وسائل الإثبات في الجرائم السيبرانية: دراسة مقارنة على الواقع اليمني

Means of Proof in Cybercrimes: A Comparative Study with Application to the Yemeni Context

أ. **مجاهد أحمد أحمد العمدي:** باحث في مرحلة الدكتوراه، قسم القانون العام، كلية الشريعة والقانون، جامعة صنعاء، اليمن.

Mujahid Ahmed Ahmed Al-Amdi: *Ph.D. Researcher, Department of Public Law, Faculty of Sharia and Law, Sana'a University, Yemen.*

Doi: https://doi.org/10.56989/benkj.v6i5.1900

تاريخ الاستلام:	2026-03-04	تاريخ القبول:	2026-03-29	تاريخ النشر	2026-05-01

الملخص:

تتناول هذه الدراسة وسائل الإثبات في الجرائم السيبرانية، دراسةً مقارنةً على الواقع اليمني، بهدف الكشف عن الطبيعة القانونية للدليل الرقمي وخصائصه الفنية (اللامادية، قابليته للتلاعب، صعوبة إتلافه)، وأنواعه، وشروط قبوله، وحجيته. تكمن المشكلة الجوهرية في التباين بين تطور تقنيات الإثبات الرقمي وعجز الإطار التشريعي والإجرائي التقليدي عن استيعابها، وهو ما يتجسد حادًا في النظام القضائي اليمني، الذي يعاني من فراغ تشريعي، وقصور فني، وضعف البنية التحتية. وباعتماد المنهجين التحليلي والمقارن، تخلص الدراسة إلى أن فعالية الدليل الرقمي تتطلب ضوابط دقيقة (المشروعية، سلامة الدليل، سلسلة الحيازة، الخبرة الفنية)، مع توصيات جوهرية تتمثل في: إصدار تشريعات يمنية متخصصة، إنشاء مختبرات جنائية رقمية، تشكيل دوائر قضائية متخصصة، ومواءمة التشريعات مع المعايير الدولية، كاتفاقية بودابست..

الكلمات المفتاحية: الإثبات الرقمي، الجرائم السيبرانية، الدليل الإلكتروني، حجية الدليل، الإجراءات الجنائية، الأدلة الرقمية، التحقيق الجنائي، الجرائم الإلكترونية

Abstract:

This study examines "Means of Proof in Cybercrimes: A Comparative Study of the Yemeni Context", digital evidence in cybercrimes through a comparative analysis of the Yemeni context, aiming to reveal the legal nature of digital evidence and its technical characteristics (immutability, manipulability, difficulty of destruction), along with its types, admissibility conditions, and probative value. The core problem lies in the disparity between evolving digital evidentiary techniques and the inability of traditional legal and procedural frameworks to accommodate them, acutely manifested in the Yemeni judicial system, which suffers from legislative vacuum, technical deficiencies, and weak infrastructure. Employing analytical and comparative methodologies, the study concludes that effective digital evidence requires precise controls (legality, evidence integrity, chain of custody, forensic expertise), with key recommendations including: enacting specialized Yemeni legislation, establishing digital forensic laboratories, forming specialized judicial chambers, and harmonizing national legislation with international standards such as the Budapest Convention.

Keywords: Digital Evidence, Cybercrime, Electronic Evidence, Evidentiary Value, Criminal Procedure, Digital Forensics, Criminal Investigation, Cyber Offenses

المقدمة:

تُعد وسائل الإثبات حجر الزاوية في العملية الجنائية، إذ يعتمد عليها القاضي في تكوين قناعته حول ارتكاب الفعل المجرَّم ونسبته إلى المتهم، ومع تطور التقنية وانتقال الجريمة إلى الفضاء السيبراني، برزت الحاجة إلى تطوير منظومة الإثبات بما يتلاءم مع طبيعة هذا النوع من الجرائم، حيث إن البيانات الرقمية هي الوسيلة الأساسية لإثبات وقوع الجريمة وتحديد هوية مرتكبها، وتتميز الأدلة في هذا المجال بكونها غير مادية، متغيرة بسرعة، وسهلة الإخفاء أو التلاعب، ما يفرض تحديات على أجهزة إنفاذ القانون، والنيابة العامة، والسلطة القضائية.

وقد تناولت التشريعات الحديثة وسائل الإثبات الرقمية باهتمام خاص، وأقرّ بعضها حجيتها متى استوفت المعايير الفنية اللازمة، ومع ذلك، فإن التعامل مع هذه الوسائل لا يزال محفوفًا بالعديد من الإشكالات القانونية والفنية، خصوصًا فيما يتعلق بسلامة الدليل، وحفظه، وإمكانية الاعتماد عليه أمام القضاء الجنائي. لذلك، يتناول هذا المبحث أهم جوانب وسائل الإثبات الرقمية في الجرائم السيبرانية، من حيث طبيعتها وأنواعها، وحجيتها القانونية، والتحديات المرتبطة بها.

مشكلة الدراسة:

تكمن المشكلة الجوهرية في التناقض بين الطبيعة المتطورة للدليل الرقمي وقصور المنظومة القانونية التقليدية عن استيعابه. ويتجلى ذلك حادًا في السياق اليمني من خلال: فراغ تشريعي صريح في قانون الإجراءات الجزائية والإثبات بشأن الدليل الرقمي، وغموض المشاريع التشريعية المقترحة وتقصيرها في ضبط مفهوم الدليل وآليات توثيقه، وغياب البنية التحتية التقنية والبروتوكولات الفنية اللازمة لضبط الأدلة، وانعدام التأهيل القضائي المتخصص في المجال الرقمي، ورفض أدلة رقمية جوهرية أو إصدار أحكام بضعف تسبيب، مما يهدد بفشل تحقيق العدالة الجنائية.

تتمثل مشكلة الدراسة في التساؤل الرئيسي التالي:

- ما هي الطبيعة القانونية للدليل الرقمي والتحديات التشريعية والفنية والقضائية التي تواجه قبوله أمام القضاء اليمني؟

ويتجسد التساؤل الرئيسي في الأسئلة الفرعية التالية:

- مفهوم الدليل الرقمي وخصائصه المميزة عن الأدلة التقليدية؟
- أنواعه وشروط اكتسابه الحجية القانونية؟
- الصعوبات (التشريعية، والإجرائية، والفنية، والقضائية) في النظام اليمني؟
- سبل تطوير الإطار التشريعي والقضائي اليمني؟

أهداف الدراسة:

- التوصيف العلمي لمفهوم الدليل الرقمي وطبيعته القانونية وخصائصه الفنية.
- التحليل المعياري لأنواع الإثبات الرقمي وشروط حجيتها القانونية والفنية.
- التشخيص الموضوعي لإشكالات وعناصر الضعف في النظام القضائي اليمني.
- صياغة مقترحات عملية تشمل التعديل التشريعي، وإنشاء مختبرات جنائية رقمية، وتأهيل الكوادر.

منهج الدراسة:

اعتمد الباحث المنهج التحليلي الاستقرائي، لتحليل النصوص القانونية المقارنة (اليمنية، والمصرية، والإماراتية، والسعودية)، ودراسة الاتفاقيات الدولية (اتفاقية بودابست)، وتحليل خصائص الدليل الرقمي وشروط قبوله وأسباب القصور اليمني.

كما تم استخدام المنهج المقارن، لمقارنة التشريعات والاجتهادات القضائية في الدول المدروسة مع الواقع اليمني، واستجلاء أوجه القصور، واستخلاص الدروس من التجارب المتقدمة.

أهمية الدراسة:

- الأهمية النظرية: تمثلت في إثراء الفقه القانوني في مجال الإجراءات الجنائية والإثبات الرقمي، وبناء إطار نظري متكامل يميز الدليل الرقمي عن الأدلة التقليدية، وتقديم قراءة نقدية للمشاريع التشريعية اليمنية، وكشف مواطن القصور.
- الأهمية العملية: تمثلت في توفير مرجعية علمية لتسريع إصدار تشريعات ناضجة تنظم الإثبات الرقمي، وإعداد دليل إرشادي للقضاة والنيابة لتقييم حجية الأدلة الرقمية، ووضع بروتوكولات واضحة للتعامل مع مسرح الجريمة الرقمية وسلسلة الحيازة، وتعزيز الثقة في قدرة القضاء على ملاحقة الجناة السيبرانيين وحماية الحقوق.

المبحث الأول: مفهوم الأدلة الرقمية وخصائصها

تتميز الأدلة الرقمية بخصوصية تجعل التعامل معها مختلفًا عن الأدلة المادية؛ فهي غير ملموسة، وقابلة للنسخ أو التعديل، وسريعة الزوال، كما أنها تنتج غالبًا من بيئات افتراضية يصعب فيها تحديد الجهة الفاعلة بدقة[1]، بخلاف الأدلة المادية التي قد يتم التعامل معها بشكل مباشر في مسرح الجريمة، فإن الأدلة الرقمية توجد غالبًا على وسائط إلكترونية وتتطلب أدوات وتقنيات متقدمة

[1]– المري، بهاء، جرائم المحمول الإنترنت، ص368.

لاكتشافها وتحليلها، مثل أدوات المسح الجنائي الرقمي وبرمجيات استعادة البيانات، كما أن طبيعَتها القابلة للتعديل تتطلب إجراءات خاصة لحمايتها منذ لحظة الضبط حتى العرض أمام القضاء[1].

وبناء على ذلك فإن التساؤل الذي يثور هنا هو: ما هو الدليل الرقمي؟ وماهي طبيعته القانونية؟ وما هي خصائصه الذاتية التي تميزه عن الدليل التقليدي؟ وما هي أنواع الدليل الرقمي؟ ونجيب على ذلك من خلال الآتي:

أولاً: مفهوم الدليل الرقمي في الإثبات الجنائي

لما كانت الجرائم السيبرانية كغيرها من الجرائم، لها أركانها وعناصرها، وتمر بذات المراحل التي تمر بها الجريمة التقليدية، من مراحل التفكير والتحضير، ثم تبدأ بعملية التنفيذ، وصولًا إلى إتمام الجريمة بتعريض المصلحة المحمية قانونًا للخطر أو إلحاق الضرر بها، وفي جميع تلك المراحل يوجد أثر مادي، وهو المتمثل في الدليل الرقمي[2].

وقد اختلفت التعريفات التي تناولت الدليل الرقمي، فمنها ما هو موسع، ومنها ما هو مضيق، ونجد أن التشريعات، على اختلافها، قد وضعت تحديدًا لمفهوم الدليل الرقمي، ومن ذلك نجد أن المشرع الإماراتي قد عرفه في قانون مكافحة الشائعات والجرائم الإلكترونية، الدليلَ الرقمي في المادة (1) بأنه: (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)[3].

وهو نفسه التعريف الذي أورده المشرع المصري في قانون مكافحة الجرائم الإلكترونية في المادة الأولى، بينما نجد أن المشاريع المتعاقبة لقانون مكافحة الجرائم الإلكترونية في اليمن لم تعر الموضوع أي اهتمام ولم تقدم أي تعريف للدليل الرقمي[4].

---

(1) الليثي، عمرو سعدالدين طه: الإثبات الجنائي في مجال الجرائم الناشئة عن استخدام شبكة المعلومات الدولية، مرجع سابق، ص66.

2 – وفق أحدث النظريات الجنائية التي يطبق عليها نظرية تبادل الآثار بين الجريمة والشخص مرتكب الجريمة والتي تعني وجود تبادل جزيئات من المواد أو الأجسام التي تلامس أو تحتك به فيتخلف عن كل جريمة آثار وهي تعد مصادر الدليل الجنائي؛ للمزيد انظر: عالية، سمير: الجرائم الإلكترونية، مرجع سابق، ص427؛ الليثي، عمرو سعدالدين طه: الإثبات الجنائي، مرجع سابق، ص66.

3 – مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

4 – جاء النص على النحو الآتي: (الدليل الرقمي: 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).

وقد جاء نظام الإثبات السعودي بتعريف الدليل الرقمي في مادته الثالثة والخمسين 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)[1].

وعرف بعض الفقهاء الدليل الرقمي بأنه:(كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو متنقلة عبرها بواسطة شبكة الاتصالات في شكل مجالات إلكترونية أو ذبذبات كهربائية أو نبضات مغناطيسية يتم استخلاصها وجمعها وتحليلها وفق إجراءات قانونية وعلمية، وترجمتها لتظهر في شكل مخرجات يقبلها العقل والمنطق ويعتمدها العلم، ويمكن استخدامها في أية مرحلة من مراحل التحقيق والمحاكمة لإثبات الجريمة وتقرير البراءة أو الإدانة)[2].

ويمكن القول بأن التعريف الأشمل للدليل الرقمي هو ما جاء عند بعض الفقهاء بأنه:(مجموعة مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية أو غيرها؛ لتقديمها إلى القضاء بغرض إثبات الوقائع الجرمية، أو لتقرير إدانة أو براءة المتهمين بارتكابها)[3].

فهذا التعريف يعطي مفهوما شاملا للدليل الرقمي من حيث بيان طبيعته الفنية والتقنية وشموله لجميع الوسائل التقنية التي تستخدم لاستخلاص الدليل الإلكتروني في الإثبات الجنائي، وعلى ذلك يمكن الوقوف على حقيقة الدليل الرقمي وفق المحددات الآتية:

1. أن الأدلة الرقمية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة.
2. الأدلة الرقمية أدلة مادية وتحليلية في شكلها وحجمها.
3. يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل.
4. سهولة الكشف عن الأدلة الرقمية المزورة.

(1)نظام الإثبات السعودي رقم (م/٤٣) وتاريخ ٢٦ /٠٥/ ١٤٤٣هـ وتعديلاته/ منشور عبر منصة نظام متاح على الرابط: https://nezams.com

(1)جمال، إبراهيم: التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص123؛ الليثي، عمرو سعدالدين طه: الإثبات الجنائي في مجال الجرائم الناشئة عن استخدام شبكة المعلومات الدولية، مرجع سابق، ص68.

(2)العمري، أحمد محمد: الدليل الرقمي وحجيته في الإثبات الجزائي، مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، سلطنة عمان، العدد 3، 2020، ص131؛ بطيخ، حاتم أحمد محمد: دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، مرجع سابق، ص388.

ويمكن التحصل على الدليل الرقمي من خلال المواقع المختلفة أو من البريد الإلكتروني أو من الفيديو الرقمي أو الصوت الرقمي أو من غرف الدردشة والمحادثات أو من المنصات الشخصية أو من الصور المرئية أو من الدخول على الشبكات من خلال مزود الخدمة وهكذا[1].

ثانياً: خصائص وسائل الإثبات الرقمية

يرى البعض أن الأدلة الرقمية ما هي إلا مرحلة متقدمة من الأدلة التقليدية المادية التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان، وأنه يمكن الاستعانة بجميع ما يبتكره العلم من وسائل التقنية العالية بما فيها جهاز الحاسب في عملية الإثبات الجنائي، بينما الواقع يثبت أن الأدلة الرقمية هي نوع آخر من الأدلة الجنائية المستحدثة التي لها من الخصائص العلمية والمواصفات القانونية ما يميزها عن غيرها من وسائل الإثبات التقليدية، وهذه الخصائص مرتبطة أساسا بطبيعة البيئة التي يتواجد فيها الدليل الرقمي[2].

1. الطبيعة الرقمية

يتميز الدليل الرقمي بأنه غير مادي[3]، فالدليل الرقمي يوجد في شكل بيانات إلكترونية مخزنة على وسائط رقمية مثل: الحواسيب، الهواتف، الخوادم، الأقراص الصلبة، وهذه البيانات لا تُفهم بشكل مباشر أو باستخدام الوسائل التقليدية، بل لا بد من وجود أجهزة وبرمجيات خاصة لتحليل محتواه. مثال: لا يمكن رؤية "الملف المحذوف" بالعين المجردة، لكنه قد يُسترجع باستخدام أدوات التحليل الجنائي الرقمي Forensic Tools، وهذا يتطلب وجود خبرة فنية للتعامل معها[4].

وعلى ذلك فلابد من التوفيق بين الدليل الرقمي المحدد وبين البيئة التي يعيش فيها أو البيئة التي ارتكبت الجريمة فيها سواء كانت مؤسسات مالية أو وسائل التواصل الاجتماعي أو غيرها من المواقع التقنية، بمعنى يجب أن يكون الدليل الرقمي مستمداً أو مستوحى أو مستنبطاً من البيئة التي ارتكبت فيها الجريمة وهي بيئة رقمية ممثلة في العالم الافتراضي[5].

---

(1) المري، مرجع سابق، ص370.

(2) حمودة، علي محمود علي: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية الذي نظمته أكاديمية شرطة دبي، 26 نيسان 2003تاريخ الانتهاء: 28 نيسان 2003، ص77.

(3) وقد أكدت محكمة النقض المصرية في الطعن رقم ١٥٢٣٠ لسنة ٨٥ قضائية على أنه "لا يشترط في الدليل أن يكون مادياً محسوساً، ما دام مؤداه واضحًا وتتمكن المحكمة من تكوين عقيدتها من خلاله"؛ للمزيد انظر: سرور، أحمد فتحي، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، 2010، ص414.

4 – المحبشي، مرجع سابق، ص123.

(1) الليثي، مرجع سابق، ص83.

2. السهولة في التغيير أو التلاعب

يُعد الدليل الرقمي هشاً من حيث قابليته للتعديل أو الحذف دون ترك أثر ملموس[1]، مقارنة بالأدلة التقليدية، ويمكن لأي مستخدم لديه صلاحيات أو مهارات معينة أن يغير أو يحذف الدليل الرقمي بكبسة زر فقط، كذلك يمكن "تزوير" دليل رقمي مثل تزوير بريد إلكتروني أو فبركة صورة أو فيديو باستخدام الذكاء الاصطناعي، ما يتطلب إجراءات صارمة لحمايته أثناء الجمع والتحريز، بمعنى آخر يجب توثيق الدليل الرقمي من لحظة جمعه باستخدام برامج توليد القيم الهاش Hash Valuesأو لقطات الشاشة الموثقة، على أن أي خلل في سلسلة الحيازةChain of Custody قد يؤدي إلى استبعاد الدليل من قبل المحكمة[2].

3. الدليل الرقمي يصعب التخلص منه

يمتاز الدليل الرقمي بصعوبة إتلافه، إذ تتطابق طريقة النسخ مع طريقة الإنشاء فالمعلومات التي يتم تخزينها في وسائط التخزين الثابتة والمتحركة من الصعوبة التخلص منها نهائيا حتى وإن تم محوها أو مسحها من خلال أنظمة التشغيل فإنه يمكن استرجاعها بواسطة برامج خاصة[3]، كما يمتاز الدليل الرقمي بإمكانية نسخه عدداً لا محدوداً من المرات دون التأثير في النسخة الأصلية، بعكس المستندات الورقية أو الأشياء المادية التي قد تتأثر من التكرار أو النقل إما بالتلف أو التغير ومحكمة النقض الإماراتية قضت بتاريخ 2016/3/20، مؤكدة أن "نسخة البريد الإلكتروني المعززة بتقرير فني من جهة محايدة تثبت مطابقتها للأصل تُعد دليلاً كافياً للإدانة.."[4].

وعلى ذلك فإن موضوع التخلص من الدليل الرقمي باستخدام خصائص من الملفات في الحاسوب أو الإنترنت لا تعد من العوائق التي تحول دون استرجاع هذه الأدلة باستخدام برمجيات رقمية معينة، فقد أثبتت التجارب أنه يمكن استعادة 95% من تلك الملفات[5].

---

(2) على الرغم من أن البعض يرى أنه يسهل كشف التعديل والتغيير الذي يطرأ على الدليل الرقمي من خلال استخدام برامج معينة، إلا أنه مع ذلك ليست كل الأدلة ينطبق عليها هذا الوصف فمنها مالا يمكن كشفه؛ للمزيد انظر: عالية، مرجع سابق، ص430.

(3) عبدالحميد، عادل، الجرائم الإلكترونية والإثبات الرقمي، دار النهضة العربية، 2018، ص205؛ عبدالفتاح، عمرو، جرائم تقنية المعلومات والإثبات الجنائي الرقمي، دار النهضة العربية، 2020، ص139.

(4) بطيخ، حاتم أحمد محمد: دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، مرجع سابق، ص400.

(1) عبدالفتاح، طارق، الإثبات في الجرائم الإلكترونية، دار الجامعة الجديدة، 2020، ص177؛ عودة، خالد، "الإثبات الإلكتروني في القانون الجنائي"، مجلة الدراسات القانونية، العدد 12، 2019، ص221.

(2) وهناك برامج وأجهزة خصصت لهذا الغرض وذلك حسب نوع التدقيقات المطلوبة على سبيل المثال: الأدلة الجنائية الرقمية للشبكات من أنواعها وأشهرها Silent Run Enterprise FTK؛ الأدلة الجنائية الرقمية للكمبيوترات

4. الحاجة إلى الخبرة الفنية لتحليله وفهمه

يتطلب فهم وتفسير الدليل الرقمي خبرة تقنية متخصصة، سواء من جانب المحقق أو القاضي أو المحامي، لأن هذا الدليل في كثير من الأحيان يتطلب استخدام برامج تحليل جنائي رقمي، فلا يمكن فحص أو تقديم الدليل الرقمي أمام القضاء دون الاستعانة بخبراء في المجال التقني[1]، ما يبرز دور "الخبير الفني الرقمي" كعنصر محوري في تفسير البيانات الإلكترونية، وتقديم تقرير فني يساعد القاضي على فهم طبيعة الدليل وتقييم حجيته[2]، وهنا نجد أن محكمة جنايات القاهرة قررت إحالة القضية إلى خبير فني لبيان ولفحص ما إذا كانت الصور المستخرجة من الهاتف الخاص بالمتهم قد تم تعديلها أو لا، معتبرة أن "الإثبات الفني هو الوسيلة الوحيدة للفصل في النزاع"[3].

5. الإمكانية العالية للتخزين والنقل

تُعد قابلية التخزين والنقل من السمات الجوهرية التي تُميز الأدلة الرقمية عن نظيراتها التقليدية فبفضل طبيعة البيانات الرقمية، يمكن تخزين كميات هائلة من المعلومات على وسائط صغيرة الحجم مثل الأقراص الصلبة، وأجهزةUSB ، والبطاقات الذكية، بل وحتى عبر منصات التخزين السحابي، دون أن يؤثر ذلك في جودة البيانات أو مساحتها[4].

كما يمكن نقل هذه الأدلة بسرعة فائقة عبر شبكات الاتصال (مثل الإنترنت أو الشبكات الداخلية) إلى أي مكان في العالم، وهو ما يسهل عملية تداولها بين جهات التحقيق والجهات القضائية والخبراء الفنيين، هذه القابلية للنقل الفوري والعابر للحدود تخلق في المقابل تحديات تتعلق بسلامة الدليل أثناء النقل، وضرورة حفظ "سلسلة الحيازة (Chain of Custody) "لضمان عدم العبث به، فقد نصت المعايير الدولية، مثل دليل بوديستا(Budapest Convention on Cybercrime) ،

والإلكترونيات من أنواعها وأشهرها Encase FTk LAP FTK وبعض الأجهزة المساندة مثل رايت بلوك Block Write؛ الأدلة الجنائية الرقمية للاتصالات من أنواعها وأشهرها Mobile FTK Forensic Oxygen XRY Phone Examiner

(3)تمر عملية استخلاص الدليل الرقمي بثلاث مراحل: مرحلة المعاينة، ومرحلة التحريز، ومرحلة المعالجة والتحليل، ثم يتم تقييم الدليل وعرض النتائج التي توصل إليها أمام الجهات القضائية، وهذا يتطلب إنشاء معامل ومختبرات خاصة وإعداد خبراء وفنيين وقانونيين. بطيخ، حاتم أحمد محمد: دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري، مرجع سابق، ص399.

(1)عبدالفتاح، مرجع سابق، ص177؛ لطفي، حسام، "الملكية الفكرية وجرائم الإنترنت"، دار المطبوعات الجامعية، 2019، ص273.

(2)حكمها في القضية رقم 4172 لسنة 2020 جنايات.

(3)مرسي، محمد، الإثبات الجنائي الإلكتروني، دار الجامعة الجديدة، الإسكندرية، 2021، ص156.

على أهمية ضمان أمن البيانات الرقمية المنقولة وتوثيق كل مراحل التعامل معها، بدءًا من جمعها ومرورًا بحفظها، وانتهاءً بعرضها على المحكمة[1].

وخلاصة القول: أن الدليل الرقمي يعد أداة فاعلة في إثبات الجرائم الإلكترونية، لكنه في الوقت ذاته يتطلب ضوابط دقيقة وإجراءات تقنية وقانونية تضمن سلامته وقبوله أمام القضاء، وهو ما أكدته الأحكام القضائية المقارنة حيث بينت أهمية مراعاة المعايير الدولية والوطنية عند جمع وتحليل وتقديم الأدلة الرقمية، لضمان تحقيق العدالة الجنائية في ظل البيئة الرقمية المعاصرة.

فالدليل الرقمي يُعد من أبرز مظاهر التطور في وسائل الإثبات الحديثة، إذ يكتسب خصوصيته من طبيعته غير المادية، وقابليته العالية للنسخ والتخزين والنقل، مما يمنحه مرونة كبيرة في الاستخدام، ولكنه يضع في المقابل عبئاً على السلطات القضائية والتحقيقية لضمان صحة هذا الدليل وسلامته، فسهولة التعديل والتلاعب تفرض ضرورة وجود إجراءات فنية دقيقة، مثل التحقق من البصمات الرقمية، والتقارير الفنية المحايدة، وسلسلة الحيازة الرقمية، لضمان حجية الدليل أمام المحاكم[2].

وتُبرز هذه الخصائص الحاجة الملحّة إلى تطوير البنية القانونية والإجرائية للتعامل مع هذا النوع من الأدلة، خاصة من حيث التأهيل الفني للقضاة وأعضاء النيابة، وتفعيل دور الخبرة الفنية الرقمية، كما أن قابلية الدليل الرقمي للنقل العابر للحدود تطرح إشكاليات قانونية في ظل تنوع التشريعات وتفاوت مستويات الحماية، ما يدعو إلى تعزيز التعاون القضائي الدولي، وتبني معايير موحدة مستندة إلى الاتفاقيات الدولية مثل اتفاقية بودابست لمكافحة الجريمة المعلوماتية.

المبحث الثاني: أنواع الدليل الرقمي وحجيته في الإثبات الجنائي:

تتعدد أنواع وسائل الإثبات الرقمية بتعدد مصادرها وأشكالها الفنية، وتشترك جميعها في كونها تنتج عن استخدام أجهزة أو نظم إلكترونية، وتُختزن غالباً على وسائط رقمية أو سحابية، ويمكن تصنيف هذه الوسائل إلى عدة أنواع رئيسية وفقاً لمصدرها وطبيعتها، على النحو الآتي:

أولاً: البريد الإلكتروني:

يُعد البريد الإلكتروني من أكثر وسائل الإثبات الرقمية استخداماً، خاصة في الجرائم الاقتصادية والسيبرانية، مثل الاحتيال، والابتزاز، والاختراق[3]، وتكمن حجيته في إمكانية توثيقه زمنياً وفنياً،

(4) Council of Europe, Convention on Cybercrime (ETS No.185), Explanatory Report,2001, para. 146.

(1) المحبشي، مرجع سابق، ص128.

(1) قضت محكمة النقض الإماراتية، في جلستها العلنية بتاريخ 2016/3/20، فقد اعتبرت نسخة البريد الإلكتروني المدعومة بتقرير فني من جهة محايدة دليلاً كافياً للإدانة.

خصوصًا في المراسلات المتبادلة، حيث يُظهر تسلسل الرسائل مدى منطقية الحوار والربط بين الفعل الجرمي والرسالة، كما يمكن التحقق من الهوية الرقمية من خلال عنوان البريد الإلكتروني والتوقيع الرقمي، أو رأس الرسالة (Headers)، فضلاً عن إمكانية التحقق من سلامة المحتوى حيث يُثبت فنيًا أن الرسالة لم تتعرض للتعديل أو الحذف وهو ما يتم من خلال التقارير الفنية من جهات محايدة[1].

وقد اعترفت العديد من التشريعات بحجية رسائل البريد الإلكتروني في الإثبات من ذلك نجد نص المادة 10 من قانون أنظمة الدفع والعمليات المالية المصرفية الإلكترونية وقد جرى نصها على النحو الآتي " يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الخطية من حيث إلزامها لأطرافها أو حجيتها في الإثبات". وهو ما نص عليه المشرع المصري في المادة 9 من قانون المعاملات الإلكترونية رقم 15 لسنة 2017م، والمشرع الإماراتي في المادة 5 من قانون المعاملات الإلكترونية وخدمات الثقة رقم 46 لسنة 2021.

كما سار القضاء على الاعتراف بالبريد الإلكتروني في الإثبات الجنائي، من ذلك نجد حكم محكمة النقض الإماراتية، حيث قضت بأن"نسخة البريد الإلكتروني المعززة بتقرير فني من جهة محايدة تثبت مطابقتها للأصل تُعد دليلاً كافياً للإدانة "[2].

كما أكدت المحاكم المصرية في العديد من أحكامها على حجية البريد الإلكتروني إذا ما توافر التوقيع الإلكتروني أو تقرير فني موثوق يثبت عدم العبث به، فقد أكدت محكمة النقض أن الرسائل الإلكترونية، بما فيها البريد الإلكتروني، تُعد وسيلة إثبات مقبولة، شريطة ثبوت نسبتها إلى صاحبها. وأوضحت أن المحرر الإلكتروني لا يشترط أن يكون مكتوبًا على ورق، بل يكفي أن يُثبت نسبته إلى صاحبه، ما يوجب قبول الدعامات الإلكترونية الأخرى في الإثبات[3].

ثانياً: المحادثات النصية ورسائل التطبيقات كوسيلة إثبات:

تشمل هذه الوسيلة كافة الرسائل النصية القصيرة(SMS)[4] أو الرسائل المتبادلة عبر تطبيقات المحادثة مثل Facebook Messenger, Signal, Telegram, WhatsApp وغيرها، وتبرز أهميتها في العديد من القضايا، خاصة المتعلقة بالتهديد، الابتزاز، التحريض، أو الاتفاقات بين الجناة،

(2)سامي يوسف حسن، الإثبات بالوسائل الإلكترونية، دار الفكر الجامعي، 2021، ص104.

(1)حكم محكمة النقض الإمارتية في جلسة 2016/3/20.

(2)في الطعن رقم 17689 لسنة 89 قضائية، جلسة 10 مارس 2020.

(3)للمزيد حول هذه الرسائل وآلية عملها انظر: الترزي، نديم محمد: الإقرار بواسطة الوسائل الحديثة في القضايا الجنائية، مكتبة الصادق، 2012، ص228.

سواء في الجرائم التقليدية أو الجرائم السيبرانية، وتتميز هذه الرسائل بأنها غالبًا ما تتضمن نصوصًا صريحة أو صورًا ووسائط متعددة (مثل تسجيلات صوتية أو فيديوهات)، ما يجعلها أداة إثبات فعالة ومباشرة، حيث تُعد الرسائل الإلكترونية، ومحادثات التطبيقات الفورية، من الأدلة الشائعة في الجرائم السيبرانية، إذ تمثل إقرارًا ضمنيًا أو دليلاً على النية الجنائية. وتتمتع هذه الأدلة بالحجية متى تم توثيقها وفقًا للقواعد المعتمدة[1].

ولقبول هذه الرسائل كدليل أمام القضاء، يجب مراعاة عدة ضوابط فنية وقانونية، منها: ربط الرسالة بهوية مستخدم محدد، مثل: رقم الهاتف، الحساب الشخصي، الجهاز المستخدم، وتحديد السياق الزمني والمكاني للرسالة (من خلال بيانات "metadata" أو سجل التطبيق)[2]. وسلامة الرسالة من التعديل أو الحذف، وذلك عبر تقارير الفحص الجنائي الرقمي. وأخيراً تأكيد أن الرسالة لم تُفبرك أو تُنتج بواسطة برامج اصطناعية (مثل deep fake أو spoofing)[3].

وهنا يتجه القضاء الحديث إلى قبول رسائل التطبيقات كدليل، متى ثبت صدورها من المتهم أو من جهاز مرتبط به، وكانت مرفقة بتقارير فنية توثق صحة المصدر وسلامة البيانات، فقد اعترفت محكمة النقض المصرية في حكم حديث لها بالأدلة الرقمية كوسيلة إثبات، عندما اعتبرت المحادثات المستخرجة من تطبيق "WhatsApp " دليلاً معتمدًا، شريطة أن يكون استخراجها قد تم بأمر قضائي وبمعرفة خبير تقني معتمد. وقد شددت المحكمة في هذا الحكم على ضرورة توافر ما يسمى ب "القرينة الرقمية"، أي وجود دلائل إضافية تدعم صدقية الدليل الرقمي وتربطه بالمتهم بشكل مباشر[4]. كما حكمت محكمة جنايات القاهرة بإدانة متهم في واقعة تحريض جنسي، مستندة إلى رسائل WhatsApp، واعتبرت أنها صادرة عن المتهم استنادًا إلى فحص جهازه، وتقرير فني أثبت أن الرسائل لم يتم تعديلها[5]، كما طبّقت المحكمة الاقتصادية في مصر هذه القاعدة في الدعوى رقم 319 لسنة 2021، حيث أمرت بتجميد بيانات حساب تيليغرام لحين استخراج الرسائل التي تضمنت عبارات التحريض والإساءة[6]، وكذا قضت محكمة أبوظبي للأسرة والدعاوى المدنية والإدارية بجواز

(1) أبو دياب، علي السيد على حسين: أضواء على حجية الرسائل في الإثبات في مواقع التواصل الاجتماعي، مجلة كلية الشريعة والقانون، جامعة الأزهر بطنطا، العدد 32، ج 3، 2017، ص956؛ الليثي، مرجع سابق، 234.

(2) الترزي، مرجع سابق، ص228.

(3) عبدالفتاح، مرجع سابق، ص184.

(4) نقض مصري، طعن رقم 540 لسنة 91 ق، جلسة 24 مارس 2021.

(1) محكمة جنايات القاهرة قضت في 2021 كما قضت المحكمة الاقتصادية لاستئناف قنا في فبراير 2024، بتغريم طبيب 6 آلاف جنيه لتهديده زوجته عبر رسائل WhatsApp. استندت المحكمة إلى الرسائل المرفقة في الدعوى كدليل على التهديد، ما يدل على قبول رسائل التطبيقات كوسيلة إثبات في القضايا الجنائية.

(2) المحكمة الاقتصادية المصرية، الدعوى رقم 319 لسنة 2021م.

الاعتماد على رسائل Telegram و WhatsApp واعتبرتها دليلًا سائغًا، طالما تم ربطها بحساب محدد، وجرى تحليلها رقميًا من قبل جهة مختصة[1].

ثالثاً: الصور ومقاطع الفيديو الرقمية(Digital Images & Videos):

تُعد الصور ومقاطع الفيديو الرقمية من أبرز أدوات الإثبات الحديثة في البيئة السيبرانية، إذ تُستخدم لإثبات الوقائع الجنائية، مثل التشهير، الابتزاز، التحرش، أو حتى إثبات الدخول غير المشروع إلى الأنظمة، وتكمن حجيتها في قدرتها على توثيق الواقعة بشكل بصري مباشر، وهو ما يمنحها قوة ثبوتية عالية إذا ما تم التأكد من صدقها وسلامتها من التلاعب، وقد تبنت هذا الموقف العديد من التشريعات الحديثة، من ذلك نجد نص المادة 15 من قانون الإثبات الإماراتي، حيث تؤكد أن الأدلة الرقمية تشمل الصور ومقاطع الفيديو بشرط التحقق من موثوقيتها ومصدرها وتمامها[2].

ولقبول هذا النوع من الأدلة فإن المحاكم تفحص مجموعة من العناصر الأساسية لها من ذلك: سلامة المصدر حيث يجب أن تكون ملتقطة من جهاز معروف أو موثق الملكية. وعدم التلاعب الرقمي بهذه الأدلة وهو ما يثبته تقرير فني من جهة محايدة باستخدام أدوات التحليل الجنائي الرقمي (Forensic tools). مع ضرورة الربط بالواقعة محل الاتهام: يجب أن تكون الصور أو المقاطع متعلقة مباشرة بالجريمة. كما يجب التحقق من التوقيت والمكان: خاصة عبر بيانات ال Metadata (مثل الوقت، الموقع، الجهاز المستخدم)[3].

وقد استقر القضاء على قبول هذه الصور ومقاطع الفيديو كدليل في الإثبات أمام القضاء، فقد قضت محكمة النقض المصرية بأن الصور الضوئية للأوراق العرفية لا حجية لها في الإثبات إلا بمقدار ما تهدي إلى الأصل الموقع عليه، وفي حالة عدم وجود الأصل وإنكار الخصم لها، لا يُعتد بها كدليل[4]، كما أقرت المحكمة العليا اليمنية حجية القرص المضغوط الذي يحتوي على تسجيل

(3)حكم صادر عن محكمة أبو ظبي للأسرة والدعاوى المدنية والإدارية في 11 أكتوبر 2023م، كما ألزمت محكمة أبوظبي للأسرة والدعاوى المدنية والإدارية شابًا بإعادة مبلغ 300 ألف درهم لصديقه، استنادًا إلى رسائل WhatsApp التي تثبت إقراض المبلغ. وأكدت المحكمة أن الرسائل الإلكترونية تُعد دليلًا مقبولًا في الإثبات، ولا تفقد أثرها القانوني لمجرد أنها جاءت في شكل إلكتروني، الحكم الصادر في جلسة 20 يوليو 2023م.

(4)القانون الاتحادي رقم 35 لسنة 2022م بشأن الإثبات، وكذا المادة 45 من القانون الاتحادي الإماراتي رقم 34 لسنة 2021، بشأن مكافحة الشائعات والجرائم الإلكترونية.

(1)المحبشي، مرجع سابق، ص261.

(2) للمزيد في مثل هذه الأحكام انظر: المري، مرجع سابق، ص372.

فيديو لواقعة اعتداء، معتبرة أنه دليل قوي إذا ثبت عدم تعرضه للتلاعب، وذلك وفقًا للمادة (155) من قانون الإثبات اليمني[1].

رابعاً: سجلات الدخول وعناوين IP

سجلات الدخول: هي ملفات رقمية تحتفظ بها الخوادم (Servers) أو نظم التشغيل أو التطبيقات، وتوثّق عمليات الدخول إلى النظام، بما في ذلك اسم المستخدم، وتوقيت الدخول والخروج، والأنشطة التي تمت أثناء الجلسة، وأما عنوان الIP (Internet Protocol Address): فهو رقم فريد يُمنح لكل جهاز يتصل بشبكة الإنترنت، ويُستخدم لتحديد موقع الجهاز الجغرافي وشبكته ومزود الخدمة.

وتمثل سجلات الاتصال الإلكتروني وسجلات الدخول (Login logs) وعناوين IP وسائل تقنية لتعقب مصدر الجريمة وتحديد هوية المستخدم، وإثبات وقت ومكان وقوع الجريمة وتحديد الجهاز المستخدم وربط الفعل الإجرامي بشخص معين وتكشف عن التسلسل الزمني للأحداث الإجرامية، فهذه السجلات تعد دليلاً في إثبات وقوع الجريمة، لكنها لا تُعد دليلًا حاسمًا بذاتها، إذ يمكن التحايل باستخدام أدوات إخفاء الهوية[2].

وقد نصت العديد من التشريعات على حجية هذه السجلات في الإثبات وحددت لها شروطاً من ذلك نجد نصي المادتين الثانية والثالثة عشرة من قانون مكافحة جرائم تقنية المعلومات الإلكترونية المصري، والمادة 12 والمادة 41 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي[3].

خلاصة القول إن صحة الدليل الرقمي لا تتوقف فقط على وجوده، بل على توافر شروط دقيقة في طريقة جمعه، وحفظه، وتحليله، وتقديمه، ويُعد الالتزام بهذه الشروط ضرورة قانونية لحماية حقوق المتهم، وضمان عدالة المحاكمة، وتعزيز الثقة في الأدلة الرقمية لدى المحاكم.

(3) الطعن رقم 61294 – جلسة 2018/7/4م.

(1) قضت محكمة جنح الاقتصادية في مصر بإدانة أحد المتهمين في جريمة سبٍّ وقذف إلكتروني، بناءً على تتبع عنوان الIP المستخدم وربطه بالمشترك في خدمة الإنترنت ([حكم جنح الاقتصادية رقم 241 لسنة 2020]).
وانظر ايضاً:
INTERPOL. (2022). Digital Forensics and Challenges in Cybercrime Investigations, pp. 44–47

(2)جاء في مشروع قانون مكافحة الجرائم الإلكترونية (27) على أن "للقاضي أو عضو النيابة المختص الأمر بالحصول على بيانات الدخول أو سجلات الخدمة...". وفي المادة (30)، أعطى القانون قوة إثبات للأدلة المستخرجة من الوسائل الرقمية متى ما تمت وفقًا للإجراءات القانونية.

خامساً: المشروعية القانونية في جمع الدليل:

لا يجوز الاعتماد على دليل رقمي تم الحصول عليه بطرق غير قانونية، كاقتحام الأجهزة الخاصة دون إذن قضائي، أو اعتراض البيانات دون تصريح، بمعنى أنه يجب ألاَّ يتعارض الدليل الرقمي مع الحقوق الدستورية، فيشترط ألا ينتهك جمع الدليل الرقمي حق الخصوصية أو حرية الاتصالات، إلا بإذن قضائي صريح ومسبب، ويُعتبر أي انتهاك لهذه الحقوق سببًا لبطلان الدليل[1].

سادساً: سلامة الدليل الرقمي:

يشترط أن يكون الدليل سليمًا ولم يتعرض لأي تعديل أو تلف أو تلاعب بعد جمعه، ويُستخدم في ذلك ما يُعرف بخوارزميات التحقق مثل التوقيع الرقمي وهاش Hash لإثبات تطابق البيانات مع الأصل[2].

فالدليل الرقمي يجب أن يكون يقينياً وغير قابل للشك، فلا مجال لدحض قرينة البراءة إلا عندما يصل القاضي إلى حد القناعة التامة والجزم واليقين بإدانة الجاني وأنه ارتكب الفعل المجرم ما يوجب عقابه[3].

سابعاً: التسلسل الزمني للحيازة:

يجب توثيق سلسلة انتقال الدليل الرقمي منذ لحظة ضبطه حتى تقديمه في المحكمة، وتحديد من قام بجمعه، ومتى، وكيف، وأين حُفِظ، فأي انقطاع أو غموض في هذه السلسلة قد يؤدي إلى الطعن في مصداقية الدليل[4].

(1) قضت المحكمة الدستورية المصرية في حكمها (الطعن رقم 5 لسنة 25 قضائية دستورية) أن حرمة الحياة الخاصة مصونة، ولا يجوز الاطلاع على محتوى الأجهزة أو المراسلات إلا بإذن قضائي؛ الليثي، مرجع سابق، ص109.

(2) حكم محكمة جنايات شبين الكوم – الاستئناف رقم 1561 لسنة 2024؛ حيث أكدت المحكمة أن الأدلة الرقمية يجب أن تكون قطعية وتعتمد على الجزم واليقين، بحيث تؤدي إلى التسليم بوقوع الجريمة وصحة إسنادها للمتهم دون أي شك. وكذا حكمها في الاستئناف رقم 1561 لسنة 2024، إذ أكدت المحكمة أن الأدلة الرقمية يجب أن تكون قطعية وتعتمد على الجزم واليقين، بحيث تؤدي إلى التسليم بوقوع الجريمة وصحة إسنادها للمتهم دون أي شك.

(3) الليثي، مرجع سابق، ص112.

(4) رفضت محكمة أمريكية (United States v. Riccardi, 2008) قبول صور رقمية كدليل لعدم وجود تسلسل حيازة موثق.

ثامناً: الاعتماد على خبرة فنية مختصة:

لا يُمكن للقاضي أو المحقق العادي فهم تفاصيل الدليل الرقمي المعقدة، لذلك يُشترط الاستعانة بخبير تقني لتحليل البيانات الرقمية وتفسيرها بلغة قانونية، حيث يجب أن يكون الخبير معتمدًا ومسجلاً لدى الجهات القضائية أو وزارة العدل. كما يجب استخدام أدوات وتقنيات معتمدة لتحليل واستخراج البيانات، وتوثيق جميع الإجراءات في تقارير فنية رسمية، يجب حفظ نسخة أصلية من الدليل وتقديم نسخ للعمل عليها أثناء المحاكمة أو التحقيق[1].

المبحث الثالث: الصعوبات التي تواجه الدليل الرقمي أمام القضاء اليمني:

في ظل تزايد الاعتماد على الأدلة الرقمية في الإثبات الجنائي، خصوصا في إثبات الجرائم السيبرانية، بات من الضروري تحليل التحديات التي تواجه قبولها وتقديرها من قبل المحاكم. وتتمثل هذه الصعوبات في أربعة محاور رئيسية: تشريعية، إجرائية، فنية، وقضائية، تظهر بشكل خاص في الأنظمة القضائية الناشئة مثل النظام القضائي اليمني.

أولًا: الصعوبات التشريعية:

رغم التطور الكبير في الجرائم السيبرانية، لا يزال قانون الإجراءات الجزائية اليمني رقم (13) لسنة 1994 خاليًا من أية إشارة صريحة للأدلة الرقمية أو الإجراءات الخاصة بجمعها وتحليلها، فلم يتم بعد تعديل القانون ليتوافق مع خصوصيات التحقيق الرقمي، فالقانون الحالي بُني على نموذج تقليدي[2] يعتمد على: الشهادة، والاعتراف، والمعاينة، والخبرة، وهذه الوسائل لا تتناسب مع الطبيعة التقنية للدليل الرقمي، ما يؤدي إلى فراغ تشريعي بشأن: مشروعية تفتيش الأجهزة الإلكترونية. وآليات الاستدعاء القانوني للبيانات الرقمية. وكذا ضوابط تحليل الأدلة الرقمية، مثل آليات تفتيش الأجهزة الإلكترونية أو ضبط البيانات المخزنة عن بعد، ما يخلق فجوة تشريعية[3].

وقد سعى مشروع قانون مكافحة الجرائم الإلكترونية إلى التصدي لمثل هذه الأمور إذ إنه ما زال يعتريه كثير من النقص والقصور، ونأمل أن يتم الانتباه لها عند إصدار القانون في صورته

(1) ورد هذا في توصيات الENFSI(الشبكة الأوروبية لعلوم الأدلة الجنائية) توجب استخدام برامج التحليل الجنائي المعتمدة مثل EnCase أوFTK . وقد أكدت ذلك محكمة النقض المصرية في الطعن رقم 3297 لسنة 95 ق (جلسة 20 يونيو 2015) أكدت المحكمة أن الأدلة الرقمية لها حجية في الإثبات الجنائي، بشرط أن يتم جمعها وتحليلها وفقًا للضوابط القانونية والفنية، والطعن رقم 5560 لسنة 7 ق (جلسة 3 مايو 2012)

(1) إن القوانين التقليدية التي كانت سائدة قبل ظهور شبكة الإنترنت وانتشارها لم تعد قادرة على مواكبة التطور المتسارع في مجال التكنولوجيا حيث باتت عاجزة عن حكم الجرائم المستحدثة.

(2) حيمي سيدي محمد: معوقات التحقيق الجنائي في الجرائم الإلكترونية، المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، العدد 1، 2022، ص1744؛ بطيخ، مرجع سابق، ص503.

النهائية، فنجد المادة 30 اكتفت بالقول: "تعد الوسائل الإلكترونية أدلة إثبات إذا ما تم توثيقها فنياً وثبتت سلامتها"، دون بيان المقصود بالتوثيق الفني، أو ضوابط سلامة الدليل، كما غابت الإشارة إلى أدوات الإثبات مثل البريد الإلكتروني، الرسائل النصية، البيانات السحابية، ولا يوجد تعريف واضح لماهية "الدليل الرقمي"، ولا تصنيف لأنواعه (صور، ملفات، تسجيلات، بيانات ميتا...)، إضافة إلى ذلك أن هناك ضبابية في المفاهيم التقنية التي استخدمها المشرع، والنتيجة أن هذا الغموض يُضعف من حجية الدليل الرقمي، ويُعرضه للطعن أمام القضاء بعدم سلامة المصدر أو التوثيق[1].

وبجانب ذلك كله نجد أن قانون الإثبات قد خلا من النص على الاعتراف بالدليل الرقمي والأمر نفسه في قانون الإجراءات الجزائية وقانون أنظمة الدفع والمعاملات المالية المصرفية، فلا يوجد معيار واضح ومحدد لبيان حجية الدليل مثل معاملة البريد الإلكتروني معاملة الكتابة الورقية وكذا الأمر بالنسبة للتسجيلات الصوتية والمرئية، وهل هي دليل كامل أو تكميلي؟ وما هي ضوابط وشروط قبولها؟[2].

وهنا يوصي الباحث المشرع اليمني بضرورة الإسراع إلى إصدار القوانين الخاصة بمواجهة الجرائم الإلكترونية والمعاملات الإلكترونية، ونقل البيانات والمعلومات الإلكترونية وإجراء تعديلات مهمة على القوانين الإجرائية لتتلاءم مع التطور التشريعي مثل قانون الإجراءات الجزائية والمرافعات وقانون الإثبات.

ثانيًا: الصعوبات الإجرائية:

رغم التطور التكنولوجي المتسارع الذي فرض حضور الدليل الرقمي في الساحة الجنائية، فإن الإجراءات المرتبطة بجمعه وتحليله وتقديمه أمام القضاء لا تزال تواجه تحديات إجرائية خطيرة تؤثر في فعاليته القانونية وحجيته القضائية[3]، لا سيما في ظل غياب إطار إجرائي منظم له في القانون اليمني.

فمن أخطر الإشكاليات الإجرائية التي تواجه الدليل الرقمي أمام القضاء أن قانون الإجراءات الجزائية لا يتضمن أي قواعد تتعلق بجمع الأدلة من الوسائط الإلكترونية، بل يعتمد على المفهوم

(1) الأكوع، عبدالله، التحقيق في الجرائم الإلكترونية – بين التشريع اليمني والمقارن، القاهرة، دار النهضة العربية، 2022، ص133.

(2) على العكس من ذلك نجد أن المشرع الإماراتي كان سباقا في ضبط حجية الدليل الرقمي فنجد نص المادة 13 من قانون الإثبات الاتحادي رقم 35 لسنة 2023: تنص على أن "البيانات والمستندات الإلكترونية لها ذات حجية المحررات الرسمية متى استوفت الشروط التقنية".

(1) محمد، مرجع سابق، ص1746.

التقليدي للتفتيش والمصادرة، بينما يتطلب الدليل الرقمي إجراءات خاصة مثل: تصوير القرص الصلب بصورة رقمية (Image)، الحفاظ على سلامة الدليل من التعديل أو التلف. وتوثيق مراحل جمع الدليل بسجل إلكتروني أو محضر رقمي (Chain of Custody)[1].

ومن جانب آخر هناك ضعف شديد في تدريب القائمين على الضبط القضائي في التعامل مع الوسائل الرقمية، إذ يعاني العديد من ضباط الشرطة والنيابة من نقص التدريب الفني اللازم للتعامل مع مسرح الجريمة الرقمية، ما يؤدي إلى: إتلاف الأجهزة أو البيانات عند ضبطها. وفقدان أدلة حيوية نتيجة عدم اتباع بروتوكولات الحفظ الرقمي. واستخدام برامج تحليل غير معتمدة، ما يُضعف من حجية النتائج[2].

ومن المشاكل الإجرائية التي تواجه الدليل الرقمي غياب آلية توثيق سلسة الحيازة Chain of Custody حيث تعد من أهم الشروط الفنية والقانونية لقبول الأدلة الرقمية، فيجب تتبع كل من تعامل مع الدليل وإثبات عدم التلاعب أو التعديل على محتوى البيانات، وهو ما سعت كثير من التشريعات إلى النص عليه تأكيدا لأهميته[3].

ومن جانب آخر: يمثل ضعف البنية التحتية الرقمية للمؤسسات القضائية أبرز الصعوبات التي تواجه الدليل الرقمي أمام القضاء، حيث يعاني النظام القضائي اليمني من ضعف كبير في البنية التحتية التقنية ما يؤثر في قدرته على تخزين الأدلة الرقمية وغياب الأجهزة والمختبرات التقنية المتخصصة التي تعمل على فحص الأدلة الرقمية والتحقق من مصدر الدليل الرقمي، والتحقق من تاريخه وتاريخ التعديل أو الإخفاء والعبث بمحتوياته، بل تفتقر المحاكم إلى التجهيزات الفنية الرقمية التي تمكنها من استخدام الأدلة الرقمية وتقديرها وحفظها[4].

وما سبق جميعه أدى إلى نتيجة حتمية وهي عدم الاعتراف بحجية الأدلة الرقمية كدليل كامل في الإثبات، ففي إحدى القضايا المنظورة أمام محكمة غرب الأمانة بصنعاء عام 2022، رفض القاضي اعتماد سجل محادثات واتساب كدليل رئيسي بحجة "سهولة التلاعب بها"، دون إحالة لفحص فني، وهو ما أدى لبراءة المتهم رغم وجود قرائن قوية.

---

(2) الوشلي، عبدالملك: التحقيق الجنائي في الجرائم الإلكترونية وفق القانون اليمني والمقارن، مجلة كلية الحقوق – جامعة عدن، العدد 5، 2022، ص155.

(3) مثال واقعي: في إحدى القضايا أمام نيابة الأموال العامة بصنعاء، تم ضبط هاتف المتهم وإرساله إلى فني حاسوب في السوق لتحليل محتوياته، وهو ما أفقد الدليل شرط الحياد الفني، وجعله غير مقبول قضائيًا.

(4) بطيخ، مرجع سابق، ص503.

(1) الليثي، مرجع سابق، ص119.

ثالثاً: الصعوبات الفنية التي تواجه الدليل الرقمي:

يمتاز الدليل الرقمي بخاصية فنية عالية، إذ يعتمد على بيانات يتم إنشاؤها أو تخزينها أو نقلها عبر وسائل إلكترونية. وبسبب هذه الطبيعة التقنية يواجه الدليل الرقمي العديد من الصعوبات الفنية التي تؤثر بشكل مباشر في سلامته وحجيته في الإثبات الجنائي، خصوصًا في البيئات القضائية التي تفتقر للبنية الرقمية الكافية مثل اليمن[1].

فمن أبرز الصعوبات الفنية التي تواجه الدليل الرقمي قابليته للتلاعب والتغيير دون ترك أثر، حيث يُعد التلاعب أحد أبرز التحديات الفنية، إذ يمكن للمستخدم أو المهاجم حذف أو تعديل البيانات الرقمية أو تزوير توقيعات إلكترونية بطرق يصعب كشفها دون برامج وأدوات تحليل متقدمة[2]، فملف إلكتروني واحد يمكن تعديله بسهولة دون أن يظهر ذلك على سطح النظام، ما يُضعف موثوقية هذا النوع من الأدلة[3].

ومن جانب آخر: هناك صعوبة في التحقق من مصادر البيانات الرقمية، فبعض الجرائم الإلكترونية تعتمد على استخدام أدوات لإخفاء الهوية (VPN – Proxy – TOR)، ما يجعل تحديد مصدر الدليل الرقمي (مثل عنوان IP أو الموقع الجغرافي) عملية معقدة وتفتقر للدقة[4].

ولعل مما يفاقم الصعوبات الفنية التي تواجه الدليل الرقمي ضعف أدوات التحليل الجنائي الرقمية، فالأجهزة الأمنية والقضائية لا تمتلك مختبرات متخصصة أو برامج متقدمة لتحليل الأدلة الرقمية، وغالبًا ما يتم تحليل هذه الأدلة باستخدام أدوات غير معتمدة أو عبر خبراء غير مختصين، ما يضعف الثقة في النتائج. ويُفقد الدليل حياديته، ويعرّضه للطعن الفني في المحاكم، ولا يختلف الأمر بالنسبة لفحص السلامة عند نسخ الأدلة الرقمية وضعف التوثيق الفني لسلسلة الحيازة، فغياب التوثيق الفني يجعل الدليل عرضة للطعن بعدم القبول[5].

وفي ظل ذلك يوصي الباحث بضرورة إنشاء مختبرات جنائية رقمية مركزية على الأقل، وتدريب الضباط والقضاة على مفاهيم التحليل الرقمي وتقنيات التحقق من الدليل، مع ضرورة اعتماد برامج معترف بها دوليًا في الفحص الرقمي مثل EnCase أو FTK. وإدراج إلزام توثيق سلسلة الحيازة

(2) المرجع السابق، ص127.

(3) محمد، مرجع سابق، ص1746.

(1) مثال ذلك: يمكن استبدال الصور أو الرسائل في الهاتف أو البريد الإلكتروني باستخدام أدوات مثل ExifTool أو FTK Imager دون أن يلاحظ المستخدم أو المحقق غير المتخصص.

4 – الليثي، مرجع سابق، ص159.

5 – المرجع السابق، ص128.

الرقمية وسلامة البيانات في اللوائح القضائية. مع ضرورة التعاون مع المنظمات الدولية (مثل UNODC وINTERPOL) في بناء القدرات الفنية.

رابعًا: الصعوبات القضائية:

يمثل القضاء المرحلة الحاسمة في مسار الدليل الرقمي، حيث يتم تقييمه، ووزنه، واتخاذ القرار بشأن قبوله أو استبعاده، غير أن غياب الإلمام الكافي بطبيعة الدليل الرقمي لدى كثير من القضاة في اليمن، بالإضافة إلى غياب سوابق قضائية مستقرة، أفرز جملة من الصعوبات القضائية التي تُعيق تحقيق العدالة في القضايا ذات الطابع السيبراني.

فالقضاء اليمني يواجه ضعفاً شديداً في التأهيل القضائي خصوصا في مجال الجرائم الإلكترونية وأدوات إثباتها، ما جعل القضاة يتعاملون مع الدليل الرقمي مثله مثل الدليل التقليدي، بل واستبعاد بعض الأدلة الرقمية وعدم قبولها في الإثبات بسبب الجهل الفني، وأحيانا يخطئ القاضي في تقدير الدليل المعروض أمامه[1]، وقد انعكس ذلك في ضعف تسبيب الأحكام بشأن قبول أو رفض الدليل الرقمي ما يجعل تلك الأحكام قابلة للنقض[2].

ومن جانب آخر: نجد أن التردد في الاعتماد على الأدلة الرقمية يعد من العوائق التي تواجه الدليل الرقمي، فكثير من القضاة يرفضون الاعتماد على الدليل الرقمي إلا إذا أرفق بقرائن مادية تقليدية (كاعتراف أو شهادة)، ما يُضعف فعالية هذا النوع من الأدلة، رغم أنه قد يكون مستقلًا وكافيًا وحده[3]، بجانب ذلك نجد أن التعاون القضائي بين القضاء والجهات الفنية يكاد يكون معدوما ما ينتج عنه وجود تقارير غير معتمدة قضائيا، والتي بدورها أدت إلى فقدان الثقة في الدليل الرقمي[4].

---

[1] – المجيدي، عبدالسلام، الإثبات الإلكتروني في القانون اليمني – دراسة تحليلية نقدية، مجلة الدراسات القانونية، جامعة تعز، العدد 10، 2022، ص65. ففي قضية أمام محكمة غرب الأمانة بصنعاء عام 2022، رفض القاضي اعتماد تقرير فني حول محادثات عبر "واتساب" بحجة عدم وجود توقيع بخط اليد، ما يُظهر سوء فهم لطبيعة التوقيع الرقمي.

[2] – ففي إحدى القضايا التي رُفعت إلى محكمة استئناف إب عام 2021، طعن محامي المتهم في الحكم الابتدائي لعدم بيان المحكمة سبب استبعاد تقرير فني يتضمن بريدًا إلكترونيًا يحمل تهديدًا واضحًا.

[3] – في قضية ابتزاز إلكتروني أمام محكمة بني الحارث الابتدائية، رُفضت صور مأخوذة من حساب "فيسبوك" خاص بالمتهم بحجة "عدم إمكانية التأكد من نسبتها له"، رغم وجود تقرير فني من مزود خدمة الإنترنت يؤكد دخوله للحساب من نفس عنوان IP.

[4] – تقرير فريق العمل القضائي حول "العقبات الفنية في إجراءات الإثبات الإلكتروني"، الصادر عن برنامج الأمم المتحدة الإنمائي – اليمن، 2021، ص23.

كما أن غياب التخصص القضائي قد ألقى بظلاله على منازعات الفضاء السيبراني، فالقضايا المتعلقة بالجرائم السيبرانية تحال إلى المحاكم العادية التي غالبا ما تكون غير مختصة وقضاتها غير مؤهلين لهذا النوع من الجرائم، ويبدو ذلك في بطء في الفصل في القضية وعدم توحيد المعايير في تقييم الدليل الرقمي، وتناقض الأحكام القضائية لغياب السوابق المستقرة، وهذا الأخير اتسم به القضاء اليمني بصفة عامة، وفي قضايا الجرائم السيبرانية على وجه الخصوص، فلا توجد اجتهادات موحدة ما يربك عمل القضاة ويفتح المجال للاجتهاد الشخصي.

ونتيجة لما سبق يوصي الباحث بضرورة إنشاء دوائر قضائية متخصصة في الجرائم الإلكترونية داخل المحاكم الابتدائية والاستئنافية، وتدريب القضاة بشكل مستمر على مفاهيم الدليل الرقمي، ووسائل التحقق من صحته، وإصدار دليل قضائي إرشادي لتقييم الأدلة الرقمية وفقًا للمعايير الفنية والقانونية الدولية، وتشجيع نشر الأحكام القضائية المتعلقة بالدليل الرقمي لتكوين اجتهادات مستقرة.

وخلاصة القول في الدليل الرقمي؛ أنه لا يكون لهذا الدليل حجية في الإثبات إلا إذا كان قاطعا ودامغا في إثبات وقوع الجريمة وإسنادها لشخص معين، وهو ما تفتقر إليه الأدلة الإلكترونية، مثلها مثل الأدلة المادية، فجميعها تخضع للسلطة التقديرية للقاضي الجنائي، فله أن يأخذ بها أو يطرحها، ومن جهة أخرى أن الدليل الرقمي دليل فني لا يصح للمحكمة عند المنازعة فيه أن تدلي بدلوها فيه وإنما عليها الاستعانة بأهل الخبرة المختصين من فنيين ومبرمجين.

كما أن الدليل الرقمي يتميز بأنه دليل علمي ذو طبيعة تقنية، إذ يتطلب للحصول عليه اتباع طرق وأساليب علمية غير تقليدية، ما يعني أنه يوصل إلى حقيقة فنية وليس إلى مجرد تحقيق العدالة، وبناء على ذلك يتعين على القاضي فحص الدليل وتمحيصه بما يخدم مصلحة العدالة.

الخاتمة:

في ختام هذه الدراسة يسعى الباحث إلى استخلاص النتائج والتوصيات التي عالجها أثناء دراسته بعد فهمها وتمحيصها، وهي عصارة ما انتهى إليه في بحثه، وتعد نتائج هذه الدراسة وتوصياتها السبيل إلى فهم موضوع الدراسة وكيفية وضعها موضع التطبيق، ونفصل ذلك على النحو الآتي:

أولاً: نتائج الدراسة:

1. تتسم الجريمة السيبرانية بأنها جريمة ناعمة يصعب اكتشافها وضبطها، كما أنها تتم عن بعد دون مراعاة للحدود الجغرافية للدول، ولذلك فهي دولية ويتم ارتكابها عن بعد، تتركز في أغلبها على البيانات والمعلومات الإلكترونية، وهذا ما يميز مرتكب الجريمة السيبرانية من أنه مجرم محترف ذو تأهيل فني وتقني، ومن هنا يحتاج لكشفها خبراء فنيون وتعاون دولي.

2. إن إجراءات التحري والضبط والتحقيق في الجرائم السيبرانية تحتاج إلى الاستعانة بخبراء تقنيين مثل: مشغلي الحاسب الآلي، وخبراء البرمجة، ومهندسي البرامج والتطبيقات، ومخططي برامج النظم، والمحلل المعلوماتي الذي يقوم بتجميع بيانات النظام، ومهندسي الصيانة، ومديري النظم، ومتعهد الوصول، ومقدم خدمات الإيواء، وناقل البيانات والمعلومات، ومورد المعلومات، ومتعهد خدمات الإنترنت، ومورد الوسائل الفنية، ومهندسي الشبكات، وكل من يرى القاضي أنه سوف يسهم في الوصول إلى ضبط المجرمين، حيث يصعب تحديد هوياتهم، فغالبًا ما يستخدم المشتبه بهم هويات مزيفة، أو أدوات لإخفاء الأثر الرقمي، وهو ما يتطلب تحليل بيانات رقمية قبل استدعائه أو توقيفه، أما عند سماع أقواله فإننا نستخدم أثناء الاستجواب تحليل الأدلة الرقمية كمستند داعم مثل: مقارنة النشاط المشبوه بسجل استخدام جهازه، ومن ثم مواجهة المشتبه به برسائل بريد إلكتروني أو سجلات دخول تقنيّة.

3. لضمان فعالية الاستجواب والمواجهة في الجرائم السيبرانية يجب إعداد كوادر تحقيق مدرّبة على فهم آليات الجرائم الإلكترونية، من حيث تدريب المحققين على المبادئ الأساسية للأمن السيبراني والأدلة الرقمية، وضرورة إعداد أدلة إجرائية خاصة بالتحقيق في الجرائم الإلكترونية تتضمن نماذج أسئلة تقنية، مع أهمية إشراك خبراء الأدلة الرقمية أثناء جلسات الاستجواب والمواجهة، مع ضرورة تحديث التشريعات لضمان فعالية المواجهة عبر الوسائل الإلكترونية، وتطوير بروتوكولات استجواب خاصة بالجرائم السيبرانية تأخذ في الاعتبار الخصوصيات التقنية.

4. يتمثل "الدليل الرقمي" في الجرائم السيبرانية في كل بيان أو معلومة مخزنة أو منقولة إلكترونيًا ويمكن أن يُستخلص منها ما يُفيد في إثبات ارتكاب الجريمة أو تحديد مرتكبها. وتشمل هذه الأدلة: الملفات الإلكترونية مثل (مستندات – صور– فديوهات)، وسجلات الدخول حيث يتم تحليل ملفات الدخول، وعناوين ال IP من خلال تحليلات حركة مرور البيانات وتتبع عنوان IP، وكذا استخراج بيانات DNS وSMTP وHTTP المرتبطة بالنشاط السيبراني، ومن مصادر الأدلة أيضاً رسائل البريد الإلكتروني، إذ يتم فحص المحفوظات ورسائل الدردشة، ويعد محتوى الأقراص الصلبة، والهواتف الذكية، والحسابات السحابية من أهم مصادر الأدلة الرقمية.

5. أجمع الفقه والتشريعات الحديثة على مشروعية التفتيش في البيئة الرقمية وبناء على ذلك يشمل التفتيش في الجريمة السيبرانية: التفتيش المادي للأجهزة، مثل تفتيش الحواسيب، الهواتف، الأقراص الصلبة، وحدات التخزين، وذلك من أجل ضمان عدم إتلاف البيانات الأصلية، وغالبًا ما يتم باستخدام أدوات التحقيق الرقمي الجنائي، إذ تُؤخذ نسخ طبق الأصل لتحليلها لاحقًا مع الحفاظ على سلامة النسخة الأصلية، كما يشمل التفتيش الرقمي عن بُعد، من خلال الدخول إلى حسابات البريد الإلكتروني، ومواقع التواصل، أو التخزين السحابي، وهنا يتم تنفيذه من قبل جهات

متخصصة باستخدام برمجيات متقدمة، مع تسجيل خطوات التفتيش والتاريخ والنتائج، وأخيراً تفتيش البيانات المتدفقة أو الحية، وهذا يُستخدم في الحالات التي يكون فيها الجهاز قيد التشغيل أثناء التفتيش، ما يسمح بالوصول إلى بيانات لم تُخزّن بعد مثل الجلسات النشطة أو التصفح الجاري.

6. إن أبرز ما يعيق التحقيق في الجرائم السيبرانية يتمثل في القصور التشريعي في مواجهة الجريمة السيبرانية، حيث لا يزال الإطار القانوني للجرائم الإلكترونية قيد الإعداد أو يفتقر إلى التفاصيل الإجرائية اللازمة، وفي الوقت ذاته لا يوجد في قانون الإجراءات الجزائية اليمني النافذ نصوص خاصة بتنظيم الإجراءات الجنائية الرقمية كالتفتيش الرقمي، أو حفظ الأدلة الرقمية، والأمر ذاته في التشريعات التي تصدت للجرائم السيبرانية إلا أنها اتسمت بالضعف في قواعد الإثبات وعلى الرغم من قبول كثير من التشريعات الأدلة الرقمية في الإثبات الجنائي لم تبين كيفية التعامل مع النسخ الأصلية والفرعية، وما هي شروط مشروعية جمع الأدلة الرقمية؟ وما هي قواعد فض النزاع بين أدلة تقنية متعارضة؟ ومن جانب آخر: يعد من معوقات التحقيق الجنائي النقص في الجوانب الفنية والتقنية، وذلك بسبب الطبيعة الخاصة للأدلة الرقمية، وتطور تقنيات الإخفاء والتشفير، بالإضافة إلى الفجوة في القدرات التقنية بين الدول، فكثير من الدول النامية تعاني من البنية التحتية لتقنية المعلومات الضعيفة بجانب البنية التحتية والفنية لأجهزة إنفاذ القانون التقليدية التي لا تصلح في ضبط الجرائم السيبرانية، فهناك غياب تام للمختبرات الجنائية الرقمية، بجانب نقص في الأدوات التقنية والفنية للتحليل الرقمي، وقد زاد الوضع سوءاً ضعف الاتصال الفعّال مع مزودي الخدمات.

7. يُعد التفاوت الكبير في التشريعات الوطنية الخاصة بمكافحة الجرائم السيبرانية من أبرز العقبات التي تعيق التعاون الشرطي الدولي، إذ إن بعض الدول لا تجرم ذات الأفعال التي تعتبر جرائم في دول أخرى، ما يُعقّد مسألة تسليم الجناة أو تبادل المعلومات، كما أن غياب الثقة السياسية وعلو مبدأ السيادة الوطنية أحد أبرز التحديات القانونية التي تعرقل التعاون الشرطي السيبراني الدولي، فكل دولة تسعى إلى حماية سيادتها الرقمية وفرض ولايتها القضائية على الأفعال التي تقع ضمن إقليمها، أو تمسّ مصالحها الحيوية، وهو ما يتعارض أحيانًا مع متطلبات التعاون الدولي التي تقتضي مشاركة البيانات أو إجراء تحقيقات عابرة للحدود، كما أن قصور البنية التحتية الرقمية والتقنية لدى عدد من الدول، لا سيما النامية منها، يعد عائقًا رئيسيًا أمام فاعلية التعاون الشرطي في مكافحة الإجرام السيبراني، حيث تُعد القدرة التكنولوجية من العناصر الحاسمة في كشف الجرائم الإلكترونية وجمع الأدلة الرقمية وتحليلها والتفاعل السريع مع الإنذارات السيبرانية العابرة للحدود، وتنعكس هذه الفجوة التقنية في ضعف الإمكانات لدى بعض الأجهزة

الشرطية من حيث أدوات تتبع عناوين الإنترنت، أنظمة تحليل الشبكات، قواعد البيانات الجنائية الرقمية، أو حتى فرق التحقيق الرقمي المؤهلة.

ثانياً: التوصيات

1. يمثل الإطار التشريعي العمود الفقري لأي نظام عدلي في مواجهة الجرائم السيبرانية، إذ تُشكل القوانين المنظمة للتحقيق والضبط والتفتيش الإلكتروني الأساس الذي تستند إليه أجهزة إنفاذ القانون، وتبرز الحاجة إلى تطوير هذا الإطار نتيجة التغير المستمر في أنماط الجريمة الرقمية وتوسعها العابر للحدود، ما يتطلب قواعد إجرائية مرنة ومتكاملة تستوعب المستجدات التقنية، وتحمي في الوقت ذاته الحقوق الدستورية للمواطنين، وهنا يوصي الباحث المشرع اليمني بضرورة الإسراع إلى إصدار القوانين الخاصة بمواجهة الجرائم الإلكترونية والمعاملات الإلكترونية، ونقل البيانات والمعلومات الإلكترونية، وإجراء تعديلات مهمة على القوانين الإجرائية لتتلاءم مع التطور التشريعي، مثل قانون الإجراءات الجزئية والمرافعات وقانون الإثبات.

2. إنشاء نظام رقمي مشترك للإنابات القضائية الإلكتروني وتبادل المجرمين وتبادل المعلومات يعمل على تقليص المدد الزمنية، وتبسيط إجراءات الطلب، وربط السلطات القضائية إلكترونيًا ببعضها، فالإنابات القضائية تتطلب تقيدًا دقيقًا بالشروط الشكلية والموضوعية المتعارف عليها دوليًا، كأن تكون الجريمة محل الإنابة معاقبًا عليها في كلا البلدين، وأن يكون هناك أساس قانوني واضح للتعاون كمعاهدة ثنائية أو اتفاقية إقليمية.

3. ضرورة إنشاء مختبرات جنائية رقمية مركزية على الأقل، وتدريب الضباط والقضاة على مفاهيم التحليل الرقمي وتقنيات التحقق من الدليل، مع ضرورة اعتماد برامج معترف بها دوليًا في الفحص الرقمي مثل EnCase أو FTK. وإدراج عبارة: (إلزام توثيق سلسلة الحيازة الرقمية وسلامة البيانات) في اللوائح القضائية، مع ضرورة التعاون مع المنظمات الدولية (مثل UNODC و INTERPOL) في بناء القدرات الفنية.

4. ضرورة إنشاء هيئات قضائية متخصصة في الجرائم الإلكترونية داخل المحاكم الابتدائية والاستئنافية، وتدريب القضاة بشكل مستمر على مفاهيم الدليل الرقمي، ووسائل التحقق من صحته، وإصدار دليل قضائي إرشادي لتقييم الأدلة الرقمية وفقًا للمعايير الفنية والقانونية الدولية، وتشجيع نشر الأحكام القضائية المتعلقة بالدليل الرقمي لتكوين اجتهادات مستقرة.

5. نوصي المشرع اليمني بضرورة تضمين القانون الجديد نصوصاً تحقق الحماية الكاملة للبيانات الشخصية ذات الطبيعة الإلكترونية، وليكن ذلك فرصة لضبط النصوص واستدراك النقص والقصور الذي اعتور المشروع المطروح.

6. نوصي المشرع الوطني بضرورة مواءمة التشريعات الوطنية مع المعايير الدولية، إذ تعد خطوة أساسية نحو تعزيز التعاون السيبراني؛ لما تمثله مواءمة التشريعات الوطنية مع الاتفاقيات الدولية من ضمان التكييف القانوني الموحد للجريمة، فالتفاوت في تعريف الجريمة الرقمية يخلق عقبات أمام تسليم الجناة أو الاعتراف المتبادل بالأدلة. ومن جانب آخر: تعزز هذه المواءمة فعالية التعاون القضائي الدولي، حيث لا يمكن تنفيذ طلبات إنابة قضائية أو مساعدة قانونية متبادلة إذا لم تكن هناك جرائم متماثلة، وأخيراً: تسهم في منع إفلات الجناة من العقاب: الجريمة السيبرانية العابرة للحدود، وقد يستغل الجناة الثغرات التشريعية للاختباء في دول لا تجرّم أفعالهم.

7. إنشاء وحدات وطنية متخصصة في الجرائم السيبرانية حيث تُعدّ الوحدات الوطنية المتخصصة في الجرائم السيبرانية ركيزةً أساسية في تعزيز فاعلية التعاون الدولي في مكافحة الإجرام الرقمي أو السيبراني، لما تتمتع به من قدرة عالية ومتخصصة في تتبع الجناة، وتحليل الأدلة الرقمية، والتفاعل التقني والقانوني مع شركاء خارجيين، وتعمل على ضمان التعامل الصحيح مع الأدلة الرقمية وفقًا للمعايير الدولية، ما يرفع من حجيتها أمام المحاكم الأجنبية.

8. يجب أن تُخضع كل صور التعاون مع الدول الأخرى مثل: تبادل البيانات، وتسليم الأدلة الرقمية، وتنفيذ مذكرات الاعتقال العابرة للحدود إلى مراقبة قضائية مستقلة، تكفل احترام سيادة القانون الوطني، وضمان عدم المساس بحقوق الأفراد كالخصوصية، والحق في الدفاع، والتحقق من سلامة الإجراءات التي تمّت خارج الحدود.

قائمة المصادر والمراجع:

الكتب العربية:

1. أبو دياب، علي السيد علي حسين. (2017). أضواء على حجية الرسائل في الإثبات في مواقع التواصل الاجتماعي. مجلة كلية الشريعة والقانون، جامعة الأزهر بطنطا، (32)، ج3.
2. الأكوع، عبدالله. (2022). التحقيق في الجرائم الإلكترونية – بين التشريع اليمني والمقارن. القاهرة: دار النهضة العربية.
3. بطيخ، حاتم محمد. (2017). دور الإنترنت في الإثبات أمام القاضي الجنائي والإداري (رسالة دكتوراه). جامعة عين شمس.
4. الترزي، نديم محمد. (2012). الإقرار بواسطة الوسائل الحديثة في القضايا الجنائية. صنعاء: مكتبة الصادق.
5. جمال، إبراهيم. (2018). التحقيق الجنائي في الجرائم الإلكترونية (رسالة دكتوراه). جامعة مولود معمري.

6. حسن، سامي يوسف. (2021). الإثبات بالوسائل الإلكترونية. دار الفكر الجامعي.
7. حمودة، علي محمود علي. (2003). الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي. بحث مقدم إلى المؤتمر العلمي الأول حول "الجوانب القانونية والأمنية للعمليات الإلكترونية"، أكاديمية شرطة دبي، 26 نيسان.
8. سرور، أحمد فتحي. (2010). الوسيط في قانون الإجراءات الجنائية. دار النهضة العربية.
9. عالية، سمير. (2020). الجرائم الإلكترونية. منشورات الحلبي.
10. عبدالحميد، عادل. (2018). الجرائم الإلكترونية والإثبات الرقمي. دار النهضة العربية.
11. عبدالفتاح، طارق. (2020). الإثبات في الجرائم الإلكترونية. دار الجامعة الجديدة.
12. عبدالفتاح، عمرو. (2020). جرائم تقنية المعلومات والإثبات الجنائي الرقمي. القاهرة: دار النهضة العربية.
13. العمري، أحمد محمد. (2020). الدليل الرقمي وحجيته في الإثبات الجزائي. مجلة الدراسات الفقهية والقانونية، المعهد العالي للقضاء، (3)، سلطنة عمان.
14. عودة، خالد. (2019). الإثبات الإلكتروني في القانون الجنائي. مجلة الدراسات القانونية، (12).
15. الليثي، عمرو سعدالدين طه. (2021). الإثبات الجنائي في مجال الجرائم الناشئة عن استخدام شبكة المعلومات الدولية (رسالة دكتوراه). جامعة عين شمس.
16. المجيدي، عبدالسلام. (2022). الإثبات الإلكتروني في القانون اليمني – دراسة تحليلية نقدية. مجلة الدراسات القانونية، جامعة تعز، (10).
17. المحبشي، عبدالسلام. (2025). الدليل الإلكتروني ومدى حجيته في الإثبات الجنائي في القانون اليمني (رسالة دكتوراه). جامعة صنعاء.
18. محمد، حيمي سيدي. (2022). معوقات التحقيق الجنائي في الجرائم الإلكترونية. المجلة الأكاديمية للبحوث القانونية والسياسية، جامعة عمار ثليجي الأغواط، (1).
19. مرسي، محمد. (2021). الإثبات الجنائي الإلكتروني. الإسكندرية: دار الجامعة الجديدة.
20. المري، بهاء. (2018). جرائم المحمول والإنترنت. منشأة المعارف.
21. الوشلي، عبدالملك. (2022). التحقيق الجنائي في الجرائم الإلكترونية وفق القانون اليمني والمقارن. مجلة كلية الحقوق، جامعة عدن، (5).

القوانين والأحكام القضائية:

1. الأدلة الجنائية الرقمية للاتصالات من أنواعها وأشهرها Mobile FTK Forensic Oxygen XRY Phone Examiner.
2. الأدلة الجنائية الرقمية للشبكات من أنواعها وأشهرها Enterprise FTK Silent Run.

3. الأدلة الجنائية الرقمية للكمبيوترات والإلكترونيات من أنواعها وأشهرها Encase FTK LAP FTK وبعض الأجهزة المساندة مثل Write Block.
4. تقرير فريق العمل القضائي. (2021). العقبات الفنية في إجراءات الإثبات الإلكتروني. برنامج الأمم المتحدة الإنمائي، اليمن.
5. حكم محكمة أبوظبي للأسرة والدعاوى المدنية والإدارية. (2023، 11 أكتوبر).
6. حكم محكمة النقض الإماراتية. (2016، 20 مارس).
7. حكم محكمة جنايات شبين الكوم – الاستئناف رقم 1561 لسنة 2024. (2024).
8. القانون الاتحادي رقم (35) لسنة 2022 بشأن الإثبات. (2022).
9. المحكمة الاقتصادية المصرية. (2021). الدعوى رقم 319 لسنة 2021.
10. المحكمة الدستورية المصرية. (د.ت). الطعن رقم 5 لسنة 25 قضائية دستورية.
11. محكمة النقض المصرية. (2015، 20 يونيو). الطعن رقم 3297 لسنة 95 ق.
12. محكمة جنح الاقتصادية في مصر. (2020). القضية رقم 241 لسنة 2020.
13. مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية. (2021).
14. نظام الإثبات السعودي رقم (م/43) وتاريخ 1443/05/26هـ. (د.ت). متاح عبر منصة نظام: https://nezams.com

المراجع الأجنبية:

1. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185): Explanatory Report.
2. INTERPOL. (2022). Digital Forensics and Challenges in Cybercrime Investigations.