنوية (إبراهيم،2009م، ص:197). ومن ذلك ما تقضي به المادة (46) من نظام الإجراءات الجزائية السعودي من أنه إذا ظهر أثناء التفتيش وجود أشياء تفيد في كشف الحقيقة وجب على الضبط الجنائي ضبطها، ويقابلها المادة (55) من قانون الإجراءات الجزائية الإماراتي التي تقضي بأنه إذا ظهرت عرضاً أثناء التفتيش أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى، قام مأمور الضبط القضائي بضبطها.

وقد أحسن كل من المنظم السعودي والمشرع الإماراتي صنعاً بوضع كلمة أشياء بنص المادتين المذكورتين حتى تشمل الأدوات ووسائل الاتصال الإلكترونية التي تمثل أدلة أو تشتمل عليها وتفيد في كشف الجرائم ومرتكبيها مثل جهاز الحاسوب الآلي والأقراص المغناطيسية وكلمات المرور وبرامج تقنية ومعلومات مخزنة بذاكرة الحاسوب. ومن ثم فإن نص هذه المادة يجب تفسيره على أنه يسمح بتفتيش مكونات الحاسوب الآلي المعنوية.

وعلى النقيض من ذلك ذهب رأي آخر في الفقه إلى أنه إذا كانت الغاية من التفتيش ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على مكونات الحاسوب الآلي غير المحسوسة (المعنوية) (إبراهيم،2009م، ص:197).

ونخلص من ذلك، أنه يجب أن يتضمن كل من النظام السعودي والقانون الإماراتي نصاً صريحاً مفاده أن تفتيش الحاسوب الآلي يجب أن يشمل المواد التي تم معالجتها عن طريقه وبياناته.

ج-تفتيش شبكات الحاسوب الآلي «التفتيش عن بعد»:

في حال وقوع جريمة معلوماتية نجد أن رجال الضبط الجنائي يواجهون صعوبات عند القيام بأعمال التفتيش المتعلقة بهذه الجريمة، وذلك بسبب أن البيانات التي تشتمل على أدلة تتوزع عبر شبكات الحاسوب الآلي في أماكن بعيدة عن الموقع المادي الذي يجرى فيه التفتيش، وإن كان بالإمكان الوصول إليها من خلال الحاسوب المأذون بتفتيشه، كما قد يقع الموقع الفعلي للبيانات ضمن الاختصاص القضائي لدولة أخرى. وعلى هذا الأساس يجب التمييز بين الفرضين التاليين:

الفرض الأول: اتصال الحاسوب الآلي للمتهم بحاسوب موجود في مكان آخر داخل الدولة:

في هذا الفرض يكون الحاسوب الآلي للمتهم أو المشتبه فيه متصلاً بحاسوب آلي آخر أو توجد نهاية طرفية لهذا الجهاز في مكان مختلف داخل الدولة (سعيداني،2013م، ص:149)، وبناء على هذا الفرض الذي يشكل عائقاً

أمام الجهة المختصة بالتفتيش وضبط الدليل الجزائي الرقمي، **يرى الباحث** أنه يمكن حل مشكلة تفتيش جهاز حاسوب آلي مرتبط بجهاز الحاسوب المأذون بتفتيشه والموجود داخل الدولة من خلال إعمال حكم المادة (81) من نظام الإجراءات الجزائية السعودي التي تنص على أنه « للمحقق أن يفتش المتهم وله تفتيش غير المتهم إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة». وبناء على ذلك يمكن مد نطاق التفتيش الذي كان محله جهاز الحاسوب الآلي للمتهم إلى جهاز آخر مرتبط به إذا كانت المعلومات المخزنة فيه يتم الدخول إليها في هذا الجهاز من خلال جهاز المتهم محل التفتيش.

الفرض الثاني: اتصال الحاسوب الآلي للمتهم بحاسوب موجود في مكان آخر خارج الدولة:

في هذا الفرض يقوم مرتكبو الجريمة المعلوماتية بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة بغرض عرقلة سلطة التحقيق في الحصول على الأدلة (إبراهيم،2009م، ص:382)، **ويرى الباحث** أن حل مشكلة تفتيش أنظمة الحاسوب الآلي العابر للحدود لابد أن يكون بموجب اتفاقية دولية تجيز امتداد التفتيش خارج الدولة أو وجود إذن صادر من الدولة الأخرى في إطار التعاون بين الدول في مجال مكافحة الجريمة المعلوماتية، ومن ثم لن يسمح بإجراء التفتيش العابر للحدود في ظل عدم وجود اتفاقية إذن بذلك صادر من دولة أخرى. وفي هذا الصدد أجازت المادة (32) من الاتفاقية الأوروبية بشأن جرائم الإنترنت لعام 2001، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون الحصول على إذنها في حالتين: **الأولى** إذا تعلق التفتيش بمعلومات متاحة لعامة الناس، **والثانية** إذا وافق على التفتيش حائز هذه المعلومات.

وانطلاقاً مما سلف فإنه على الرغم من أن كلاً من المنظم السعودي والمشرع الإماراتي لم ينظما إجراءات تفتيش الحاسوب الآلي وشبكات المعلومات إلا أنه غالباً ما تتخذ ذات الإجراءات التي نظماها للبحث عن الأدلة التقليدية، مع إتباع المبادئ العامة في التشريعات.

المطلب الثاني

الإجراءات التقنية لجمع الدليل الرقمي

بما أن المعلومات في البيئة الافتراضية ليست دائماً ساكنة، بحيث يمكن أن تكون متحركة عبر شبكة من الشبكات المتحركة، فإن ذلك يحتم أن يتلاءم الإجراء مع طبيعة المعلومات محل هذا الإجراء، مما يتطلب ذلك بيان الإجراءات المتعلقة بالبيانات الساكنة (الفرع الأول) والإجراءات المتعلقة بالبيانات المتحركة (الفرع الثاني).

الفرع الأول

الإجراءات المتعلقة بالبيانات الساكنة

تتمثل الإجراءات المتعلقة بالبيانات الساكنة في التحفظ العاجل على هذه البيانات (أولاً)، ثم الأمر بتقديم البيانات الشخصية الرقمية المتعلقة بالمستخدم (ثانياً).

أولاً: الأمر بالتحفظ العاجل على المعلومات المخزنة

التحفظ العاجل هو إجراء أولي أو تمهيدي الغرض منه هو محاولة الاحتفاظ بالبيانات خشية فقدانها. ويقصد به توجيه السلطة المختصة لمقدمي الخدمات في مجال الاتصالات الإلكترونية بالتحفظ على معلومات إلكترونية مخزنة في حوزته أو تحت سيطرته، في انتظار إجراءات نظامية أخرى (بن قارة،2009م، ص:98).

وفي هذا الصدد نصت الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست لسنة 2001) على ضرورة أن تأمر الدول الأطراف في هذه الاتفاقية مقدمي الخدمات في مجال الاتصالات الإلكترونية لديها بالتحفظ العاجل على البيانات المخزنة بواسطة نظام معلوماتي، خلال مدة 90يوماً، كحد أقصى قابلة للتمديد، طالما وجدت أسباب تدعو للاعتقاد أن هذه المعلومات معرضة للفقد أو التغير.

وعلى غرار ذلك نصت المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة2012، على إلزام من بحيازته أو سيطرته بيانات تقنية مخزنة بحفظها وسلامتها لمدة 90 يوماً كحد أقصى قابلة للتمديد، بغية تمكين السلطات المختصة بالبحث والتقصي.

ويتبين مما سبق، أن إجراء حفظ البيانات يعد أداة تحقيق مستحدثة في إطار مكافحة الجرائم المعلوماتية، فهو يتلاءم مع طبيعة هذه الجرائم من حيث قابلية البيانات فيها للمحو والفقد بسرعة.

وقد نص على هذا الإجراء نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، في الفقرة (2) من المادة (18) منه، على أنه «على جهة التحكم الاحتفاظ بالبيانات الشخصية حتى بعد انتهاء الغرض من جمعها في الحالتين الآتيتين:

أ-إذا توافر مسوغ نظامي يوجب الاحتفاظ بها مدة محددة، وفي هذه الحالة يجرى إتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول.

ب-إذا كانت البيانات الشخصية متصلة اتصالاً وثيقاً بقضية منظورة أمام جهة قضائية وكان الاحتفاظ بها مطلوباً لهذا الغرض، وفي هذه الحالة يجري إتلافها بعد استكمال الإجراءات القضائية الخاصة بالقضية». وهذا الإجراء

يفرضه مسوغ نظامي محدد واعتبارات التعاون مع الجهات القضائية التي تبرر الاحتفاظ بتلك البيانات لمدة محددة.

ثانياً: الأمر بتقديم البيانات الشخصية الرقمية المتعلقة بالمستخدم

الأصل أن البيانات الشخصية الرقمية المتعلقة بمستخدم شبكة الإنترنت بيانات تدخل في إطار الحق في الخصوصية الذي تحميه التشريعات الوطنية والاتفاقيات الدولية، إلا أن بعض التشريعات تسمح للمحققين القضائيين أن يصدروا أوامر للأشخاص بتسليم ما بحوزتهم من أشياء لتقديمها كأدلة ومن بينها البيانات الشخصية المتعلقة بالمستخدم.

فنجد أن المنظم السعودي أجاز للمحقق الاطلاع على البيانات الشخصية الرقمية بهدف الحصول على الدليل الجزائي الرقمي، حيث نصت المادة (85) من نظام الإجراءات الجزائية، على أنه « إذا توافرت لدى المحقق أدلة على أن شخصاً معيناً يحوز أشياء لها علاقة بالجريمة التي يحقق فيها، فيستصدر أمراً من رئيس الدائرة التي يتبعها بتسليم تلك الأشياء إلى المحقق، أو تمكينه من الاطلاع عليها، بحسب ما يقتضيه الحال «. كما أجاز ذلك المشرع الإماراتي بموجب المادة (78) من قانون الإجراءات الجزائية الاتحادي «لعضو النيابة أن يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه...».

أما بالنسبة لاتفاقية بودابست فقد نصت في المادة (18) منها على أنه « يجوز للدول الأطراف في تلك الاتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم البيانات المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته « ويشترط في هذه البيانات أن تكون مخزنة، ويستثنى من ذلك البيانات المتعلقة بحركة ومحتوى البيانات ذات العلاقة باتصالات مستقبلية حيث تندرج ضمن البيانات المتحركة التي سيتم تناولها فيما بعد.

وقد حددت الاتفاقية المقصود بتلك البيانات، وهي: البيانات المتعلقة بنوع خدمة الاتصال المشترك فيها الشخص والوسائل الفنية لتحقيقها، العنوان البريدي أو الجغرافي ورقم هاتف المشترك، ورقم دخول المستخدم للحصول على تلك الخدمة والفواتير المرسلة إليه، وأي بيانات متعلقة بطريقة الدفع (مثل بطاقة الائتمان أو حسابه البنكي)، أو أي بيانات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين المستخدم ومقدم الخدمة (عطا الله،2007م، ص:161).

ويتبين مما سبق، أن المستخدم لا يتمتع بالحق في الخصوصية بالنسبة لهذه النوعية من البيانات مادامت تفيد كدليل في جريمة معينة ارتكبت بالفعل.

الفرع الثاني

الإجراءات المتعلقة بالبيانات المتحركة

تتجسد الإجراءات المتعلقة بالبيانات المتحركة في اعتراض الاتصالات الإلكترونية، والمقصود بهذا المراقبة الإلكترونية أثناء عملية بثها، وليس الحصول على اتصالات إلكترونية مخزنة.

وفي هذا الشأن يثار التساؤل حول طبيعة البريد الإلكتروني غير المفتوح والمنتظر في صندوق خطابات مقدم خدمات الإنترنت حتى يقوم الشخص المرسل إليه بعملية إدخاله في نظامه المعلوماتي (أي استرداده)، فهل يمكن اعتبارها بيانات مخزنة وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات الساكنة؟ أم أنها بيانات في مرحلة النقل والتحويل؟ ومن ثم تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة، والمتمثلة في اعتراض الاتصالات الإلكترونية، ومن ثم لا يتم الحصول عليها إلا بناء على إذن من السلطة المختصة.

وفي هذا الصدد ميزت اتفاقية بودابست بين نوعين من البيانات المعلوماتية محل الاعتراض، وهما البيانات المتعلقة بالمرور، والبيانات المتعلقة بمحتوى الاتصال. وذلك من ناحية درجة المساس بالحق في الخصوصية لكل من النوعين، حيث تزداد بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن ثم ضمانات أكثر عند تجميع محتوى البيانات في الزمن الفعلي عن حركة البيانات سواء من حيث الجرائم التي من أجلها يتم اتخاذ هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة. كما أكدت اتفاقية بودابست هذا التمييز من خلال وضع كل إجراء تحت عنوان خاص، فخصت تجميع حركة البيانات بعنوان «التجميع في الزمن الفعلي لبيانات المرور»، أما تجميع محتوى البيانات فجاء تحت عنوان «اعتراض محتوى البيانات»(بن قارة،2009م، ص:105).

وعلى خلاف ذلك نجد أن بعض تشريعات الدول تضع مفهومًا موحدًا لكل من تجميع حركة البيانات ومراقبة محتوى البيانات، دون ثمة تمييز بينهما، ومن ثم يسري عليهما نفس الضمانات الخاصة عند اتخاذ أي من الإجراءين، بغض النظر عن الحساسية التي تحاط بها مراقبة محتوى البيانات، ومرد ذلك أن النظام لا يميز بين نوعية البيانات عند وضعه الضمانات المتعلقة بمراقبتها، حيث لا يوجد لديه اختلاف حول المصلحة في الخصوصية أو لتشابه إجراءات التجميع الرقمي، ومن هذه التشريعات نظام الإجراءات الجزائية السعودي فقد نص على تحديد شروط اتخاذ اجراء المراقبة، حيث جاء في المادة (56) منه، على أنه « للرسائل البريدية والبرقية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة، فلا يجوز الاطلاع عليها أو مراقبتها إلا بأمر مسبب ولمدة محددة،

وفقاً لما ينص عليه هذا النظام». وقد أشارت المادة (36) من اللائحة التنفيذية للنظام إلى أنه « يشمل حكم المادة (السادسة والخمسين) وسائل التواصل الإلكترونية الحديثة غير العلنية». مما يعني أن إجراء المراقبة يسري على الاتصالات الإلكترونية أي التي تتم عن طريق الكمبيوتر والتي تتخذ شكل البريد الإلكتروني أو شكل المحادثة الفورية، بالإضافة إلى الاتصالات السلكية واللاسلكية.

ونصت المادة (57) من النظام نفسه على أنه «لرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل والخطابات والمطبوعات والطرود، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها، متى كان لذلك فائدة في ظهور الحقيقة في جريمة وقعت، على أن يكون الأمر أو الإذن مسبباً ومحدداً بمدة لا تزيد على عشرة أيام قابلة للتجديد وفقاً لمقتضيات التحقيق».

وفي هذا الصدد جاء قانون الإجراءات الجزائية الاتحادي الإماراتي رقم 35 لسنة 1992 والمعدل بالقانون رقم 28 لسنة 2020 ووضع شروطاً معينة للمراقبة في المادة (75) إذ نص على أنه: « لعضو النيابة العامة أن يفتش المتهم ولا يجوز له تفتيش غير المتهم أو منزلاً غير منزله إلا إذا اتضح من أمارات قوية أنه حائز لأشياء تتعلق بالجريمة. ويجوز له بموافقة النائب العام أن يضبط لدى مكاتب البريد جميع المكاتبات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات، وأن يراقب ويسجل المحادثات بما في ذلك السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك».

ويتضح من نص هاتين المادتين أن كلاً من المنظم السعودي والمشرع الإماراتي استلزما توافر شروطاً محددة لإجراء المراقبة. والعلة من ذلك، أن هذا الإجراء فيه استثناء على القاعدة العامة المتمثلة في حرمة الحياة الخاصة للفرد وسرية مراسلاته ومحادثاته، نظراً للفائدة المرجوة من إجراء المراقبة وهي إظهار الحقيقة بكشف غموض جريمة ارتكبت خاصة الجريمة المعلوماتية وضبط مرتكبيها، مما يعد ذلك ضمانة لازمة لمشروعية هذا الإجراء.

المبحث الثالث

سلطة المحكمة المختصة في قبول الدليل الرقمي

يعتبر الوصول إلى مرحلة المحاكمة من أهم المراحل التي تمر بها إجراءات الدعوى الجزائية، لأنها المرحلة الحاسمة لأطراف الدعوى، فهي مرحلة الجزم واليقين بتوافر الدليل الذي تقتنع به المحكمة إما بالبراءة أو الإدانة، وعليه فإن المحكمة الجزائية بما لها من سلطة أن تتأكد من توافر مشروعية الدليل

الرقمي ويقينيته في الإثبات (المطلب الأول) وضوابط قبول الدليل الرقمي كوسيلة إثبات (المطلب الثاني).

المطلب الأول

مشروعية الدليل الرقمي ويقينيته في الإثبات

يخضع الدليل الجزائي الرقمي مثل باقي الأدلة الجزائية لقواعد الإثبات الجزائي من حيث مشروعيته (الفرع الأول) ومن حيث يقينية صحته وسلامته (الفرع الثاني).

الفرع الأول

مبدأ مشروعية الدليل الرقمي في الإثبات الجنائي

مما لا شك فيه أن مبدأ المشروعية في الدليل يستقيم به البنيان النظامي وينعكس بشكل إيجابي على قواعد الإثبات الجزائي والتي تخضع بالتالي لمبدأ المشروعية، ومسألة مشروعية الدليل تعد أول المسائل التي تنظر لها المحكمة الجزائية، قبل حتى أن يخضع لتقديرها، لذلك لابد أن يكون الدليل الرقمي مشروعاً لضمان توافر حجيته النظامية، وتتمثل مشروعية الدليل الجزائي الرقمي في مشروعية وجوده ومشروعية الحصول عليه.

أولاً: مشروعية وجود الدليل الرقمي:

ويقصد به اعتراف المنظم بالدليل الجزائي الرقمي، بمعنى أن النظام يجيز للمحكمة الاستناد إليه لتكوين عقيدتها للحكم بالإدانة، ويتحدد موقف الأنظمة من قبول الدليل الجزائي الرقمي من عدمه بحسب طبيعة نظام الإثبات السائد في الدولة، ويعد من المبادئ المهمة في عملية الإثبات هو أن يكون للمحكمة الجزائية كامل الحرية بالاقتناع بأي دليل يؤدي إلى إثبات الجريمة أو نفيها، إعمالاً في ذلك لمبدأ « حرية القاضي الجزائي في الاقتناع» (الرشودي،2008م، ص:334).

وأكدت هذا المبدأ المادة (170) من نظام الإجراءات الجزائية السعودي، التي جاءت على أنه « للمحكمة أن تصدر أمراً إلى أي شخص بتقديم شيء في حيازته، وأن تأمر بضبط أي شيء متعلق بالقضية إذا كان في ذلك ما يفيد في ظهور الحقيقة». وعلى غرار ذلك نصت المادة (179) من قانون الإجراءات الجزائية الاتحادي الإماراتي، على أنه «للمحكمة أن تأمر من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لإظهار الحقيقة».

ويتبين مما سبق، أن كلًا من المنظم السعودي والمشرع الإماراتي لم يعتمدا نهج وضع نصوص تتضمن أدلة للإثبات الجزائي بعينها، كما لم يضعا نصوص تقييد من سلطة المحكمة سواء في قبولها أو رفضها لأي دليل رقمي وعليه، فإن الدليل الرقمي يشكل دليلًا فنيًا مشروعًا وفقًا لمبدأ المشروعية ومن ثم يقبل للأخذ به في الإثبات الجزائي.

ثانياً: مشروعية الحصول على الدليل الجزائي الرقمي

الدليل الرقمي كغيره من الأدلة التي يتم تقديمها للمحكمة الجزائية لتبني عليه حكمها ومن ثم لابد أن يتم الحصول عليه بشكل مشروع أي وفق القواعد التي أقرها وحددها النظام وعليه فإنه إذا تم جمع الأدلة الرقمية من الأجهزة الإلكترونية بشكل غير مشروع ومخالف للقواعد الإجرائية التي حددها النظام فلا يعتد بها ولا تصلح لبناء الإدانة عليها للإثبات الجزائي، وعلى الرغم من أن كل من المنظم السعودي والمشرع الإماراتي لم ينصا صراحة أو ضمناً على مراعاة مبدأ النزاهة عند البحث عن الدليل الرقمي إلا أن الاجتهادات الفقهية والقضائية حرصت على أن تكون عملية جمع الأدلة الجزائية أو التنقيب عليها أن تتم بطريقة نزيهة وشرعية (الدليمي،2012م، ص:193). إلا أنه في المقابل قد أقر كل من المنظم السعودي والمشرع الإماراتي مجموعة من الإجراءات الواجبة الإتباع عند استقصاء الأدلة الجزائية سواء التقليدية أو الرقمية، وألزمت رجال الضبط الجنائي أو القضائي وأعضاء النيابة العامة بإتباعها وتطبيقها بشكل كلي وإلا أصبح الإجراء باطل، ومن ثم لا تأخذ به المحكمة الجزائية مهما كانت دلالته قوية على الجريمة وذلك مرده عدم مشروعيته.

الفرع الثاني

مبدأ يقينية الدليل الرقمي في الإثبات الجنائي

تكمن أهمية يقينية الدليل الجنائي في اتصاله المباشر بما ستؤول إليه المحكمة في إصدار الحكم الجزائي، لذا يتطلب الأمر بيان مفهوم يقينية الدليل الرقمي، بالإضافة إلى بيان القواعد التي تحكمها.

أولاً: مفهوم مبدأ يقينية الدليل الجزائي الرقمي في الإثبات الجزائي

يقصد بهذا المبدأ يقين المحكمة واقتناعها بالأدلة المقدمة له كحجة ثابتة وقطعية. وأما اليقين في مجال الأدلة الجزائية الرقمية، فإنه يشترط في هذا النوع من الأدلة نفس ما يشترط في باقي الأدلة الجزائية، بحيث أن تكون غير قابلة للشك حتى يمكن الحكم بإدانة المتهم، وذلك لأنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا في حال وصول اقتناع القاضي إلى حد اليقين (ثنيان،2012م، ص:77).

ونجد أن بعض التشريعات تضع شروطاً لتحقق اليقين بالأدلة الرقمية أياً كانت، ومنها نظام الإثبات السعودي الذي اشترط في المادة (60) منه أن «يقدم الدليل الرقمي بهيئته الأصلية، أو بأي وسيلة أخرى رقمية أخرى، وللمحكمة أن تطلب تقديم محتواه مكتوباً، متى كانت طبيعته تسمح بذلك».

كما نصت المادة (64) من الأدلة الإجرائية

لنظام الإثبات السعودي على أنه» يقدم محتوى الدليل الرقمي مكتوباً -إن كانت طبيعته تسمح بذلك-وفي حال منازعة الخصم، يقدم الدليل الرقمي على النحو الآتي:

1- بهيئته الأصلية؛ متى أتيح للمحكمة الاطلاع عليه مباشرة.

2- بوسيلة رقمية أخرى؛ متى قدمت نسخة منه، بما في ذلك تقديمه في وسائط رقمية، وعلى مقدم الدليل الرقمي الاحتفاظ بالدليل بهيئته الأصلية.»

ثانياً: القواعد التي تحكم مبدأ يقينية الدليل الرقمي في الإثبات الجزائي

أن ما تتمتع به المحكمة الجزائية من سلطة في تقدير الأدلة الرقمية لا تتسع لتشمل هذه الأدلة، فثقافة قضاتها القانونية لا تمكنهم من إدراك حقيقة الأدلة الرقمية، فهذه الأدلة من حيث قوتها الثبوتية يتوافر فيها مبدأ اليقين. ومن ثم لا تترك لتقدير المحكمة، ولذلك تم وضع قواعد محددة من طرف مختصين تحكم يقينيته (الطوالبة،2007م، ص:11)، وذلك للتأكد من سلامته من التلاعب به وصحة الإجراءات المتبعة في الحصول عليه، وهي:

1-تقييم الدليل الرقمي بالنسبة لخلوه من التلاعب:

من المحتمل أن يتعرض الدليل الرقمي للتلاعب، ويعبر عن واقعة بشكل يخالف الحقيقة دون أن يكون بمقدور غير المتخصص اكتشاف هذا التلاعب، وعليه فإن مضمون تقييم الدليل الجزائي الرقمي هو التأكد من سلامته من التلاعب به عبر إتباع مجموعة من الوسائل أهمها استعمال عملية تحليل تناظري رقمي، من خلال مضاهاة الدليل الرقمي (الأصلي) المقدم للقضاء بالنسخة المستخرجة (عبد المطلب،2006م، ص:125).

ولذلك فإنه لضمانة سلامة الدليل الرقمي من أي عبث يدمره أو يجعله يثبت وقائع غير صحيحة يوصي المتخصصين بالحفاظ على النسخة الأصلية منه، واستغلال الميزة التي يتمتع بها وهي استخراج العديد من النسخ المطابقة له (Debra,2006: p.552).

2-تقييم الدليل الرقمي من حيث صحة الإجراءات المتبعة في الحصول عليه:

أثناء اتخاذ بعض الإجراءات التقنية للحصول على الدليل الجزائي الرقمي، يمكن أن تعتري هذه الإجراءات أخطاء قد تشكك في صحة النتائج، ويعود ذلك لسببين:

أ-أخطاء في استخدام الأدوات الفنية: مسبباتها الاستعمال الخاطئ للشفرة في استخراج الدليل أو استخدام مواصفات فنية غير سليمة.

ب-أخطاء في استخلاص الدليل الرقمي: مسبباتها اتخاذ قرارات باستخدام أداة تقل نسبة صحتها عن 10% ويحدث هذا في الأغلب

الأعم نتيجة معالجة بيانات الدليل الرقمي، بطريقة مغايرة للطريقة الأصلية التي أنشئت بها بيانات الدليل الرقمي.

وعلى أساس ذلك، ينبغي في هذه الحالة الاعتماد على اختبارات محددة كوسيلة للتأكد من صحة الإجراءات المتبعة في الحصول على الدليل الرقمي. (عبد المطلب،2006م، ص:127).

ويتبين مما تقدم، أن التحقق من يقينية الدليل الرقمي، لا تتعلق بمضمونه كدليل، وإنما بعدة عوامل تستقل عنه. ولكنها تلعب دوراً كبيراً في اكتمال حجيته في الإثبات الجزائي، وهذا بسبب طبيعته الفنية. وتجدر الإشارة إلى أنه على الرغم من أن المنظم السعودي -على خلاف المشرع الإماراتي-لم يتناول صراحة الأدلة الرقمية في الإطار الجزائي لها، إلا أن إجراءات استخلاصها تشبه إلى حد كبير إجراءات استخلاص الأدلة التقليدية، وتنظم تلك المسألة مجموعة من القواعد الأخلاقية والمبادئ العامة لإضفاء المشروعية على هذا الدليل لضمان حجيته أمام القضاء، كما سيأتي لاحقاً.

المطلب الثاني

ضوابط قبول الدليل الرقمي كوسيلة إثبات

تعد مرحلة قبول الدليل الجزائي الرقمي الخطوة الثانية التي تلي البحث عنه وتقديمه من قبل جميع الأطراف ومسألة قبول هذا الدليل وتقديره لا ينال منها سوى اقتناع المحكمة بها وإخضاعه للتقدير القضائي، وهو ما سوف يوضحه الباحث من خلال تناول مبدأ حرية الإثبات الجزائي باعتباره أساساً لقبول الدليل الرقمي (الفرع الأول) وبيان الأسس النظامية لقبول الدليل الجزائي الرقمي (الفرع الثاني). والتطرق لمبدأ حرية الاقتناع القضائي والنتائج المترتبة على تطبيقه (الفرع الثالث).

الفرع الأول

مبدأ حرية الإثبات الجزائي أساساً لقبول الدليل الرقمي

إن إعمال مبدأ الإثبات يتميز بفاعلية دور المحكمة، إذ يجعلها تتمتع بدور إيجابي في إظهار الحقيقة تجاه الأدلة المطروحة للنقاش، ويبدو هذا الدور عبر حريتها في توفير الأدلة المناسبة والضرورية للفصل في الدعوى، وحريتها في قبول الأدلة التي يمكن أن تتولد منها قناعة المحكمة بما في ذلك الدليل الرقمي، كذلك تتمتع بذات الحرية عند تقدير القيمة الإقناعية للأدلة حسبما تتكشف لوجدانها (أحمد،2007م، ص:122).

فمن حق المحكمة الجزائية أن تبحث وتنقب عن الحقيقة وليس لها أن تقتنع بما يقدمه إليها أطراف الدعوى، وإنما على المحكمة أن تبحث بنفسها عما يعتقد أنه مفيد في إظهار واكتشاف الحقيقة في كل نطاقها ذلك أن الأضرار الناجمة عن الجريمة ليست أضراراً فردية فحسب،

وإنما أضرار عامة تهدد مصالح المجتمع في أمنه واستقراره. ولذلك فإن للمحكمة الجزائية أن تأمر باتخاذ ما تراه مناسباً وضرورياً للفصل في الدعوى.

وتخضع المحكمة الجزائية لسلطة المحكمة العليا التي لا تقر رأيها إذا تبين لها عدم صحة الحكم، وهو أكدته المحكمة العليا السعودية في قرارها رقم (34) وتاريخ 1439/9/23هـ، باعتماد الدليل الرقمي واعتباره حجة معتبرة في الإثبات، شريطة أن يكون سليماً من العوارض، وأن قوته وضعفه تكون على حسب ظروف الواقعة وملابساتها المحيطة بها وما يأتي من قرائن، وقد قررت المحكمة هذا المبدأ القضائي بعد دراسته والاطلاع على البحوث التي أعدت فيه، وذلك بحكم اختصاصها في تقرير المبادئ القضائية، بعد أن ورده إليها خطاب وزير العدل بشأن تعزيز حجية الأدلة الرقمية لدى جهات التحقيق والقضاء، **ويرى الباحث** أن تقرير المحكمة العليا لهذا المبدأ القضائي يعد بمثابة اعتراف بحجية الوسائل الرقمية الحديثة في الإثبات بعد أن كان القضاء يشكك في حجيتها ويرفضها، وهذا القرار يعد دلالة على مواكبة القضاء السعودي للتطور الحاصل في مجال الجرائم المستحدثة وطرق اكتشافها في مجال تقنية المعلومات، ولا يوجد قرار مماثل لهذا القرار في القضاء الإماراتي.

وتجدر الإشارة إلى أن النظم القانونية تختلف من حيث موقفها بالنسبة للأدلة التي تقبل كأساس للحكم بالإدانة وفقاً للاتجاه الذي تتبناه، فهناك ثلاث مذاهب مختلفة، الأول نظام الإثبات المقيد، والثاني نظام الإثبات الحر، والثالث نظام الإثبات المختلط.

أولاً: مذهب الإثبات المقيد:

وفقاً لهذا المذهب نجد أن النظام هو الذي يحدد الأدلة التي يجوز للمحكمة اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية للأدلة بحيث يكون دور المحكمة الجزائية في هذا المذهب دوراً سلبياً يقتصر على مجرد فحص الأدلة للتأكد من توافر الشروط التي حددها النظام، فلا سبيل لها للاستناد إلى أدلة أخرى لم ينص عليها صراحة ضمن أدلة الإثبات، وهذا المذهب ينتمي للنظم الانجلوسكسونية مثل بريطانيا وأمريكا (Thomas,2004: p.227). ويؤخذ على مذهب الإثبات المقيد أنه يقيد المحكمة الجزائية على نحو يفقدها سلطتها في الحكم بما يتفق مع الواقع، فتحكم في كثير من الدعاوى بما يخالف قناعتها التي تكونت لديها من أدلة لا يعترف بها المنظم.

ثانياً: مذهب الإثبات الحر:

تتمتع المحكمة وفقاً لهذا النظام بحرية مطلقة بشأن الأدلة المعروضة عليها فلا يلزمها النظام بأدلة معينة للاستناد عليها في تكوين

قناعتها، ونجد هذا المذهب في الأنظمة اللاتينية والمحكمة في هذه النظم تتمتع بدور إيجابي في مقابل انحصار دور المنظم. ومن مزايا هذا المذهب أنه لا يميز بين الأدلة فكل الأدلة تتساوى قيمتها الثبوتية في نظر المنظم، كما يكون للمحكمة سلطة واسعة في استخلاص الأدلة.

وقد أخذ بهذا النظام من قانون الإجراءات الجزائية الاتحادي الإماراتي في المادة (179) [1] نجد أنه جعل إقامة الدليل تتم بكافة طرق الإثبات كمبدأ عام، وكذا للمحكمة الجزائية الحكم في الدعوى وفقاً لقناعتها الشخصية.

ثالثاً-مذهب الإثبات المختلط:

وهذا المذهب يقف وسطاً بين المذهبين السابقين، إذ يكفل للمحكمة الجزائية دوراً في عملية الإثبات على شكل مجموعة من الاستثناءات على هذا المبدأ بهدف الوصول للغاية التي يسعى إليها المنظم وهي نسبة الحقوق لأصحابها.

ففي هذا المذهب لا تتقيد المحكمة الجزائية بأدلة محددة تستند عليها لتكوين قناعتها، وإن كان النظام قد خصص أدلة محددة لبعض الجرائم، والتي يلزم المحكمة بالتقيد بها. كما هو الحال في نظام الإثبات السعودي، حيث يكون الإثبات مقيداً بالنسبة لجرائم الحدود، وحراً بالنسبة للجرائم التعزيزية، نظراً لقيامه على الشريعة الإسلامية التي تأخذ بمذهب الإثبات الحر كلما كان حقاً للعبد، أما ما يكون حقاً لله عز وجل فإنها تأخذ بمذهب الإثبات المقيد.

الفرع الثاني

بيان الأسس النظامية لقبول الدليل الجزائي الرقمي

الدليل الجزائي الرقمي يجب أن يتوافر فيه من الشروط والمصداقية ما يجب توافره في غيره من الأدلة الجزائية، كما هناك أسساً يقوم عليها هذا النوع من الأدلة. ومن هذه الأسس عدم المساس بخصوصية الفرد، فهناك العديد من الأدلة الرقمية قد ساعد في الحصول عليها استخدام وسائل تقنية متطورة، مثل، استعمال كاميرات التصوير والفيديو وأجهزة الهواتف النقالة، فكما لهذه الوسائل إيجابيات وفوائد، لتسهيل مهمة الكشف عن الحقيقة فإنها قد تعصف بخصوصية وحرية الأفراد، إذا لم يحسن استعمالها.

وإذا كانت القاعدة العامة تحظر استعمال مثل هذه الوسائل إذا كان في ذلك مساس بحريات الأفراد كما تمنع أي تدخل غير نظامي يؤدي إلى المساس بحرمة الحياة الخاصة، ومن ضمنها المراسلات بكل أنواعها والاتصالات وغيرها من وسائل الاتصال الحديثة، وهو ما كفله النظام الأساسي للحكم السعودي

1. تنص المادة (179) من قانون الإجراءات الجزائية الاتحادي الإماراتي، على أنه» للمحكمة أن تأمر من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لإظهار الحقيقة».

الصادر بالمرسوم الملكي رقم (أ/90) بتاريخ 1412/8/27هـ، من خلال المادة (40) منه التي تنص على أنه « المراسلات البرقية، والبريدية، والمخابرات الهاتفية وغيرها، من وسائل الاتصال، مصونة ولا يجوز مصادراتها، أو تأخيرها، أو الاطلاع عليها، أو الاستماع إليها، إلا في الحالات التي يبينها النظام».

كما نص دستور الإمارات العربية المتحدة الصادر في 2ديسمبر 1971م (المعدل في سنة2009)، في المادة (31) منه، على « حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال وسريتها مكفولتان وفقاً القانون».

وعلاوة على ذلك فإنه إذا ما تم النظر إلى الأمور من الناحية الواقعية نجد أن الحماية المقررة لخصوصية الأفراد وحرمة حياتهم الخاصة ليست مطلقة، وإنما ترد عليها استثناءات قد تمليها دواعي أمنية ونظامية، فاستخدام الجناة الوسائل الرقمية الحديثة في تنفيذ مخططاتهم الإجرامية، جعل الجهات الأمنية تلجأ إلى استخدام نفس الوسائل في الكشف عن الجرائم والتعرف على الجناة ومن ثم ضبط الأدلة التي تحكم ببراءة أو إدانة المتهمين، وهذا ما هو معمول به في أغلب الدول، فأصبح الحاسوب الآلي يستعمل على نطاق واسع كوسيلة لكشف الجرائم وضبط الجناة، وخصوصاً في الجرائم الإرهابية وجرائم الاحتيال الإلكتروني وسرقة البنوك.

وبالمقابل فإن أي إجراء تتخذه السلطات المختصة يجب أن يكون بناء على إذن مسبب، مع ضرورة تحديد المدة النظامية الكافية لمثل هذا الإجراء لكيلا يكون الدليل المستمد منه دليلاً تثار حوله الشكوك في مسألة تعبيره عن الحقيقة، وكذلك لضمان عدم التعسف في استعمال الحقوق من جانب المحكمة الجزائية، إذ ينبغي على المحكمة أن تضمن تحقيق التوازن بين المصالح.

وفي هذا الصدد نصت المادة (56) من نظام الإجراءات الجزائية السعودي على أنه «للرسائل البريدية والبرقية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة، فلا يجوز الاطلاع عليها أو مراقبتها إلا بأمر مسبب ولمدة محددة، وفقاً لما ينص عليه هذا النظام».

ونصت المادة (75) من قانون الإجراءات الجزائية الاتحادي الإماراتي، على أنه «... ويجوز له بموافقة النائب العام أن يضبط لدى مكاتب البريد جميع المكاتبات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق جميع البرقيات، وأن يراقب ويسجل المحادثات بما في ذلك السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك».

ونخلص أنه يجب إتباع إجراءات محددة في استقصاء الأدلة الرقمية بالنسبة للدعاوي

الجزائية وإلا أصبحت الإجراءات فاسدة وبالتالي فساد الأدلة.

الفرع الثالث

مبدأ حرية الاقتناع القضائي والنتائج المترتبة على تطبيقه

الغصن الأول

مبدأ حرية الاقتناع القضائي أساساً لحرية تقدير المحكمة المختصة للدليل الرقمي

السائد في الفقه الجنائي وبالاستناد إلى مبدأ حرية الاقتناع القضائي أن سلطة المحكمة الجزائية في تقدير الدليل الرقمي يحكمها حريتها في الاقتناع، مما يستتبع ذلك حتماً نتيجة مهمة ألا وهي حرية المحكمة الجزائية في تقدير الأدلة (David,1991: p.125).

وهناك العديد من الأسباب التي تسوغ الأخذ بهذا المبدأ نذكر منها ظهور الأدلة العلمية الحديثة وتقدمها مثل تلك المستمدة من الطب الشرعي والتحاليل الطبية والأدلة المستخرجة من الوسائل الرقمية وغيرها. وهذه الأدلة بطبيعتها لا تقبل إخضاع سلطة المحكمة الجزائية لأي قيود بشأنها، بل يتحتم أن يترك أمر تقديرها لمحض اقتناعها، لاسيما وأنها في كثير من الأحوال تتضارب مع باقي أدلة الدعوى، فضلاً عن احتمالية أن يتضارب في شأنها آراء المختصين (حسني،1988م، ص:412).

ويتبين من ذلك أن الدليل الرقمي لا يحظى أمام المحكمة الجزائية بقوة حاسمة في الإثبات، وإنما هو مجرد دليل لا تختلف قيمته ولا تزيد حجته عن غيره من الأدلة، وهذا أثر من آثار المحكمة الجزائية في الاقتناع، وعلى هذا الأساس يصح للمحكمة الجزائية أن تؤسس اقتناعها على الدليل الرقمي كما يصح أن تهدره تبعاً لاطمئنانها، ولا يجوز مطالبة المحكمة أو إلزامها بالاقتناع بالدليل الرقمي ولو لم تكن في الدعوى أدلة سواه.

ولما كان الدليل الرقمي يعتبر تطبيقاً من تطبيقات الدليل العلمي، وذلك بما يتميز به من حياد وموضوعية وكفاءة، مما يجعل اقتناع المحكمة الجزائية أكثر جزماً ويقيناً، حيث يساعده على التقليل من الأخطاء القضائية، والاقتراب إلى العدالة بخطى أوسع، والتوصل إلى الحقيقة بشكل أسرع.

تلك السمات التي يتميز بها الدليل الرقمي قد تدفع البعض(أحمد،2007م، ص:48) إلى الاعتقاد بأن مقدار اتساع نطاق الأدلة العلمية ومن بينها الدليل الجزائي الرقمي بمقدار ما يتضاءل دور المحكمة الجزائية في التقدير، خاصة أمام نقص الخبرة الفنية للمحكمة، ومن ثم فإن مهمتها تصبح شبه آلية، حيث يكون الدور الأكبر للخبراء الذي يسيطرون على عملية الإثبات، ولن يبق أمام المحكمة الجزائية إلا التسليم برأي الخبراء، دون أي تقدير من

جانبها.

ونرى أن الإشكالية التي تثار هنا ليست على درجة كبيرة من الأهمية، خاصة إذا كان نظام الإثبات السائد في الدولة يقوم على تحقيق التوازن بين الاقتناع القضائي والإثبات العلمي، بحيث يعمل بالإثبات العلمي في إطار مبدأ الاقتناع القضائي.

وفي هذا الإطار نص نظام التعاملات الإلكترونية السعودي الصادر بالمرسوم الملكي رقم (م/18) بتاريخ 1428/3/8هـ، في المادة (9) منه على أنه « يقبل التعامل الإلكتروني أو التوقيع الإلكتروني دليلاً في الإثبات إذا استوفى سجله الإلكتروني متطلبات حكم المادة (الثامنة) من هذا النظام»، حيث جاءت المادة (8) بأنه «يعد السجل الإلكتروني أصلاً بذاته عندما تستخدم وسائل وشروط فنية تؤكد سلامة المعلومات الواردة فيه من الوقت الذي أنشئ فيه بشكله النهائي على أنه سجل إلكتروني، وتسمح بعرض المعلومات المطلوب تقديمها متى طلب ذلك».

كذلك نصت الفقرة الثانية من المادة (9) من النظام نفسه، على أنه « يعد كل من التعامل الإلكتروني أو التوقيع الإلكتروني والسجل الإلكتروني حجة يعتد بها في التعاملات وأن كلا منها على أصله (لم يتغير منذ إنشائه) ما لم يظهر خلاف ذلك».

وجاءت المادة (10) من القانون الاتحادي الإماراتي رقم (1) لسنة2006 بشأن المعاملات والتجارة الإلكترونية، ونصت على أنه» لا يحول دون قبول الرسالة الإلكترونية أو التوقيع الإلكتروني كدليل إثبات: أ-أن تكون الرسالة أو التوقيع قد جاء في شكل إلكتروني».

ونصت الفقرة الثانية من المادة نفسها على أنه « في تقدير حجية المعلومات الإلكترونية في الإثبات، تراعى العناصر الآتية:

أ-مدى إمكانية الاعتداد بالطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات إدخال المعلومات، أو إنشائها، أو تجهيزها، أو تخزينها، أو تقديمها، أو إرسالها.

ب-مدى إمكانية الاعتداد بالطريقة التي استخدمت في المحافظة على سلامة المعلومات».

وتستقي الدراسة من النصوص السابقة أن الدليل الجزائي الرقمي في كل من نظام الإثبات السعودي والقانون الاتحادي الإماراتي بشأن مكافحة الشائعات والجرائم الإلكترونية يُعد دليلاً معتبراً ومقبولاً ويمكن الأخذ به في المسائل الجزائية مع إمكانية إعطائه حجية نظامية كاملة وقوة إثبات تعادل الدليل الجزائي المادي.

وبطبيعة الحال فإن تقدير حجية الدليل الرقمي في الإثبات يحتاج لخبرة في استخلاصه من الحاسوب الآلي وإثبات أصليته وأنه لم يخضع لأي تعديل أو تغيير أو إتلاف بأي طريقة كانت.

وتخضع كافة هذه المسائل للسلطة التقديرية للمحكمة الجزائية.

فالأدلة العلمية ومن بينها الدليل الرقمي شأنها شأن باقي أدلة الإثبات تخضع لتقدير قضاة المحكمة الجزائية ومدى تأثيره في الاقتناع الذاتي للمحكمة، وأنه لا يمكن للخبراء مهما كانت دقة نتائجهم وموضوعيتها أن تحتل مكانة المحكمة الجزائية في إيجاد العدالة، والتي يتطلب إيجادها توافر حس مختص لا يدركه غير قضاة المحكمة الجزائية، ويتوافر هذا الحس من خلال التكوين العلمي والقضائي الرفيع، والذي تنهض به الجهات العلمية القانونية بشكل عام والقضائية بشكل خاص، ليتكون معه أساساً رصيناً في التقدير السليم للأدلة. والتي من خلالها تصل المحكمة الجزائية إلى قرارها العادل الذي يكون عنواناً للحقيقة (محمد،2005م، ص:155).

وتماشياً مع ما تم ذكره فإن الأدلة الرقمية لا تتعارض مع سلطة المحكمة الجزائية في تقديرها، بل إن هذه الأدلة ستكفل للمحكمة وسائل فعالة للوصول إلى الحقيقة.

الغصن الثاني

النتائج المترتبة على تطبيق مبدأ حرية الاقتناع القضائي

أقر نظام الإجراءات الجزائية السعودي لطرفي الدعوى مبدأ حرية الإثبات مع حق كل طرف في استخدام كافة وسائل الإثبات بينما تقوم المحكمة الجزائية بتقييم تلك الأدلة، ومن ثم التوصل إلى قناعة معينة بخصوص تلك الأدلة. وإذا كان الأمر ينطبق على الأدلة المادية التقليدية، فإنه بذلك لا تثار أي إشكالية إذا ما طبق على الأدلة العلمية الحديثة ومن ضمنها الدليل الجزائي الرقمي، وعندما تقوم المحكمة الجزائية بتقدير هذا الدليل لا تتطرق إلى قيمته العلمية لأنها حقيقة قاطعة وثابتة، فليس من اختصاص المحكمة مناقشة الأمور العلمية البحتة، وإنما هي مسألة من اختصاص الخبراء في هذا المجال، وبمقدور المحكمة الاستعانة بهم للتعرف على حقيقة هذا الدليل، وأما بالنسبة للظروف والملابسات التي وجد فيها الدليل الجزائي الرقمي فإنها تدخل في نطاق التقدير الذاتي للمحكمة ، فهي من صميم وظيفتها القضائية، بحيث يكون بإمكان المحكمة أن تطرح هذا الدليل إذا تبين لها أن وجوده لا يتفق منطقياً مع ظروف الواقعة وملابساتها، حيث تولد الشبهة لدى المحكمة الجزائية، ومن ثم تقضي في إطار تفسير الشك لصالح المتهم (Wasilk,1993:p.231).

وعلى هذا الأساس، يصح للمحكمة المختصة أن تؤسس اقتناعها على الدليل الرقمي، كما يصح لها أن تطرحه بالرغم من قطعيته من الناحية العلمية، ذلك أن توافر الدليل الرقمي لا يعني أن

المحكمة الجزائية ملزمة بالحكم بموجبه مباشرة سواء بالإدانة أم البراءة، دون بحث الظروف والملابسات المحيطة به، فالدليل الرقمي ليس آلية معدة لتقرير اقتناع المحكمة الجزائية بخصوص مسألة غير مؤكدة، بل هو دليل إثبات قائم على أسس علمية، وللمحكمة النظر إليها في ضوء هذه الظروف والملابسات.

وهذا من دون شك يُظهر مدى خضوع الدليل الرقمي للسلطة التقديرية للمحكمة الجزائية، فإن رأت أن وجوده كافي ومنطقي فباستطاعتها أن تعتمد عليه في إظهار الحقيقة بحيث يمكنها أن تستمد منه اقتناعها في الحكم الذي تنتهي إليه، مادام أن الدليل الرقمي مشروعًا وسليمًا هذا من جانب، ومن جانب آخر أن يكون اقتناع المحكمة الجزائية مبنياً على أدلة مطروحة أمامها في الدعوى.

خاتمة

قامت هذه الدراسة بالبحث حول حجية الدليل الرقمي في الإثبات الجنائي، وأكدت الدراسة أن الدليل الرقمي فرض نفسه كدليل إثبات في المجال الجزائي يتمتع بقوة ثبوتية وحجية نظامية، وبالتالي فإن القاضي الجزائي بإمكانه الاستعانة بالدليل الجزائي الرقمي في الإثبات، هذا نتائج أعرضها في فقرة النتائج، ومن خلال هذه الدراسة (حجية الدليل الرقمي في الإثبات الجنائي في النظام السعودي) توصلت إلى حزمة من النتائج والتوصيات نعرض أبرزها على النحو التالي:

أولاً: النتائج

1- لم ينظم كل من المنظم السعودي والمشرع الإماراتي إجراءات تفتيش الحاسوب الآلي وشبكات المعلومات إلا أنه غالباً ما تتخذ ذات الإجراءات التي نظماها للبحث عن الأدلة التقليدية، مع إتباع المبادئ العامة في التشريعات.

2- ساير كل من نظام الإثبات السعودي والقانون الاتحادي الإماراتي بشأن مكافحة الشائعات والجرائم الإلكترونية حالات استخدام التكنولوجيا الرقمية في مجال استخدام وسائل الاتصال الإلكترونية للإثبات الجزائي، ووضع الضوابط النظامية التي تمنع إساءة استخدامها، كما هو الحال بالنسبة لمراقبة المحادثات السلكية واللاسلكية وتسجيلها.

3- أعطى القانون الإماراتي-على خلاف النظام السعودي-الأدلة الرقمية المستخرجة من المكونات المادية أو المعنوية للحاسوب الآلي حجية في الإثبات تعادل حجية الأدلة الجزائية التقليدية.

4- توصلت إلى أن كلاً من المنظم السعودي والمشرع الإماراتي لم يعتمدا نهج وضع

نصوص تتضمن أدلة للإثبات الجزائي بعينها، كما لم يضعا نصوص تقييد من سلطة المحكمة سواء في قبولها أو رفضها لأي دليل رقمي.

5- أخذ النظام السعودي بمذهب الإثبات المختلط، وذلك بأن يكون الإثبات مقيداً بالنسبة لجرائم الحدود وحراً بالنسبة للجرائم التعزيزية.

6- توصلت إلى أن القضاء السعودي واكب التطور الحاصل في مجال الجرائم المعلوماتية، بصدور قرار المحكمة العليا رقم (43) وتاريخ 9341/9/32هـ، باعتماد الدليل الرقمي واعتباره حجة معتبرة في الإثبات الجزائي، ولا يوجد قرار مماثل لهذا القرار في القضاء الإماراتي.

ثانياً: التوصيات

1- ضرورة تعديل كل من نظام الإجراءات الجزائية السعودي وقانون الإجراءات الجزائية الاتحادي الإماراتي فيما يتعلق بالتعامل مع الدليل الرقمي على نحو يتوافق مع طبيعة الجريمة المعلوماتية ويساهم في إثبات وقوع الجريمة وضبط مرتكبيها، مع وضع آليات نظامية بشأن جمع الأدلة الجزائية الرقمية واستخلاصها وإبراز قيمتها الاستدلالية ودورها في الإثبات.

2- نوصي النظام السعودي النص صراحةً -على غرار القانون الإماراتي- بأن يعتد بالأدلة الرقمية كأدلة إثبات جزائي، والاعتراف لها بنفس حجية الأدلة المادية في الإثبات الجزائي، مع النص على وسائل التأكد من سلامة الأدلة الرقمية باعتبارها شرطاً لقبول هذه الأدلة.

3- نوصي كل من النظام السعودي والقانون الإماراتي بالعمل على إضافة نصوص نظامية تحدد بوضوح كيفية إجراء الضبط والتفتيش الإلكتروني وأخذ الدليل الجزائي الرقمي من تفتيش الحاسوب الآلي وشبكات المعلومات دون المساس بحرمة الحياة الخاصة للأفراد وحريتهم الشخصية.

4- إنشاء محاكم متخصصة للنظر في الجرائم المعلوماتية وذلك لصعوبة كشف هذه الجرائم وجمع الأدلة الجزائية الرقمية اللازمة لإثباتها والتحقيق فيها وحاجتها إلى معطيات خاصة قد لا تتوفر في القضاء العادي.

المصادر والمراجع

أولاً/ المصادر والمراجع العربية:

إبراهيم، خالد ممدوح. (2008م). الجرائم المعلوماتية: الإسكندرية: دار الفكر الجامعي.

إبراهيم، خالد ممدوح. (2009م). فن التحقيق الجنائي في الجرائم الإلكترونية: الإسكندرية: دار الفكر الجامعي.

أحمد، هلالي عبداللاه. (2007م). جرائم المعلوماتية عابرة الحدود « أساليب المواجهة وفقاً لاتفاقية بودابست: القاهرة: دار النهضة العربية.

البشرى، محمد الأمين. (2004م). التحقيق في الجرائم المستحدثة: مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية: الرياض.

الحلبي، خالد عياد. (2011م). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت: الأردن: دار الثقافة للنشر والتوزيع.

الدليمي، عامر علي. (2012م). أهمية الاستجواب (في مرحلة التحقيق الابتدائي الدعوى الجنائية): الأردن: دار زهران للنشر.

الرشودي، أحمد عبد الله. (2008م). حجية الرسائل الإلكترونية في الإثبات الجنائي :(دراسة تأصيلية مقارنة). أطروحة دكتوراه الفلسفة في العلوم الأمنية، الرياض: جامعة نايف العربية للعلوم الأمنية.

الصغير، جميل عبد الباقي. (2002م). الإنترنت والقانون الجنائي: القاهرة: دار النهضة العربية.

الطوالبة، علي حسن. (2007م). مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي: دراسة مقارنة، دولة البحرين: مركز الإعلام الأمني.

العبيدي، فارس محمد. (2020م). دور الدليل الرقمي في الاثبات الجنائي في النظام السعودي: دراسة مقارنة بالقانون الإماراتي. رسالة ماجستير، السعودية، كلية العدالة الجنائية: جامعة نايف العربية للعلوم الأمنية.

العتيبي، سليمان غازي. (2016م). دور البحث الجنائي في الكشف على الجرائم المعلوماتية: (دراسة تطبيقية على شرطة منطقة مكة المكرمة). أطروحة دكتوراه الفلسفة في العلوم الأمنية، الرياض: جامعة نايف العربية للعلوم الأمنية.

الهادي، محمد محمد. (1988م). المعجم الشارح لمصطلحات الكمبيوتر: الرياض: دار المريخ للنشر.

إبن منظور. (1999م). لسان العرب. ط3. ج3: بيروت: دار إحياء التراث العربي.

بن قارة مصطفى، عائشة. (2009م). حجية الدليل الإلكتروني في مجال الإثبات الجنائي: رسالة ماجستير، مصر، كلية الحقوق: جامعة عين شمس.

بن يونس، عمر محمد. (2004م). الجرائم الناشئة عن استخدام الإنترنت: أطروحة دكتوراه، مصر، كلية الحقوق: جامعة عين شمس.

ثنيان، ناصر ثنيان. (2012م). إثبات الجريمة الإلكترونية: دراسة تأصيلية تطبيقية. رسالة ماجستير، السعودية، كلية الدراسات العليا: جامعة نايف العربية للعلوم الأمنية.

حسن، مروى عبد الواحد. (2018م). سلطة القاضي الجزائي في قبول الدليل الإلكتروني: رسالة ماجستير، الجزائر، كلية القانون والعلوم السياسية: الجامعة العراقية.

حسني، محمود نجيب. (1988م). شرح قانون الإجراءات الجنائية: الطبعة الثانية، القاهرة: دار النهضة العربية.

سعيداني، نعيم. (2013م). آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري: رسالة ماجستير، الجزائر، كلية الحقوق والعلوم السياسية: جامعة الحاج لخضر.

فرغلي، عبد الناصر محمد-سعيد، محمد عبيد (2007م)، ورقة عمل بعنوان الاثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية: المؤتمر العربي الأول لعلوم الأدلة الجزائية والطب الشرعي، الرياض: جامعة نايف العربية للعلوم الأمنية، المنعقد في الفترة من 12-14نوفمبر2007م.

قنديل، أشرف عبد القادر. (2015م). الإثبات الجنائي في الجريمة الإلكترونية: الإسكندرية: دار الجامعة الجديدة.

عبد السلام، أحمد. (2022). الإثبات بالدليل الرقمي في النظام السعودي. بروتكول نقل النصوص التشعبي (https//saudicontract.com)

عبدالعال، أسامة حسين. (2021). حجية الدليل الرقمي

فـي الإثبـات الجنائـي للجرائـم المعلوماتيـة. مجلـة البحـوث القانونيـة والاقتصاديـة، كليـة الحقـوق جامعـة المنصـورة، (76)، 596-730.
عبـد المطلـب، طاهـر. (2014م). الإثبـات الجنائـي بالأدلـة الرقميـة. رسـالة ماجسـتير: الجزائـر، كليـة الحقـوق والعلـوم السياسـية: جامعـة المسـيلة.
عبـد المطلـب، ممـدوح عبـد الحميـد. (2006م). البحـث والتحقيـق الجنائـي الرقمـي فـي جرائـم الكمبيوتـر والإنترنـت: المحلـة الكبـرى: دار الكتـب القانونيـة.
عطـا الله، شـيماء عبـد الغنـي. (2007م). الحمايـة الجنائيـة للتعامـلات الإلكترونيـة: الإسـكندرية: دار الجامعـة الجديـدة.
لعـوارم، وهيبـة. (2014م). الدليـل الرقمـي فـي مجـال الإثبـات الجنائـي وفقـاً للتشـريع الجزائـري. المجلـة الجنائيـة القوميـة. المركـز القومـي للبحـوث الاجتماعيـة والجنائيـة، 57(2)، 67-115.
محمـد، فاضـل زيـدان. (2005م). سـلطة القاضـي الجنائـي فـي تقديـر الأدلـة: دراسـة مقارنـة. عمـان: دار الثقافـة.
يعقـوب، أميـل بديـع. (2004م). المعجـم المفصـل فـي المجمـوع: لبنـان: دار الكتـاب العلميـة.

ثانياً/ المراجع العربية المترجمة للإنجليزية:

Abdul Muttalib, Mamdouh Abdul Hamid. (2006). Research and digital forensic investigation of computer and Internet crimes (in Arabic). El-Mahalla El-Kubra, Dar Al-kutub Al-qanuneya.

Abdul Muttalib, Taher (2014). Forensic evidence with digital evidence (in Arabic). Master's thesis, Algeria, Faculty of Law and Political Science, University of M'Sila.

Ahmed, Hilali Abdellah. (2007). Cross-Border Information Crimes "Combating Methods According to the Budapest Agreement" (in Arabic). Cairo, Dar Al -Nahda Al-Arabia.

Al-Bishri, Mohamed Al-Amin. (2004). Investigation of new crimes (in Arabic). Markaz AL-dirasat walbuhuth, Naif Arab University for Security Sciences, Riyadh.

Al-Dulaimi, Amer Ali. (2012). The importance of interrogation (at the stage of the preliminary investigation of criminal proceedings) (in Arabic). Jordan, Dar Zahran lil-nashr.

Al-Hadi, Mohamed Mohamed . (1988). Explanatory dictionary of computer terms (in Arabic). Riyadh, Dar Al-Marikh lil-nashri.

Al-Halabi, Khaled Ayyad (2011). Procedures of investigation in computer and Internet crimes (in Arabic). Jordan, Dar Al- Thaqafat lil-nashr wal-tawziei.

Al-Rashudi, Ahmed Abdullah. (2008). Authenticity/Credibility of e-mails in criminal evidence: (a comparative foundation study) (in Arabic). PhD thesis in security sciences, Riyadh, Naif Arab University for Security Sciences.

Al-Otaibi, Suleiman Ghazi. (2016). The role of criminal investigation in detecting information crimes: (an applied study on the Makkah region police) (in Arabic). PhD thesis in security sciences, Riyadh, Naif Arab University for Security Sciences.

Al-Saghir, Jamil Abdel-Baqi. (2002). Internet and Criminal Law (in Arabic). Cairo, Dar Al -Nahda Al-Arabia.

AL-Tawalbeh, Ali Hassan. (2007). Legality of electronic evidence derived from criminal inspection: a comparative study (in Arabic). State of Bahrain, Markaz Al-ielam Al-amni.

. Atallah, Shaima Abdel Ghani. (2007). Criminal protection of electronic transactions (in Arabic). Alexandria, Dar Al -jamiea Al-jadida.

Ben Qara Mustafa, Aisha. (2009). Authenticity of electronic evidence in the field of criminal evidence (in Arabic). Master's Thesis, Egypt, Faculty of Law, Ain Shams University.

Ben Younes, Omar Muhammad. (2004). Crimes arising from the use of the Internet (in Arabic). PhD thesis, Egypt, Faculty of Law, Ain Shams University

Farghali, Abdel Nasser Mohamed and Said, Mohamed Obaid (2007), a working paper titled Criminal Evidence with Digital Evidence from the Legal and Technical Perspectives (in Arabic). The First Arab Conference on Forensic Evidence Sciences and Forensic Medicine, Riyadh, Naif Arab University for Security Sciences, held from 12-14 November 2007.

Hosni, Mahmoud Najib. (1988). Explanation of the Code of Criminal Procedure (in Arabic). (2nd ed.). Cairo: Dar Al -Nahda Al-Arabia.

Ibrahim, Khaled Mamdouh. (2008). The art of criminal investigation in Information crimes (in Arabic). Alexandria: Dar Al-Fikr Al-jamei.

Ibrahim, Khaled Mamdouh. (2008). Information crimes (in Arabic). Alexandria: Dar Al-Fikr Al-jamei.

Jacob, Emil Badie. (2004). Almujam al-mufassel fel-majmoua (in Arabic). Lebanon: Dar Al-Kitab Al-Ilmiya

Kandil, Ashraf Abdel Qader. (2015). Criminal evidence in cybercrime (in Arabic). Alexandria: Dar Al -jamiea Al-jadida.

Mohamed, Fadel Zeidan. (2005). The authority of the criminal judge in evaluating evidence: a comparative study (in Arabic). Oman, Dar Al- Thaqafat lil-nashr wal-tawziei.

Omar, Ahmed Mukhtar. (2008). Contemporary Arabic Language Lexicon (in Arabic). Egypt, Alam Al-kutub.

Saidani, Naim. (2013). Mechanisms of research and investigation of information crime in Algerian law (in Arabic). Master's Thesis, Algeria, Faculty of Law and Political Science, Hadj Lakhdar University.

Thunayan, Nasser Thunayan. (2012). Evidence of electronic crime: an applied rooting study (in Arabic). Master's Thesis, Saudi Arabia, College of Graduate Studies, Naif Arab University for Security Sciences.

ثالثاً-المراجع باللغة الإنجليزية:

Alan Gahtan, electronic evidence.(1999). Thomas Canada limited.

Brian Carrier.(2005). File System forensic Analysis, Pearson Education (Inc), United states of America.

Debra Littlejohn Shinder(2002). Scene of the Cyber Crime (Computer forensic Handbook), Publishing by Syngress (Inc), United states of America.

David Thompson.(1991). Current Trends in Computer Crime. Computer Control Quarterly. vol. 9. No. 1.

Eoghan Casey.(2011). Digital Evidence and Computer Crime, Third Edition, Published by Elsevier Inc, London.

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

Steve Bunting and William Wei.(2006). Encase Computer forensic, Wiley Publishing (inc), United States of America.

Thomas J. Gardner. Terry M. Anderson.(2004). Criminal Evidence. Principles and cases (5) fifth edition. Thompson Wadsworth Publisher.

Wasilk (Martin).(1993). Computer crime and others crimes against information technology in United Kingdom. R. I.D.P.

رابعاً-الأنظمة والقوانين والاتفاقيات الدولية:

الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست لسنة 2001).

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012.

النظام الأساسي للحكم السعودي الصادر بالمرسوم الملكي رقم (أ/90) بتاريخ 1412/8/27هـ.

دستور الإمارات العربية المتحدة الصادر في 2ديسمبر 1971م (المعدل في سنة2009).

قانون المعاملات الإلكترونية الاتحادي للولايات المتحدة الأمريكية لعام 1999.

نظام التعاملات الإلكترونية السعودي الصادر بالمرسوم الملكي رقم (م/18) بتاريخ 1428/3/8هـ.

القانون الاتحادي الإماراتي رقم 1لسنة2006 في شأن المعاملات والتجارة الإلكترونية.

نظام الإثبات السعودي، الصادر بالمرسوم ملكي رقم (م/43) وتاريخ 1443/5/26هـ.

الأدلة الإجرائية لنظام الإثبات السعودي الصادرة بقرار وزير العدل رقم (921) وتاريخ 1444/3/16هـ.

القانون الاتحادي الإماراتي رقم 10لسنة1992 والمعدل بالقانون رقم 36 لسنة 2006 بشأن قانون الاثبات في المعاملات المدنية والتجارية.

نظام الإجراءات الجزائية السعودي الصادر بالمرسوم الملكي رقم (م/2) بتاريخ 1435/1/22هـ.

قانون الإجراءات الجزائية الاتحادي الإماراتي رقم 35 لسنة 1992 والمعدل بالقانون رقم 28 لسنة2020.

القانون الاتحادي الإماراتي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم(م/19)بتاريخ1443/2/9هـ.