The Validity of Digital Evidence in Criminal Evidence

Mohammed Salim Abdullah
University of Sharjah / College of Law
U19102892@sharjah.ac.ae

Manal Marwan Almunjed
University of Sharjah / College of Law
mmonajjed@sharjah.ac.ae

Accepted Date: 29/10/2025. **Publication Date: 1/4/2026.**

Abstract

The research objective is based on the strong conclusiveness of evidence in the Emirati diversity, as this type of diversity is characterized by rapid development and the possibility of renewal, and is not familiar to men and investigation in the other army whose traditional need, therefore it sought to identify the requirements of digital evidence and its conclusiveness, and to discuss it and confirm conviction of it, and it searched on descriptive and analytical electronic models, due to its suitability to the research topic, and the research reached several results, the most important of which are: that the intangible components of the computer are suitable for inspection and seizure, due to the possibility of conferring the character of social status on it. Talking in the registry and comparative jurisprudence considers the information stored in the computer and its outputs as one of the best available evidence for proof, and enjoys the certainty required in criminal proof and what is known legally as the elimination of crimes and crimes in the Emirates, therefore the results were controlled after determining the following performance: Control of a group of procedural evidence that enables Internet service providers to collect information within the Internet, as well as when this information can be revealed in electronic law. The researcher must also consider the UAE

legislator over the Egyptian legislator only Article 6 of the Egyptian Electronic Law No. 175 of 2018, in addition to the period required for monitoring it, and dealing with the service provider.

Keywords: Legitimacy of evidence - Digital evidence - Criminal evidence

حجية الدليل الرقمي في الاثبات الجنائي

محمد سالم الشامسي [*]
جامعة الشارقة/ كلية القانون
U19102892@sharjah.ac.ae

منال مروان المنجد [**]
جامعة الشارقة/ كلية القانون
mmonajjed@sharjah.ac.ae

تاريخ القبول: 2025/10/29. **تاريخ النشر: 2026/4/1.**

المستخلص

هدف البحث الوقوف على حجية الدليل الرقمي ودوره في إثبات الجرائم الإلكترونية في التشريع الإماراتي، حيث أن هذا النوع من الجرائم يتميز بسرعة التطور وقابلية التجدد، ولم يألفه رجال الأمن والتحقيق في الجرائم الأخرى التي تسمى الجرائم التقليدية، لذا سعى البحث التعرف على شروط قبول الدليل الرقمي وحجيته، ومناقشته والاقتناع اليقيني به، وقد اعتمد البحث على المنهجين الوصفي والتحليلي، لمناسبته لموضوع البحث، وتوصل البحث لعدة نتائج كان أهمها: أن مكونات الحاسوب المعنوية تصلح محلا للتفتيش والضبط ، نظرا لإمكانية إسباغ الصفة المادية عليها، إن الاتجاه الحديث في التشريع والفقه المقارن يعد المعلومات المخزنة في الحاسوب ومخرجاته من أفضل الأدلة المتاحة للإثبات ، وتتمتع باليقين المتطلب في الإثبات الجزائي وهذا ما ذهب إليه قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي، وبناءً على تلك النتائج تم وضع التوصيات التالية: يوصي الباحث بوضع مجموعة من القواعد الإجرائية التي تمكن مقدمي خدمة الإنترنت جمع المعلومات داخل شبكة الإنترنت، وكذلك متى يكون لهم كشف هذه المعلومات لجهات إنفاذ القانون. كما يوصي الباحث بأن يأخذ المشرع الإماراتي على غرار المشرع المصري بتطبيق المادة السادسة من قانون الجرائم الإلكترونية المصري رقم 175 لسنة 2018 بشأن المدة المستحقة لمراقبة المشتبه بهم، والتعامل مع مقدم الخدمة.

الكلمات المفتاحية: مشروعية الدليل - الدليل الرقمي- الاثبات الجنائي

[*] طالب ماجستير
[**] أستاذ دكتور

المقدمة

Introduction

يحظى الدليل الإلكتروني بأهمية قصوى، نظرًا لكونه يُشكِّل الأساس الذي يُبنى عليه الحكم الذي يُعدُّ بمثابة الفصل الختامي للقضاء، والهدف النهائي للنظام القضائي؛ وتكمن سلامة الحكم في مدى دقة وصحة تقدير الأدلة المُستخدمة.

ويتساوى الدليل الإلكتروني مع سائر الأدلة في خضوعه للقواعد القانونية التي سار عليها القانون الحالي؛ والتي تشمل سلطة القاضي الجنائي في الاعتراف بالدليل الإلكتروني وتقديره. إذ لا يُعتد بأي دليل إلا إذا كان مقبولًا وفقًا لمبادئ الشرعية القانونية، والتي بدونها لا يُمكن للدليل الإلكتروني أن يُولِّد أية آثار قانونية مُلزمة.

وفي ضوء الخصائص المميزة للدليل الإلكتروني والإجراءات المعقدة المصاحبة للحصول عليه، يُمكن أن يُثير استخدامه في الإثبات تحديات جمّة. إذ تُعد الوسائط الإلكترونية مستودعًا لهذه الأدلة، مما يجعل احتمال التلاعب بها وتحريفها أمرًا محتملًا. وهنا يثور التساؤل الجوهري: كيف يُمكن ضمان صدق الدليل الإلكتروني وتمثيله الدقيق للوقائع المراد إثباتها في الدعوى الجنائية؟

مشكلة الدراسة Study Problem

والتي تتمثل في بيان مدى حجية الدليل الرقمي في إثبات ومكافحة الجرائم الإلكترونية في ظل التقدم الهائل في أنظمة المعلومات، ومدى حجيّة الدليل الإلكتروني المستمد من هذه الإجراءات في الإثبات الجنائي.

تساؤلات البحث Research Questions

والتي تسعى للإجابة على السؤال الرئيسي التالي:

مدى حجية الدليل الرقمي في الإثبات الجنائي؟

وتتفرع عن هذا التساؤل الرئيسي التساؤلات التالية:

1. ما هي شروط قبول الدليل الرقمي ؟
2. ما هي حجية اقتناع القاضي الجنائي بالدليل الرقمي ؟

أهمية الدراسة:

تتجلى أهمية الدراسة فيما يلي:

الأهمية العلمية:

- التعمّق في دراسة المواجهة الإجرائية للجريمة الإلكترونية بكافة جوانبها في ظل التطور الهائل الذي يشهده العالم في استخدام التقنيات الحديثة، وذلك من خلال إيضاح مفهوم الجريمة الإلكترونية ومراحل تطورها وأسبابها ووسائل ارتكابها، وأساليب وإجراءات مكافحتها.

- توضح للقائمين على أعمال مكافحة الجريمة الإلكترونية المعوقات التي قد تظهر أثناء إجراءات التحقيق الجنائي، القائم بها المختصون بالعمل الشرطي في هذا المجال بوزارة الداخلية، مع إبراز هذه المعوقات بشتى أنواعها، في محاولة إيجاد حلول لتسهيل أعمال المكافحة والبعد عن الأخطاء التي قد تلحق بإجراءات التحقيق.

الأهمية العملية:

- تسهم الدراسة في أن يستخلص من خلالها بعض الآليات، التي تهدف لتدريب الكوادر للتعامل مع مسرح الجريمة الإلكترونية.
- نتائج وتوصيات الدراسة ذات أهمية خاصة للقائمين على وضع الخطط الإستراتيجية الأمنية في مجال مكافحة الجرائم الإلكترونية، في ظل تطورها وسرعتها وانتشارها، وتساعد على وضع الاستراتيجيات الأمنية وإرساء القواعد والضوابط العملية المنظمة لأعمال المكافحة بصورة دقيقة، لتجنب المعوقات التي قد تؤدي لفشل إجراءات التحقيق، وذلك للوصول إلى المجرمين وتقديمهم للعدالة وتجنيب المجتمع شرورهم.

أهداف الدراسة Study Objectives

تهدف هذه الدراسة إلى الآتي:

1. إظهار أوجه اختصاص التحقيق الجنائي في الجرائم الإلكترونية.
2. اسقاط الضوء على الشروط التي يجب توفرها لقبول الدليل الرقمي.
3. الوصول لكيفية اقتناع القاضي الجنائي بالدليل الإلكتروني.

منهج الدراسة

اعتمدت الدراسة على المنهجين الوصفي والتحليلي المقارن، وذلك كما يلي:

1. من خلال وصف موضوع البحث في مختلف جوانبه، والذي يسعى الباحث من خلاله إلى استعراض الشروط التي يجب ان تتوفر في الدليل الرقمي الجنائي في الجرائم الإلكترونية أثناء المحاكمة والتي يبني عليه القاضي قناعته، من خلال إيضاح القصور التشريعي والصعوبات المرتبطة بالقضاء مع تناول الحلول التشريعية والإدارية والفنية والتدريبية، سعياً وراء تقويم الأداء الأمني في مجال التحقيق، من خلال الاعتماد على التخطيط والتدريب وسد الفراغ التشريعي والتنسيق مع الكيانات الدولية.

2. المنهج المقارن من خلال المقارنة بين التشريع الإماراتي والتشريع المصري وبعض التشريعات الأخرى، وخاصة فيما يتعلق بالدليل الإلكتروني، شروطه، وحجيته في الاثبات.

هيكل البحث:

تم تناول البحث من خلال مقدمة ومبحثين كما يلي:

المبحث الأول: شروط قبول الدليل الرقمي

المبحث الثاني: مناقشة الدليل الرقمي والاقتناع اليقيني به

الخاتمة:

النتائج والتوصيات

المراجع

المبحث الأول
شروط قبول الدليل الرقمي
Section One
Conditions for Accepting Digital Evidence

من المتعارف عليه أن القاضي الجنائي يتمتع بسلطات تقديرية في أدلة الإثبات، وأن يتحري عن الحقيقة بجميع الأدلة، ما دامت مقبولة لديه، وأنها صالحة وملائمة[1] ، وقد استقر القضاء الإماراتي على: "الأصل في المحاكمات الجزائية هو اقتناع القاضي بناء على الأدلة المطروحة عليه فله أن يكون عقيدته من أي دليل أو قرينة يرتاح إليها إلا إذا قيده القانون بدليل معين ينص عليه، ومن المقرر أن تقدير الأدلة ووزن أقوال الشهود وتقديرها إلى محكمة الموضوع ومن إطلاقاتها تنزله المنزلة التي تراها"[2]

والاتجاه الغالب في القضاء والتشريع والفقه المقارن أن قبول الأدلة الرقمية الحديثة أمام القضاء الجنائي، يجب تتوافر شروط معينة تضمن سلامة الأدلة ولديها قيمة في الإثبات وبها مصداقية، ومن أهم هذه الشروط أن تحفظ بنفس الهيئة التي وجدت عليها وكذلك يشترط كفاءة النظام المستخرج منه سواء من ناحية التخزين والعرض، وأخيراً ضرورة تخزين المخرجات التقنية المؤمن عليها تقنياً.

المطلب الأول
استخلاص المعلومات الإلكترونية وحفظها بصورتها الأصلية
The First Requirement: Extracting Electronic Information and Storing It in Its Original Form

إن الاحتجاج بالبيانات الرقمية في إثبات الوقائع الجرمية يقتضي أن يكون أصلها موجودا، وأن يتم تقديمه إلى المحكمة ، وقد يحتج البعض بالقول إن هذا الأمر يحول غير قبول البيانات الرقمية كدليل إثبات ؛ لأن ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب ذاتها، وإنما نسخا عنها تخزن في أقراص ممغنطة

أو أشرطة أو غيرها ، أو تطبع في أوراق ، لكن هذه الحجة لم يعد لها وزن وتم تذليلها ، وذلك من خلال إسناد المشرع الإماراتي للحجية القضائية الكاملة للأدلة الإلكترونية بموجب "المادة 65 من مرسوم مكافحة الشائعات والجرائم الإلكترونية، وبالمثل فعل المشرع المصري في المادة (11) من قانون مكافحة تقنية المعلومات رقم (175) لسنة 2018، فقد إرساء دعائم جديدة لنظام الإثبات الجنائي، إذ صار بالإمكان الاعتماد على هذه الأدلة بصورة مماثلة للأدلة المادية في إثبات وقوع الجرائم الإلكترونية وتحميل مرتكبيها المسؤولية"[3].

ويرى الباحث أن المشرع الإماراتي أظهر رؤيته المستقبلية في مجال الإثبات الجنائي من خلال توسيع نطاق الأدلة الرقمية لتشمل كافة أنواع البيانات الرقمية المخزنة أو المنقولة عبر الأجهزة والأنظمة الإلكترونية، بما في ذلك البيانات المستخرجة من الأجهزة الإلكترونية، المعدات، الوسائط، الدعامات، النظم الإلكترونية، برامج الحاسوب، وأي وسيلة أخرى لتقنية المعلومات.

وتعكس عبارة "أي وسيلة أخرى لتقنية المعلومات" التي استخدمها المشرع الإماراتي في عجز المادة سالفة الذكر، إدراكه الكامل للتطور السريع لتقنيات المعلومات وتعدد وسائل ارتكاب الجرائم الإلكترونية، فجاءت هذه العبارة لتغطي كافة الأجهزة والبرامج التي يمكن أن يستخدمها المجرم كأداة لارتكاب جريمته أو مصدر للدليل الإلكتروني، وأي تقنية جديدة قد تظهر في المستقبل[4].كما نصت بعض التشريعات في بعض الدول بالنص على انه : "إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإن أى مخرجات مطبوعة منها أو مخرجات يمكن قرائتها بالنظر إليها وتعكس دقة البيانات ، تعد بيانات أصلية"[5]، وبناء عليه فإن ما يستخرج بواسطة الطابعة من بيانات أو ملفات مخزنة في الحاسوب أو على شبكة المعلوماتية تعد دليلاً أصلياً.

وقد أكدت على ذلك المادة (17) مكررًا من القانون الاتحادي رقم (10) لسنة 1992م بشأن إصدار قانون الإثبات في المعاملات المدنية والتجارية"على الاعتراف بحجية الأدلة الرقمية في الإثبات، مسيرة بذلك مع التطور التشريعي المعاصر. كما تماشى مع هذا التوجه القانون النموذجي للأمم المتحدة بشأن التجارة الإلكترونية، المعتمد في 12 يونيو 1996، إذ أقر بالدليل الكتابي الإلكتروني، وأوضح أن اشتراط الكتابة، حيثما نص عليه القانون، يُعد مستوفيًا متى أمكن تخزين البيانات الإلكترونية بطريقة تتيح الاطلاع عليها عند الاقتضاء، بما يحقق الغاية المقصودة من شرط الكتابة دون الإخلال بالوسيلة التقنية المستخدمة"[6].

كما يرى الباحث أنه يجب ضمان عدم تعرض الملفات الإلكترونية لأي عبث أو تلف أو تغيير في محتوياتها ، وأن الدليل الذي قدم إلى المحكمة هو الدليل نفسه الذي تم جمعه وحفظه ، ولم يطرأ عليه أي تعديل ، وأنه تمت مراعاة سلامته حتي يبقي بالحالة نفسها التي ضبط بها.

كما اعتبرت المادة (25) من قانون مكافحة الجريمة المعلوماتية السوري على "أن تقدير قيمة الدليل الرقمي يعود إلى تقدير المحكمة، شريطة أن يتحقق من عدد من الشروط الأساسية، أهمها التأكد من أن الدليل الرقمي المُقدّم إلى المحكمة قد تم حفظه بصورة سليمة، دون أن يطرأ عليه أي تعديل أو تغيير طوال فترة حفظه".

يذكر أن وجود احتمال أو شك في صدق مضمون الملفات لا يقدح في إمكانية الاستناد إليها وتمتعها بحجية في دلالتها على الوقائع التي تتضمنها ، إذا أمكن التغلب على هذا الشك، والتأكد من دقة تلك الملفات بإخضاعها لاختبارات فنية، أو بعرضها على العضو الذي كان حاضرا عند ضبطها وسماع شهادته للتأكد من صحتها[7].

ولتأمين سلامة البيانات المخزنة في الحاسوب وعدم تعرضها للعبث، يري الفقه أنه عند معاينة مسرح الجريمة المعلوماتية وضبط البيانات الرقمية ، يجب مراعاة عدة أمور ، وهي[8]:"

1. حصر أجهزة الكمبيوتر الكائنة بمحل المعاينة، وتعيين موقع كل منها بدقة، وعزل الحواسيب عن الشبكة ، وتصوير الأجهزة الموجودة بالحالة التي هي عليها.
2. حظْر نقل أي دليل رقمي من مسرح الجريمة الرقمية إلا بعد إجراء فحص دقيق وشامل للمحيط الخارجي لموقع الحاسوب، وذلك للتحقق من خلوه تماماً من أي مجال لقوى مغناطيسية أو أي مؤثرات أخرى ذات طبيعة مماثلة قد تؤدي إلى محو البيانات المسجلة أو إتلافها.
3. قصر صلاحية معاينة محل الجريمة وضبط ما فيه من أجهزة وشبكات واسترجاع المعلومات، على الباحثين والمحققين الذين يتمتعون بكفاءة علمية راسخة وخبرة فنية متعمقة وتدريب مكثف في هذا المجال".

المطلب الثاني

التحقق من سلامة الحاسوب الآلي ودقته وحفظ مخرجات الحاسوب في بيئة مناسبة

The Second Requirement: Verify The Integrity And Accuracy Of The Computer And Store Computer Output In A Suitable .Environment

يجب على القاضي أن يتحقق من الظروف التي حصل على الدليل الرقمي وكذلك الكيفية التي حصل عليها ويجب التأكد من سلامة جهاز الكمبيوتر وجميع ملحقاته وقت أخذ الدليل ويجب استبعاد أي دليل إذا كان هناك خلل أو عطل يوقف عمل الجهاز بالشكل الطبيعي[9]؛ ويجب التأكد من سلامة جهاز الكمبيوتر وعدم تأثير أي شيء خارجي على الجهاز الممغنط أو مواد فيزيائية قد تمس وتؤثر بشكل مباشر أو غير مباشر على تخزين الدليل الإلكتروني محل الجريمة.

وقد جاء في المادة (25) من قانون مكافحة الجريمة المعلوماتية السوري انه : " يعود للمحكمة تقدير قيمة الدليل الرقمي، شريطة أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدة منها هذا الدليل تعمل على نحو سليم".

ولضمان سلامة الحاسب الآلي وتخزين بياناته في بيئة سليمة ، يري الفقه المقارن أن على رجل الضابطة القضائية عندما يصل إلى مسرح الجريمة ، مراعاة الآتي[10]:"

1. أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات أو أنظمة المعلومات أو البرامج أو الدعامات الرقمية وغيرها.

ومنها على الأخص تقنية Write Blocker Digital Images Hash، وغيرها من التقنيات المماثلة.

2. حظر نقل أي مادة معلوماتية من مسرح الجريمة قبل التحقق التام من خلو محيط الحاسوب من أي حقول مغناطيسية أو مؤثرات مماثلة قد تعرّض البيانات للمحو أو التلف.

3. أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريره بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة على أن يبين في محاضر الضبط أو التقارير الفنية نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود و خوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به

4. في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص والتحليل.

5. حجز الحاسوب أو القرص الصلب ، وجميع الحاويات المادية والذواكر، كالسواقات والأقراص الممغنطة.

6. وضع ملصقات على الأشياء المضبوطة ، وتوثيقها وتغليفها، وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص.

7. ضبط وتحريز الدعائم الأصلية للمعطيات التي لها دلالة عند عرضها للمحكمة، وعدم الاكتفاء بضبط النسخ، وعدم الضغط على القرص بوضع أشياء ثقيلة عليه.
8. توفير الحرارة والرطوبة المناسبة لتخزين الأحراز المعلوماتية وإبعادها عن الأتربة أو الغبار ، لمنع تأثيرها على السطح المغناطيسي، ما يجعله غير قابل للقراءة أو الكتابة.
9. حماية وتأمين البرامج المضبوطة قبل تشغيلها فنيا.
10. وضع علامات مادية خاصة تميز كل دليل إلكتروني عن غيره".

المبحث الثاني
مناقشة الدليل الرقمي والاقتناع اليقيني به
Section Two
Discussion of the Digital Evidence and Certain Conviction

من المستقر في الفقه والقانون المقارن أن للقاضي سلطة واسعة في تقدير الأدلة واستنباط ما تتضمنه الوقائع من دلالات ، سعيا منه لكشف الحقيقة ، لكن مقتضيات تحقيق العدالة وتجنب إدانة شخص بريء أو إفلات مجرم من العقاب ، توجب على القاضي الجزائي قبل إصدار حكمه، أن يقوم بفحص الأدلة الجزائية ، ومن بينها الأدلة الرقمية وطرحها في الجلسة ليتناولها الخصوم بالمناقشة، وتكوين اقتناعه اليقيني بها، وصولا إلى الحقيقة التي ترضي ضميره وتحقيقا للعدالة.

المطلب الأول
مناقشة الدليل الرقمي
First Requirement
Discussion of Digital Evidence

إن مبدأ المواجهة، الذي يعد من أهم القواعد التي تحكم إجراءات المحاكمة الجزائية ، يفرض على القاضي الجزائي أن يطرح الدليل الرقمي على الخصوم لمناقشته، ويبني على ذلك أن يكون لهذا الدليل أصل ثابت في أوراق الدعوى، وأن تتاح الفرصة أمام الخصوم للإطلاع عليه ومناقشته، تفصيلا في الجلسة، وهذا ما تؤكده قوانين الإجراءات الجزائية ؛ إذ تقضي بأنه لا يمكن للقاضي اعتماد أي دليل قد تم تقديمة أثناء المحاكمة وتم مناقشتها خلال الجلسات بين أطراف القضية ويجب أن يعتمد كذلك على التقرير الفني للمختبر[11]. وهذا الحكم ينطبق على الدليل الرقمي ، أيا كانت صورته أو شكله ، فعلى المحكمة أن تطرح الدليل على بساط البحث في الجلسة، وتجعله محلا للمناقشة بحضور الخصوم ، وأن تستمع على أقوالهم بشأنه، قبل أن تعتمده كدليل إثبات في الدعوي المعروضة أمامها.[12]

ولا شك أن إقرار هذا المبدأ والالتزام به يعد من جهة أولي ضمانة مهمة من ضمانات المحاكمة العادلة ، وركيزة أساسية لحق الدفاع في أثناء مرحلة المحاكمة؛ إذ تتيح الفرصة لكل طرف في الخصومة الجزائية بتقديم ما لديه من مستندات ، بما فيها الأدلة الرقمية ، وإطلاع الطرف الآخر عليها، ومنحه الوقت الكافي؛ لتحضير دفاعه والرد عليها[13]، فضلا عما يحققه هذا المبدأ من رقابة المحكمة الجزائية على الأعمال والإجراءات السابقة على المحاكمة ، ومراقبة التقدير الذي خلصت إليه سلطة التحقيق[14] ، ومن جهة ثانية يهدف مبدأ المواجهة إلى غاية أساسية تتمثل في أن يكون للدليل الرقمي أصل في أوراق الدعوي ، فيكون اقتناع القاضي مبنيا على أساس من الأدلة القضائية (أي التي طرحت في الجلسة بحضور الخصوم).[15]

وبناء على مبدأي المواجهة والحضورية **يرى الباحث** أنه لا يجوز للقاضي أن يبني اقتناعه استنادا إلى معلوماته الشخصية، أو إلى اقتناع ورأي غيره، بل لابد أن يكون اقتناعه مبنيا على عقيدته التي استخلصها من الأدلة التي قدمت أثناء المحاكمة وتناقش بشأنها الخصوم؛ لأنه من خلال هذه المناقشة تتضح قوة أو ضعف الأدلة، فيبني القاضي قناعته من خلال الأخذ بها أو باستبعادها[16].

وتتجلى أهمية الشفوية في مجال الشهادة في أن يتسنى للمتهم مناقشة الشهود، فلا يمكن للمحكمة أن تكتفي بشهادة الشهود الموجودة في محضر التحقيق الابتدائي دون أن تسمعهم بنفسها وتتسنى للخصوم مناقشتهم، فإذا هي لم تفعل ذلك تكون قد أخلت بمبدأ شفوية المرافعة، وجاء حكمها مشوبا بالإخلال بحق الدفاع، كذلك تقرير الخبراء لا يستطيع القاضي أن يستند إليه في تكوين عقيدته إلا إذا عرض على أطراف الدعوى وتسنى لهم مناقشته، ومن قضاء النقض في هذا الخصوص أن الأصل في المحاكمة الجنائية أنها تقوم على التحقيق الشفوي الذي تجريه المحكمة في مواجهة المتهم بالجلسة وتسمع فيه الشهود لإثبات التهمة أو نفيها، ولا يسوغ الخروج على هذا الأصل إلا إذا تعذر سماعهم لأي سبب من الأسباب أو قبل المتهم أو المدافع عنه ذلك قبولا صريحا أو ضمنيا.([17])

وتجدر الإشارة إلى أن اشتراط طرح الدليل الجنائي أمام القاضي في جلسات المحاكمة، لا يعني أنه يشترط تلاوة أوراق محاضر جمع الاستدلالات أو التحقيق الابتدائي، أو تقارير الخبراء في الجلسة علنية، وإنما يكفي أن تكون كافة الأدلة التي تتضمنها هذه المحاضر والتقارير تحت نظر المحكمة وخاضعة للمناقشة الشفوية؛ بحيث يتسنى للخصوم جميعا الاطلاع عليها والإدلاء برأيهم فيها إذا أرادوا، فلهم أن يطلبوا من المحكمة وفي هذه الحالة وجبت مناقشتها، وإلا كان الحكم معيبا للإخلال بحق الدفاع، فإن لم يفعلوا فليس من حقهم النعي على المحكمة بعد ذلك بحجة عدم طرح الأمر للمناقشة في جلسات المحاكمة ([18]).

ومن خلال الطرح السابق لمناقشة الدليل الرقمي **يرى الباحث** أنه يتعين على القاضي أن يبين في حكمه العناصر التي استمد منها رأيه والأسانيد التي بني عليها قضاءه مما عرض عليه في جلسات المحاكمة، فلا يقبل منه أن يذكر الدليل الذي استند إليه في تأسيس حكمه أو أن يشير إليه فقط، وإنما يتوجب عليه أن يبين مؤداه بصورة كافية يتضح منها مدى تأييده للواقعة كما اقتنعت بها المحكمة، ويترتب على مخالفة ذلك أن يكون حكمه معيبا. وترتيبا على ما تقدم فإذا استند الحكم إلى تقرير الخبير في مجال تقنية المعلومات دون أن يعرض للأسانيد التي أقيم عليها هذا التقرير، ودون أن يذكر نتيجة المناقشات التي دارت حوله بجلسة المحاكمة أو دون أن يناقش أوجه الاعتراض التي أثارها الخصوم في خصوص مضمونه، يجعل هذا الحكم معيبا مستوجبا نقضه.

المطلب الثاني

الاقتناع اليقيني والجازم بالدليل الرقمي

The Second Requirement: Absolute and Firm Conviction Based On Digital Evidence

إن مبدأ القناعة الداخلية يخول القاضي الجزائي حرية كاملة وسلطة واسعة في تقدير الأدلة التي تطرح أمامه في الدعوي، بما فيها الأدلة الرقمية، واستخلاص اقتناعه من هذا الدليل أو ذاك ، وبأية وسيلة يراها موصلة إلى الحقيقة، شرط أن يصدر القاضي حكمه عن اقتناع يقيني بالأدلة ، وبخاصة الأدلة المتحصلة من الحاسب الآلي ومخرجاته الإلكترونية ، فسلطة القاضي الجزائي في تقدير الأدلة مقيدة بضرورة أن يؤسس قناعته على أدلة قاطعة وحاسمة، لأن الأحكام الجزائية لا تبني على الشك أو التخمين بل على الجزم واليقين[19]، والوصول إلى يقينية الدليل الرقمي يتم عن طريق ما يستنتجه القاضي بمختلف وسائل إدراكه من خلال معاينته لهذا الدليل، وما يتوارد في ذهنه من أفكار أو تصورات ذات درجة مرتفعة من اليقين عن طريق التحليل والاستنتاج والربط بين الوقائع[20].

وإذا كانت سلطة القاضي الجزائي في تقدير الدليل تتسع لتشمل الأدلة العلمية، إلا أن تطور العلوم وتشعب فروعها، ومقتضيات المنطق والعقل والعدالة توجب على القاضي، (وهو ذو تكوين قانوني غير قادر على إدراك الحقائق المتعلقة بأصالة الدليل الرقمي)، أن يؤسس اقتناعه بالدليل الرقمي على رأي الخبرة الفنية في هذا المجال [21]، فيجعل من هذا الرأي سندا له في تمتع الدليل الرقمي بقيمة إثباتية قد تصل إلى حد اليقين ، فتحديد القيمة العلمية للدليل أمر لا يملك القاضي أية سلطة في تقديرها؛ لأنها حقيقة ثابتة ، وليس من مهامه أن يناقش الأمور ذات الصبغة الفنية وإنما تقع في اختصاص ذوي الخبرة في هذا الشأن[22]، وليس للمحكمة الجزائية أن تبت فيها من تلقاء ذاتها[23]، كما أنها لا تستطيع أن تحل نفسها محل الخبير الفني في المسائل الفنية البحتة ، وعليها الاستعانة بخبير تخضع خبرته ورأيه لتقديرها[24].

أما بالنسبة إلى الظروف المحيطة بالجريمة والملابسات التي وجد فيها الدليل ، فالقاضي الجزائي يستطيع أن يرفض هذا الدليل إذا تبين له أن وجوده لا يتناسب منطقيا مع ظروف الجريمة الواقعية؛ لأن القاضي يتمتع بسلطة تقدير الأدلة ، والتحقق من سلامة إجراءات الحصول عليها ومشروعيتها.

ويعد الرأي الغالب في الفقه المقارن أن الأدلة المأخوذة من الحاسوب تتمتع باليقين المنشود في الأحكام الجزائية ، ومن ثم هي من أحسن وأفضل الأدلة [25] ، باعتبارها أحد الأدلة العلمية ، بل أكثر منها حجية في الإثبات للجريمة ؛ لأنها محكمة بقواعد فنية علمية وحسابية معقدة قاطعة لا تقبل التأويل[26]. ويمكن وصول القاضي إلى اليقين في هذه الحالة من خلال ما يعرض عليه من مخرجات إلكترونية بمختلف أنواعها وأشكالها ، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة إليها، وأن يحدد قوتها الاستدلالية على صدق نسبة الجريمة إلى شخص معين أو لشخص آخر[27].

وقد نصت قوانين بعض الدول على اعتبار النسخ المستخرجة من البيانات والمعلومات المخزنة في الحاسوب من أفضل الأدلة المتاحة لإثبات هذه البيانات ، ومن ثم تعد من أفضل الأدلة ويتحقق مبدأ اليقين فيها[28]، واستلزام يقينية المخرجات الإلكترونية يعد ضمانة أساسية تحد من احتمال انحراف القاضي بممارسة سلطته في تقدير الأدلة ، وتضفي عليها المصداقية واقترابها من الحقيقة ، ومن ثم قبولها كأدلة إثبات في المواد الجزائية، فلا محل لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين ، والذي يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من مخرجات الحاسوب سواء أكانت مخرجات إلكترونية أم كونها مخرجات على شاشة خارجية أو على الطرفيات ، كما اشترطت بعض التشريعات ، كاليوناني والنمساوي والسويسري والنرويجي، في سبيل يقينية الدليل الجزائي أن يكون الدليل الرقمي مقروءا، سواء كان مطبوع أو غير مطبوع على ورق خارجي أو كان على شاشة الحوسبة[29].

وبناء على ما تقدم نستطيع القول أن القاضي الجزائي إذا قرر صحة الدليل الرقمي ، وإن استخلاصه كان متسقا مع ظروف الواقعة وملابساتها ، فإنه يستطيع بناء قناعته عليه[30]، شرط أن تتوفر الضمانات التي يستلزمها القانون لكي يأتي الاقتناع القضائي سليما ، ولكن من الواجب أن يؤسس القاضي الجزائي قناعته على جزم ويقين ، مستندا إلى حجج ثابتة وقطعية، تجعل هذا اليقين ثابتا لا يناقضه شك أو احتمال آخر، فالدليل الرقمي من حيث إثباته للوقائع الإجرامية ، تتوفر فيه شروط اليقين ، ويترتب على ثبوت التهمة بلوغ الاقتناع بالإدانة درجة اليقين من جانب القاضي الجزائي لأن الاقتناع ثمرة اليقين[31]، وبناء عليه يسمح الدليل الرقمي للقاضي بأن يستند إليه كدليل إثبات ، ويكون الحكم الذي بني عليه حكما سليما وعادلا.

الخاتمة

Conclusion

تناولنا في هذا البحث الدليل الرقمي ، فبينا ماهية ، والخصائص التي يتميز بها، وأنواعه والأشكال التي يظهر بها ، كما عرضنا لمدي الحجية التي يتمتع بها كدليل إثبات أمام القضاء الجزائي، وقد خلصنا إلى بعض النتائج نبينها، ثم نرفقها بالتوصيات .

أولا النتائج:

1. تواجه سلطات البحث والتحقيق مشاكل في ما يتعلق بالقيمة القانونية للأدلة الإلكترونية المتحصل عليها أثناء عملية الإثبات الجنائي، إذ أن عملية استخلاص الدليل الالكتروني سواء بالطرق الإجرائية التقليدية أو المستحدثة ليس بالأمر الهين، بل تعيقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الإلكتروني أو بالعامل البشري.
2. يجب أن يحاط الدليل الإلكتروني المتحصل عليه من مرحلة التفتيش بجملة من الشروط حتى يعتبر ذا قيمة قانونية، أن يكون مشروعاً، وأن تكون له حجيته على الوقائع المراد إثباتها وان يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على الهيئة نفسها التي تم جمعه عليها، بدون أن يطرأ عليه أي تغبير أو تحريف خلال فترة حفظه.
3. إن الاتجاه الحديث في التشريع والفقه المقارن يعد المعلومات المخزنة في الحاسوب ومخرجاته من أفضل الأدلة المتاحة للإثبات ، وتتمتع باليقين المتطلب في الإثبات الجزائي وهذا ما ذهب إليه قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي .
4. قبول الدليل الإلكتروني من عدمه مسألة تخضع في المطلق لتقدير القاضي الجزائي، الذي يتمتع بدور إيجابي في مناقشة وموازنة القيمة القانونية للدليل الإلكتروني قبل أن يطمئن إليه شأنه في ذلك شأن باقي الأدلة.

وبناء على النتائج السابقة تم وضع التوصيات التالية:

1. نوصي ضم ذوي الخبرة من الفنيين والتقنيين لمأموري الضبط القضائي المسؤوولين عن البحث والتحقيق في الجرائم الالكترونية وذلك لخبرتهم في مجال تتبع واستخراج الدليل الإلكتروني بالطرق الشرعية والمحافظة عليه.
2. نوصي بوضع مجموعة من القواعد التي تمكن مقدمي خدمة الإنترنت جمع المعلومات داخل شبكة الإنترنت، وكذلك متى يكون لهم كشف هذه المعلومات لجهات إنفاذ القانون هذه القواعد تنظم إجراء مقدم خدمة الإنترنت

المراقبة اتصالات الإنترنت ولا تركز بشكل عام على الإجراء القانوني. لكن بالأحرى على الظروف الواقعية التي يحظر فيها القانون على مقدم الخدمة إجراء المراقبة وكشف المعلومات .

3. نوصي بزيادة الدورات التدريبية وورش العمل التي تبحث في كيفية استخراج الدليل الإلكتروني والتي تشارك فيها أجهزة الضبط والتحقيق، مع إرسالهم بعثات للخارج من أجل صقل مهاراتهم.

4. يوصي الباحث بأن يحذو المشرع الإماراتي حذو المشرع المصري بتطبيق المادة السادسة من قانون الجرائم الإلكترونية المصري رقم 175 لسنة 2018 بشأن المدة المستحقة لمراقبة المشتبه بهم، والتعامل مع مقدم الخدمة.

الهوامش
Endnotes

[1] في ذلك نصت المادة (180) من قانون الإجراءات الجزائية رقم (38) لسنة 2022 الإماراتي على " للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لإظهار الحقيقة.

[2] المحكمة الاتحادية العليا الطعن رقم 101 لسنة (10) قضائية ع جزائي جلسة 1989/1/4م ، والطعن رقم 179 لسنة 13 جزائي جلسة 1992/4/22م.

[3] خالد علي عراقي، قانون مكافحة الجرائم الإلكترونية والشائعات، المتحدة للنشر والتوزيع، الشارقة، 2022م، ص431.

[4] لورانس سعيد حوامدة، حجية الأدلة الرقمية في الإثبات الجنائي، مجلة البحوث الفقهية والقانونية، جامعة طيبة، السعودية، ع36، 2021، ص849.

[5] انظر المادة : 1001/ 3 من قانون الإثبات الفيدرالي الأمريكي.

[6] الأمم المتحدة، قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية، 2018، على الرابط تم الدخول عليه بتاريخ 10-3-2022،
https://uncitral.un.org/ar/texts/ecommerce/modellaw/electronic_transferable_records

[7] قبلت إحدي المحاكم الدليل الرقمي رغم الدفوع المتعلقة بالعبث بهذا الدليل ، لأن هذه الدفوع جاءت على شكل تخمين ، دون أن يوجد أي دليل يدعمها. وفي قضية أخرى قررت المحكمة: " إن حقيقة وجود احتمال بتعديل البيانات الموجودة في الحاسوب غير كافية للقول بعدم جدارة الدليل." كما ذكرت وزارة العدل الأمريكية في المرشد الفيدرالي لتفتيش وضبط الحواسيب الصادر 2002، وصولا إلى الدليل الإلكتروني في التحقيقات الجزائية : " إن غياب دليل واضح على حدوث العبث في الدليل ، لا يؤثر على أصالة ودقة سجلات الحاسوب".
Casey, Eoghan (2004), Digital Evidence and Computer Crime, Second Edition, Elsevier. ISBN 0-12-163104-4,P.170.

[8] جاسم خربيط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية ، مجلة القانون للدراسات والبحوث القانونية ، جامعة ذي قار ، 2016، العدد 12، ص19، مركز هردو، مركز هردو لدعم التعبير الرقمي، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجزائي، ص27-28.

[9] انظر المادة 69 من قانون الشرطة والإثبات الجزائي البريطاني (Pace) المعدل في 14 تشرين الأول 2002.

[10] جاسم خربيط خلف، الرئيسية، التفتيش في الجرائم المعلوماتية، مجلة الخليج العربي، العراق، مج41، ع3، 2013، ص254. طارق الخن، مرجع سابق، ص126.

[11] ذلك طبقاً للمواد (180) من قانون الإجراءات الجزائية الاتحادي.

[12] حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، دار النهضة العربية، 2018، ص1029

[13] طاهري عبد المطلب، الإثبات الجزائي بالأدلة الرقمية، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة المسيلة، 2015، ص56.

[14] طارق أحمد ماهر زغلول، شرح قانون الإجراءات الجزائية العماني، الجزء الثاني، المحاكمة وطرق الطعن في الأحكام ، ط1، دار الكتاب الجامعي ، 2016، ص211، ص157.

[15] المحكمة الاتحادية العليا، الطعن رقم (102) لسنة 2017 جزائي جلسة 2017/4/4م.

[16] زهية معمش ونسيمة غانم، الإثبات الجنائي في الجرائم المعلوماتية، رسالة ماجستير كلية الحقوق والعلوم السياسية ، جامعة عبدالرحمن ميرة بجاية، 2013، ص74.

[17] الطعن رقم 4917 لسنة 69 ق، مجموعة أحكام النقض، جلسة 3-4-2012، س53، رقم94، ص578.
[18] حسن ربيع، دور القاضي الجنائي في الإثبات، دار النهضة العربية، القاهرة، 2012، ص .165
[19] محمود نجيب حسني، شرح قانون العقوبات القسم العام، دار النهضة العربية، القاهرة، ط3، 1989، ص102.
[20] طارق أحمد ماهر زغلول ، شرح قانون الإجراءات الجزائية العماني، مرجع سابق، ص222.
[21] الدليل الإلكتروني وأثره في مجال نظرية الإثبات الجنائي، مرجع سابق، ص188.
[22] وفي هذا نصت الفقرة الثانية من المادة (180) من قانون الإجراءات الجزائية الاتحادي على " ولها من تلقاء نفسها أن تأمر بإعلان الخبراء لمناقشتهم فيما ورد في التقارير المقدمة منهم في التحقيق الابتدائي أم أمام المحكمة وعليها إجراء ذلك إذا طلب الخصوم".
[23] حوراء موسى، الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، مرجع سابق، ص1030 - 1031.
[24] كريم مدربل، الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة لنيل شهادة الماجستير، جامعة أكلي محند أولحاج البويرة كلية الحقوق والعلوم السياسية ، قسم القانون العام، 2019م، ص38.
[25] زهية معمش ونسيمة غانم، مرجع سابق، ص75، علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، مركز الإعلام الأمني، البحرين، 2009، ص9.
[26] محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الرياض، جامعة نايف العربية للعلوم الأمنية، 2004، ص250.
[27] زهية معمش ونسيمة غانم ، مرجع سابق، ص75، طاهري عبد المطلب، مرجع سابق، ص52، الدليل الإلكتروني وأثره في نظرية الإثبات الجنائي، مرجع سابق، ص140، وما يليها.
[28] على حسن الطوالبة، مرجع سابق، ص8.
[29] ميسون الحمداني، ميسون خلف حمد الحمداني ، مشروعية الأدلة الإلكترونية في الإثبات الجنائي ، مجلة كلية القانون ، جامعة النهرين، 2016، ص 47، 48.
[30] من الجدير ذكره هنا أن الاجتهاد القضائي المصري استقر ، حديثا وفي عدد من القضايا ، على الأخذ بالأدلة الرقمية والاعتراف بحجية الملفات التي يتم الحصول عليها من الوسائل الإلكترونية ، متي اطمأن إليها القاضي الجزائي ، ولو كانت ذات طبيعة خاصة، باعتبارها أدلة إثبات في المواد الجزائية، انظر في ذلك بهاء المري، الإثبات الجنائي وأثر ألادلة العلمية والإلكترونية في اقتناع القاضى، دار الأهرام للنشر والتوزيع والإصدارات القانونية، 2021م، ص1112.
[31] زهية معمش ونسيمة غانم، مرجع سابق، ص75.

المصادر
References

General References:

I. Al-Ardi, R. K. J. (2019). Electronic evidence and its impact on the theory of criminal evidence: A comparative study. Beirut: Zain Legal and Literary Publications.
II. Al-Bishri, M. A. (2004). Investigation of emerging crimes (1st ed.). Riyadh: Naif Arab University for Security Sciences.
III. Al-Bishri, M. A. (2004). Investigation of emerging crimes. Riyadh: Naif Arab University for Security Sciences.
IV. Al-Khan, T. (2011). Cybercrime. Damascus: Syrian Virtual University Publications.
V. Al-Marri, B. (2021). Criminal evidence and the impact of scientific and electronic evidence on the judge's conviction. Cairo: Dar al-Ahram for Legal Publications.
VI. Al-Saghir, J. A. B. (2012). Criminal evidence and modern technology (radar devices, computers, and DNA fingerprinting): A comparative study. Cairo: Dar al-Nahda al-Arabiya.
VII. Al-Talaba, A. H. (2009). The legitimacy of electronic evidence derived from criminal investigation. Bahrain: Security Media Center.
VIII. Hosni, M. N. (1989). Explanation of the penal code: General section (3rd ed.). Cairo: Dar al-Nahda al-Arabiya.
IX. Ibrahim, K. M. (2015). Cybercrimes. Alexandria: Dar al-Fikr al-Jamiʿi.
X. Iraqi, K. A. (2022). The law on combating cybercrimes and rumors. Sharjah: United Publishing and Distribution.
XI. Mukhlif, H. R. M. (2011). Rules of weighing conflicting evidence in civil lawsuits: A comparative study (Vol. 1). Beirut: Zain Legal Publications.
XII. Musa, H. (2018). Crimes committed through social media: A comparative study. Cairo: Dar al-Nahda al-Arabiya.

XIII. Shahin, M. K. (2018). Procedural aspects of cybercrime in the preliminary investigation stage: A comparative study. Alexandria: Dar al-Jamiah al-Jadida.

XIV. Younis, O. M. A. B. (2004). Crimes arising from the use of the Internet. Cairo: Dar al-Nahda al-Arabiya.

XV. Younis, O. M. (2007). Digital evidence (1st ed.). Cairo: Dar al-Nahda al-Arabiya.

Theses and Dissertations

I. 1-Al-Hadhiri, A. T. A. (2016). Criminal evidence using modern scientific methods: A comparative study between Libyan criminal law and contemporary jurisprudence (Master's thesis). Maulana Malik Ibrahim State Islamic University of Malang.

II. 2-Al-Mansouri, S. M. (2018). Application of the principle of judicial conviction to electronic evidence (Master's thesis). United Arab Emirates University.

III. 3-Ghanem, N., & Maʿmash, Z. (2013). Criminal evidence in cybercrimes (Master's thesis). University of Abderrahmane Mira, Bejaia.

IV. 4-Madrabel, K. (2019). Evidence using digital evidence in criminal matters (Master's dissertation). University of Akli Mohand Oulhadj, Bouira.

V. 5-Taheri, A. (2015). Criminal evidence using digital evidence (Master's dissertation). University of M'Sila.

VI. Conferences and Symposia

VII. 6-Al-Jamali, T. (2009). Digital evidence in the field of criminal evidence. Paper presented at the First Maghreb Conference on Informatics and Law, Academy of Graduate Studies, Tripoli, October 28–29.

VIII. 7-Farghali, A. N. M., & Al-Masmari, M. U. S. (2006). Criminal evidence using digital evidence: Legal and technical perspectives. Paper presented at the First Arab Conference on Forensic Sciences and Forensic Medicine, Naif Arab University for Security Sciences, Riyadh, November 2–4.

IX. 8-Zaghloul, T. A. M. (2016). Explanation of the Omani criminal procedure code: Part two, trial and appeal methods (1st ed.). Sharjah: Dar al-Kitab al-Jamiʿi.

Journals and Periodicals

I. 1-Al-Hamdani, M., & Al-Hamdani, M. K. H. (2016). The legitimacy of electronic evidence in criminal evidence. Journal of the College of Law, University of Al-Nahrain.
II. 2-Kharbit, J. K. (2013). Investigation in cybercrimes. Arabian Gulf Journal, 41.(3)
III. 3-Kharbit, J. K. (2016). Difficulties of criminal evidence in cybercrimes. Journal of Law for Legal Studies and Research, University of Dhi Qar.
IV. Laws
V. 1-State of Palestine. (2018). Cybercrime law (Law No. 10). Ramallah: Palestinian Authority.
VI. 2-Syrian Arab Republic. (2012). Law regulating communication on the Internet and combating cybercrime (Law No. 17). Damascus: Syrian Government.
VII. 3-United Arab Emirates. (1992). Law of evidence in civil and commercial transactions (Federal Law No. 10). Abu Dhabi: UAE Government.
VIII. 4-United Arab Emirates. (2021). Federal law on combating rumors and cybercrimes (Federal Law No. 34). Abu Dhabi: UAE Government.
IX. 5-United Kingdom. (2002). Police and Criminal Evidence Act (PACE) (Amended October 14). London: UK Government.
X. United Nations. (2018). UNCITRAL model law on electronic commerce. New York: United Nations.

Judicial Decisions

I. 1-Court of Cassation (UAE). (1989). Criminal appeal No. 101/10, Session of January 4, 1989.
II. 2-Court of Cassation (UAE). (1992). Criminal appeal No. 179/13, Session of April 22, 1992.

III. 3-Federal Supreme Court (UAE). (2017). Criminal appeal No. 102, Session of April 4, 2017.

Foreign References

I. Casey, E. (2004). Digital evidence and computer crime (2nd ed.). Amsterdam: Elsevier. ISBN 0-12-163104.

Websites

I. Kamel, M. (n.d.). Criminal investigation of cybercrimes. Retrieved from https://amday5