

د. محمود زكي زكي زيدان
مدرس القانون الجنائي كلية الحقوق جامعة طنطا

الطبيعة القانونية للميتاداتا وحجيتها في الإثبات الجنائي دراسة مقارنة

■ **المراسلة:** د. محمود زكي زكي زيدان
مدرس القانون الجنائي كلية الحقوق جامعة طنطا

■ **معرف الوثيقة الرقمي (DOI):** jolets.v5i2.244/10.54873

■ **نسق توثيق البحث** د. محمود زكي زكي زيدان
الطبيعة القانونية للميتاداتا وحجيتها في الإثبات الجنائي
المجلد الخامس، العدد الثاني، أكتوبر ٢٠٢٥

أبرز التحول الرقمي المتسارع واقعًا إجراميًا جديدًا اتسم بتغيّر طبيعة السلوك الإنساني ووسائل ارتكاب الجرائم، وهو ما انعكس بصورة مباشرة على منظومة الإثبات الجنائي التقليدية، التي باتت عاجزة في كثير من الأحيان عن استيعاب خصوصيات الدليل الرقمي وطبيعته غير المادية. وفي هذا السياق، برزت الميتاداتا (Metadata) بوصفها أحد أهم مكونات البيئة الرقمية المعاصرة، لما تنطوي عليه من قدرة على كشف السياق الزمني والمكاني والتقني للوقائع الرقمية، وربط الأفعال بأشخاص وأجهزة محددة، حتى في غياب محتوى البيانات ذاته.

يهدف هذا البحث إلى دراسة الطبيعة القانونية للميتاداتا وحجبتها في الإثبات الجنائي، من خلال تحليل مفهوميها، وأنواعها، وخصائصها الفنية، وتمييزها عن البيانات الأصلية وبيانات الاتصالات، مع بيان موقعها داخل منظومة الأدلة الجنائية الرقمية. كما يتناول البحث الإشكاليات القانونية الدقيقة التي تثيرها الميتاداتا، وعلى رأسها مدى اعتبارها ببيانات شخصية، وحدود خضوعها لمبدأ سرية الاتصالات، وشروط مشروعيتها عند الجمع والتحليل والاستخدام القضائي.

واعتمد البحث على منهج تحليلي مقارنة نقدي، من خلال دراسة المواقف التشريعية والفقهية والقضائية في الأنظمة القانونية المقارنة، ولا سيما التشريعات الأوروبية والأمريكية والفرنسية، مع إبراز القصور التشريعي في بعض الأنظمة العربية، وعلى رأسها غياب تنظيم صريح للميتاداتا، وما يترتب على ذلك من اضطراب في التطبيق القضائي وتهديد لمبدأ الأمن القانوني.

وانتهى البحث إلى أن الميتاداتا لا يمكن توصيفها توصيفًا واحدًا جامدًا، بل تتمتع بطبيعة قانونية وظيفية مرنة، تتحدد بحسب قدرتها العملية على الكشف عن هوية الشخص أو موقعه أو نمط سلوكه الرقمي. وبناءً عليه، خلص إلى أن الميتاداتا تُعدّ في الأصل قرينة تقنية قوية، قد ترتقي إلى مرتبة الدليل الجنائي المباشر متى ثبتت أصالتها، وسلامة سلسلة حيازتها الرقمية، واتساقها مع باقي عناصر الإثبات. كما أثبت البحث أن التمييز الشكلي بين محتوى الاتصال والميتاداتا لم يعد كافيًا في ضوء التحليل التجميعي الحديث، إذ قد تؤدي الميتاداتا - وحدها - إلى مساس فعلي بالخصوصية دون الاطلاع على مضمون الاتصال.

كما تناول البحث دور التقنيات الحديثة، ولا سيما الذكاء الاصطناعي، في تعزيز فعالية تحليل الميتاداتا وإعادة بناء مسرح الجريمة الرقمي، مع التنبيه إلى المخاطر القانونية المصاحبة لذلك، مثل غموض الخوارزميات، وصعوبة الطعن الفني،

والانحياز الخوارزمي، وما يترتب عليها من تحديات تمس ضمانات المحاكمة العادلة.

ويخلص البحث إلى ضرورة تدخل تشريعي صريح لتنظيم الميتاداتا، يوازن بين متطلبات الفعالية في مكافحة الجريمة الرقمية وضمانات حماية الخصوصية والحريات الفردية، ويضع إطاراً قانونياً واضحاً يضبط شروط جمعها وتحليلها وتقدير حجيتها أمام القضاء.

الكلمات المفتاحية :

الميتاداتا (Metadata) - الإثبات الجنائي الرقمي - الدليل الرقمي - القرينة التقنية - الخصوصية الرقمية - سرية الاتصالات - البيانات الشخصية - سلسلة الحيازة الرقمية (Chain of Custody) - التحقيق الجنائي الرقمي - الذكاء الاصطناعي والأدلة الجنائية.

Abstract

The rapid digital transformation has given rise to a new criminal reality characterized by a fundamental change in the nature of human behavior and the means by which crimes are committed. This transformation has had a direct impact on the traditional criminal evidence system, which has increasingly proven incapable of accommodating the particularities of digital evidence and its intangible nature. In this context, metadata has emerged as one of the most significant components of the contemporary digital environment, due to its ability to reveal the temporal, spatial, and technical context of digital events and to link actions to specific individuals and devices, even in the absence of the data content itself.

This study aims to examine the legal nature of metadata and its evidentiary value in digital criminal proceedings by analyzing its concept, types, and technical characteristics, and by distinguishing it from content data and traffic data, while clarifying its position within the framework of digital criminal evidence. The study also addresses the delicate legal issues raised by metadata, foremost among them whether metadata should be considered personal data, the extent to which it is subject to the principle of communications secrecy, and the conditions governing its lawful collection, analysis, and judicial use.

The study concludes that metadata cannot be characterized through a single rigid legal definition; rather, it possesses a flexible functional legal nature, determined by its practical capacity to reveal a person's identity, location, or digital behavioral patterns. Accordingly, the study finds that metadata constitutes, in principle, a strong technical presumption, which may rise to the level of direct criminal evidence when its authenticity is established, its digital chain of custody is preserved, and it is consistent with other elements of proof. The research further demonstrates that the for-

mal distinction between communication content and metadata is no longer sufficient in light of modern aggregate analysis, as metadata alone may result in a real infringement of privacy even without access to the content of communications

The study also examines the role of modern technologies – particularly artificial intelligence– in enhancing the effectiveness of metadata analysis and reconstructing the digital crime scene, while cautioning against the accompanying legal risks, such as algorithmic opacity, difficulties in technical challenge, and algorithmic bias, all of which raise serious concerns regarding the guarantees of a fair trial

The study ultimately calls for explicit legislative intervention to regulate metadata in a manner that balances the requirements of effective digital crime control with the protection of privacy and individual freedoms, and that establishes a clear legal framework governing the conditions for the collection, analysis, and evidentiary assessment of metadata before the courts

Keywords

Metadata – Digital Criminal Evidence – Digital Evidence – • Technical Presumption – Digital Privacy – Secrecy of Communications – Personal Data – Digital Chain of Custody – Digital Criminal Investigation – Artificial Intelligence and Criminal Evidence

المقدمة

مع ظهور شبكة الإنترنت وتنامي الاعتماد على التكنولوجيا الحديثة، شهد مفهوم مسرح الجريمة تحولاً جوهرياً عما كان عليه في السابق. فلم يعد مسرح الجريمة مقصوراً على المكان المادي التقليدي الذي يحوي الأدلة الجنائية^١ الذي تُرتكب فيه الأفعال الإجرامية وتُجمع منه الأدلة الملموسة، بل امتد ليشمل البيئة الرقمية التي أصبحت حاضنة رئيسية للأنشطة الإجرامية المعاصرة.^٢ مما دعا إلي بروز علم يعرف بـ علم الأدلة الجنائية الرقمية Digital Forensics، بوصفه فرعاً علمياً متخصصاً يُعنى بجمع وتحليل وحفظ الأدلة الرقمية المستخرجة من الوسائط الإلكترونية، وفق منهجيات فنية وقانونية تضمن سلامتها وقابليتها للاعتماد القضائي. وقد جاء ظهور هذا العلم استجابةً مباشرةً للتطور الهائل في جمع وتخزين ومعالجة البيانات الرقمية، وما ترتب عليه من تعقيد في طبيعة الجرائم وأساليب ارتكابها وإخفائها.^٣

ومما لا شك فيه أن التحقيق الجنائي الرقمي، شأنه شأن التحقيق الجنائي التقليدي، يسعى الي التتقيب عن الأدلة من مجموعة من الأسئلة النموذجية الجوهرية التي تسعى جهات التحقيق إلى الإجابة عنها، وهي: متى وقع الحادث؟ وأين؟ وماذا حدث؟ ولماذا؟ وكيف وقع؟ وتمثل الإجابة الدقيقة عن هذه الأسئلة الأساس المنطقي لبناء التصور القانوني للواقعة الإجرامية، وتحديد أركانها، وربطها بالفاعل أو المشتبه فيه.

ومن هذا المنطلق نجد أن الميتاداتا (Metadata) تؤدي دوراً محورياً في التحقيقات الجنائية الرقمية، إذ تُعد - في جوهرها - «بيانات عن بيانات»، تمكّن من الانتقال من المحتوى الرقمي الجامد إلى فهم السياق الزمني والمكاني والتقني الذي أنشئ فيه هذا المحتوى أو استخدم أو عدّل. ويختلف المحتوى الدقيق للميتاداتا باختلاف نظام الملفات (File System) ونوع الملف محل الفحص، غير أنها تتكوّن - بوجه عام - من عناصر رئيسية، في مقدمتها: الطابع الزمنية الخاصة بإنشاء الملف وتعديله والوصول إليه، ومعلومات ملكية الملفات، والبيانات التقنية المرتبطة بوحدة تخزين الميتاداتا ذاتها.

١ د. محمود أحمد طه: التحقيق الجنائي العملي، بدون دار نشر، بدون سنة نشر، ص ٤٠

٢ د. خالد ممدوح إبراهيم: فن التحقيق في الجرائم الالكترونية، دار الفكر الجامعي، ٢٠١٠، ص ١٦٥

٣ د. محمود حسين سيد أبو سيف: الأدلة الرقمية أمام المحكمة الجنائية الدولية، مجلة القانون والتكنولوجيا، كلية القانون، الجامعة البريطانية بمصر، مجلد ٤، غ ١، إبريل ٢٠٢٤، ص ٣٢٨

٤ د. محمود محمد سويف: سرية التحقيق الابتدائي بين اعتبارات تحقيق المصلحة العامة ومتطلبات الحق في الاعلام دراسة مقارنة، دار الجامعة الجديدة، ٢٠٢١، ص ٣١

ولقد شهدت السنوات الأخيرة تطوراً ملحوظاً في توظيف الميتادات في التحقيق الجنائي الرقمي الآلي حيث امكانية استخدام الترابط بين الميتادات لتحديد مصدر الملفات التي تم تنزيلها، حتى في الحالات التي لا يكون فيها المحتوى ذاته كافياً لإثبات هذا المصدر. ويكشف هذا التوجه عن تحول نوعي في دور الميتادات، من مجرد بيانات وصفية مساعدة إلى أداة استدلالية مركزية في كشف الحقيقة الرقمية.⁵

إشكاليات البحث:

١. إلى أي حد يمكن اعتبار الميتادات بيانات شخصية تخضع لأنظمة حماية الخصوصية؟
٢. هل تخضع الميتادات لمبدأ سرية الاتصالات، أم تخرج من نطاقه بوصفها بيانات غير محتوى؟
٣. ما القيمة الثبوتية للميتادات في الإثبات الجنائي: هل هي دليل مباشر أم قرينة تقنية، وما شروط ارتقائها إلى مرتبة الدليل؟
٤. ما أثر الذكاء الاصطناعي في تعزيز موثوقية الميتادات، وما المخاطر القانونية المترتبة على توظيفه في التحقيق الجنائي؟
٥. كيف يمكن معالجة القصور التشريعي في بعض الأنظمة القانونية، ولا سيما العربية، لضمان استخدام مشروع ومتوازن للميتادات؟

صعوبات البحث

يواجه البحث جملة من الصعوبات المنهجية والموضوعية، في مقدمتها غياب تعريف تشريعي موحد للميتادات في أغلب الأنظمة القانونية، وما يترتب على ذلك من اضطراب في التكييف القانوني واختلاف في المعالجة القضائية. فالخلاف لا يقتصر على تحديد المفهوم، بل يمتد إلى تحديد ما إذا كانت الميتادات تُعدّ بيانات شخصية، أو مجرد بيانات تقنية، أو بيانات اتصالات، وهو ما ينعكس مباشرة على نطاق الحماية الدستورية والإجرائية المقررة لها.

5 Xiaoyu Du and Mark Scanlon: "Methodology for the Automated Meta-data-Based Classification of Incriminating Digital Forensic Artefacts," in Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19) (Canterbury, UK: ACM, 2019), p3 <https://doi.org/10.1145/3339252.3340517>.

وتتجلى صعوبة أخرى في الطابع التقني المعقّد للميتاداتا، الذي يفرض على الباحث القانوني التعامل مع مفاهيم فنية دقيقة (كالطابع الزمنية، وسجلات النظام، وبيانات الموقع، وسلسلة الحياة الرقمية)، بما يستلزم تداخلاً واعياً بين التحليل القانوني والفهم التقني، دون الوقوع في التبسيط المخل أو النقل التقني غير المنضبط. ويُضاف إلى ذلك صعوبة تقييم الحجية الإثباتية للميتاداتا، في ظل قابليتها للتعديل أو العبث دون آثار ظاهرة، وما يثيره ذلك من إشكاليات تتعلق بسلامة الدليل، وعبء الإثبات، ودور الخبرة الفنية.

كما يواجه البحث تحدياً خاصاً يتمثل في تباين المواقف التشريعية والقضائية المقارنة، ولا سيما بين الاتجاه الأوروبي القائم على معيار وظيفي صارم لحماية الخصوصية، والاتجاه الأمريكي الذي عرف تطوراً تدريجياً من مقارنة شكلية إلى مقارنة أكثر حساسية للأثر الكاشف للميتاداتا، فضلاً عن القصور التشريعي في بعض الأنظمة العربية، وعلى رأسها غياب تنظيم صريح للميتاداتا في التشريع المصري، وهو ما يُحمّل الباحث عبئاً إضافياً في استنباط المركز القانوني لهذه البيانات من خلال التفسير المنهجي المتكامل للنصوص.

أهمية البحث

تتبع أهمية هذا البحث من كونه يتناول موضوعاً يُمثّل أحد أعقد التحديات المعاصرة لمنظومة الإثبات الجنائي في ظل التحول الرقمي المتسارع. فالاعتماد المتزايد على الميتاداتا في التحقيقات الجنائية الرقمية، بوصفها أداة قادرة على إعادة بناء السياق الزمني والمكاني والسلوكي للوقائع، يفرض ضرورة ضبط طبيعتها القانونية وحجيتها، منعاً للانزلاق إلى ممارسات تمس جوهر الحق في الخصوصية والحريات الفردية.

وتكمن الأهمية العلمية للبحث في إعادة بناء المفهوم القانوني للميتاداتا على أساس وظيفي، يربط الحماية القانونية بقدرة البيانات على الكشف عن هوية الشخص أو سلوكه أو تحركاته، لا بمجرد تصنيفها التقني. كما تبرز أهمية البحث في تحليله المقارن العميق للمواقف الأوروبية والأمريكية والفرنسية، وربطها بالواقع التشريعي العربي، بما يسهم في سد فجوة معرفية قائمة في الفقه الجنائي العربي حول الأدلة الرقمية غير المحتوائية.

منهج البحث:

تستلزم الدراسة الرجوع الي النصوص القانونية المختلفة واحكام القضاء وتحليلها مما يقتضي اعتماد البحث علي المناهج التالية:

١. المنهج التحليلي: وذلك من خلال تحليل مفهوم الميتادات، وخصائصها، وأنواعها، وطبيعتها القانونية، مع تفكيك الإشكاليات المرتبطة بحجيتها ومشروعيتها في الإثبات الجنائي الرقمي.
٢. المنهج المقارن: عبر مقارنة موقف التشريعات العربية بمواقف التشريعات الأجنبية، ولا سيما الأوروبية والأمريكية والفرنسية، مع الاستعانة باجتهادات القضاء المقارن، وبخاصة أحكام المحكمة الأوروبية لحقوق الإنسان، ومحكمة العدل للاتحاد الأوروبي، والمحكمة العليا الأمريكية.
٣. المنهج النقدي: من خلال تقييم مدى كفاية الأطر التشريعية القائمة، ورصد أوجه القصور والخلل في التنظيم القانوني للميتادات، ونقد الاتجاهات التي توسّع أو تقيّد استخدامها على نحو يخلّ بالتوازن بين متطلبات التحقيق الجنائي وضمانات الحقوق والحريات.

خطه البحث:

قسمت البحث الي ثلاث مباحث علي النحو التالي:

- **المبحث الأول:** ماهية الميتادات.
- **المبحث الثاني:** التكييف القانوني للميتادات ودورها في الإثبات الجنائي.
- **المبحث الثالث:** الإشكالات القانونية والفنية المتعلقة للميتادات.

المبحث الأول

الإطار المفاهيمي للميتاداتا

يُعدّ ضبط مفهوم الميتاداتا المدخل المنهجي الضروري لفهم دورها القانوني والإثباتي في البيئة الرقمية المعاصرة، إذ لا يمكن تقييم حجيتها أو تحديد مركزها داخل منظومة الإثبات الجنائي الرقمي دون الوقوف على ماهيتها، وخصائصها، وحدود تمايزها عن غيرها من البيانات الرقمية. فالتكييف القانوني السليم لأي دليل رقمي يقتضي ابتداءً تحديد طبيعته الفنية ووظيفته المعلوماتية، قبل الانتقال إلى بحث مشروعيته وحجيته أمام جهات التحقيق والقضاء لذا سنستعرض في هذا المبحث الآتي:

المطلب الأول: مفهوم الميتاداتا.

المطلب الثاني: التمييز بين الميتاداتا وما يتشابه معها.

المطلب الثالث: خصائص الميتاداتا.

المطلب الأول

مفهوم الميتاداتا

أولاً: تعريف الميتاداتا:

تعد الميتاداتا بيانات عن البيانات⁶ (Data about Data)، أي أنها تمثل الطبقة التفسيرية التي تسمح بفهم المحتوى الرقمي وتحديد مصدره وسلامته وتطوّره الزمني. وتكمن أهميتها في أنها تمكّن من إعادة بناء السياق الرقمي للواقعة، بما في ذلك تتبّع تسلسل الأحداث الرقمية، والتحقق من أصالة الملف وعدم العبث به، وربط المحتوى بشخص أو جهاز أو زمان ومكان محددين⁷.

على الرغم من الجاذبية الظاهرية للتعريف الأولي القائل بأن «الميتاداتا هي بيانات عن البيانات»، فإن هذا التعريف، على بساطته وسهولة تداوله، يظل تعريفاً قاصر لا يعبر بدقة عن الطبيعة الحقيقية لمفهوم البيانات الوصفية في سياقه المعاصر.

6 ZENG, Marcia Lei; QIN, Jian. Metadata. American Library Association, 2020.p33

7 Yan Zhao: Metadata Management for Data Lake Governance. PhD diss., Université Toulouse 1 Capitole, 2021,p18

إذ إن هذا الوصف الأولي يعجز عن استيعاب التعقيدات التقنية والقانونية التي اكتسبتها الميتاداتا في البيئات الرقمية الحديثة، ولا يحيط بالدور الجوهرى الذي باتت تؤديه خارج إطار الوصف الشكلى للمحتوى الرقمية. فالإكتفاء باعتبار الميتاداتا مجرد «بيانات تشرح بيانات أخرى» قد يكون ملائماً كنقطة انطلاق أو مدخل تمهيدى للمفهوم، إلا أنه يظل قاصراً عن تفسير وظيفتها البنيوية في أنظمة المعلومات المعاصرة، وعن بيان أثرها العميق في مجالات إدارة البيانات، والمراقبة الرقمية، والإثبات الجنائي.⁸ ذلك أن الميتاداتا لم تعد أداة مساعدة ثانوية، بل تحولت إلى عنصر حاسم في إعادة بناء السياق الرقمية للوقائع، وتتبع الأنشطة، وتحديد المسؤوليات، وتقدير حجية الدليل الرقمية.⁹

ولذا فإن التمسك بهذا التعريف البسيط دون تطويره يُفضي إلى فهم ناقص للمفهوم، ويحول دون إدراك أبعاده القانونية الخطيرة، لا سيما ما يتصل بالحق في الخصوصية، وحدود المراقبة المشروعة، وقواعد قبول الدليل الرقمية أمام جهات التحقيق والقضاء. ولذلك، يقتضى البحث العلمى الجاد تجاوز هذا التعريف الأولى نحو تصور أشمل للبيانات الوصفية بوصفها بنية تفسيرية وتنظيمية ذات أثر قانونى مباشر، لا مجرد وصف تقني محايد للمحتوى الرقمية.¹⁰

وفي هذا الإطار، يثور تساؤل منهجى جوهرى حول ما إذا كان هناك تعريف موحد لمفهوم الميتاداتا أم أن المصطلح يؤدي دلالات مختلفة باختلاف السياق الذى يُستخدم فيه. مما لا شك فيه أن الراجح فقهيًا وعلميًا أن الميتاداتا لا تخضع لتعريف واحد، وإنما تمثل مفهومًا وظيفيًا مرناً، يتغير مضمونه بحسب الغرض من استخدامه؛ فالتعريف الذى يصلح لإدارة المكتبات وتنظيم الموارد المعرفية قد لا يكون كافياً للتحقيق الجنائي الرقمية، كما أن التعريف التقني للبحث قد يكون قاصراً عن استيعاب الأبعاد القانونية المرتبطة بالخصوصية وحجية الدليل.

ولعل الرجوع إلى الأصل الاصطلاحي لمصطلح «Meta-data» يُبرز بوضوح البنية الثنائية لمفهوم الميتاداتا ودلالاته المعرفية. فكلمة «Meta»، المشتقة من الأصل اليوناني *meta*، لا تفهم في هذا السياق بوصفها مجرد إضافة لغوية، وإنما تحمل معاني أعمق، من بينها: «ما وراء»، أو «فوق»، أو «نظرة أعلى» إلى الشيء

8 GILLILAND, Anne J. Setting the stage. Introduction to metadata, 2008, 3: p19.

9 Christopher T. Anglim, ed: Privacy Rights in the Digital Age, 1st ed. (Amenia, NY: Grey House Publishing, 2015), p356

10 BACA, Murtha (ed.). Introduction to metadata. Getty Publications, 2016.p1

محل الوصف.¹¹ وهي بذلك تعبر عن الانتقال من مستوى المعطيات الرقمية الأولية إلى مستوى تحليلي أعلى يتجاوز تسجيل المحتوى إلى تفسيره وتأطيره. ويُفهم هذا المقطع، في سياق المياداتا، على أنه يشير إلى طبقة تحليلية مرافقة للبيانات الأصلية، لا تقتصر وظيفتها على الوصف الشكلي، وإنما تضطلع بدور تفسيري وتنظيمي يُمكن من وضع البيانات الرقمية في إطارها الزمني والمكاني والتقني الصحيح. فالمياداتا، بهذا المعنى، لا تمثل مجرد معلومات إضافية، بل تُنشئ زاوية نظر عليا تسمح بفهم طبيعة المحتوى، وتتبع مساره، وتقيم سلامته ومصداقيته، وربطه بسياقه الواقعي والقانوني.¹²

وعليه، فإن استخدام مصطلح المياداتا لا يعني الاكتفاء بوصفها «بيانات عن بيانات»، وإنما يعكس تحولاً نوعياً في مستوى التحليل من مضمون المعلومة إلى شروط وجودها، وكيفية إنشائها، وتداولها، واستخدامها. تشير إلى مجموعه من المعايير الدولية (FAIR)¹³ التي تهدف إلى ضمان أن تكون البيانات قابلة للاكتشاف، والوصول، والتشغيل البيئي، وإعادة الاستخدام، بما يعزز موثوقيتها وقيمتها العلمية والقانونية، ويضمن استدامتها في البيئات الرقمية.

وهو ما يفسر الدور المحوري الذي تؤديه المياداتا في البيئات الرقمية المعاصرة، ولا سيما في مجال الإثبات الجنائي الرقمي، حيث تُستخدم هذه النظرة لإعادة بناء الوقائع الرقمية وتقدير حجية الأدلة على نحو يتجاوز المحتوى الظاهر إلى بنيته وسياقه العميق.¹⁴

فلقد عرفت المياداتا بالبيانات الوصفية (Metadata) وهي تلك المعطيات المرافقة للبيانات الرقمية، والتي تُنشأ إما تلقائياً بواسطة الأنظمة التقنية أو يدوياً من قبل المستخدم، وذلك بهدف وصف البيانات الأصلية وتحديد خصائصها وسياق وجودها. إلا أنها لا تعبر عن مضمون المحتوى الرقمي ذاته، وإنما تكشف عن الظروف التقنية

11 Oxford English Dictionary, s.v. “meta-” <https://www.oed.com/?tl=true>, accessed 16.12.2025, 3:28am)

12 MILLER, Steven Jack. Metadata for digital collections. American Library Association, 2022.p1

13 F : Findable – قابلة للاكتشاف

A: Accessible – قابلة للوصول

I: Interoperable – قابلة للتشغيل البيئي

R: Reusable – قابلة لإعادة الاستخدام

ZENG, Marcia Lei; QIN, Jian: Metadata. American Library Association, 2020.p11

14 Haynes, David. Metadata for Information Management and Retrieval: Understanding Metadata and Its Use. 2nd ed. London: Facet Publishing, 2018,p10

والزمنية والمكانية التي أنشئ أو استخدم أو عُذِل فيها هذا المحتوى.¹⁵

ومن المعلوم أن الميتاداتا تشمل – على سبيل المثال لا الحصر – تاريخ ووقت إنشاء الملف، وتاريخ ووقت آخر تعديل أُجري عليه، وهوية منشئ الملف أو المستخدم الذي قام بالتعديل، ونوع الملف وصيغته التقنية وحجمه، فضلاً عن الجهاز أو البرنامج المستخدم في إنشائه أو معالجته.¹⁶

وبناءً على ذلك، فإن الميتاداتا ليست مجرد بيانات إضافية مرافقة، بل هي بيانات تصف البيانات أو تفسرها أو تنظمها، بما يسمح بفهمها واستخدامها بصورة واعية. غير أن الاستخدام المعاصر للمفهوم وسّع من مدلول كلمة «البيانات» ذاتها، فلم تعد تُفهم على أنها مجرد أرقام أو رموز تقنية، بل باتت تشمل المعلومات، والموارد المعلوماتية، والكيانات الحاملة للمعلومة، أيّاً كانت طبيعتها أو وسيطها.

ويترتب على هذا التوسّع أن الميتاداتا قد تتعلق اليوم ليس فقط بالملفات الرقمية التقليدية، بل أيضاً بالوثائق، والصور، والتسجيلات الصوتية، ومقاطع الفيديو، وقواعد البيانات، بل وحتى الكيانات الرقمية المعقدة مثل الحسابات الإلكترونية ومنصات التواصل الاجتماعي. وهو ما يفتح المجال أمام إدراج مختلف المواد الوثائقية – بمختلف أشكالها ووسائطها – ضمن نطاق البيانات الوصفية، ويُضفي على هذا المفهوم طابعاً شمولياً يتجاوز الحدود التقنية الضيقة.¹⁷

فمن ثم فإن الميتاداتا تكتسب قيمة خاصة في مجال الإثبات الجنائي الرقمي، إذ تُعدّ أداة أساسية للتحقق من نسبة الدليل الرقمي إلى صاحبه، ولبسط الرقابة على مشروعية جمعه واستخدامه، كما تُسهم في تمييز الدليل الصحيح عن الدليل المشوب بالتلاعب أو التعديل اللاحق. ولذلك، لا يُمكن تفسير المحتوى الرقمي تفسيراً صحيحاً أو تقييم حجته القانونية بمعزل عن الميتاداتا المرافقة له، باعتبارها عنصراً جوهرياً في فهم الدليل الرقمي وتقدير قوته الثبوتية أمام جهات التحقيق والقضاء.

وفي البيئات الرقمية الحديثة، ولا سيما ما يُعرف بـ «بحيرات البيانات» (Data Lakes)، تشمل الميتاداتا وصف مجموعات البيانات الرقمية، وعمليات معالجتها، والعلاقات التي تربط بينها، فضلاً عن تسجيل المعلومات السياقية العامة المرتبطة بها،^{١٥} د. أروي نصار الميليبي: تطويع الميتاداتا كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، ج٣، ع٣٦٢، ٢٠٢١، ٢٠٢٢.

16 Simson L Garfinkel: Digital forensics research: The next 10 years. Digital Investigation 7 (2010), S69

17 Christopher T. Anglim, ed: Privacy Rights in the Digital Age, 1st ed. (Amenia, NY: Grey House Publishing, 2015), p255

بما يسمح بتتبع مسار البيانات منذ إنشائها وحتى استخدامها النهائي.¹⁸

ثانياً: أنواع الميتاداتا:

الميتاداتا الإنشائية (Structural Metadata): يُقصد بالميتاداتا الإنشائية تلك الفئة من الميتاداتا التي تُعنى بوصف البنية الداخلية للملف الرقمي وطريقة تنظيم مكوناته التقنية، دون أن تمتد إلى مضمون المحتوى ذاته.¹⁹ فهي تُحدّد الشكل الذي يتخذه الكيان الرقمي، والهيكل الذي تُرتّب فيه عناصره، بما يسمح بفهم كيفية إنشائه وقراءته وتشغيله من الناحية التقنية.²⁰

وتشمل الميتاداتا الإنشائية - على سبيل المثال لا الحصر - نوع الامتداد أو الصيغة التقنية للملف (مثل PDF، DOCX، JPEG)، وعدد الصفحات أو الإطارات، ودقة الصورة وأبعادها، ونظام الترميز المستخدم، وخصائص الصوت أو الفيديو، فضلاً عن العلاقات الداخلية بين أجزاء الملف الواحد، كترتيب الصفحات أو المقاطع.²¹

وتكمن أهمية هذه الفئة من الميتاداتا في أنها تمكّن من التعرّف على طبيعة الملف الرقمية والتحقق من قابليته للفتح أو التشغيل بوسائل تقنية معينة، كما تُستخدم في الكشف عن التلاعب البنيوي بالملف، كتحويل صيغته، أو دمج محتويات مختلفة، أو العبث بترتيب مكوناته.²² ومن ثمّ، تكتسب الميتاداتا الإنشائية قيمة خاصة في مجال الإثبات الجنائي الرقمي، إذ تُسهم في التحقق من سلامة الكيان الرقمي من الناحية التقنية، وتمييز الملف الأصلي عن النسخ المعدّلة أو المركّبة.²³

١٨ يُعدّ مستودع البيانات (Data Lake)، سواء في الأوساط الأكاديمية أو الصناعية، أحد الحلول الرائجة والمنتشرة في مجال تحليلات البيانات الضخمة، بوصفه بنية مرنة تتيح تخزين كميات هائلة من البيانات الخام بمختلف أنواعها وأشكالها، سواء كانت مهيكلة أو شبه مهيكلة أو غير مهيكلة. ومع ذلك، لا يزال مفهوم مستودع البيانات يفتقر - حتى اليوم - إلى تعريف موحد يحظى بإجماع عام، إذ تتباين التعريفات الواردة في الأدبيات العلمية تبعاً للزاوية التي تنطلق منها كل مقاربة، سواء كانت تقنية، أو تنظيمية، أو تحليلية.

١ Yan Zhao: Metadata Management for Data Lake Governance. PhD diss., Université Toulouse ١٨, ٢٠٢١, Capitole

19 Eoghan Casey, *Digital Evidence and Computer Crime* (4th ed., 2020) p 285

20 ISO/IEC 23081-1:2017 – Information Governance – Metadata- (Section 3.2.3).

21 CARRIER, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.p131

22 Dublin Core Metadata Initiative (DCMI), *DCMI Metadata Terms* (2020)-(Section 1.4).

23 RILEY, Jenn. Understanding metadata. Washington DC, United States:

وبهذا المعنى، تمثل الميتاداتا الإنشائية الأساس البنيوي الذي يُبنى عليه فهم الملف الرقمي، وهي شرطٌ لازم لتقييم مشروعية الدليل الرقمي وقوته الثبوتية، حتى قبل الانتقال إلى فحص محتواه أو ميتاداتا الوصفية أو الإدارية الأخرى.

١ - الميتاداتا الوصفية (Descriptive Metadata)

يقصد بالميتاداتا الوصفية تلك الفئة من الميتاداتا التي تُعنى بتوفير المعلومات التعريفية الأساسية المرتبطة بالملف أو الكيان الرقمي، والتي تهدف إلى تمييزه والتعريف به وتيسير البحث عنه واسترجاعه داخل

النظم المعلوماتية. فهي لا تصف البنية التقنية للملف، وإنما تتناول سماته التعريفية والدلالية²⁴.

وتشمل الميتاداتا الوصفية - على سبيل المثال لا الحصر - عنوان الملف أو الوثيقة، واسم المنشئ أو المؤلف، والكلمات المفتاحية، وموضوع المحتوى، وملخصه، وأي أوصاف نصية أخرى تُستخدم لتصنيف الملف وربطه بسياقه المعرفي أو الوظيفي. وقد تنشأ هذه الميتاداتا يدويًا بواسطة المستخدم، أو تُستخلص تلقائيًا بواسطة الأنظمة البرمجية.²⁵

وتكمن أهمية الميتاداتا الوصفية في أنها تمثل واجهة التعريف الأولى بالكيان الرقمي، وتُعدّ أداة محورية في أنظمة الفهرسة والتكشيف وقواعد البيانات ومحرركات البحث. غير أن دورها لا يقتصر على الجانب التنظيمي، بل يمتد إلى المجال القانوني، حيث يمكن أن تُستخدم في نسبة المحتوى الرقمي إلى صاحبه، أو في دعم القرائن المتعلقة بقصد الاستخدام أو طبيعة النشاط الرقمي.²⁶

يُلاحظ أن الميتاداتا الوصفية تُعدّ - من حيث طبيعتها - أكثر عرضة للتعديل أو التلاعب الإرادي مقارنة بالميتاداتا الإنشائية أو الزمنية، لكونها غالبًا ما تُدخل يدويًا.²⁷ ومن ثمّ، فإن قيمتها الإثباتية لا تكون مطلقة، وإنما تخضع لتقدير المحكمة

National Information Standards Organization (<http://www.niso.org/publications/press/UnderstandingMetadata.pdf>), 2017, 23.2017: p6

24 Rachel L. Frick, "Descriptive Metadata for Digital Collections," *Library Trends* 59, no. 4 (2011): p 655

25 GARTNER, Richard.: Metadata. Springer, 2016.p7

26 ZENG, Marcia Lei; QIN, Jian. Metadata. American Library Association, 2020.p31

27 Mark Pollitt, "A History of Digital Forensics," in *Advances in Digital Fo-*

في ضوء بقية عناصر الدليل الرقمي، وما يحيط بها من قرائن فنية وتقنية. وتؤدي الميادات الوصفية وظيفية مزدوجة، تتمثل في تنظيم المعرفة الرقمية من جهة، والإسهام في بناء القرينة الجنائية من جهة أخرى، مع ضرورة التعامل معها بحذر منهجي عند تقييم حجيتها القانونية^{٢٨}.

٢ - الميادات الإدارية (Administrative Metadata)

يُقصد بالميادات الإدارية تلك الفئة من الميادات التي تُعنى بتوثيق إدارة الكيان الرقمي عبر الزمن، من حيث نشأته وتداوله وتعديله، والوسائل التقنية التي استُخدمت في التعامل معه. فهي لا تتعلق بمضمون المحتوى أو بنيته الداخلية، وإنما تُجسّد التاريخ الإداري والتقني للملف. وتشمل الميادات الإدارية - على سبيل المثال لا الحصر - تاريخ ووقت إنشاء الملف، وتاريخ ووقت آخر تعديل أجري عليه، وعدد مرات التعديل، والأدوات أو البرمجيات المستخدمة في التحرير أو المعالجة، فضلاً عن معلومات تتعلق بحقوق الوصول،

وأذونات الاستخدام، وبيانات النسخ الاحتياطي أو الحفظ.^{٢٩}

وتكمن الأهمية القانونية لهذه الفئة من الميادات في كونها تمثل السجل الزمني والإجرائي للملف الرقمي، بما يسمح بتتبع مسار حياته الرقمية منذ لحظة إنشائه وحتى آخر تعامل عليه. وهي بذلك تؤدي دوراً محورياً في التحقق من أصالة الدليل الرقمي، وكشف ما إذا كان قد خضع لتعديل لاحق، أو أعيد إنشاؤه، أو عولج بأدوات معينة قد تثير الشك في سلامته.

وفي مجال الإثبات الجنائي الرقمي، تُعدّ الميادات الإدارية من أقوى أنواع الميادات قيمةً من حيث الحجية، لأنها غالباً ما تُنشأ تلقائياً بواسطة النظام، وتكون أقل قابلية للتعديل الإرادي غير المرصود. ومن ثمّ، يمكن الاستناد إليها في مقارنة التواريخ والأزمنة، وربط الفعل الإجرامي بمرحلة زمنية معينة، أو نفي وقوعه في وقت محدد.^{٣٠}

غير أنّ قيمتها الإثباتية تظل مشروطة بسلامة إجراءات الضبط والاستخراج والحفظ الفني، وبإثبات عدم العبث بها خلال مراحل جمع الدليل، وهو ما يفرض الالتزام

rensics (Springer, 2009)p 15

28 Stephen Mason, *Electronic Evidence* (5th ed., 2021)p 470

29 ZENG, Marcia Lei; QIN, Jian. Metadata. American Library Association, 2020.p19

30 United States v. Mann, 701 F.3d 274 (8th Cir. 2012)p284

الصارم بسلسلة حفظ الأدلة الرقمية³¹ (Chain of Custody). وتمثل الميتاداتا الإدارية أداة مركزية في تقييم مشروعية الدليل الرقمي وقوته الثبوتية، وتُعدّ ركيزة أساسية في بناء القناعة القضائية بشأن صحة الوقائع الرقمية محل الاتهام أو الدفاع.

٣- ميتاداتا الملاحة وتحديد المواقع (Geolocation Metadata)

يُقصد بـ (ميتاداتا الملاحة وتحديد الموقع) تلك الفئة من الميتاداتا التي تتعلق بتسجيل الموقع الجغرافي المرتبط بإنشاء أو التقاط أو استخدام الكيان الرقمي، وذلك اعتماداً على تقنيات تحديد الموقع، وعلى رأسها نظام تحديد المواقع العالمي (GPS) أو غيره من وسائل تحديد الموقع القائمة على الشبكات اللاسلكية أو أبراج الاتصالات. وتشمل هذه الميتاداتا - على سبيل المثال لا الحصر - إحداثيات الموقع الجغرافي (خطوط الطول والعرض)، وارتفاع الموقع عن سطح البحر، ووقت الالتقاط، ودقة القياس، وقد تُدمج هذه البيانات ضمن ملفات الصور أو مقاطع الفيديو أو التسجيلات الصوتية التي تُلتقط بواسطة الهواتف الذكية أو الكاميرات الرقمية أو الأجهزة المحمولة الأخرى.³²

وتكمن الأهمية التقنية لهذه الفئة من الميتاداتا في قدرتها على تحديد مكان الالتقاط أو الاستخدام بدقة عالية، وربط الكيان الرقمي بموقع جغرافي محدد في لحظة زمنية معينة. أما من الناحية القانونية، فإن ميتاداتا تحديد الموقع تكتسب قيمة إثباتية بالغة، إذ تُستخدم في نسبة الواقعة إلى مكان معين، وتأكيد أو نفي وجود شخص في مسرح الجريمة، أو دعم القرائن الزمنية والمكانية المرتبطة بالفعل الإجرامي³³.

غير أنّ هذه الميتاداتا، على الرغم من قوتها الإثباتية، تثير إشكاليات دقيقة تتعلق بالخصوصية، نظراً لقدرتها على تتبع تحركات الأفراد وأنماط سلوكهم المكاني. ومن ثمّ، فإن جمعها أو تحليلها أو استخدامها في التحقيق الجنائي يقتضي احترام مبدئي الضرورة والتناسب، واستصدار الإذن القضائي اللازم وفقاً للتشريعات المنظمة لحماية البيانات الشخصية والاتصالات³⁴. كما يجب التعامل مع ميتاداتا تحديد الموقع

31 NIST SP 800-86, 4-8 (2006); ISO/IEC 27037:2012, §7.2.

٣٢ للمزيد أنظر د. تامر محمد صالح: التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية، **المجلد ١١، العدد ١ - الرقم المسلسل للعدد ١**، عدد خاص بالمؤتمر الدولي السنوي العشرون الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات أغسطس ٢٠٢١، ص ٧١١-٧٦٢

٣٣ د. ياسر محمد النيداني: الجوانب القانونية لتقنية تحديد الموقع الجغرافي، مجلة روح القانون، كلية الحقوق، جامعة طنطا، ع ١٠٨٤، أكتوبر ٢٠٢٤، ص ٩٧٨

34 national Information Standards Organization (NISO Understanding metadata. NISO Press). (2004).p7.

بحذر منهجي، نظراً لإمكانية التلاعب التقني أو الخطأ في تحديد الموقع في بعض الحالات، سواء بفعل إعدادات الجهاز أو تدخل المستخدم أو العوامل البيئية. الأمر الذي يفرض إخضاعها للفحص الفني الدقيق، وعدم التعويل عليها منفردة دون دعمها ببقية عناصر الدليل الرقمي أو المادي. وتمثل مبادرات الملاحاة وتحديد الموقع أداة إثبات قوية ولكن حساسة، تتطلب موازنة دقيقة بين فعاليتها في كشف الحقيقة الجنائية، وضمان احترام الحق في الخصوصية وحماية الحريات الفردية.

٤- سجلات النظام (Log Metadata)

يُقصد بسجلات النظام تلك الفئة من المبادرات التي تُنشأ تلقائياً بواسطة أنظمة التشغيل، والخوادم، وقواعد البيانات، والتطبيقات الرقمية، بغرض توثيق الأنشطة التي تتم داخل النظام أثناء تشغيله واستخدامه.^{3٥} وهي تُعدّ من أكثر أنواع المبادرات استخداماً وأهمية في التحقيق الجنائي الرقمي، لما توفره من سجل تفصيلي للأحداث التقنية. وتشمل سجلات النظام - على سبيل المثال لا الحصر - أنشطة الدخول والخروج من النظام (Login / Logout)، ومحاولات النفاذ الفاشلة، وعمليات إنشاء الملفات أو حذفها أو تعديلها، وتغيير الصلاحيات، وتشغيل أو إيقاف الخدمات، فضلاً عن تسجيل الأخطاء والأعطال التقنية (Error Logs)، والتنبيهات الأمنية، والأنشطة المرتبطة بالشبكات والاتصالات داخل النظام.

وتكمن الأهمية القانونية والإثباتية لسجلات النظام في كونها تمثل تسلسلاً زمنياً دقيقاً للأحداث الرقمية، يُمكن من إعادة بناء الوقائع التقنية المرتبطة بالجريمة، وتحديد هوية المستخدم أو الحساب الذي قام بالفعل، وربط النشاط الإجرامي بزمان ومكان ونقطة وصول محددة. كما تُستخدم هذه السجلات في كشف النفاذ غير المشروع، أو إساءة استخدام الصلاحيات، أو محاولات إخفاء الآثار الرقمية للجريمة. وتتميز سجلات النظام بقوة حجيتها مقارنة ببعض أنواع المبادرات الأخرى، لكونها غالباً ما تُنشأ آلياً دون تدخل مباشر من المستخدم، وتكون محمية بإعدادات تقنية تمنع تعديلها أو تُظهر آثار التعديل عند وقوعه. ومع ذلك، فإن الاعتماد عليها إثباتياً يظل مشروطاً بإثبات سلامة النظام ذاته، وصحة إعدادات التسجيل، وعدم العبث بالسجلات أو تعطيلها قبل أو أثناء أو بعد ارتكاب الفعل محل التحقيق.³⁶

تقرض سجلات النظام التزاماً صارماً بقواعد الضبط الفني وسلسلة حفظ الدليل

٣٥ مسعود بن حميد المعمرى، "الدليل الإلكتروني لإثبات الجريمة الإلكترونية"، مجلة كلية القانون الكويتية العالمية، ملحق خاص، ع ٣، ج ٢، أكتوبر ٢٠١٨، ص ٢٠٢-٢٠٣.

36 BACA, Murtha (ed.). Introduction to metadata. Getty Publications, 2016.p10

الرقمي (Chain of Custody)، إلى جانب ضرورة تحليلها بواسطة خبراء مختصين، وربطها ببقية عناصر الدليل الرقمي أو المادي، تجنباً للاعتماد المنفرد عليها دون سند داعم. تُعدّ سجلات النظام العمود الفقري للأدلة الرقمية في الجرائم المعلوماتية والجرائم المرتكبة باستخدام الوسائط الإلكترونية، وتمثل أداة حاسمة في بناء القناعة القضائية متى أحسن جمعها وتفسيرها وتقديمها أمام القضاء.³⁷

المطلب الثاني

التمييز بين الميتاداتا وما يتشابه معها

أولاً: التمييز بين الميتاداتا والبيانات الأصلية (Content Data):

يقتضي التحليل القانوني الدقيق للبيانات الرقمية التمييز بوضوح بين البيانات الأصلية (Content Data) والميتاداتا (Metadata)، لما لهذا التمييز من آثار جوهرية على مستوى التكيف القانوني وحجية الدليل الرقمي. فالبيانات الأصلية تتمثل في مضمون الملف الرقمي ذاته، أي المحتوى الظاهر الذي يُدرك مباشرة، مثل النص المكتوب في محرر إلكتروني، أو الصورة الرقمية، أو التسجيل الصوتي، أو مقطع الفيديو، وهي تعبّر عن ما قيل أو كُتب أو صُوّر أو سُجِّل، وتشكّل محل الإدراك الحسي المباشر للدليل الرقمي³⁸. أما الميتاداتا، فلا تتصرف إلى مضمون هذا المحتوى، وإنما تتعلق بالسياق المحيط به، أي الكيفية التي أنشئ بها، والزمان الذي وُجد فيه، والمكان الذي ارتبط به، والوسيلة التقنية التي استُخدمت في إنتاجه أو تعديله، وهوية الشخص أو الجهاز الذي قام بذلك³⁹. فهي تُجيب عن أسئلة كيف؟ ومتى؟ وأين؟ ومن؟، دون أن تتناول سؤال ماذا؟ المتعلق بمضمون الرسالة أو الملف.

ويترتب على هذا التمييز أن الميتاداتا قد تظل قائمة وفعّالة حتى في الحالات التي يتم فيها حذف البيانات الأصلية أو تعديلها أو العبث بها. فقد يُغيّر محتوى ملف

37 Souradip Nath, Keb Summers, Jaejong Baek, and Gail-Joon Ahn, "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics," in 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (Washington, DC, USA: IEEE, 28–31 October 2024), <https://doi.org/10.1109/TPS-ISA62245.2024.00012>.

38 Shahzad Saleem, Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics (PhD diss., Stockholm University, 2015), p22.

39 د. مصطفى إبراهيم العربي. دور الدليل الرقمي في الإثبات الجنائي. مجلة البحوث القانونية، 6 المجلد ٦، ع. ٢٠١٩، ص ٣٨٠.

رقمي أو يُفَرِّغ من مضمونه، بينما تظل المياداتا - كلياً أو جزئياً - محتفظة بآثار هذا التعديل، مثل تاريخ آخر تعديل، أو هوية المستخدم، أو اختلاف البصمة الزمنية للملف. وهو ما يجعل المياداتا شاهداً رقمياً صامتاً على ما طرأ على المحتوى، حتى بعد المساس به.⁴⁰ لذا فنكتسب المياداتا قيمة إثباتية مستقلة عن البيانات الأصلية، إذ لا تُستمد حجيتها من مضمون المحتوى، بل من قدرتها على إعادة بناء المسار الزمني والتقني للملف، وكشف ما إذا كان قد تعرّض للتلاعب أو التعديل أو الإنشاء اللاحق على خلاف الحقيقة. ولذلك، قد تُعدّ المياداتا في بعض الحالات أقوى دلالة من المحتوى ذاته، لكونها أقل قابلية للتلاعب الظاهر، وأكثر ارتباطاً بالبنية التقنية للنظام. وبالإنعام علي ما تقدم فإن الفصل بين المياداتا والبيانات الأصلية ليس مجرد تمييز تقني، بل هو تمييز قانوني جوهري، يترتب عليه اختلاف في طرق الجمع، والتقييم، والرقابة القضائية، وحجية كل منهما في الإثبات الجنائي الرقمي. وتأسيساً على ذلك، لا يجوز الخلط بين المياداتا ومحتوى البيانات عند تقدير مشروعية الدليل أو قوته الثبوتية، لأن لكل منهما طبيعة قانونية ووظيفة إثباتية متميزة.

ثانياً: التمييز بين المياداتا وبيانات الاتصالات:

يعد هذا التمييز من المسائل الدقيقة في مجال الإثبات الجنائي الرقمي، لما يترتب عليه من آثار مباشرة على التكيف القانوني للبيانات، ونطاق الحماية الدستورية المقررة لها، وشروط مشروعيتها عند الضبط والتحليل والاستخدام القضائي. فبيانات الاتصالات تتصل بعملية نقل البيانات أو الاتصال ذاتها، أي بالمسار التقني الذي تنتقل عبره الرسائل أو الملفات، دون أن تتناول مضمونها. وتشمل، على سبيل المثال، عناوين بروتوكول الإنترنت (IP)، وأوقات الإرسال والاستقبال، وأطراف الاتصال، ومدته، ونوع الوسيلة المستخدمة. وهي بذلك تعبّر عن ديناميكية الاتصال لا عن طبيعة الكيان الرقمي المنقول.⁴¹ أما المياداتا، فترتبط بالملف أو الكيان الرقمي ذاته، بغض النظر عن كونه قد نُقل عبر شبكة اتصالات من عدمه. فهي تصف خصائصه الداخلية وسياق إنشائه وتعديله وتخزينه، مثل تاريخ الإنشاء، وهوية المنشئ، ونوع الصيغة، والجهاز أو البرنامج المستخدم.

٤٠. د.روب كيتشن ترجمة د.محمد بن أحمد غروي: ثورة البيانات البيانات الكبيرة والبيانات المفتوحة والبنية التحتية للبيانات والنتائج المترتبة عنها، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، ٢٠١٨، ص٣٣

41 ALbeladi SS, Othman FA: The effective role of big data in supporting the telecommunications sector – an analytical study. Journal of Information Studies & Technology 2023:1.5. <https://doi.org/10.5339/jist.2023.p5>

د.أحمد حسام طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربية، 2003، ص111

ومن ثمّ، فإن الميتادات لا تتعلق بعملية النقل، وإنما بالوجود التقني للبيان الرقمي ذاته، فالعلاقة بين الميتادات وبيانات الاتصالات هي علاقة تمايز لا تطابق؛ فلكل منهما نطاقه الوظيفي والتقني المتميز، وإن كان كلاهما يندرج - من حيث المبدأ - ضمن فئة ما يُعرف بالبيانات غير المحتوائية (Non-Content Data)، أي البيانات التي لا تكشف عن مضمون الاتصال أو الرسالة، وإنما عن ظروفها وسياقها.

غير أنّه يُلاحظ عملياً أن بعض التشريعات الوطنية، وكذلك بعض الممارسات الإجرائية، لا تحسن التفرقة بين الميتادات وبيانات الاتصالات - بل وأحياناً بينها وبين البيانات الأصلية (Content Data) - فتُخضعها جميعاً لنظام قانوني واحد، سواء من حيث شروط الضبط، أو متطلبات الإذن القضائي، أو نطاق الحماية الإجرائية. ويُعدّ هذا النهج توسّعاً غير منضبط، لا يستقيم مع الطبيعة المختلفة لكل نوع من هذه البيانات. ويترتب على هذا الخلط آثار قانونية خطيرة؛ إذ قد يؤدي إلى مساس غير مبرر بالحق في الخصوصية عندما تُخضع بيانات ذات طبيعة أقل حساسية لإجراءات صارمة أو مراقبة موسعة دون مقتضى^{٤٢}، كما قد يفضي - على النقيض - إلى إهدار دليل رقمي مشروع إذا أخضع لقيود إجرائية لا تتناسب مع طبيعته، أو إذا أُبطل بسبب سوء توصيفه القانوني. فإن التمييز الدقيق بين الميتادات وبيانات الاتصالات لا يُعدّ ترفاً نظرياً، بل يمثل ضرورة قانونية وإجرائية لضمان سلامة الدليل الرقمي، وتحقيق التوازن الواجب بين مقتضيات التحقيق الجنائي ومتطلبات حماية الخصوصية والحريات الفردية. وهو ما يقتضي من المشرّع والقاضي والجهات القائمة على الضبط والتحليل الفني تبني توصيف قانوني دقيق لكل نوع من البيانات، وإخضاعه للنظام الإجرائي الملائم لطبيعته ووظيفته.^{٤٣}

٤٢ د. يوسف بن سعيد الكلباني: الحماية الجزائية للبيانات الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعه عين شمس، ٢٠١٦، ص ٢١٨.

٤٣ د. أحمد محمد علي الخديم: الحماية الجنائية للبيانات الشخصية في ظل مكافحة الجرائم الالكترونية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعه المنصورة، ٢٠٢٥، ص ٧٩.

المطلب الثالث

خصائص الميادات

أولاً: الارتباط غير المرئي بالمحتوى:

تتسم الميادات بخاصية أساسية تتمثل في كونها مرتبطة ارتباطاً بنوياً غير مرئي بالمحتوى الرقمي، إذ تُدمج ضمن البنية التقنية للملف أو الكيان الرقمي عند إنشائه أو معالجته، دون أن تكون ظاهرة للمستخدم العادي أثناء الاطلاع على المحتوى أو استخدامه. فهي لا تظهر في الواجهة المرئية للنص أو الصورة أو التسجيل، وإنما توجد في الطبقات الخفية للنظام الرقمي.⁴⁴ وتكمن أهمية هذه الخاصية في أن الميادات تُنشأ - في الغالب - تلقائياً بواسطة النظام أو البرنامج المستخدم، دون تدخل إرادي مباشر من المستخدم، وهو ما يقلل من احتمالات العبث المتعمد بها، ويمنحها درجة أعلى من الموثوقية التقنية مقارنة ببعض عناصر المحتوى الظاهرة. كما أن عدم ظهورها للمستخدم العادي يجعلها بمنأى عن التعديل العرضي أو غير المقصود.⁴⁵ لذا تُضفي هذه الخاصية على الميادات قيمة إثباتية خاصة في مجال التحقيق الجنائي الرقمي، إذ تُعدّ بمثابة أثر رقمي خفي يمكن لجهات التحقيق والخبراء الفنيين استخراجه وتحليله لإعادة بناء الوقائع الرقمية، وكشف ما إذا كان المحتوى قد أنشئ أو عدّل أو نُقل في زمان أو مكان معينين، حتى في الحالات التي يُحاول فيها الفاعل إخفاء نشاطه الإجرامي عبر حذف المحتوى أو تغييره.

غير أن هذه الخاصية، رغم أهميتها، تفرض في المقابل التزاماً قانونياً صارماً بضرورة مشروعية الضبط والاستخراج، نظراً لكون الميادات غير ظاهرة، وقد يؤدي الوصول إليها دون إذن قانوني إلى مساس بالحقوق الخصوصية أو تجاوز نطاق الإذن القضائي. ومن ثمّ، فإن التعامل مع الميادات يتطلب موازنة دقيقة بين فعاليتها في كشف الحقيقة الجنائية، وضمان احترام الضمانات الإجرائية وحماية الحقوق والحريات الفردية. وبذلك، يُمكن القول إن الارتباط غير المرئي للمحتوى يُشكل أحد أهم خصائص الميادات، إذ يجمع بين القيمة الإثباتية العالية من جهة، والحساسية القانونية من جهة أخرى، وهو ما يبرّر المكانة المركزية التي تحتلها في منظومة الأدلة الرقمية المعاصرة.

٤٤ د. جميل عبد الباقي الصغير: أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠٠٢، ص ١٢٥.

45 Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, London, 2011, p7.

ثانياً: القابلية للتعديل دون ترك آثار واضحة:

من الخصائص الجوهرية للميتاداتا أنها قابلة للتعديل تقنياً دون أن يخلف ذلك - في كثير من الأحيان - آثاراً مرئية أو مباشرة على المحتوى الرقمي نفسه. فبخلاف التعديل الذي يطال البيانات الأصلية ويترك عادةً علامات ظاهرة في النص أو الصورة أو التسجيل، يمكن لبرامج متخصصة في تحرير الميتاداتا أن تُغيّر عناصر حساسة، مثل تاريخ وقت الإنشاء، أو تاريخ التعديل، أو بيانات الموقع الجغرافي، دون أن يظهر هذا التغيير في الواجهة المرئية للملف أو يلفت انتباه المستخدم العادي، ويزداد هذا الخطر مع تطور برمجيات محو الأدلة الرقمية، التي لا تقتصر على حذف الملفات فحسب، بل تمتد إلى طمس الميتاداتا أو إفسادها بصورة منهجية، بما يحول دون استعادتها أو تتبعها. ومن أبرز الأمثلة على ذلك ما يُعرف في الأدبيات التقنية ببرامج القنبلة المعلوماتية (Information Bomb / Logic Bomb)، وهي أدوات تُصمّم لإتلاف البيانات والميتاداتا إتلافًا تدريجيًا أو فجائيًا، إما عند تحقق شرط زمني معين، أو عند تنفيذ فعل محدد داخل النظام، أو بمجرد تشغيل الملف ذاته.⁴⁶ وتُمثّل هذه الخاصية مكن خطر حقيقي في مجال الإثبات الجنائي الرقمي، إذ تفتح المجال أمام التلاعب المتعمّد بالسياق الزمني أو المكاني للدليل الرقمي بقصد تضليل جهات التحقيق أو التأثير في تقدير المحكمة لحجية الدليل.⁴⁷ وقد يؤدي الاعتماد غير المدقّق على الميتاداتا المعدّلة إلى بناء استنتاجات خاطئة بشأن زمن الواقعة أو مكانها أو هوية من قام بها.

ومن ثمّ، تفرض هذه الخاصية ضرورة إخضاع الميتاداتا إلى تدقيق فني متقدّم، لا يقتصر على قراءة القيم الظاهرة فحسب، وإنما يمتد إلى فحص الاتساق الداخلي للميتاداتا، ومقارنتها ببقية أنواع الميتاداتا المصاحبة، وسجلات النظام، وبيانات الاتصالات، وغيرها من القرائن الرقمية. كما يقتضي الأمر الاستعانة بأدوات وخبرات فنية قادرة على كشف مؤشرات التلاعب غير المباشر، مثل عدم التناسق بين تواريخ مختلفة، أو التعارض بين نوع الجهاز والبرنامج المستخدم، أو عدم تطابق الموقع الجغرافي مع بيانات أخرى مستقلة.⁴⁸ و تؤثر هذه القابلية للتعديل على تقدير حجية الميتاداتا، إذ لا يجوز التعويل عليها وحدها دون سند فني داعم، ولا اعتبارها دليلاً قاطعاً

46 Mark L. Krotoski: "Effectively Using Electronic Evidence Before and at Trial," United States Attorneys' Bulletin 59, no. 6, November 2011 -p52.

47 د. طه أحمد متولي: الدليل العلمي وأثره في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠٠٧، ص ٣٠٠.

48 د. رامي متولي القاضي: الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية والتشريعات المقارنة، مجلة القانون والتكنولوجيا، كلية القانون الجامعة البريطانية بمصر، المجلد ٢، ١٤، إبريل ٢٠٢٢، ص ١٩٩.

بذاتها، بل يتعين تقييمها في إطار منظومة متكاملة من الأدلة الرقمية. كما تُلقَى هذه الخاصية بعبء إضافي على جهة الاتهام لإثبات سلامة الميادات وعدم العبث بها، وعلى المحكمة لتمحيصها بعناية قبل بناء قناعتها. وعليه فإن القابلية للتعديل دون ترك آثار واضحة، رغم كونها خاصية تقنية، تتحول في المجال القانوني إلى مسألة منهجية حاسمة، تفرض تشديد معايير الفحص، وتعزيز دور الخبرة الفنية، ضماناً لعدم إهدار العدالة أو الاعتماد على دليل رقمي مشوب بالتلاعب.

ثالثاً: إنتاج أدلة استدلالية عميقة:

تتميز الميادات بقدرتها الفائقة على إنتاج أدلة استدلالية عميقة تتجاوز حدود الدلالة المباشرة لكل عنصر على حدة، إذ إن قيمتها الحقيقية لا تكمن في كل بيان منفرد، وإنما في التحليل التجميعي والترابطي لمجموع عناصرها. فعبر جمع الميادات من مصادر متعددة وتحليلها زمنياً ومكانياً ووظيفياً، يمكن تكوين صورة رقمية متكاملة عن سلوك المستخدم، وأنماط نشاطه، وتوقيت أفعاله، ومسارات تحركه، دون الحاجة إلى الاطلاع على مضمون البيانات أو محتواها الأصلي⁴⁹. وتسمح هذه القدرة الاستدلالية بإعادة بناء الوقائع الرقمية على نحو يُمكن جهات التحقيق من استخلاص أنماط سلوكية متكررة، وربط أحداث متفرقة ظاهرياً في سياق واحد، واستنتاج نية الاستخدام أو طبيعة النشاط، سواء كان مشروعاً أو غير مشروع. وبذلك، تتحول الميادات من مجرد معطيات تقنية وصفية إلى أداة تحليل سلوكي ذات أثر بالغ في توجيه الاتهام أو تدعيمه.

غير أن هذه الخاصية، رغم أهميتها الإثباتية، تثير إشكاليات قانونية دقيقة، لاسيما فيما يتصل بالحقوق في الخصوصية وحماية الحياة الخاصة⁵⁰. فإنتاج صورة عن الفرد، حتى دون فحص المحتوى، قد يكشف عن تفاصيل دقيقة تتعلق بعلاقاته الاجتماعية، وتحركاته اليومية، وأنماط حياته، وهو ما قد يمس جوهر الحرية الفردية إذا لم يُضبط بضوابط قانونية صارمة. ومن ثم، فإن التعويل على الميادات في إنتاج أدلة استدلالية عميقة يقتضي الالتزام الصارم بمبادئ الضرورة والتناسب والتحديد الدقيق للغرض، فضلاً عن إخضاع عمليات الجمع والتحليل لرقابة قضائية فعّالة. كما يتعين على المحكمة التعامل مع هذه الاستنتاجات بحذر منهجي، وعدم اعتبارها أدلة قطعية بذاتها، بل قرائن قوية يجب دعمها بعناصر إثبات أخرى، منعاً للانزلاق إلى الاستنتاج الافتراضي أو الاتهام القائم على الاحتمال. وبذلك، تمثل هذه الخاصية إحدى أكثر

49 Simson L. Garfinkel: Digital Forensics Research: The Next 10 Years- Digital Investigation 7 , 2010- pS71

50 Daniel J. Solove: Understanding Privacy- Harvard University Press, 2008- p 42.

خصائص الميتادات قوة وخطورة في آن واحد، إذ تجمع بين القدرة على كشف الحقيقة الجنائية من جهة، واحتمال المساس العميق بالخصوصية من جهة أخرى، وهو ما يستوجب موازنة دقيقة بين متطلبات العدالة الجنائية وضمانات الحقوق والحريات الفردية.

رابعاً: إمكانية التتبع الزمني:

يُعدّ الطابع الزمني (Timestamp) من أهم - إن لم يكن أهم - العناصر الفنية في منظومة الميتادات، لما يتمتع به من قدرة على تحديد الإطار الزمني الدقيق للوقائع الرقمية. فهو الأداة التي تمكن المحقق من رسم خط سير زمني متكامل للأحداث، وربط أفعال المستخدم أو النظام بلحظات زمنية محددة، سواء تعلّق الأمر بإنشاء ملف، أو تعديله، أو نقله، أو حذفه.⁵¹ وتكمن الأهمية الجوهرية للطابع الزمني في كونه يسمح بترتيب الوقائع الرقمية ترتيباً منطقيّاً متسلسلاً، يُمكن من إعادة بناء تسلسل الأفعال وربطها بسياقها الزمني، بما يساعد على تحديد لحظة ارتكاب الفعل الإجرامي، أو نفي نسبته إلى المتهم إذا ثبت تعارض التوقيت مع وجوده أو نشاطه. ومن ثمّ، يشكّل الطابع الزمني حجر الزاوية في تحليل العلاقة بين الفعل والفاعل والزمان.⁵²

و يكتسب الطابع الزمني قوة خاصة، لكونه غالباً ما يُنشأ تلقائياً بواسطة النظام وفق إعدادات زمنية معيارية، ويكون مدمجاً في البنية التقنية للملف أو النظام. وهو ما يجعل دحضه أو الطعن عليه أكثر صعوبة مقارنة ببعض عناصر الميتادات الأخرى، لاسيما إذا تأكد اتساقه مع سجلات النظام وبيانات الاتصالات ومصادر زمنية مستقلة.⁵³ غير أنّ القوة الإثباتية للطابع الزمني (Timestamp)، على ما لها من أهمية محورية في التحقيق الجنائي الرقمي، لا تعني إطلاق حجّيته أو افتراض صحته على نحوٍ قاطع. إذ يظل الطابع الزمني - شأنه شأن سائر عناصر الميتادات -

51 Digital Forensic Artefacts and Their Evidential Value In Law: A Guide for Civil and Criminal Defence Lawyers, Computer Forensics Lab, accessed 2025-12-14 at 11:47 AM <https://computerforensicslab.co.uk/digital-forensic-artefacts-evidential-value/>

52 Céline Vanini, Christopher J. Hargreaves, Harm Beek, and Frank Breitinger, "Was the Clock Correct? Exploring Timestamp Interpretation through Time Anchors for Digital Forensic Event Reconstruction," Forensic Science International: Digital Investigation 49 - 2024, p 4 <https://doi.org/10.1016/j.fsi-di.2024.301759>.

53 Important Role of Timestamps in Forensic Science, NBFTools, accessed 14 December 2025 at 11:52 AM <https://www.nbftools.com/important-role-of-timestamps-in-forensic-science/>.

خاضعاً للفحص الفني الدقيق، ولا يُعتمد به إلا بقدر ما يثبت خلوه من عوامل التشويه أو التلاعب التقني. ويزداد هذا القيد أهمية في الحالات التي قد يتأثر فيها الطابع الزمني بعوامل تقنية متعددة، من قبيل:

- تغيير ساعة النظام يدوياً قبل أو بعد ارتكاب الواقعة؛
- اختلاف المناطق الزمنية (Time Zones) بين الجهاز محل الفحص وخوادم الشبكة أو مقدمي الخدمة؛
- عدم مزامنة الجهاز مع خوادم وقت موثوقة (NTP Servers)، بما قد يؤدي إلى انحراف التوقيت المسجل عن التوقيت الحقيقي.

لذا يتعين على جهة التحقيق، قبل التعويل على الطابع الزمني كعنصر إثبات، أن تتحقق من سلامة البيئة التقنية التي أنشئ فيها، وأن تُجري مقارنات فنية بينه وبين باقي المؤشرات الزمنية المتاحة في النظام أو في مصادر خارجية. فالعبرة لا تكون بزمان واحد معزول، وإنما بتكامل الدلالات الزمنية واتساقها داخل السياق الرقمي العام للواقعة. وتُظهر التطورات الحديثة في الطب الشرعي الرقمي (Digital Forensics) أن الطوابع الزمنية لم تعد المصدر الوحيد للمعلومات الزمنية، بل بات من الممكن الاعتماد على ما يُعرف بـ المؤشرات الزمنية الضمنية، مثل:

- تسلسل أرقام السجلات (Log Sequence Numbers)؛
- ترتيب الأحداث داخل ملفات النظام؛
- آثار الوصول والتشغيل والحذف؛
- العلاقات الزمنية بين العمليات المختلفة داخل النظام.

وتُسهم هذه المؤشرات مجتمعة في إعادة بناء تسلسل زمني مُحكم للوقائع الرقمية، حتى في الحالات التي يثبت فيها التلاعب بالطوابع الزمنية المباشرة أو عدم تزامنها مع مصادر وقت خارجية. وبذلك، يتحقق قدر أعلى من الدقة والموثوقية في استنتاج الزمن الحقيقي للأفعال محل الاتهام.⁵⁴ وبناءاً على ما تقدم نجد أن الطابع

54 Lisa M. Dreier et al: Beyond Timestamps: Integrating Implicit Timing Information into Digital Forensic Timelines,” Forensic Science International: Digital Investigation 49 - 2024, p5 Article 301755, <https://doi.org/10.1016/j.fsidi.2024.301755>.

الزمني لا يُعد دليلاً زمنياً مطلقاً بذاته، بل قرينة تقنية قوية تتعزز أو تضعف بحسب سلامتها الفنية، وبمدى توافقها مع باقي الأدلة الرقمية والقرائن الزمنية الأخرى. ويظل للقاضي، في جميع الأحوال، سلطة تقديرية في وزن هذه العناصر مجتمعة، والتحقق من مدى كفايتها لبناء قناعة قضائية سليمة، دون إفراط في الثقة التقنية أو إهدار غير مبرر لقيمة الدليل الرقمي.

المبحث الثاني

التكييف القانوني للميتاداتا ودورها في الإثبات الجنائي

تتفاقم هذه الإشكالية في ظل غياب تعريف تشريعي جامع للميتاداتا في معظم الأنظمة القانونية، واعتماد التشريعات - في الغالب - على مفاهيم متجاوزة مثل بيانات الاتصال أو البيانات المروية أو البيانات التقنية، دون ضبط دقيق لحدود كل منها. وقد أدى هذا الغموض المفاهيمي إلى تباين واضح في التكييف القانوني للميتاداتا، انعكس بدوره على اختلاف مستويات الحماية الإجرائية المقررة لها، وعلى تضارب التطبيقات القضائية بشأن مشروعيتها وقيمتها الإثباتية. كما أن التطور التقني المتسارع، ولا سيما في مجال التحليل التجميعي والترابطي للبيانات، قد أسهم في إعادة تشكيل النظرة التقليدية للميتاداتا، إذ لم تعد تُنظر إليها بوصفها معطيات خارجية محايدة لا تمس الخصوصية، بل كأداة قادرة - بذاتها أو بالاقتران بغيرها - على الكشف العميق عن هوية الشخص وسلوكه وتحركاته ونمط حياته. وهو ما يفرض إعادة النظر في الأسس التي يقوم عليها تكييفها القانوني، بعيداً عن المعايير الشكلية الضيقة.

المطلب الأول

التكييف القانوني للميتاداتا

أولاً: خضوع الميتاداتا للبيانات الشخصية :

يثير توصيف الميتاداتا بوصفها بيانات شخصية إشكالاً قانونياً دقيقاً تبعاً لمعيار الارتباط بالشخص الطبيعي ومدى إمكانية التعرف عليه بصورة مباشرة أو غير مباشرة من خلال هذه البيانات. ولا ينصرف الخلاف إلى الطبيعة التقنية للميتاداتا في ذاتها، بقدر ما ينصبّ على أثرها الوظيفي وقدرتها العملية على كشف الهوية أو تتبع السلوك.

١- الاتجاه الأوروبي

يتبنّى التشريع الأوروبي، في اللائحة العامة لحماية البيانات (GDPR)، معيارًا واسعًا لتعريف البيانات الشخصية، قوامه أن كل معلومة تتعلق بشخص طبيعي مُحدّد أو قابل للتحديد تُعدّ بيانات شخصية، بصرف النظر عن طبيعتها التقنية أو شكلها الظاهري.^{٥٥} ووفقًا لهذا المعيار وإن لم ينص صراحه علي الميتاداتا الا انه ، عدّ الميتاداتا بيانات شخصية متى أمكن - سواء منفردة أو بالاقتران مع بيانات أخرى - الكشف من خلالها عن هوية الشخص، أو موقعه الجغرافي، أو أنماط سلوكه الرقمي^{٥٦}. ويتجلى ذلك بوضوح في صور متعددة من الميتاداتا، مثل:

- ميتاداتا تحديد الموقع الجغرافي (GPS Metadata)
- عناوين بروتوكول الإنترنت (IP Addresses)
- الطوابع الزمنية (Timestamps)
- سجلات النظام وسجلات النشاط (Logs)

فهذه البيانات، عند تجميعها وتحليلها، تُمكن من رسم صورة دقيقة عن تحركات الفرد، واتصالاته، وعاداته الرقمية، بما يجعلها ذات أثر بالغ على الحياة الخاصة. ومن ثمّ، لا ينظر الإطار الأوروبي إلى الميتاداتا من حيث توصيفها التقني المجرد وإنما من حيث وظيفتها الكاشفة ونتيجتها العملية^{٥٧}. وقد استقر الفقه والقضاء الأوروبيان على أن خطورة الميتاداتا لا تقل عن خطورة محتوى البيانات ذاته، متى أدّت إلى مساس

55 ' Art. 4 -GDPR -Definitions » personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; <https://gdpr-info.eu/art-4-gdpr/>

56 ¹ Jacob Leon Kröger, Recognizing Information Inferred about Individuals as Personal Data (Technische Universität Berlin, 2022), SSRN Electronic Journal, posted February 8, 2023, p243 (accessed 18 December 2025 at 12:28AM, <https://papers.ssrn.com/abstract=4349200>).

57 Sheri B. Pan, "Get to Know Me: Protecting Privacy and Autonomy Under Big Data's Penetrating Gaze", Harvard Journal of Law & Technology 30, no. 1 (Fall 2016): p244 accessed 18 December 2025 at 12:49 AM <https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech239.pdf>.

فعلي بالخصوصية، وهو ما يبرّر إخضاعها لذات منظومة الحماية الصارمة المقررة للبيانات الشخصية. فلقد اضطلعت محكمة العدل للاتحاد الأوروبي بدور محوري في إعادة توصيف الطبيعة القانونية لجمع البيانات، ولا سيما الميتادات، من مجرد إجراء تقني أو استدلالي مساعد إلى تدخّل جوهري بالغ الخطورة في الحياة الخاصة للأفراد، يستلزم إخضاعه لأعلى معايير الشرعية والتناسب والرقابة.

ففي حكمها المفصلي *Digital Rights Ireland Ltd v Minister for Communications* (2014)، تصدّت المحكمة للطعن في توجيه الاحتفاظ ببيانات الاتصالات (*Data Retention Directive*)، وانتهت إلى تقرير عدم مشروعيته لمخالفته الصريحة للمادتين 7 و 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي. وقد أسست المحكمة قضاءها على أن الاحتفاظ الشامل وغير المميّز ببيانات الاتصالات، بما في ذلك الميتادات، يتيح للسلطات العامة تكوين صورة شبه متكاملة عن حياة الأفراد الخاصة، تشمل أنماط تواصلهم، وعلاقاتهم الاجتماعية، وتحركاتهم، وعاداتهم اليومية، دون اشتراط وجود شبهة محددة أو صلة مباشرة بتهديد فعلي. واعتبرت المحكمة أن هذا النمط من الاحتفاظ يمثل تدخلاً جسيماً (*Serious Interference*) في جوهر الحق في الخصوصية، لا يمكن تبريره بمجرد اعتبارات عامة تتعلق بمكافحة الجريمة أو الأمن، ما لم يكن منضبطاً بضمانات دقيقة ومتناسبة، وهو ما افترق إليه التوجيه محل الطعن.⁵⁸

وجاء حكم *Tele2 Sverige AB & Watson* (2016) ليعمّق هذا الاتجاه ويضع معايير أكثر صرامة، حيث أكدت المحكمة، بوضوح لا لبس فيه، عدم جواز فرض التزام عام وشامل على مزودي خدمات الاتصالات بالاحتفاظ ببيانات المرور والموقع لجميع المستخدمين دون تمييز. وقررت أن أي جمع أو احتفاظ ببيانات الاتصالات - بما فيها الميتادات - لا يكون مشروعاً إلا إذا استوفى جملة من الشروط التراكمية، في مقدمتها: أن يكون محدد الهدف بدقة، ومقصوراً على فئات معينة من البيانات والأشخاص، ومقيّداً بمدة زمنية ضرورية فقط، فضلاً عن خضوع النفاذ إلى هذه البيانات لرقابة قضائية مسبقة أو رقابة مستقلة فعّالة. وأكدت المحكمة أن غياب هذه الضمانات يحوّل الإجراء من وسيلة مشروعة للتحقيق إلى انتهاك بنيوي للحقوق الأساسية.⁵⁹

58 *Digital Rights Ireland Ltd v. Minister for Communications*, Joined Cases C293/12 and C594/12, Judgment of 8 April 2014.

59 *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and Others*, Joined Cases C203/15 and C698/15, Judgment of 21 December 2016.

ويكتمل هذا المسار القضائي الأوروبي بإضافة حكم محكمة العدل للاتحاد الأوروبي في قضية Patrick Breyer v. Bundesrepublik Deutschland، Case C-582/14، الصادر في ١٩ أكتوبر ٢٠١٦، الذي يُعدّ حلقة مفصلية في بلورة المفهوم القانوني للميتاداتا وتحديد مدى خضوعها لنظام حماية البيانات الشخصية. ففي هذه القضية، عالجت المحكمة مسألة ما إذا كانت عناوين بروتوكول الإنترنت الديناميكية (Dynamic IP Addresses) تُعدّ بيانات شخصية من عدمه، عندما لا يكون لدى الجهة التي تحتفظ بها (مقدّم خدمة المحتوى) القدرة المباشرة على تحديد هوية المستخدم، بينما تظل هذه القدرة متاحة لجهة أخرى (مقدّم خدمة الإنترنت). وقد انتهت المحكمة إلى تقرير مبدأ بالغ الأهمية، مفاده أن المعلومة تُعدّ «بيانات شخصية» متى كان من الممكن قانوناً وواقعياً ربطها بشخص طبيعي مُحدّد أو قابل للتحديد، ولو تم هذا الربط عبر طرف ثالث، وليس بالضرورة عبر الجهة الحائزة للبيانات ذاتها.

وأوضحت المحكمة أن عناوين الـ IP الديناميكية، رغم طابعها التقني الظاهري، تمكّن - بالاقتران ببيانات إضافية تحتفظ بها جهات أخرى - من تحديد هوية المستخدم أو تتبّع نشاطه الرقمي، ومن ثمّ تندرج ضمن مفهوم البيانات الشخصية بالمعنى الوارد في توجيه حماية البيانات (EC/95/46 آنذاك). وبذلك رفضت المحكمة أي تفسير ضيق يستبعد هذا النوع من الميتاداتا من نطاق الحماية، مؤكدة أن العبرة ليست بطبيعة البيانات في ذاتها، بل بقدرتها الوظيفية على الكشف عن هوية الشخص أو سلوكه.⁶⁰

يُضاف حكم Patrick Breyer إلى ما قرره محكمة العدل للاتحاد الأوروبي في قضيتي Digital Rights Ireland و Tele2 Sverige & Watson ليرسخ اتساقاً قضائياً واضح المعالم، قوامه أن الميتاداتا - مهما بدت منفصلة عن مضمون الاتصال - لا تُعدّ بيانات ثانوية أو محايدة من حيث الأثر القانوني. فقد أكدت المحكمة أن هذه البيانات، متى نُظر إليها في مجموعها و بالاقتران بغيرها من المعطيات، تمتلك قدرة عالية على رسم صورة دقيقة للحياة الخاصة للأفراد، تشمل أنماط تواصلهم، وتحركاتهم، وعلاقاتهم الاجتماعية، وسلوكهم اليومي. ومن ثمّ، فإن جمع الميتاداتا أو الاحتفاظ بها أو معالجتها لا يجوز إخضاعه لنظام قانوني مُخفّف أو استثنائه من ضمانات حماية البيانات، بل يتعيّن أن يتم في إطار حماية صارمة للبيانات الشخصية، قائمة على مبادئ الشرعية، والضرورة، والتناسب، وتحت رقابة قضائية فعّالة ومستقلة.⁶¹

60 Patrick Breyer v. Bundesrepublik Deutschland, Case C582/14, Judgment of 19 October 2016. https://collab.dpa.gr/wp-content/uploads/2023/07/CJEU_C-582.14-Breyer_en.pdf

61 Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020pp 548-553

ويُستخلص من هذه الأحكام، في مجموعها، أن القضاء الأوروبي قد حسم بصورة قاطعة الجدل المتعلق بالطبيعة القانونية للميتادات، رافضاً أي مقارنة تُقلّل من حساسيتها أو تختزلها في كونها أقل خطراً من محتوى الاتصالات. فقد اعتبرت محكمة العدل أداة قائمة بذاتها قادرة على إحداث مساس عميق بجوهر الحق في الخصوصية وحماية البيانات، وهو ما يقتضي عدم التعامل مع جمعها أو الاحتفاظ بها باعتباره إجراءً استدلالياً بسيطاً أو عرضياً. وعلى العكس، فإن هذا الإجراء يُشكّل تدخلاً جوهرياً في الحقوق الأساسية، لا يُتصور مشروعيته إلا إذا استوفى معايير الشرعية الصارمة، والتناسب الدقيق، والضرورة القصوى، مقروناً بضمانات إجرائية وقضائية عالية المستوى. وبهذا المعنى، أسست محكمة العدل للاتحاد الأوروبي معياراً مرجعياً متقدماً في التشريعات المقارنة، يُعيد رسم الحدود الدقيقة بين مقتضيات الأمن ومتطلبات صون الحقوق والحريات الأساسية.

٢- التشريع الفرنسي

يتماشى التشريع الفرنسي مع الإطار الأوروبي لحماية البيانات الشخصية، ولا سيما أحكام اللائحة العامة لحماية البيانات (GDPR)، وذلك من خلال التطبيق الصارم لقانون المعلوماتية والملفات والحريات (Loi Informatique et Libertés) ^{٦٢} بصيغته المعدلة، فضلاً عن الاجتهادات القضائية ذات الصلة. ويُعدّ مفهوم البيانات أو المعطيات الشخصية (personal data – les données personnelles) من المفاهيم المحورية في هذا الإطار، وهو مفهوم لم يتبلور في التشريع الفرنسي دفعة واحدة، بل جاء ثمرة تطور تدريجي عكس تحوُّلاً جوهرياً في فلسفة الحماية القانونية للخصوصية.

فقد استخدم المشرّع الفرنسي، في الصيغة الأولى للقانون رقم ٧٨-١٧ الصادر في ٦ يناير ١٩٧٨، مصطلح البيانات الاسمية (les données nominatives) على نحوٍ أساسي، مع حضور محدود لتعبير البيانات الشخصية. وكان المقصود بالبيانات الاسمية، وفق الفهم السائد آنذاك، كل معلومة – أيّاً كان شكلها أو وسيلة التعبير عنها – تسمح بصورة مباشرة أو غير مباشرة بتحديد هوية شخص طبيعي معيّن أو قابل للتحديد، سواء تمت معالجتها من قبل شخص طبيعي أو شخص اعتباري. ^{٦٣} غير أن هذا المفهوم، رغم اتساعه النسبي، ظلّ مرتبطاً تاريخياً بفكرة الإسناد الاسمي، بما

62 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée notamment par la loi n° 2018-493 du 20 juin 2018

63 Simon Caqué: Le régime juridique des données publiques numériques (thèse de doctorat, Université de Rennes 1, 2020), dirigée par Hélène Muscat, soutenue le 10 septembre 2020, p98

قد يُوحى، على نحو مضلل، بقصر نطاق الحماية على البيانات التي تكشف الهوية بصورة صريحة.⁶⁴

ومن ثمّ، جاء التعديل الجوهري الذي أدخله القانون رقم ٢٠٠٤-٨٠١ الصادر في ٦ أغسطس ٢٠٠٤ ليُكرّس تحوُّلاً مفاهيمياً حاسماً، تمثل في استبدال مصطلح "البيانات الاسمية" بمصطلح "البيانات ذات الطابع الشخصي"، مع تبني تعريف أوسع يركّز على قابلية الشخص للتحديد لا على الطبيعة الاسمية للبيانات. وقد مثّل هذا التحول استجابة مباشرة لمقتضيات القانون الأوروبي، وتأكيداً على أن الحماية القانونية لا تنصرف فقط إلى البيانات التي تكشف الاسم أو الهوية المباشرة، بل تمتد إلى كل معطى يسمح، منفرداً أو بالاقتران بغيره، بتحديد الشخص أو تتبّع نشاطه أو المساس بحياته الخاصة.⁶⁵

فقد استقر اجتهاد القضاء الفرنسي، ولا سيما قضاء محكمة النقض (Cour de cassation)، على أن البيانات التقنية المتعلقة بحركة الاتصالات، وبخاصة بيانات الهاتف المحمول، بما تتضمنه من عناصر التتبع الجغرافي وتحديد الموقع، لا تُعد مجرد بيانات تقنية محايدة أو ثانوية، بل تُشكّل بيانات ذات طبيعة حساسة، تتجاوز مفهوم "البيانات التقنية البسيطة"، لما تتطوي عليه من قدرة عالية على الكشف عن أنماط

حياة الأفراد وتحركاتهم اليومية.

وأكدت محكمة النقض الفرنسية في أكثر من حكم أن العبرة لا تكون بالوصف الشكلي للبيانات، وإنما بالأثر العملي المترتب على استخدامها. فمتى استُخدمت بيانات الاتصال أو البيانات التقنية - بما في ذلك المياداتا - على نحو يسمح بتتبع نشاط الشخص، أو إعادة بناء شبكة علاقاته، أو تحديد تحركاته الزمانية والمكانية، فإنها تخرج عن نطاق المعالجة التقنية البحتة، وتُعدّ تدخلاً جوهرياً في الحياة الخاصة.⁶⁶

٦٤ د. محمد سعيد القرعة: المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية علي ضوء القانون رقم ١٥١ لسنة ٢٠٢٠، المجلة القانونية، كلية الحقوق، جامعة القاهرة فرع الخرطوم، المجلد ١٨، ع ٣٤، نوفمبر ٢٠٢٣، ص ١٥٨١

65 Lucie Cluzel-Métayer et Émilie Debaets : Le droit de la protection des données personnelles : la loi du 20 juin 2018 », Revue française de droit administratif, no 6 (novembre-décembre 2018) p. 1101.

66 Cour de cassation, crim., 18 avril 2019, n° 18-82.159, Bull. crim. n° 81, Considérant 5.

&Cour de cassation, crim., 12 juillet 2016, n° 15-87.374, Considérant 4.

ويترتب على هذا التكيف أن جمع هذه البيانات أو استغلالها في المجال الجنائي لا يكون مشروعاً إلا إذا تم في إطار ضمانات إجرائية وقضائية صارمة، وعلى رأسها صدور إذن قضائي مسبق من السلطة المختصة، وتقيّد الإجراء بمبادئ الضرورة والتناسب والهدف المحدد. أما إذا جرى جمع هذه البيانات أو تحليلها بالمخالفة لهذه الضوابط، فإن الدليل المستمد منها يكون مشوباً بعدم المشروعية، وترتب على ذلك بطلانه واستبعاده من دائرة الإثبات.

ويتضح أن النظام الفرنسي لا يتعامل مع الميتاداتا من منظور تقني ضيق، بل يعتمد معياراً وظيفياً يربط الحماية القانونية بقدرة البيانات على المساس بالحياة الخاصة، لا بمجرد تصنيفها الاسمي. وهو توجه يُجسّد تطوراً مهماً في الفقه والقضاء المقارنين، ويؤكد أن البيانات التقنية قد تتحول - بحسب طريقة استخدامها - إلى أدلة شديدة الخطورة على الحقوق والحريات، بما يستوجب إخضاعها لرقابة قضائية فعّالة.⁶⁷

ويتعزز هذا الاتجاه بما قرّره المجلس الدستوري *Conseil constitutionnel* الذي أخضع بيانات الاتصال والبيانات التقنية للحماية الدستورية متى كان من شأنها تمكين السلطات العامة من مراقبة الأفراد أو تتبّع سلوكهم، مؤكداً أن مشروعيتها تظل رهينة باحترام مبادئ الضرورة والتناسب، وتوفير رقابة فعّالة على جمعها واستخدامها.⁶⁸ ويكتسب هذا التطور المفاهيمي في تعريف البيانات ذات الطابع الشخصي أهمية خاصة عند الانتقال إلى بحث الوضع القانوني للميتاداتا، إذ إن الجدل حول طبيعتها لا يمكن فصله عن التحول الذي شهده مفهوم البيانات الشخصية ذاته في التشريع الأوروبي والفرنسي.⁶⁹ فكما تخلّى المشرّع الفرنسي عن المقاربة الشكلية الضيقة التي كانت تربط الحماية القانونية بفكرة البيانات الاسمية، واتجه إلى اعتماد معيار قابلية الشخص للتحديد بصورة مباشرة أو غير مباشرة، فإن هذا المعيار ذاته هو الذي أتاح إدراج فئات جديدة من البيانات - ومنها الميتاداتا - ضمن نطاق الحماية القانونية، رغم افتقارها الظاهري إلى أي مضمون اسمي أو محتوى اتصالي.⁷⁰

67 Cour de cassation, criminelle, Chambre criminelle, 22 octobre 2013, 13-81.945, Publié au bulletin

68 Conseil constitutionnel, décision n° 2015-713 DC, 23 juillet 2015, Considérant 92.

& Bastien Le Querrec, "European metadata retention: news from the EU court", about:intel.eu, 11 March 2020, accessed 19 December 2025, <https://aboutintel.eu/european-metadata-retention/>.

69 Serge Slama, "Données de connexion et vie privée," *Revue française de droit constitutionnel* 168 (2021): p 835.

70 Laurent Mucchielli, "Les données de connexion devant la jurisprudence: de la forme au fond," *Revue de science criminelle et de droit pénal comparé* 4

لذا لا تُفهم الميَّادات، في الإطار القانوني المعاصر، باعتبارها بيانات تقنية محايدة أو مجرد معطيات تشغيلية لازمة لعمل نظم الاتصالات، بل بوصفها امتداداً وظيفياً لمفهوم البيانات الشخصية متى كانت قادرة، منفردة أو بالاقتران بغيرها، على تحديد هوية الشخص، أو رسم ملامح سلوكه، أو تتبّع نشاطه وتحركاته. وعلى هذا الأساس، فإن إدراج الميَّادات ضمن نطاق الحماية القانونية لم يكن تطوراً عرضياً أو استثناءً قضائياً، بل نتيجة منطقية لمسار تشريعي وفقهي وقضائي متكامل، انتقل فيه القانون من حماية الاسم والهوية الصريحة إلى حماية الشخص في بعده الرقمي الوظيفي. وهو ما مهّد لتكريس مبدأ مفاده أن جمع الميَّادات أو الاحتفاظ بها أو تحليلها لا يُعد إجراءً تقنياً بسيطاً، بل تدخلاً جوهرياً في الحق في الخصوصية وحماية البيانات، يستوجب الخضوع لمبادئ الشرعية، والضرورة، والتناسب، ولرقابة قضائية فعّالة، وهو ما سيتم تفصيله عند تناول التنظيم القانوني للميَّادات وطبيعتها في مجال الإثبات الجنائي.

٣- النظام الأمريكي:

مرّ الموقف القضائي الأمريكي إزاء الميَّادات بتطور لافت، يمكن ضبطه تحليلياً من خلال مرحلتين رئيسيتين متميزتين، تعكسان انتقال القضاء من مقارنة شكلية ضيقة للخصوصية إلى مقارنة وظيفية أكثر عمقاً، تضع في الاعتبار الأثر الكاشف للبيانات لا مجرد طبيعتها التقنية.

أ- المرحلة التقليدية:

تأسس الموقف الأمريكي التقليدي على حكم المحكمة العليا في قضية *Smith v. Maryland*، حيث قررت المحكمة مشروعية لجوء السلطات إلى جمع بعض صور الميَّادات، وعلى رأسها أرقام الاتصال الهاتفية، دون الحاجة إلى أمر تفتيش قضائي. وقد استند هذا التوجه إلى ما يعرف بنظرية الطرف الثالث (Third-Party Doctrine)، ومفادها أن الفرد يفقد أي توقع معقول للخصوصية إزاء البيانات التي يُسلمها

طوعاً إلى طرف ثالث، كالشركات المقدّمة لخدمات الاتصالات^{٧١}.

(2019p752).

&CJEU Confirms That National Data Retention Laws May Only Be Adopted Where “Strictly Necessary”, InsidePrivacy.com, January 6, 2017, accessed 19 December 2025, <https://www.insideprivacy.com/international/european-union/cjeu-confirms-that-national-data-retention-laws-may-only-be-adopted-where-strictly-necessary/>.

71 *Smith v. Maryland*, 442 U.S. 735 (1979).

Hanni Fakhoury, “*Smith v. Maryland Turns 35, But Its Health Is Declining*,” Electronic Frontier Foun-

وبموجب هذا المنطق، اعتبرت الميتادات - في حدودها التقليدية - بيانات غير مشمولة بالحماية الدستورية المنصوص عليها في التعديل الرابع للدستور الأمريكي، باعتبارها لا تتعلق بمضمون الاتصال، وإنما تقتصر على معطيات تقنية لازمة لإتمام الخدمة. وقد أدى هذا التصور إلى إضفاء مشروعية واسعة على ممارسات جمع الميتادات دون رقابة قضائية مسبقة، طالما جرى تسليم هذه البيانات لمزودي الخدمة في إطار التعامل العادي.⁷² غير أن هذا الاتجاه اتسم بطابع تجريدي وشكلي، إذ افترض مسبقاً أن جميع صور الميتادات متساوية من حيث خطورتها على الخصوصية، دون اعتبار لقدرتها الفعلية على الكشف عن السلوك الشخصي أو أنماط الحياة.

ب- المرحلة الحديثة:

شهد هذا البناء التقليدي تحولاً جوهرياً مع حكم المحكمة العليا في قضية *Carpenter v. United States*، الذي مثل نقطة انعطاف حاسمة في تقييم الطبيعة الدستورية للميتادات. فقد قضت المحكمة بوجوب حصول السلطات على أمر قضائي مسبق لجمع بيانات الموقع الجغرافي التاريخية (Cell-Site Location Information - CSLI)، رغم كونها ميتاداتاً محتفظاً بها لدى شركات الاتصالات.⁷³

وقد أسست المحكمة هذا التحول على أن بيانات الموقع الجغرافي، بحكم تراكُمها الزمني ودقتها، تمكّن من إعادة بناء تحركات الشخص اليومية، وأنماط حياته، وعلاقاته الاجتماعية، على نحو يُقارب - بل يفوق أحياناً - خطورة الاطلاع على مضمون الاتصالات ذاته. ومن ثم، رأت المحكمة أن تطبيق نظرية الطرف الثالث بصورة آلية على هذا النوع من الميتادات يفضي إلى تفويض جوهر الحق في الخصوصية الذي يحميه التعديل الرابع.⁷⁴

ويكشف حكم *Carpenter* بوضوح عن انتقال القضاء الأمريكي من معيار

ation Deeplinks Blog, June 24, 2014, accessed 19 December 2025 at 1:05 AM <https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining>.

72 G. Ramirez, "The Erosion of Smith v. Maryland," Case Western Reserve Law Review (2019), Case Western Reserve University School of Law Scholarly Commons, p 493 accessed (19 December 2025) <https://scholarlycommons.law.case.edu/caselrev/vol?iss?article=4856&context=caselrev>.

73 *Carpenter v. United States*, 585 U.S. ____ (2018) (No. 16-402) <https://supreme.justia.com/cases/federal/us/585/16-402/> (accessed 19 December 2025).

74 G. Ramirez, "What Carpenter Tells Us About When a Fourth Amendment Search Is Required," Case West. Reserve Law Rev. (2019) (unpaginated), Case Western Reserve Law Review, p190 , (accessed 19 December 2025) <https://scholarlycommons.law.case.edu/caselrev/vol71/iss3/>

شكلي يقوم على مصدر البيانات أو طبيعة تسليمها، إلى معيار وظيفي يربط مشروعية جمع الميادات بمدى قدرتها الكاشفة وتأثيرها العملي على الحياة الخاصة. فالعبرة لم تعد بكون البيانات "غير محتوى"، بل بقدرتها الواقعية على رسم صورة دقيقة عن الشخص وسلوكه.

٤- التشريع المصري:

بالتمّعن في أحكام قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، والقانون رقم ١٥١ لسنة ٢٠٢٠ المتعلق بحماية البيانات الشخصية، يتبين أن المشرّع المصري لم يضع نصًا صريحًا ومباشرًا يُنظّم جمع الميادات أو يحدّد طبيعتها القانونية على نحو مستقل وواضح، سواء من حيث تعريفها أو من حيث الضوابط الإجرائية الخاصة بجمعها واستخدامها في الإثبات الجنائي. غير أن هذا الغياب الصريح لا يعني بالضرورة خروج الميادات عن نطاق الحماية القانونية، إذ يمكن استنباط مركزها القانوني من خلال التفسير المنهجي المتكامل لنصوص القانون.

وبالامعان نجد أن المشرّع المصري، في كلّ من قانون مكافحة جرائم تقنية المعلومات وقانون حماية البيانات الشخصية، قد تبني تعريفًا واسعًا للبيانات الشخصية، يقوم على معيار الارتباط بالشخص الطبيعي القابل للتحديد، دون اشتراط أن تكون البيانات في ذاتها محتوى صريحًا أو إفصاحًا مباشرًا عن الهوية^{٧٥} وهو ذات المعيار الذي استقر عليه الفقه المقارن والتشريعات الأوروبية. كما أن تعريف حركة الاتصال في القانون رقم ١٥٧ لسنة ٢٠١٨ - بما يشمله من بيانات تتعلق بتوقيت الاتصال، ومدته، ووسيلته، وأطرافه - يقترب في جوهره من المفهوم الفني للميادات، باعتبارها بيانات تصف سياق الاتصال لا مضمونه.^{٧٦}

فمما لا شك فيه أن الربط المنهجي بين تعريف البيانات الشخصية الوارد في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، والقانون رقم ١٥١ لحماية البيانات الشخصية وتعريف حركة الاتصال الوارد في مادة التعريفات في القانون رقم ١٥٧ لسنة ٢٠١٨، والأحكام الإجرائية المنصوص عليها في المادة (6) من القانون الأخير، يفضي إلى نتيجة قانونية بالغة الأهمية، مؤداها أن المشرّع

٧٥ المادة (تعريفات) البيانات الشخصية: أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية ع ٣٢ مكرر (ج) أغسطس ٢٠١٨
٧٦ حركة الاتصال (بيانات المرور): بيانات ينتجها نظام معلوماتي تبين مصدر الاتصال وجهته والوجهة المرسل منها والمرسل إليها والطريق الذي سلكه وساعته وتاريخه وحجمه ومدته ونوع الخدمة

المادة ١ (التعريفات)

المصري قد تعامل - ولو بصورة ضمنية - مع الميتاداتا باعتبارها من قبيل البيانات الشخصية، متى

كانت قادرة على الارتباط بشخص طبيعي أو الكشف عن نشاطه أو تتبّع سلوكه الرقمي.

كما تعزز هذا الفهم الأحكام الإجرائية الواردة في المادة (6) من قانون مكافحة جرائم تقنية المعلومات، والتي خوّلت جهات التحقيق إصدار الأوامر اللازمة لمنع استعمال الأنظمة، أو حذف أو تعديل أو تدمير الأدلة الرقمية أو بيانات الشبكة، وكذلك إصدار أوامر التعاون الفني أو المراقبة أو الإيقاف المؤقت للأنظمة والمعدات محل التحقيق. ويُفهم من ذلك أن المشرّع تعامل مع بيانات الشبكة وحركة الاتصال - وهي من صميم الميتاداتا - بوصفها عناصر ذات خطورة خاصة، تستوجب إخضاعها لضوابط إجرائية وقضائية، حمايةً للحقوق والحريات.⁷⁷

وعليه، فإن غياب نص صريح يُسمّي الميتاداتا بذاتها لا ينفي خضوعها للحماية القانونية، طالما اندرجت - من حيث وظيفتها العملية - ضمن البيانات القادرة على تحديد الشخص أو تتبّع نشاطه أو رسم نمط سلوكه الرقمي. فالعبرة، وفقًا للتفسير القانوني السليم، ليست بالمسمّى التقني، وإنما بالأثر الكاشف للبيانات وبقدرتها على المساس بالخصوصية. وبذلك، يمكن القول إن المشرّع المصري قد تنبّأ - بصورة غير مباشرة - معيارًا وظيفيًا في توصيف الميتاداتا، يقترب في مضمونه من الاتجاه الأوروبي، ويُخضعها لمنظومة البيانات الشخصية متى تجاوزت دورها الفني البحث إلى أداة لكشف الهوية أو النشاط أو السلوك. غير أن هذا التنظيم الضمني يظل قاصرًا عن تحقيق اليقين القانوني، ويُبرز الحاجة إلى تدخل تشريعي صريح يُحدّد على نحو قاطع المركز القانوني للميتاداتا وضوابط جمعها وحجيتها، ضمانًا لحماية الخصوصية، ومنعًا لتفاوت التطبيقات القضائية.

٧٧ لجهة التحقيق المختصة - بحسب الأحوال - أن تصدر أمرًا مسبقًا، لمأموري الضبط القضائي المختصين، لمدة لا تزيد على ثلاثين (٣٠) يومًا قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة في ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يلي: ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه، ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لها مقتضى. البحث والتفتيش والدخول والنفوذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط. أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات ومعلومات تتعلق بنظام معلوماتي أو جهاز تقني موجود تحت سيطرته أو مخزنه لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام أو النظام التقني وفي كل الأحوال يجب أن يكون أمر جهة التحقيق المختصة مسببًا

ويرى الباحث أن الميتاداتا تُعدّ من قبيل البيانات الشخصية متى تجاوزت دورها الوصفي أو الفني إلى الكشف - بصورة مباشرة أو غير مباشرة - عن هوية الشخص، أو موقعه، أو نشاطه، أو نمط سلوكه الرقمي. والعبرة، في جميع الأحوال، ليست بالشكل التقني للبيانات، وإنما بوظيفتها الواقعية وأثرها الكاشف، وهو ما يفرض إخضاعها لنظام قانوني خاص يوازن بين مقتضيات الإثبات الجنائي الفعّال وضمانات حماية الخصوصية والحرية الفردية.

ثانيًا: خضوع الميتاداتا لقواعد سرية الاتصالات:

اتجه النظام القانوني البريطاني، قبل صدور Investigatory Powers Act 2016، إلى تبني تمييز مماثل بين محتوى الاتصال وبيانات الاتصال (Communications Data)، التي تشمل الميتاداتا. وكان يُسمح بالحصول على هذه البيانات بموجب أوامر إدارية أو شبه قضائية، دون إخضاعها لنظام الاعتراض الصارم المقرر لمحتوى الاتصالات، استنادًا إلى افتراض عدم مساسها بجوهر السرية^{٧٨}.

غير أن هذا التوجه تعرّض لانتقادات حادة، سواء على الصعيد القضائي الداخلي أو في ضوء رقابة القضاء الأوروبي، لكونه لم يُواكب التطور التقني الذي جعل الميتاداتا أداة قادرة على تقديم صورة شبه مكتملة عن حياة الفرد الرقمية. وقد أسهم ذلك في إعادة تقنين هذا المجال في قانون سلطات التحقيق لعام ٢٠١٦، مع إخضاع جمع بيانات الاتصال لنظام رقابي أكثر تشددًا، وإن ظلّ دون مستوى الحماية المقررة لمحتوى الاتصال^{٧٩}.

ثالثًا: الاتجاه المُشدّد: الميتاداتا جزء من سجلات الاتصالات:

تتجه بعض الأنظمة القانونية، وعلى رأسها النظامان الأمريكي والبريطاني، إلى اعتبار الميتاداتا جزءًا من سجلات الاتصالات (Communication Records / Call Detail Records)، ومن ثمّ تخضعها - من حيث المبدأ - لنظام السرية الإجرائية المقررة للاتصالات، ولو بدرجة أقل من محتوى الاتصال ذاته. حيث لا يُنظر إلى الميتاداتا بوصفها مجرد بيانات تقنية محايدة، وإنما باعتبارها بيانات قادرة على الكشف عن نمط الاتصال والعلاقات الاجتماعية، وتحديد أطراف التواصل، وتوقيته، ومدته، ومكانه. ويستند هذا الاتجاه إلى فكرة مفادها أن سرية الاتصال لا تنحصر في مضمون الرسالة فقط، بل تمتد إلى العناصر المحيطة بها متى كان من شأنها، منفردة

Investigatory Powers Act 2016 ٧٨

Matthew Tokson, "The Telephone Metadata Program and Carpenter v. United States," Notre Dame Law Review 94, no. 5 (2019):p 1885 ٧٩

أو مجتمعة، أن تكشف عن جوهر العلاقة الاتصالية أو أنماطها. وهو ما دفع القضاء الأمريكي والبريطاني إلى اشتراط أمر قضائي أو إذن قانوني خاص للحصول على هذه البيانات، لا سيما بعد اتساع نطاق التحليل التجميعي للميتادات وما يكشفه من صورة شبه كاملة عن حياة الأفراد.

١- التحول في القضاء الأمريكي:

شهد القضاء الأمريكي تحولًا جوهريًا مع حكم المحكمة العليا حيث قضت المحكمة بأن الحصول على سجلات تحديد الموقع الجغرافي عبر الهاتف المحمول (Cell-Site Location Information – CSLI)، وهي في جوهرها ميتاداتا، يُعدّ مساسًا جوهريًا بالخصوصية، ويستلزم أمرًا قضائيًا قائمًا على سبب محتمل.⁸⁰ وأكدت المحكمة أن: «التحليل التجميعي لبيانات الموقع يمكّن الحكومة من إعادة بناء تحركات الشخص على نحو دقيق، بما يكشف عن تفاصيل حميمة من حياته الخاصة، وهو ما لا يمكن قبوله دون رقابة قضائية صارمة». وقد تراجعت المحكمة صراحة عن التطبيق الجامد لنظرية الطرف الثالث، وأقرت بأن خطورة الميتادات لا تقل عن خطورة محتوى الاتصال متى أدت إلى رسم صورة شاملة عن حياة الفرد.

من ناحية أخرى، أقرّ الكونغرس الأمريكي في يونيو ٢٠١٥ قانون (USA FREEDOM ACT) الذي عدّل العديد من أحكام قانون باتريوت، وفرض قيودًا على بعض برامج الجمع الشامل التي كانت تديرها وكالة الأمن القومي،^{٨١} ولا سيّما جمع البيانات الوصفية الخاصة بالاتصالات. حيث نصت المادة ١٠١ منه علي: «لا يجوز للحكومة جمع السجلات أو الأشياء المادية بموجب المادة ٥٠١ من قانون مراقبة الاستخبارات الأجنبية (المعروفة بالمادة ٢١٥ من قانون باتريوت) على نحو جماعي أو شامل.^{٨٢} ويُشترط أن يكون أي طلب للحصول على سجلات أو أشياء مادية محدّدًا تحديّدًا خاصًا (Specific Selection Term)»^{٨٣} بما يكفي لحصر نطاق الجمع في

80 Carpenter v. United States, 585 U.S. (2018)

81 USA FREEDOM Act of 2015 (Pub. L. 114-23), enacted June 2, 2015.

82 “(b) Prohibition on Bulk Collection.—

(1) IN GENERAL.—No order issued under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) shall authorize the collection of any tangible things (such as books, records, papers, or documents) where the production of such tangible things is not directed at an individual, account, address, or personal device (or any specified selection term related to such an individual, account, address, or personal device).”

٨٣ يقصد بعبارة «مصطلح تحديدي خاص» مصطلحًا يُستخدم لتحديد شخص أو كيان أو حساب

أو عنوان أو جهاز معين، وبما لا يسمح بجمع واسع النطاق أو غير مقيّد للمعلومات» (The term «specific selection term» means a term used to uniquely identify a discrete

person, entity, account, address, or device, or to identify a specific facility or

(«place

شخص، أو حساب، أو عنوان، أو جهاز محدد⁸⁴»

٢ - تحول النظام البريطاني:

يمثل حكم *Watson v. Secretary of State for the Home Department* نقطة تحول

جوهرية في الموقف القضائي البريطاني من مسألة الاحتفاظ ببيانات الاتصالات والميتادات⁸⁵، إذ جاء هذا الحكم متسقاً مع الاتجاه الأوروبي الذي أرسته محكمة العدل للاتحاد الأوروبي في القضايا المجمعة *Tele2 Sverige AB* و *Watson*، والتي أعادت رسم الحدود القانونية لمشروعية جمع بيانات الاتصالات في ضوء الحقوق الأساسية.

فقد قرّرت محكمة الاستئناف في المملكة المتحدة، استناداً إلى هذا الاجتهاد الأوروبي، أن تشريعات الاحتفاظ ببيانات المراقبة لأغراض مكافحة الجريمة لا يجوز أن تكون عامة أو شاملة، بل يجب أن تقتصر على الجرائم الخطيرة فقط، وأن يكون الوصول إلى البيانات المحتفظ بها خاضعاً لرقابة مسبقة من القضاء أو من هيئة إدارية مستقلة تتوافر لها ضمانات الحياد والاستقلال. وبذلك، لم يعد مقبولاً - من منظور هذا الحكم - إتاحة الاطلاع على الميتادات بموجب أوامر إدارية واسعة أو غير مقيدة، حتى وإن لم تتعلق هذه البيانات بمحتوى الاتصال ذاته.⁸⁶

وقد طُرحت مسألة الامتثال لقانون الاتحاد الأوروبي بوضوح في هذا السياق، ولا سيما فيما يتصل بالمادتين 7 و 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي، اللتين تكفلان الحق في احترام الحياة الخاصة والحق في حماية البيانات الشخصية. إذ رأت المحكمة أن تشريع *Data Retention and Investigatory Powers Act* 2014، في صورته التي كانت سارية آنذاك، لا يحقق التوازن المطلوب بين متطلبات

84 USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101(b)(1), 129 Stat. 268 (codified at 50 U.S.C. § 1861).

85 *Secretary of State for the Home Department v. Watson* [2018] EWCA Civ 1839, paras. 126, 132 (UK Court of Appeal).

86 *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson*, Joined Cases C203/15 and C698/15, CJEU Judgment of 21 December 2016.

الأمن ومكافحة الجريمة من جهة، وضمانات الخصوصية وحماية البيانات من جهة أخرى⁸⁷، لكونه يسمح بالاحتفاظ الواسع وغير المقيد ببيانات الاتصالات، بما في ذلك الميتادات، دون ضوابط كافية⁸⁸.

وتكمن أهمية هذا الحكم في أنه نقل النقاش من التمييز الشكلي بين محتوى الاتصال وبياناته المحيطة، إلى معيار الأثر الفعلي⁸⁹. فلم تعد العبرة - وفقًا لهذا الاتجاه - بكون البيانات "غير محتوية"، وإنما بقدرتها العملية على كشف أنماط الاتصال، وتحركات الأشخاص، وشبكات علاقاتهم. فإذا كان جمع الميتادات والاحتفاظ بها يسمح بإعادة بناء الحياة الخاصة للفرد على نحو شامل، فإن إخضاعها لسرية الاتصالات ولضمانات قضائية مشددة يصبح أمرًا لازمًا، حتى دون الاطلاع على مضمون الرسائل أو المكالمات⁹⁰.

يُجسّد حكم Watson، في انسجامه مع اجتهاد محكمة العدل للاتحاد الأوروبي، تراجعًا واضحًا عن الاتجاه المُخفّف الذي كان يبرّر جمع الميتادات دون رقابة صارمة، ويكرّس بدلًا منه اتجاهًا مُشدّدًا وظيفيًا، يُخضع الميتادات لنظام حماية قريب - في جوهره - من النظام المقرر لمحتوى الاتصالات، متى أدّت وظيفتها التحليلية إلى مساس فعلي بالخصوصية⁹¹. وهو اتجاه يعكس تطورًا عميقًا في الفهم القانوني لمفهوم السرية في العصر الرقمي، ويؤكد أن حماية الحياة الخاصة لا تتحقق بالفصل الشكلي بين أنواع البيانات، بل بضبط آثار استخدامها ومخاطرها الواقعية.

87 Data Retention and Investigatory Powers Act 2014 (c. 27), §1 (UK) (declared incompatible with EU law in Watson [2018] EWCA Civ 1839).

88 Secretary of State for the Home Department v. Watson, Global Freedom of Expression, Columbia University, accessed 18 December 2025, <https://globalfreedomofexpression.columbia.edu/cases/secretary-state-home-department-v-watson/>.

89 Orla Lynskey, "After Watson: Mandatory Data Retention and the CJEU," European Data Protection Law Review 3 (2017)p89

90 David Anderson QC, A Question of Trust: Report of the Investigatory Powers Review (2015), Independent Reviewer of Terrorism Legislation.p245 &Orla Lynskey: After Watson: Mandatory Data Retention and the CJEU," European Data Protection Law Review 3 (2017p 89.

91 Lilian Edwards, "From DRIPA to IPA: The UK's Journey Towards Privacy-Compliant Surveillance," International Journal of Law and Information Technology 26 (2018p12

المطلب الثاني

دور الميادات وطبيعته الإثباتية

أولاً: دور الميادات في الإثبات الجنائي:

تقوم الميادات بدور حاسم في مسائل الإثبات الجنائي، ويتمثل هذا الدور فيما يلي:

١ - تحليل الصور والفيديو (Image & Video Forensics) :

يُعدّ تحليل الصور ومقاطع الفيديو من أهم مجالات توظيف الميادات في التحقيق الجنائي الرقمي، لما تمثّله هذه الوسائط من خطورة خاصة في تكوين القناعة القضائية، نظراً لقوتها الإقناعية الظاهرة وسهولة تداولها.⁹²

وتؤدي الميادات دوراً محورياً في تفكيك الصورة أو الفيديو من الداخل، والانتقال من المظهر الخارجي المضلل إلى الحقيقة التقنية الكامنة وراءه.⁹³ فتمكّن الميادات المحقق من كشف التعديلات المصطنعة التي قد تطال الصور أو مقاطع الفيديو، سواء تعلّق الأمر ببرامج تحرير تقليدية مثل Photoshop، أو بتقنيات أكثر تعقيداً كالصور والفيديوهات المصطنعة بتقنية التزييف العميق (Deepfake). فاختلاف بيانات البرنامج المستخدم في الإنشاء أو التعديل، أو عدم اتساق الطابع الزمني مع سياق الواقعة، أو ظهور آثار تحرير غير منطقية في سجل الميادات، كلها مؤشرات تقنية قوية على العبث بالمحتوى الأصلي.⁹⁴

ويُضاف إلى ذلك أن مقارنة الميادات بين النسخ المختلفة من الملف قد تُظهر فجوات زمنية أو تقنية لا يمكن تفسيرها إلا بحدوث تعديل لاحق، وهو ما يُضعف الثقة في أصالة الدليل المرئي ويحول دون التعويل عليه دون فحص معمّق.⁹⁵

92 NIST Guidelines on Digital Evidence, Special Publication 800-86 (2006) pp4-12

93 Eoghan Casey :Digital Evidence and Computer Crime, 3rd ed. Academic Press, 2011, pp. 463–468.&Eoghan Casey, *Digital Evidence and Computer Crime* (4th ed., Academic Press, 2020)p287

94 Hany Farid :Photo Forensics (MIT Press, 2016), pp. 31–38& Siwei Lyu et al., “A Review of Deep Learning Methods for Detecting Deepfakes,” *IEEE Transactions on Information Forensics and Security* 16 (2021): p3462

95 Eoghan Casey :Handbook of Digital Forensics and Investigation -Academic Press, 2010 p. 529

٢- تحديد مكان التقاط الصورة أو الفيديو:

تُتيح ميتاداتا تحديد الموقع الجغرافي (Geolocation Metadata)، المرافقة للصور ومقاطع الفيديو، إمكانية تحديد مكان الالتقاط بدقة عالية، لاسيما عند استخدام أجهزة أو هواتف ذكية تُفَعِّل خاصية تحديد الموقع تلقائياً.^{٩٦} وتُعد هذه البيانات ذات أهمية قصوى في ربط الدليل المرئي بمسرح الجريمة، أو في نفي وجود المتهم في مكان معين وقت وقوع الواقعة.^{٩٧} غير أن التعويل على هذه الميتاداتا يظل مشروطاً بالتحقق من عدم تعطيل خاصية تحديد الموقع، أو تعديل البيانات يدوياً، وهو ما يفرض ضرورة التحقق من اتساقها مع مصادر أخرى، كبيانات الشبكات وسجلات النظام.^{٩٨}

٣- التحقق من التوقيت الحقيقي للالتقاط:

يُعدّ الطابع الزمني المضمّن في ميتاداتا الصور والفيديو عنصراً حاسماً في تحديد التوقيت الحقيقي للالتقاط، وتمييزه عن تاريخ النشر أو الإرسال. ويساعد هذا العنصر في إعادة بناء التسلسل الزمني للوقائع، وربط الحدث المصوّر بسياقه الزمني الصحيح.^{٩٩} غير أن أهمية الطابع الزمني تقتضي التحقق من سلامة ساعة الجهاز المستخدم، ومزامنتها مع خوادم الوقت الموثوقة، فضلاً عن مقارنة التوقيت مع قرائن أخرى، منعاً للاعتماد على بيانات زمنية قد تكون عرضة للتعديل أو الخطأ.^{١٠٠}

٤- تتبّع البيانات المحذوفة وإعادة بنائها:

لا يؤدي حذف الملفات الرقمية، في الغالب، إلى زوالها الفعلي من الناحية

٩٦ “Smartphone location data embedded in photographs provides precise geolocation information, warranting Fourth Amendment protections equivalent to physical searches. Riley v. California, 573 U.S. 373 (2014) p398

٩٧ د.محمد عبد الفتاح عبد المقصود: القواعد الإجرائية للجرائم التي تقع عبر شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعه طنطا، ٢٠١٥، ص٤٢٤،

٣rd ed. (Charles River, John R. Vacca, Computer Forensics: Computer Crime Scene Investigation Media, ٢٠٠٥), pp. ٣١٦-٣١٢.

GPS metadata in EXIF headers“): (٢٠٢٠) INTERPOL Digital Evidence Guidelines enables precise correlation of visual evidence with crime scenes. Verification against network data and (”.device logs is essential to detect spoofing

٩٨ Sarah Morrissey, “Geolocation Metadata in Mobile Forensics,” *Journal of Digital Forensics, Security and Law* 15, no. 2 (2020): p52

٩٩ Simson L. Garfinkel :Digital Forensics Research: The Next 10 Years - Digital Investigation 7, 2010- pp. S70-S74.

١٠٠ Brian Carrier, File System Forensic Analysis -Addison-Wesley, 2005-pp. 86-92.

التقنية، وإنما يقتصر أثر الحذف على إزالة المؤشر الذي يدل على موقع الملف داخل نظام التشغيل، مع بقاء البيانات - بما فيها الميتاداتا - مخزنة في الوسيط الرقمي إلى أن يُعاد الكتابة فوقها. ونتيجة لذلك، تُعد الميتاداتا عنصراً حاسماً في عمليات استعادة الملفات المحذوفة وإعادة بنائها. وتُستخدم في هذا الإطار أدوات جنائية متخصصة (Forensic Tools) قادرة على استخراج الميتاداتا حتى بعد الحذف، بما يسمح بإعادة بناء خصائص الملف المحذوف، مثل نوعه الأصلي، وتاريخ إنشائه، وتعديله، ومسار تخزينه، وأحياناً ربطه بالمستخدم أو الجهاز الذي أنشأه. ويؤدي هذا الدور إلى تقويض محاولات إخفاء الأدلة الرقمية، ويجعل من الحذف وسيلة غير كافية - في حد ذاته - للإفلات من المساءلة الجنائية.

ومن الناحية القانونية، تكتسب هذه القدرة أهمية خاصة، إذ تمكّن جهات التحقيق من إثبات نية الإخفاء أو العبث بالدليل، وهو ما قد يشكل قرينة إضافية على القصد الجنائي. غير أن التعويل على الميتاداتا المستخرجة من الملفات المحذوفة يظل مشروطاً بإثبات سلامة إجراءات الاستخراج، واحترام سلسلة الحيازة، والتحقق من أن البيانات المستعادة لم تتعرض للتشويه أو الخلط ببيانات أخرى.¹⁰¹

٥- سجلات الدخول Track-log:

تُعدّ سجلات الدخول والنشاط (Logs) من أكثر أنواع الميتاداتا استخداماً في التحقيق الجنائي الرقمي، ولا سيما في جرائم الاختراق والاعتداء على النظم المعلوماتية. فهي تمثل سجلاً زمنياً دقيقاً يُدوّن تلقائياً بواسطة الأنظمة والخوادم، ويكشف عن مجمل الأنشطة التي تمت على النظام محل الاعتداء.¹⁰² وتُبين هذه السجلات، على وجه الخصوص:

- محاولات الدخول الناجحة والفاشلة، بما يسمح بتتبع أسلوب الهجوم وتحديد ما إذا كان يعتمد على التخمين أو على بيانات اعتماد مسروقة.
- الأوامر المنفّذة داخل النظام، وهو ما يتيح تحديد نطاق الاختراق، وما إذا اقتصر على الاطلاع أو امتد إلى التعديل أو الحذف أو تعطيل الخدمات.
- مدة الاتصال وتوقيته، بما يسمح بربط النشاط الإجرامي بزمان محدد، ومقارنته

101 CARRIER, Brian: File system forensic analysis. Addison-Wesley Professional, 2005.p140

١٠٢ د. محمد عبد الفتاح: مرجع سابق، ص٣٤٢ &

Eoghan Casey: ibid p 405

بوجود المتهم أو نشاطه المادي أو الرقمي في ذات الفترة.¹⁰³

وتكمن القوة الإثباتية لسجلات النشاط في أنها تُنشأ آلياً وبصورة دورية، دون تدخل مباشر من المستخدم، وهو ما يمنحها درجة عالية من الموثوقية، متى ثبتت سلامة النظام وعدم العبث بهذه السجلات. ولهذا، كثيراً ما تعتمد المحاكم على الـ Logs بوصفها قرائن تقنية قوية، وقد ترتقي إلى دليل مباشر إذا اتسقت مع باقي عناصر الإثبات وثبتت أصالتها. غير أن هذه الحجية لا تُفترض على إطلاقها، إذ يظل من الضروري التحقق من عدم تعطيل نظام التسجيل، أو التلاعب بالسجلات، أو تعديلها بأثر رجعي، وهي مسائل تفرض إخضاعها لفحص فني دقيق وربطها بمصادر أدلة أخرى.

ثانياً: دور التقنيات الحديثة في تعزيز موثوقية الميتاداتا:

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي (Artificial Intelligence)، ولا سيما خوارزميات التعلم الآلي والتعلم العميق، إلى إحداث نقلة نوعية في آليات تحليل الميتاداتا، سواء من حيث السرعة أو الدقة أو القدرة الاستدلالية. فلم يعد تحليل الميتاداتا مقتصرًا على الفحص اليدوي أو المقارنات المحدودة، بل أصبح يتم في إطار أنظمة ذكية قادرة على معالجة كميات هائلة من البيانات وربطها

واستخلاص أنماط معقدة منها.¹⁰⁴ ويبرز هذا الدور جلياً فيما يلي:

١ - تحليل كميات ضخمة من الميتاداتا في زمن قياسي:

تُمكن تقنيات الذكاء الاصطناعي جهات التحقيق من تحليل كتل ضخمة من الميتاداتا (Big Metadata) في فترات زمنية وجيزة، وهو ما كان يتعذر عملياً بالوسائل التقليدية. فخوارزميات الذكاء الاصطناعي قادرة على فحص ملايين السجلات الزمنية، وبيانات الموقع، وسجلات الدخول، وملفات النظام، في وقت واحد، مع رصد أوجه التشابه والاختلاف والتكرار.¹⁰⁵ ويترتب على ذلك تعزيز فعالية التحقيق الجنائي الرقمي، لا سيما في القضايا المعقدة التي تتعدد فيها الأجهزة، أو المستخدمون، أو الوقائع

١٠٣ د. يوسف بن سعيد الكلبي: مرجع سابق، ص ٣٠١

104 Dong Bin Oh et al: volGPT: Evaluation on Triaging Ransomware Process in Memory Forensics with Large Language Model,” Forensic Science International: Digital Investigation 49, Supplement- 2024, Article 301756, <https://doi.org/10.1016/j.fsidi.2024.301756>.

١٠٥ د. وفاء محمد صقر: المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، ع ٩٦٤، أكتوبر ٢٠٢١، ص ٢٩

الزمنية المتشابكة، إذ يسمح هذا التحليل الشامل بإعادة بناء الوقائع الرقمية على نحو أكثر دقة واتساقاً.¹⁰⁶

٢ - اكتشاف الأنماط السلوكية غير الظاهرة:

من أبرز ما يميز الذكاء الاصطناعي في تحليل الميئاتا قدرته على اكتشاف الأنماط السلوكية غير الظاهرة للعين البشرية. فبفضل التحليل الترابطي والتنبؤي، يمكن للخوارزميات الذكية استخلاص أنماط استخدام أو تواصل أو تنقل لا تظهر عند فحص كل عنصر على حدة. ويتيح ذلك الكشف عن:

- أنماط دخول غير اعتيادية إلى الأنظمة.

- تكرار زمني أو مكاني يُشير إلى نشاط إجرامي منظم.

- علاقات خفية بين مستخدمين أو أجهزة لم تكن ظاهرة في التحليل التقليدي.

ومن ثمّ، تتحول الميئاتا - عبر الذكاء الاصطناعي - من مجرد قرائن منفصلة إلى نموذج سلوكي متكامل قد يُستخدم في إثبات الاعتياد الإجرامي أو نفيه.¹⁰⁷

٣ - كشف التلاعب الدقيق بالصور والفيديو : (Deepfake Detection)

أسهم الذكاء الاصطناعي كذلك في تطوير أدوات متقدمة لكشف التلاعب الدقيق بالصور ومقاطع الفيديو، ولا سيما ما يُعرف بـ التزييف العميق (Deepfake). فهذه الأدوات لا تكتفي بتحليل المحتوى المرئي ذاته، بل تعتمد بدرجة كبيرة على تحليل الميئاتا المرافقة له، مثل سجلات الإنشاء والتعديل، وأنماط الترميز، وعدم الاتساق بين البيانات التقنية والمحتوى الظاهر^{١٠٨}. وتسمح هذه التقنيات برصد الفوارق الدقيقة

106 Sandra Wachter and Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (Columbia Business Law Review 2019(2), p121- posted October 5, 2018, revised June 25, 2019, SSRN, <https://papers.ssrn.com/abstract=3248829> (accessed 16 December 2025 at 12:15 am

١٠٧. سعود عبد القادر الشاعر: دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، المجلد ١٣، العدد ٨٣ - الرقم المسلسل للعدد ٨٣، مارس ٢٠٢٣، ص ٢٨

108 Siwei Lyu et al., "Metadata-Assisted Deepfake Detection: EXIF and Encoding Analysis," *IEEE Transactions on Information Forensics and Security* 17 (2022): p1129

التي يصعب اكتشافها بالوسائل التقليدية، كاختلافات غير منطقية في الطوابع الزمنية، أو استخدام برامج تحرير لا تتفق مع سياق الالتقاط، أو أنماط ضغط وترميز تشير إلى إعادة المعالجة أو الدمج.¹⁰⁹ فقد أدى توظيف الخوارزميات المتقدمة في تحليل الميتادات إلى تمكين جهات التحقيق من إعادة بناء مسرح الجريمة الرقمي على نحو يقترب، من حيث المنهج، من إعادة بناء مسرح الجريمة المادي في الجرائم التقليدية.¹¹⁰ ويقوم هذا الأسلوب على دمج وتحليل عناصر زمنية ومكانية وتقنية متعددة، بما يسمح بإنتاج تصور شامل لتسلسل الوقائع الرقمية.¹¹¹

وتعتمد هذه العملية، بوجه خاص، على الطوابع الزمنية (Timestamps) التي تُمكن من ترتيب الأفعال الرقمية ترتيباً دقيقاً، (سجلات النشاط Logs التي تكشف عن طبيعة الأوامر المنفذة ومحاولات الدخول ومدد الاتصال، فضلاً عن بيانات الموقع الجغرافي التي تربط النشاط الرقمي بمكان محدد). ومن خلال التحليل الترابطي لهذه العناصر، يمكن تحديد لحظة بدء النشاط الإجرامي، ومساره، ونهايته، وربط ذلك بالمستخدم أو الجهاز المعني. ويُسهّم هذا النهج في تقديم تصور زمني ومكاني متكامل للواقعة الإجرامية، يُعزّز من القدرة على إثبات الركن المادي للجريمة أو نفيه، ويُساعد المحكمة على فهم السياق الرقمي الذي وقعت فيه الأفعال محل الاتهام. غير أن قيمة هذا التصور تظل مرهونة بثبوت أصالة الميتادات، وسلامة سلسلة الحيازة، واتساق النتائج المستخلصة مع باقي عناصر الإثبات.¹¹² وعلى الرغم من المزايا البالغة التي يوفرها الذكاء الاصطناعي في تحليل الميتادات وإعادة بناء مسرح الجريمة الرقمي، فإن توظيفه يثير مخاطر قانونية جوهرية لا يجوز إغفالها، لما لها من أثر مباشر على ضمانات المحاكمة العادلة.

ولعل أول هذه المخاطر يتمثل في غموض الخوارزميات أو ما يُعرف بظاهرة الصندوق الأسود (Black Box)، حيث تُنتج الأنظمة الذكية نتائج واستنتاجات دون أن يكون من السهل - أو الممكن أحياناً - تتبع المسار المنطقي أو التقني الذي أدى إليها.¹¹³ ويُضعف هذا الغموض قدرة المحكمة على التحقق من سلامة الاستنتاج، كما

١٠٩. اسعود عبد القادر الشاعر: دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، المجلد ١٣، العدد ٨٣ - الرقم المسلسل للعدد ٨٣، مارس ٢٠٢٣، ص ٢٦.

110 Hany Farid, *Photo Forensics* (MIT Press, 2016)p245

111 Abbas Karimi et al., "Cybercrime Detection Using Semi-Supervised Neural Network," *Computer Science Journal of Moldova* 29, no. 2 (86) (2021): p156.

١١٢ د. محمود سلامة الشريف، «الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته»، *المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي*، جامعة نايف الأمنية، السعودية، مج ٢، ع ٣٤، ص ٣٤١.

113 Rebecca Wexler, "Life, Liberty, and Algorithmic Detection of Recidi-

يُقَدِّد حق الدفاع في مناقشة الدلائل مناقشة فعّالة.¹¹⁴

وثانيها صعوبة الطعن الفني من جانب الدفاع، إذ يتطلب تفنيد نتائج الذكاء الاصطناعي خبرة تقنية متقدمة، وإمكانية الوصول إلى نماذج الخوارزميات وبيانات التدريب، وهي أمور قد تكون محجوبة بدعوى السرية التجارية أو الاعتبارات الأمنية. ويُفضي هذا الوضع إلى اختلال مبدأ تكافؤ السلاح بين الادعاء والدفاع.¹¹⁵ أما الخطر الثالث فيمكن في الانحياز الخوارزمي (Algorithmic Bias)، حيث قد تعكس الخوارزميات - دون قصد - تحيزات كامنة في البيانات التي دُرِّبَت عليها، أو في الافتراضات المسبقة لمصمميها. وقد يؤدي ذلك إلى نتائج غير دقيقة أو تمييزية، بما يُقوِّض الثقة في حياد الدليل المستخلص آلياً.¹¹⁶

ثالثاً: الطبيعة الثبوتية الجنائية للميتاداتا:

يثير تحديد الطبيعة الإثباتية للميتاداتا إشكالاً دقيقاً في الفقه الجنائي الرقمي، يتمحور حول ما إذا كانت تُعدّ دليلاً مباشراً قائماً بذاته، أم مجرد قرينة تقنية على الواقعة محل الاتهام. فالقرينة بلا شك هي إحدى وسائل الإثبات غير المباشرة¹¹⁷، ويقصد بها استخلاص الواقعة المطلوب إثباتها من واقعة أخرى ثابتة بالدليل، بحيث تكون الواقعة الثانية مجهولة، ويتم الوصول إليها عن طريق الاستدلال العقلي والمنطقي انطلاقاً من واقعة أولى معلومة. وعلى هذا النحو، فإن القرينة تمثل نتيجة استنباطية يُجريها القاضي للوصول إلى الحقيقة، دون أن تكون الواقعة محل الإثبات قد ثبتت بدليل مباشر.¹¹⁸ ولقد ذهب الاتجاه الغالب في الفقه الجنائي إلى اعتبار الميتاداتا قرينة تقنية قوية، إذ إنها لا تُثبت - في صورتها المعتادة - مضمون الفعل الإجرامي ذاته وهو الأمر المجهول، وإنما تُثبت السياق الزمني والمكاني والتقني الذي وقع فيه هذا الفعل وهو الأمر المعلوم بذلك هي استنباط أمر مجهول من أمر معلوم¹¹⁹. ومن ثم

vism,” *Supreme Court Review* 70 (2020): p325

١١٤ د. ممدوح حسن مانع: المسؤولية الجنائية عن أفعال الذكاء الاصطناعي غير المشروعة، مجلة دراسات علوم الشريعة والقانون، الأردن، المجلد ٤٨، ع ٢٠٢١، ص ٤٠٠

115 Andrew D. Selbst, “A Due Process Theory for Algorithmic Discrimination,” *California Law Review* 108 (2020): p 1652

116 Sarah Larson, Surya Mattu, Lauren Kirchner, and Julia Angwin, “How We Analyzed the COMPAS Recidivism Algorithm,” ProPublica, May 23, 2016, archived at Perma.cc, <https://perma.cc/8BXL-NU4D> (accessed 9 May 2025).

١١٧ د. أمال عبد الرحيم عثمان: شرح قانون الإجراءات الجنائية، الهيئة المصرية للكتاب، بدون تاريخ نشر، ص ٦٧١

١١٨ د. مأمون محمد سلامه: الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، ١٩٩٢، ص ٢٣٧

١١٩ د. أحمد عبد اللاه المراغي: دور الدلائل الكافية في مباشرة الإجراءات الجنائية، مجلة الدراسات

تُسهّم في ربط الواقعة بفاعل معيّن، أو نفي هذه الصلة، من خلال تحديد التوقيت، والموقع، والجهاز المستخدم، ومسار النشاط الرقمي. ومن جماع ذلك تُعدّ الميتادات قرينة استنتاجية تُكمّل الأدلة الأخرى، ولا تقوم عادةً مقام الدليل المباشر الذي يُثبت الركن المادي للجريمة بذاته، كالسجل الصوتي أو المرئي أو المستند الرقمي الذي يتضمن الفعل محل التجريم. غير أن هذه القاعدة ليست مطلقة؛ إذ قد ترتقي الميتادات إلى مرتبة الدليل المباشر متى توافرت شروط فنية وقانونية صارمة، في مقدمتها:

- ١- ثبوت أصالة الميتادات: أي التأكد من أنها أنشئت تلقائياً بواسطة النظام، ولم تتعرض للتعديل أو العبث، مع التحقق من سلامة البيئة التقنية التي وُلدت فيها.
- ٢- سلامة سلسلة الحيازة^{١٢٠} (Chain of Custody): بحيث يُثبت أن الميتادات انتقلت من مصدرها إلى جهة التحقيق ثم إلى المحكمة دون انقطاع أو تلاعب، مع توثيق كل مرحلة من مراحل الضبط والفحص^{١٢١}.

٣- اتساقها مع أدلة رقمية أخرى: كالسجلات النظامية، وبيانات الاتصالات، والطوابع الزمنية المتطابقة، بما يعزز موثوقيتها ويُخرجها من نطاق الاحتمال.^{١٢٢} وفي هذه الحالة، قد تُثبت الميتادات واقعة إجرامية محددة بذاتها، كإثبات وجود المتهم في مكان وزمان ارتكاب الجريمة الرقمية، أو قيامه بفعل تقني معيّن في توقيت حاسم، بما يجعلها دليلاً مباشراً لا مجرد قرينة.

وقد اتجه القضاء المقارن إلى إرساء ضوابط صارمة تحكم التعامل مع البيانات التقنية والميتادات، دون أن يذهب إلى اعتبارها دليلاً مباشراً قائماً بذاته على نحو مطلق، بل ربط حجيتها بمدى احترام الضمانات الدستورية والإجرائية المصاحبة لجمعها واستخدامها. ففي حكم المحكمة العليا الأمريكية في قضية Carpenter v. Unit^{١٢٣}

القانونية، كلية الحقوق، جامعة أسيوط، المجلد ٥٨، ٢٠٢٢ع، ٣، ص ٥٨

١٢٠ سلسلة الحيازة هي الإطار الإجرائي الذي يوثق كل مرحلة من مراحل ضبط الدليل، نقله، فحصه، تخزينه، وتحليله، بحيث يُظهر بشكل واضح ومفصل من فعل ماذا، متى، وكيف، ومن ثم لا يمكن إثبات سلامة أو أصالة أي دليل ذا صلة بالذاكرة الرقمية إلا إذا بقيت هذه السلسلة غير منقطعة وغير معدّلة طوال دورة الحياة القانونية للدليل.

Taha Gharaibeh, Ibrahim Baggili, and Anas Mahmoud: On Enhancing Memory Forensics with FAME: Framework for Advanced Monitoring and Execution- Forensic Science International: Digital Investigation, ٤٩, Supplement, ٢٠٢٤, p٥, <https://doi.org/10.1016/j.fsi.2024.301707>.

121 Mark L. Krotoski: Effectively Using Electronic Evidence Before and at Trial - United States Attorneys' Bulletin 59, no. 6, 2011- pp. 52-55.

122 Brian Carrier: ibid, pp. 60-67

123 Carpenter v. United States, 138 S. Ct. 2206 (2018). <https://www.ifs.org/wp-content/uploads/2018/10/Carpenter-Amicus.8.14.pdf>

(ed States 2018)، أكدت المحكمة أن بيانات الموقع الجغرافي للهاتف المحمول (CSLI)، رغم كونها في أصلها بيانات وصفية، إلا أنها تتطوي على قدرة عالية على كشف نمط حياة الفرد وتحركاته بصورة شاملة، الأمر الذي يقتضي إخضاع جمعها لإذن قضائي مسبق، وإلا عُدَّ ذلك مساسًا غير مشروع بالحق في الخصوصية المكفول بموجب التعديل الرابع للدستور الأمريكي.

وعلى الصعيد الأوروبي، أرست المحكمة الأوروبية لحقوق الإنسان في حكمها الصادر في قضية *Malone v. United Kingdom*^{١٢٤} مبدأ مفاده أن مراقبة الاتصالات وجمع البيانات التقنية المصاحبة لها لا يكون مشروعاً ولا صالحاً للاعتداد به قانوناً إلا إذا استند إلى إطار تشريعي واضح ومحدد، وهو الاتجاه ذاته الذي أكدته المحكمة ذاتها في حكم الغرفة الكبرى في قضية *Roman Zakharov v. Russia*^{١٢٥} و يفهم من هذه الاجتهادات أن المیتاداتا، وإن كانت تُعدّ جمع بيانات الاتصالات.١٢٥ و يفهم من هذه الاجتهادات أن المیتاداتا، وإن كانت تُعدّ قرينة تقنية ذات دلالة قوية، فإن قيمتها الإثباتية تظل مشروطة باحترام مبدأ المشروعية الإجرائية وسلامة آليات جمعها وحفظها.

تعقيب:

من المعلوم أن القرينة القضائية تختلف اختلافاً جوهرياً عن القرينة القانونية؛ ففي حين يتولى المشرع في القرينة القانونية افتراض الواقعة المجهولة وربطها بواقعة معلومة بنص القانون، بحيث لا يملك القاضي سلطة في إنشائها أو تعديلها، فإن القرينة القضائية هي نتاج العقل القضائي، ينشئها القاضي بنفسه من خلال تحليل الوقائع وربطها، مستنداً إلى سلطته التقديرية وخبرته في تقدير الأدلة من ثم بالامعان في كلا التعريفين نجد أن الميئادات تتقارب مع القرينة القضائية.¹²⁶ حيث أن الميئادات و القرينة القضائية لا يقدر أيُّ منهما - في الأصل - على إثبات الواقعة الإجرامية إثباتاً مباشراً، وإنما يقومان على استخلاص النتيجة من مقدمات ثابتة. فالقرينة القضائية تُستخلص

124 Malone v. the United Kingdom, Application no. 8691/79, Judgment of
2 August 1984, Series A no. 82 (European Court of Human Rights). [https://
hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-57533%22%5D%7D](https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-57533%22%5D%7D)

125 Roman Zakharov v. Russia, Application no. 47143/06, Judgment of 4 December 2015 (Grand Chamber), European Court of Human Rights. <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-159324%22%5D%7D>

١٢٦ د.محمود أحمد طه: الموسوعة الفقهية والقضائية شرح قانون الإجراءات الجنائية، ج٣، دار الكتب القانونية، ٢٠١٣، ص٣١٠

من وقائع مادية أو ظروف محيطية تثبت أمام المحكمة،^{١٢٧} بينما تُستخلص الميتادات من معطيات تقنية موضوعية تُنتجها الأنظمة الرقمية تلقائياً أو شبه تلقائياً، ويُعاد تحليلها لاستخلاص الدلالة الجنائية.

غير أن مصدر الدلالة يختلف بينهما اختلافاً جوهرياً؛ فالقرينة القضائية تقوم أساساً على الاستنباط الذهني للقاضي، الذي يربط بين وقائع الدعوى وفق المنطق والخبرة القضائية العامة، دون حاجة إلى معرفة فنية متخصصة. أما الميتادات، فتعتمد على التحليل الفني والتقني بوصفه شرطاً لازماً لاستخراج معناها، إذ لا تُفهم دلالتها إلا من خلال خبرة تقنية تُفسّر الطوابع الزمنية، وسجلات النظام، وبيانات الموقع، وهو ما يجعلها قرينة فنية قبل أن تكون قانونية.^{١٢٨} كما تختلف درجة اليقين بين الوسيلتين؛ فالقرينة القضائية بطبيعتها تقديرية، قد تتعدد دلالاتها وتحتل أكثر من تفسير، وتظل خاضعة لتقدير القاضي وحده في ضوء مجموع الأدلة.^{٢٩} أما الميتادات، فتميل - متى ثبتت أصالتها وسلامة سلسلة حيازتها - إلى درجة أعلى من الموضوعية التقنية، إذ تُنشأ غالباً بمعزل عن إرادة الشخص، وتُدوّن آلياً في النظام، بما يقلل من تدخل العنصر البشري في إنتاجها، ويمنحها قوة استدلالية أكثر صلابة. ترقى الي درجة الدليل.

بيد أن هذه التقنية لا تجعل الميتادات بمنأى عن الطعن؛ إذ إن قابليتها للتعديل أو التلاعب الفني تفرض إخضاعها لفحص دقيق، شأنها شأن القرينة القضائية التي قد تنهار إذا تعارضت مع وقائع ثابتة أو أدلة أقوى. لذا فإن كليهما يظل دليلاً غير قطعي في الأصل، لا يُبنى عليه الحكم بالإدانة إلا إذا تعزز بسائر عناصر الإثبات.^{١٣٠} ويظهر الاختلاف أيضاً في الإطار القانوني المنظم؛ فالقرينة القضائية تخضع للقواعد العامة في قانون الإثبات، وتُستمد مشروعيتها من مبدأ الاقتناع القضائي الحر. أما الميتادات، فتخضع - فضلاً عن قواعد الإثبات - لضوابط إضافية تتعلق بمشروعية الجمع، وسرية الاتصالات، وحماية البيانات الشخصية، وهي اعتبارات لا تنثور عادةً عند التعامل مع القرائن التقليدية.^{١٣١}

١٢٧ د.محمود نقيب حسني: شرح قانون الإجراءات الجنائية، دار النهضة العربية، المجلد الثاني، الطبعة الخامسة، ٢٠١٦، ص ٩٤٢.

١٢٨ د.حسام توكيل موسي: حجية الأدلة في الإثبات الجنائي دراسة في ضوء القانون ١٥٧ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، دار البحوث والدراسات القانونية، ٢٠٢٤، ص ٦١٨.

١٢٩ د.جلال ثروت: الإجراءات الجنائية (الخصومة الجنائية)، بدون دار نشر، ٢٠٠٢، ص ١٧٨.

١٣٠ د. أشرف توفيق شمس الدين: شرح قانون الإجراءات الجنائية، طبعه مزيده ومنقحة لأحدث التعديلات التشريعية ونصوص دستور ٢٠١٤، بدون دار نشر، بدون سنة نشر، ص ٦٦٨.

١٣١ د.محمد عبد الحميد عرفه: مدي حجية الأدلة الالكترونية الرقمية في الإثبات في المواد الجنائية، دراسة تحليلية تطبيقية مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الإسكندرية، ع ٢٠١٨، ص ٤٨١.

وخلاصة القول يمكن القول إن الميادانات تمثل في المجال الرقمي امتداداً تقنياً معاصراً لفكرة القرينة القضائية، إذ تشترك معها في الطبيعة الاستنتاجية القائمة على استخلاص الدلالة من معطيات ثابتة، غير أنها تتميز عنها بكونها نتاجاً فنياً آلياً يصدر عن النظام الرقمي ذاته، لا عن الذهن البشري. فإذا كانت القرينة القضائية ثمرة للاستنباط العقلي للقاضي عند تفسير الوقائع وربطها وفق منطق الخبرة القضائية، فإن الميادانات هي نتاج موضوعي للنظام التقني يُعاد تفسيره وتكييفه قانونياً من قبل القاضي.

وتجدر الإشارة إلى أن هذا التشابه لا يبرر إسناد الميادانات كلياً إلى مفهوم القرينة القضائية، ذلك أن الميادانات قد تتجاوز، في بعض الأحوال، مجرد الدور الاستنتاجي لتشكل دليلاً مباشراً على الواقعة الإجرامية، متى ثبتت أصالتها الفنية، وسلامة سلسلة حيازتها، وانتفى عنها احتمال التلاعب أو الخطأ التقني. وهو ما يميزها جوهرياً عن القرينة القضائية التي تظل - بطبيعتها - دليلاً غير مباشر لا يرقى بذاته إلى إثبات الركن المادي للجريمة. لذا يمكننا القول أن الميادانات لا يمكن إدراجها على نحو قطعي ضمن طائفة القرائن، ولا اعتبارها دائماً دليلاً مباشراً، بل يتعين تكييفها تكييفاً مرئياً متدرجاً بحسب قوتها الفنية وحجيتها الإجرائية في كل حالة على حدة. فهي قد تؤدي وظيفة القرينة التقنية في بعض الوقائع، وقد تنهض إلى الدليل الرقمي المباشر في وقائع أخرى، وهو ما يجعل قيمتها الإثباتية نسبية ومتغيرة، وليست ثابتة أو جامدة.

المبحث الثالث

الإشكالات القانونية والفنية المتعلقة بالميتادات

لا تقف الإشكالات المتعلقة بالميتادات عند حدود الجوانب الفنية، بل تمتد لتشمل قيودًا تشريعية وقضائية تفرضها اعتبارات مشروعية الدليل وحماية الحقوق والحريات الأساسية. فجمع الميتادات وتحليلها قد يتقاطع مع مبادئ دستورية راسخة، مثل الحق في الخصوصية، وسرية الاتصالات، وحماية البيانات الشخصية، وهو ما يستوجب إخضاعها لضوابط قانونية دقيقة تختلف من نظام قانوني إلى آخر. كما يضطلع القضاء بدور محوري في رسم حدود هذه القيود من خلال رقابته على مشروعية إجراءات الضبط والتحليل، وتقديره لمدى التناسب بين المصلحة الجنائية المرجوة والقيود المفروضة على حقوق الأفراد. ويهدف هذا المطلب إلى بيان هذه القيود، وتحليل أثرها في تحديد مدى حجية الميتادات وقبولها كدليل أمام القضاء الجنائي.

المطلب الأول

مشكلات الأصالة وسلسلة الحيازة الرقمية

أولاً: ضعف الثقة في أصالة الميتادات:

تُعَدُّ أصالة الميتادات من أكثر المسائل إثارة للإشكال في مجال الإثبات الجنائي الرقمي، ذلك أن الطبيعة التقنية لهذه البيانات، وما توفره الأدوات البرمجية الحديثة من إمكانيات واسعة للتعديل، تجعلها عرضة للتلاعب دون أن يخلف ذلك، في كثير من الأحيان، آثاراً ظاهرة يمكن اكتشافها بالمعاينة السطحية. فباستخدام أدوات مجانية أو متاحة على نطاق واسع، يمكن تعديل تاريخ الإنشاء، أو التعديل، أو بيانات الموقع الجغرافي، أو هوية المستخدم، بما يهدد الثقة في القيمة الإثباتية للميتادات إذا لم تخضع لفحص فني دقيق.¹³² وبناءً على ما تقدّم نجد أن الوجود المادي للميتادات، في حد ذاته، لا يُنشئ قرينة على أصالتها أو سلامتها، ولا يُسوّغ التسليم بحجيتها تلقائياً لمجرد كونها مرافقة لملف رقمي محل الضبط.¹³³ ذلك أن الطبيعة التقنية للميتادات، وما

١٣٢ د. أيمن عبد الله فكري: الشاهد الإلكتروني في الإثبات الجنائي، مجلة الشريعة والقانون، كليه الشريعة والقانون بالجامعة، القاهرة، ٤٤٤، نوفمبر ٢٠٢٤، ص ٣٥٦٦

Jan-Niclas Hilgert, Axel Mahr, and Martin Lambertz, "Forensic Implications of Stacked File Systems," in DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, Forensic Science International: Digital Investigation 48, Supplement (2024): Article 301678, <https://doi.org/10.1016/j.fsidi.2023.301678>

133 Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007)553ح

يعتريها من قابلية للتعديل أو المحو دون آثار ظاهرة، تفرض إخضاعها لإجراءات تحقق فنية صارمة، تضمن عدم العبث بها منذ لحظة جمعها وحتى عرضها على جهة التحقيق أو القضاء^{١٣٤}. مما يبرز استخدام قيم الهاش (Hash Values) بوصفه أداة فنية محورية للتحقق من سلامة الأدلة الرقمية، بما في ذلك الميتاداتا. فقيمة الهاش تمثل بصمة رقمية فريدة للملف،^{١٣٥} وأي تغيير - ولو طفيفاً - يطرأ على محتواه أو على بياناته الوصفية يفضي حتماً إلى تغيير هذه القيمة. ومن ثم، فإن المقارنة بين قيمة الهاش المُستخرجة عند الضبط وقيمتها عند الفحص أو التحليل اللاحق تُعد وسيلة قاطعة للتحقق من عدم حدوث تعديل أو تحريف أو تحديث في الملف أو في ميتاداتاه خلال مراحل الحياة والفحص^{١٣٦}.

ولقد كرّس المشرّع المصري هذا المبدأ صراحةً في المادة (٩) من اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، إذ نصّ على أن الأدلة الرقمية تكون لها ذات القيمة والحجية المقررة للأدلة الجنائية المادية في الإثبات الجنائي، شريطة توافر ضوابط فنية محددة، من أبرزها: 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 للبيانات أو المعلومات، أو إتلاف الأجهزة أو المعدات أو أنظمة المعلومات أو البرامج أو الدعامات الإلكترونية، وغيرها ومنها على الأخص تقنيات Digital Images Hash و Write Blocker، وغيرها من التقنيات المماثلة^{١٣٧}.

وبالإمعان في هذا النص نجد أن المشرّع لم يكتفِ بالإقرار المبدئي بحجية الدليل الرقمي، بل قيّد هذه الحجية بشرط جوهري يتمثل في الالتزام الصارم بالمعايير الفنية التي تحافظ على سلامة البيانات والميتاداتا، وتمنع أي تدخل بشري أو تقني من شأنه المساس بأصالتها. كما يفهم منه أن الإخلال بهذه الضوابط لا يُعد مجرد مخالفة فنية، بل ينعكس مباشرةً على مشروعية الدليل وحجيته، وقد يفضي إلى استبعاده كلياً من دائرة الإثبات.

134 State v. Eichstedt, 2009 WI App 91 (Wis. Ct. App. 2009)

135 NIST SP 800-86: Guide to Integrating Forensic Techniques (2006)

136 Simson Garfinkel & Alex Schatz, "Quantifying Forensicability," Journal of Digital Investigation 8 (2011): S46; & Eoghan Casey, Digital Evidence and Computer Crime, 4th ed. (2020), 315.

١٣٧ اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ - بشأن مكافحة جرائم تقنية المعلومات الصادرة بقرار رئيس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠

لذا فإن الاعتماد القضائي على الميتاداتا يظل مرهوناً، ليس فقط بقيمتها الدلالية، وإنما - على نحو أولي - بسلامة إجراءات جمعها وفحصها وتوثيقها،^{١٣٨} وعلى رأسها توثيق قيم الهاش وسلسلة الحيازة الرقمية. وبغير ذلك، تتحول الميتاداتا من أداة لكشف الحقيقة الرقمية إلى عنصر مثير للشك، يُقوّض الثقة في الدليل، ويُضعف الأساس الذي تُبنى عليه القناعة القضائية.^{١٣٩} وبناءً عليه فإن ضعف الثقة في أصالة الميتاداتا لا يُفضي إلى إهدارها كوسيلة إثبات، بقدر ما يفرض تعزيز الضمانات الفنية والإجرائية المحيطة بها. فالميتاداتا لا تُستبعد لذاتها، وإنما تُقبل أو تُرفض بحسب مدى الالتزام بقواعد التحقق الفني والتوثيق الإجرائي، وهو ما يعكس التحول الحديث في الإثبات الجنائي من التركيز على الدليل في ذاته إلى التركيز على سلامة منهج الحصول عليه.^{١٤٠}

ثانياً: سلسلة الحيازة : (Chain of Custody)

تُعَدّ سلسلة الحيازة من الركائز الجوهرية في قبول الأدلة الرقمية بوجه عام، والميتاداتا بوجه خاص، إذ تمثل الإطار الإجرائي الذي يضمن سلامة الدليل منذ لحظة ضبطه وحتى عرضه أمام المحكمة.^{١٤١} ويترتب على أي خلل أو انقطاع في هذه السلسلة سقوط الثقة في الدليل، ومن ثمّ إهدار حجيتها القانونية، حتى ولو بدا في ظاهره سليماً من الناحية الفنية. حيث إن العبرة في الدليل الرقمي لا تقف عند مضمونه أو الميتاداتا المرافقة له فحسب^{١٤٢}، وإنما تمتد - على نحو حاسم - إلى كيفية انتقاله وتداوله بين جهات الضبط والتحقيق والفحص الفني. فالدليل الرقمي، بطبيعته غير المادية وقابليته العالية للتعديل، يظل عرضة للتشكيك متى شاب مسار حيازته أدنى خلل إجرائي أو فني.^{١٤٣}

138 United States v. Vaghari, 335 F. Supp. 3d 19 (D.D.C. 2018)p27

139 State v. Collins, 2017 Tenn. Crim. App. LEXIS 456 (Tenn. Crim. App. 2017)

140 Stephen Mason & Daniel Seng, *Electronic Evidence* (5th ed., 2021)p 456 & George L. Paul, *Foundations of Digital Evidence* (ABA Book Publishing, 2019)p289

United States v. Brewer, 1 F. Supp. 2d 334 (S.D.N.Y. 1998)p231

١٤١

142 INTERPOL Digital Evidence Guidelines (2020) (Section 7.3) (“Chain of custody logs must identify every custodian, timestamp access, record tools used; gaps justify evidence exclusion regardless of hash integrity.”)

143 Souradip Nath et al., “Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics,” in Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (Washington, DC, USA, 28–31 October 2024): 11–20,

وعلى هذا الأساس، إذا ثبت أن الملف الرقمي قد انتقل بين الجهات المختصة دون توثيق دقيق، أو خضع لتداول من قبل أشخاص غير مختصين، أو عولج باستخدام أدوات أو برامج غير معتمدة فنيًا، فإن ذلك يُنشئ احتمالاً جدياً للعبث أو التعديل. وهذا الاحتمال، في ذاته، يكفي لزعزعة القناعة القضائية وإهدار الثقة في سلامة الدليل،^{١٤٤} دون حاجة لإثبات وقوع العبث فعلياً، إذ إن العدالة الجنائية لا تتطلب اليقين التقني المطلق بقدر ما تتطلب انتفاء الشك المعقول حول سلامة الدليل^{١٤٥}.

وهو ما أكدّه المشرّع المصري في الفقرة الثالثة من المادة (٩) من اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، إذ نصّت على: «أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخوّل لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتمين من جهات التحقيق أو المحاكمة، على أن يُبيّن في محاضر الضبط أو التقارير الفنية نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزم 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»^{١٤٦}.

ويُستفاد من هذا النص أن المشرّع قد ربط حجية الدليل الرقمي – بما في ذلك الميئادات – بسلامة سلسلة حيازته (Chain of Custody)، من حيث الأشخاص القائمين على التعامل معه، والأدوات المستخدمة، والتوثيق الدقيق لكل مرحلة من مراحل الضبط والفحص. كما يظهر بجلاء أن توثيق قيمة الهاش ليس إجراءً شكلياً، وإنما ضمانة جوهرية تهدف إلى الحفاظ على أصالة الدليل ومنع أي تشكيك في سلامته ولذلك تشترط القواعد المستقرة في التحقيق الجنائي الرقمي توثيق عناصر محددة على

<https://doi.org/10.1109/TPS-ISA62245.2024.00012>.

١٤٤ د. شيماء سيد عبد الرحمن الشقيري، «مدى حجية الأدلة الرقمية في إثبات الجرائم التقليدية: دراسة فقهية»، مجلة الشريعة والقانون بالقاهرة ٤١، عدد ٤١ (أبريل ٢٠٢٣): ص ٨٩٨

Stephen Mason, *Electronic Evidence* (5th ed., ٢٠٢١) p462

145 Christopher Hargreaves, Alex Nelson, and Eoghan Casey, “An Abstract Model for Digital Forensic Analysis Tools – A Foundation for Systematic Error Mitigation Analysis,” *Forensic Science International: Digital Investigation* 48, Supplement (2024): Article 301679, <https://doi.org/10.1016/j.fsi-di.2023.301679>.

د. محمود عبد الحكيم: الشك في مجال الإجراءات الجنائية، دراسة مقارنة، كلية الحقوق جامعة حلوان، رسالة دكتوراه، 2023، ص 260

١٤٦ المادة ٩ من اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الصادرة بقرار رئيس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠

نحو دقيق، من أبرزها:

١- تاريخ ووقت الضبط: بما يحدد اللحظة الزمنية التي خرج فيها الدليل من حيازة صاحبه إلى حيازة السلطة المختصة، ويستخدم هذا التوقيت لاحقًا لمقارنة الطابع الزمنية والتحقق من عدم حدوث تعديل لاحق.

٢- اسم وصفة القائم بالفحص أو التداول: مع بيان الجهة التي ينتمي إليها، ضمانًا للمساءلة، ولمنع تداول الدليل بين أشخاص غير مخولين قانونًا أو فنيًا.

٣- الأدوات والبرمجيات المستخدمة في الفحص: مع توثيق نسخها وإصداراتها، نظرًا لأن اختلاف الأدوات قد يؤدي إلى نتائج فنية متباينة، أو إلى تغيير غير مقصود في الميتادات.

٤- النسخ الاحتياطية (Forensic Copies) وذلك من خلال إنشاء نسخة طبق الأصل (Image) من الدليل الرقمي، والعمل عليها دون المساس بالأصل، مع توثيق قيمة الهاش لكل من الأصل والنسخة، بم

يضمن التطابق الكامل بينهما.¹⁴⁷

وبهذا المعنى، لا تُعدّ سلسلة الحيازة إجراءً شكليًا أو تنظيميًا، بل تمثل ضمانة جوهرية لحماية الدليل الرقمي من العبث، ولصون حقوق الدفاع، ولتمكين المحكمة من الاطمئنان إلى أن ما عُرض عليها هو ذات الدليل الذي تم ضبطه، دون زيادة أو نقصان.

١٤٧ المادة ٩ من اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات الصادرة بقرار رئيس الوزراء رقم ١٦٩٩ لسنة ٢٠٢٠: «يتم توصيف وتوثيق الدليل الرقمي من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأي وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات التالية على كل منها:

- ١- تاريخ ووقت الطباعة والتصوير.
- ٢- اسم وتوقيع الشخص الذي قام بالطباعة والتصوير.
- ٣- اسم أو نوع نظام التشغيل ورقم الإصدار الخاص به.
- ٤- اسم البرنامج ونوع الإصدار أو الأوامر المستعملة لإعداد النسخ.
- ٥- البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.
- ٦- بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة».

المطلب الثاني

القيود التشريعية والقضائية على استخدام الميادات

أولاً: مشروعية جمع الميادات:

تُعدّ مشروعية جمع الميادات من أكثر المسائل إشكالاً في مجال الإثبات الجنائي الرقمي، نظراً لاختلاف التكييف القانوني لهذه البيانات بين الأنظمة التشريعية، وتباين النظرة إليها ما بين كونها بيانات شخصية تمس الخصوصية، أو مجرد بيانات تقنية مساعدة لا تستوجب ذات الضمانات المقررة لمحتوى الاتصال.¹⁴⁸ فمما لا شك فيه أن مبدأ الشرعية الإجرائية يقوم على قاعدة جوهرية مؤداها أن الدليل الجنائي لا يكتسب قيمته القانونية من قوته الدلالية أو من قدرته على كشف الحقيقة فحسب، وإنما - في المقام الأول - من مشروعية الإجراء الذي تم الحصول به، ومن مدى التزام هذا الإجراء بالضمانات التي قررها القانون. وبمقتضى هذا المبدأ، لا يجوز للقضاء أن يأخذ أو يُقيم دليلاً لم يتم الحصول عليه وفق الطرق التي رسمها القانون، تحقيقاً للتوازن العادل بين حق الدولة في العقاب وحق الفرد في الحرية وصون كرامته الإنسانية.¹⁴⁹

ويكتسب هذا المبدأ أهمية خاصة عند تطبيقه على الميادات، بالنظر إلى طبيعتها الكاشفة وقدرتها على النفاذ إلى عمق الحياة الخاصة دون الاطلاع المباشر على محتوى البيانات. فالواقع العملي يُثبت أن الميادات - من خلال الطوابع الزمنية، وبيانات الموقع، وسجلات النشاط - قادرة على تتبع سلوك الشخص وتحركاته وبناء صورة دقيقة عن حياته الرقمية، وهو ما يجعلها تمسّ الحق في الخصوصية أساساً مباشراً أو غير مباشر. ومن ثمّ، فإن مشروعية جمع الميادات تُعدّ شرطاً لازماً للاعتداد بها دليلاً جنائياً. فلا يجوز ضبطها أو استخراجها أو تحليلها إلا في إطار إجراء قانوني صحيح، وبالالتزام بالضمانات المقررة، وعلى رأسها صدور إذن قضائي مسبق متى كان جمعها من شأنه المساس بالحياة الخاصة، أو تجاوز نطاق البيانات العامة أو المتاحة للجمهور. وأي تجاوز لهذه الضوابط يُفضي إلى وصف الميادات بأنها دليل غير مشروع، يتعيّن استبعاده من عداد الأدلة.¹⁵⁰

ولا يقف أثر عدم مشروعية الميادات عند حد استبعادها بذاتها من دائرة الإثبات، بل يمتد - متى ثبت أن إجراءات لاحقة قد تأسست عليها - إلى بطلان ما

١٤٨ د. محمد صالح جاد: مرجع سابق، ص ٩٤

١٤٩ د. أحمد ضياء الدين خليل: مشروعية الدليل الجنائي في المواد الجنائية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ١٩٨٣، ص ٥٨٥

١٥٠ د. أحمد عوض بلال: قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، ٢٠١٣، ص ٢١

ترتب عليها من أدلة رقمية أخرى، وذلك تطبيقاً لقاعدة إجرائية مستقرة مفادها أن «ما بُني على باطل فهو باطل».^{١٥١} فالمشروعية الإجرائية لا تتجزأ، ولا يجوز تصحيح مسار إثباتي فاسد في أساسه بالاستناد إلى نتائجه اللاحقة. وقد كرّس المشرع المصري هذا المبدأ صراحةً في المادة (٣٣٦) من قانون الإجراءات الجنائية، إذ نصّت على أنه: «إذا تقرر بطلان أي إجراء فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ولزوم إعادته متى أمكن ذلك».

ومؤدى هذا النص أن البطلان لا يقتصر على الإجراء المعيب في ذاته، وإنما ينسحب حكمه على كل ما كان وليدًا له أو مترتبًا عليه مباشرة، طالما قامت بينهما علاقة سببية قانونية. وبذلك، فإن البطلان يمتد إلى الأدلة اللاحقة التي استُمدت من إجراء غير مشروع، ولو كانت هذه الأدلة في ظاهرها صحيحة أو مستقلة^{١٥٢}. وتطبيقاً لذلك في مجال الأدلة الرقمية والميتادات، فإنه إذا استندت جهات التحقيق إلى ميتاداتا جُمعت أو استُخرجت بغير سند قانوني، أو بالمخالفة للضمانات الإجرائية المقررة، ثم بُني على هذه الميتادات إجراء لاحق - كتعبّ متهم، أو تفتيش جهاز إلكتروني، أو ربط شخص بواقعة إجرامية - فإن جميع النتائج المتحصلة من هذا المسار الإثباتي تكون عرضة للإبطال، باعتبارها ثمرة مباشرة لإجراء باطل في أصله، غير أن امتداد البطلان يظل مقيداً بحدود العلاقة السببية المباشرة بين الإجراء الباطل والآثار المترتبة عليه، وهو ما استقر عليه قضاء محكمة النقض المصرية، إذ قررت في هذا الشأن أن: «البطلان - طبقاً للمادة ٣٣٦ من قانون الإجراءات الجنائية - لا يلحق إلا بالإجراء المحكوم ببطلانه والآثار المترتبة عليه مباشرة، وهو لا يعلق بما سبقه من إجراءات، كما أنه لا يؤثر في قرار النيابة بإحالة الواقعة إلى غرفة الاتهام أو قرار غرفة الاتهام بإحالة الدعوى إلى محكمة الجنايات، ولا يمكن أن يترتب على مثل هذا البطلان - إن صح - إعادة القضية إلى النيابة، بل يكون للمحكمة أن تُصحّح الإجراء الباطل طبقاً للمادة ٣٣٥ إجراءات».^{١٥٣}

ومؤدى هذا القضاء أن بطلان إجراء جمع أو استخراج الميتادات لا يمتد إلى الإجراءات السابقة عليه متى كانت قد اتُخذت صحيحة ومستقلة، كما لا ينسحب - بذاته - على قرارات الإحالة أو السير في الدعوى الجنائية. غير أن هذا لا ينال من القاعدة الجوهرية القائلة بأن كل دليل رقمي أو إجراء لاحق تأسس مباشرة على ميتاداتا غير مشروعة يظل باطلاً بطلاناً تبعياً، ولا يجوز التعويل عليه في تكوين القناعة

١٥١ الطعن رقم ١٧٤ لسنة ٤٣ - جلسة ١٩٧٣/٠٤/٠٩ - س ٢٤ ع ٢ ص ٥٠٦ ق ١٠٥

١٥٢ د.محمود أحمد طه: التعدي علي حق الانسان في سرية اتصالاته الشخصية بين التجريم والمشروعية، دار الكتب القانونية، ٢٠١٢، ص ١٢٨

١٥٣ الطعن رقم ٣٦ لسنة ٢٦ - جلسة ١٩٥٦/٠٣/١٥ - س ٧ ع ١ ص ٣٦١ ق ١٠٧

القضائية¹⁰⁴. ولا يُشترط في هذا الصدد إثبات وقوع ضرر فعلي أو التحقق يقيناً من العبث بالبيانات، إذ يكفي أن يكون الإجراء المؤسس قد شابه عيب عدم المشروعية، بما يُنشئ شكاً جدياً في سلامة الدليل. فالعدالة الجنائية لا تسمح بأن تُبنى القناعة القضائية على أدلة مشتقة من مصدر غير مشروع، حتى ولو بدت هذه الأدلة من الناحية الفنية مقنعة أو قوية الدلالة.¹⁵⁵

كما أن القاضي الجنائي، في إطار سلطته التقديرية، لا يجوز له أن يُكوّن عقيدته أو يصدر حكمه بالإدانة أو البراءة اعتماداً على الميئادات، إلا بعد التحقق من سلامتها الفنية ومشروعية مصدرها معاً. فالميئادات، شأنها شأن سائر الأدلة الرقمية، تخضع لمبدأ الشرعية، ولا تُعفى من رقابة المشروعية بحجة أنها بيانات ذات طبيعة تقنية محايدة. وبذلك، يتضح أن إخضاع الميئادات لمبدأ الشرعية الإجرائية يُعد ضماناً أساسية لحماية الخصوصية ومنع التعسف في استعمال الوسائل التقنية، ويُشكل في الوقت ذاته شرطاً جوهرياً لاكتسابها الحجية القانونية في الإثبات الجنائي. فالحقيقة الجنائية، وإن كانت غاية مشروعة، لا يجوز بلوغها عبر ميئادات جُمعت أو استُخدمت على نحو يُخالف القانون، إذ إن العدالة الجنائية لا تقوم على صحة النتيجة فحسب، بل على مشروعية الطريق المؤدي إليها.¹⁵⁶

ثانياً: حماية الخصوصية:

تُثير الميئادات مخاطر جسيمة على الحق في الخصوصية، قد تفوق - في كثير من الأحيان - المخاطر المرتبطة بمحتوى البيانات ذاته. فهذه البيانات، وإن كانت لا تكشف ظاهرياً عن مضمون الاتصال أو المحتوى الرقمي، فإنها تتيح، من خلال التحليل التجميعي والترابطي، تتبّع الحركة اليومية للمستخدم، وتحديد أماكن تواجده، وتوقيت حضوره، ومسارات تنقله، على نحو يُفضي إلى رسم خريطة دقيقة ومتكاملة لحياته الخاصة.¹⁵⁷ ولا يقتصر الأثر الكاشف للميئادات على البعد المكاني والزمني، بل يمتد ليشمل أنماط السلوك والعادات الرقمية، سواء من حيث أوقات النشاط، أو طبيعة

١٥٤ د.رحاب عمر سالم: محاولات التخفيف من نطاق البطلان، في ضوء الغرضين النفعي والمعنوي للإجراء الجنائي، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ٩٤٤، يوليو ٢٠٢١، ص ٥٠.

١٥٥ د.ميروك محمد علام مهران: الحد من أثار البطلان في قانون الإجراءات الجنائية والفقہ الإسلامي، دراسه مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٢٥، ص ٣٧٣.

١٥٦ د. محمد سيد الجمال: الدليل العلمي وحجيته الجنائية، دراسة مقارنة بين القانونين المصري والأمريكي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠١٢، ص ١٤٤.

157 Sandra Wachter et al.: "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *SSRN Working Paper* (2018p15

التفاعل مع المنصات المختلفة، أو أنماط الاتصال بالأشخاص والجهات. ويسمح هذا النمط من التحليل باستخلاص مؤشرات دقيقة تتعلق بأسلوب الحياة، وشبكة العلاقات الاجتماعية، والاهتمامات، بل وقد يصل - في بعض الحالات - إلى استنتاج ميول شخصية أو تفضيلات حساسة. ويتضاعف هذا الخطر كلما جرى الربط بين أنواع متعددة من الميتادات، كبيانات الموقع والطوبع الزمنية وسجلات الدخول وسجلات الاتصالات¹⁵⁸.

والأخطر من ذلك أن الميتادات تمكّن من تكوين ملف شخصي (Profiling) شبه متكامل عن الفرد، يتم إنشاؤه دون علمه أو رضاه، ودون الحاجة إلى الاطلاع على محتوى بياناته أو مراسلاته. وهو ما يجعلها أداة ذات طبيعة مزدوجة: فهي من جهة وسيلة فعّالة لدعم التحقيق الجنائي وتحليل الأنماط الإجرامية،¹⁵⁹ ومن جهة أخرى تشكل خطراً بنيوياً على الخصوصية الفردية إذا جرى استخدامها أو جمعها خارج إطار قانوني صارم. ومن ثمّ، فإن إخضاع الميتادات لنظام حماية أخفّ بدعوى كونها «بيانات غير محتوائية» يُعدّ تصوراً قاصراً، لا ينسجم مع واقع التحليل الرقمي المعاصر، ولا مع المفهوم الموضوعي والوظيفي للخصوصية.

وبناءً عليه، يقتضي التوازن السليم بين متطلبات الأمن الجنائي وصون الحقوق والحريات الأساسية إخضاع جمع الميتادات واستخدامها لمبادئ الضرورة والتناسب والتحديد الدقيق للغرض¹⁶⁰، مع اشتراط رقابة قضائية فعّالة كلما كان من شأن هذه البيانات - منفردة أو مجتمعة - المساس بالحياة الخاصة أو تمكين السلطات من إعادة بناء السلوك الشخصي للفرد. ويُعدّ هذا الإطار الوظيفي هو الكفيل بضمان عدم تحوّل

الميتادات من أداة مشروعة للتحقيق إلى وسيلة شاملة للمراقبة غير المنضبطة.¹⁶¹

158 Malone v. United Kingdom, Application no. 8691/79, para. 64 (ECtHR, 1984); Digital Rights Ireland Ltd (C-293/12), para. 27 (CJEU, 2014).

& Paul M. Schwartz & Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law," Georgetown Law Journal 106 (2017): p142.

159 Recognizing Information Inferred about Individuals as Personal Data", SSRN Working Paper (2023)p8

160 Roman Zakharov v. Russia [GC] (47143/06), ECtHR, 4 December 2015 (Any interference with Article 8 must be 'in accordance with the law,' prescribed by clear, foreseeable rules, pursue a legitimate aim, and be necessary in a democratic society)

Christopher T. Timko, "Metadata and the Fourth Amendment," Boston University Law Review 97 (2017)p412

161 Daniel J. Solove, "Digital Metadata and Privacy: The Privacy Interest in

ثالثاً: سلطة القاضي في تقدير حجية الميتادات:

في ظل غياب تنظيم تشريعي صريح ومحدد يُبين الطبيعة القانونية للميتادات ويضع ضوابط دقيقة لحجيتها في الإثبات الجنائي، تبرز سلطة القاضي الجنائي بوصفها العنصر الحاسم في تقدير قيمتها الإقناعية ومدى التعويل عليها في تكوين القناعة القضائية. فالقاضي، في هذه الحالة، لا يجد أمامه نصاً خاصاً تحكم الميتادات بذاتها، وإنما يلجأ إلى القواعد العامة في الإثبات، وإلى سلطته التقديرية في وزن الأدلة، مسترشداً بما يطرحه النزاع من معطيات فنية وقانونية. وتعتمد المحاكم في هذا الإطار على مجموعة من العناصر المتداخلة، في مقدمتها الخبرة الفنية، التي تُعد الأداة الرئيسية لفهم الطبيعة التقنية للميتادات. فالخبير الفني يُبين مدى أصالة الميتادات، وسلامة إجراءات استخراجها وحفظها، وإمكانية التلاعب بها أو تعديلها من عدمه، فضلاً عن مدى اتساقها مع باقي الأدلة الرقمية المعروضة في الدعوى. ويُعد هذا التقرير الفني - متى استوفى مقوماته العلمية - عنصراً جوهرياً في بناء القناعة القضائية، دون أن يُقيّد القاضي على نحو آلي، إذ يظل له سلطة تقدير مدى الاطمئنان إليه.

وفي هذا السياق، تستند المحاكم كذلك إلى القرائن القضائية المستخلصة من ظروف الدعوى وملابساتها، وإلى مدى ترابط الميتادات مع وقائع ثابتة بأدلة أخرى، بما يسمح باستنتاج الواقعة الإجرامية على نحو منطقي ومتماسك. فالميزان في النهاية هو سلامة الاستدلال لا مجرد الطابع التقني للدليل. وقد أكدت محكمة النقض المصرية هذا الأصل العام في الإثبات بقولها: «الأصل أن الجريمة - على اختلاف أنواعها - إلا ما استثنى منها بنص خاص، يجوز إثباتها بكافة الطرق القانونية، ومنها البينة وقرائن الأحوال»^{١٦٢}.

وإلى جانب الخبرة الفنية، يستند القاضي إلى سلطته التقديرية في الاقتناع، فيوازن بين الميتادات وسائر أدلة الدعوى، ويتحقق من مدى اتساقها مع الوقائع الثابتة في الأوراق، وعدم تعارضها مع منطق الأحداث أو مع أدلة أقوى منها دلالة أو أثراً.^{١٦٣} فلا تُعامل الميتادات - في هذا الإطار - بوصفها دليلاً قاطعاً بذاته، وإنما تُدرج ضمن منظومة أدلة متكاملة، يُقدّر وزنها في ضوء مجمل الملف الجنائي. وقد رسّخت محكمة النقض المصرية هذا المفهوم في قضائها المستقر، إذ قضت بأن: «مؤدى ذلك أن الأدلة في المواد الجنائية متساندة يكمل بعضها بعضاً، ومنها مجتمعة تتكون عقيدة القاضي، فلا يُنظر إلى دليل معين لمناقشته على حدة دون باقي الأدلة، بل يكفي أن

Metadata,” *Minnesota Law Review* 102 (2017): p 1445

١٦٢ الطعن رقم ٨٩٣ لسنة ٣٥ ق جلسة ١٩٦٥/١٠/١٨ س ١٦ ص ٧٠٢.

١٦٣ د. محمد عبد الحميد مكي: شرح قانون الإجراءات الجنائية، بدون نشر، ٢٠٢٤، ص ٦٩٠.

تكون الأدلة في مجموعها كوحدة مؤدية إلى ما قصده الحكم منها، ومنتجة لاكتمال اقتناع المحكمة واطمئنانها إلى ما انتهت إليه»^{١٦٤}

وبناء على هذا فإن الميتاداتا لا تُقَيِّم بمعزل عن غيرها من عناصر الإثبات، بل تُستَخدم بوصفها عنصراً استدلالياً قد يُعَزِّز أدلة أخرى أو يُسَانِدُها، وقد يضعف إذا انفرد أو تعارض مع باقي الوقائع الثابتة. فحجية الميتاداتا ليست ذاتية أو مفترضة، وإنما حجية تقديرية تتوقف على سلامتها الفنية، ومشروعيتها الإجرائية، ومدى انسجامها مع باقي الأدلة^{١٦٥}. تتحدد القيمة القانونية للميتاداتا، بوصفها أحد الصور الرقمية المستحدثة تبعاً للنظام الإثباتي الذي يحكم الدعوى الجنائية. فالميتاداتا لا تُقَدَّر في فراغ، وإنما تُقَوِّم في ضوء الفلسفة العامة لنظام الإثبات المعمول به، ومدى اتساع أو ضيق سلطة القاضي في قبول الأدلة وتقدير قيمتها الإقناعية. ومن المعروف سلفاً أن نظم الإثبات في القوانين المقارنة ثلاث نظم فستستعرض مكانه الميتاداتا في هذه الأنظمة علي النحو التالي:

١ - الميتاداتا في نظام الإثبات الحر (أو المطلق):

في إطار نظام الإثبات الحر، الذي يسود غالبية التشريعات الجنائية تُعدّ الميتاداتا دليلاً مقبولاً من حيث المبدأ، طالما جرى الحصول عليها بوسيلة مشروعة ولم يشبها عيب إجرائي جوهري. فلا يفرض هذا النظام على أطراف الخصومة الجنائية تقديم نوع معين من الأدلة، ولا يستبعد مسبقاً أي وسيلة إثبات لمجرد حدوثها أو طبيعتها التقنية.^{١٦٦}

ويترك للقاضي الجنائي في هذا النظام تقدير القيمة الإقناعية للميتاداتا، سواء تعلّق الأمر ببيانات زمنية، أو سجلات نشاط، أو بيانات موقع، أو غيرها من صور الميتاداتا. ويجوز للقاضي أن يُعَوَّل عليها وحدها متى اطمأن إلى سلامتها الفنية، أو أن يكمل بها أدلة أخرى، دون أن تخضع قناعته في ذلك لرقابة محكمة النقض^{١٦٧}، ما دام الحكم قد بُني على أسباب سائغة و منطقية ومستمدة من أوراق الدعوى^{١٦٨} حيث

١٦٤ الطعن رقم ٨٣٠ لسنة ٤٧ ق جلسة ٢٦/١٢/١٩٧٧ س ٢٨ ص ١٠٨، الطعن رقم ٢٢٦٠٣ لسنة ٨٧ جلسة ٢٠٢٠/١٢/٢، الطعن رقم ١١١٧ لسنة ٩٠ جلسة ٢٠٢٢/١٢/١٣

١٦٥ د.جميل الشرفاوي: الإثبات في المواد المدنية، دار النهضة العربية، ١٩٩٠، ص ٦

١٦٦ د.محمود محمود مصطفى: الإثبات في المواد الجنائية في القانون المقارن مطبعة جامعة القاهرة، ط ١، سنة ١٩٧٧، ص ١٧

١٦٧ د. وفاء محمد أبو المعاطي صقر: دور الحشرات في الإثبات الجنائي، دار الجامعة الجديدة، ٢٠٢٤، ص ٩٠

١٦٨ د. محمود سويف: دور بصمة المخ في الإثبات الجنائي، دار الجامعة الجديدة، ٢٠٢٢، ص ٤٦

جاء حكم محكمة النقض المصرية صريحا بانه: (إن القانون قد أمد القاضي في المسائل الجنائية بسلطة واسعة وحرية كاملة في سبيل تقصي ثبوت الجرائم أو عدم ثبوتها والوقوف على حقيقة علاقة المتهمين ومقدار اتصالهم بها ففتح له باب الإثبات على مصراعيه يختار من كل طرقه ما يراه موصلاً إلى الكشف عن الحقيقة ويزن قوة الإثبات المستمدة من كل عنصر بمحض وجدانه فيأخذ بما تطمئن إليه عقيدته وي طرح ما لا ترتاح إليه غير ملزم بأن يسترشد في قضائه بقرائن معينة، بل له مطلق الحرية في تقدير ما يعرض عليه منها ووزن قوته التدليلية في كل حالة حسبما يستفاد من وقائع كل دعوى وظروفها. بغيته الحقيقة ينشدها أنى وجدها ومن أي سبيل يجده مؤدياً إليها، ولا رقيب عليه في ذلك غير ضميره وحده. هذا هو الأصل الذي أقام عليه القانون الجنائي قواعد الإثبات لتكون موائمة لما تستلزمه طبيعة الأفعال الجنائية وتقتضيه مصلحة الجماعة من وجوب معاقبة كل جان وتبرئة كل بريء. ولذلك كان القاضي غير مطالب إلا بأن يبين في حكمه العناصر التي استمد منها رأيه والأسانيد التي بنى عليها قضاءه، وذلك فقط للتحقق مما إذا كان ما اعتمد عليه من شأنه أن يؤدي عقلاً إلى النتيجة التي خلص هو إليها. على شرط أن يكون ذلك كله مما عرض على بساط البحث أمامه بالجلسة حتى لا يؤخذ به الخصوم على غرة منهم، وألا يكون مما حرم الاستشهاد به استثناء على خلاف الأصل بمقتضى نص في القانون لعله اقتضتها المصلحة العامة. وكلما كان الأمر كذلك صح الحكم وامتنعت مجادلة القاضي في تقدير قوة الدليل وكفايته في الإثبات^{١٦٩}. ويُعد نظام الإثبات الحر الأكثر مرونة في استيعاب الميئادات، غير أن هذه المرونة قد تثير مخاوف تتعلق بتفاوت الأحكام القضائية تبعاً لاختلاف درجة إلمام القضاة بالجوانب الفنية للأدلة الرقمية.^{١٧٠}

٢ - الميئادات في نظام الإثبات المقيد:

أما في نظام الإثبات المقيد، السائد في القوانين فإن قبول الميئادات يخضع لقيود أكثر صرامة. فالأصل في هذا النظام أن القانون يُحدّد الأدلة التي يجوز تقديمها، ويضع شروطاً دقيقة لقبولها^{١٧١}، وهو ما يفرض على الميئادات أن تجد لها تكييفاً قانونياً محدداً ضمن منظومة الأدلة المعترف بها. وفي هذا الإطار، لا يُعوّل على الميئادات إلا بعد استيفاء متطلبات فنية وإجرائية دقيقة، من بينها إثبات سلامة مصدر البيانات، وعدم العبث بها، وصحة سلسلة الحياة، وقابلية الدليل للفحص والمناقشة من جانب الدفاع. ويخضع تقدير المحكمة لقيمة الميئادات لرقابة مشددة، سواء من حيث مشروعية

١٦٩ (الطعن رقم ١٠٠٤ لسنة ٩ ق جلسة ١٩٣٩/٦/١٢ س ٤ ص ٥٧٥)

١٧٠ د. محمد صالح جاد المولي: الدليل الرقمي وحجيته في إثبات جرائم المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠١٨، ص ١٩٤.

١٧١ د. أسامة أحمد شوقي المليجي: القواعد الإجرائية للإثبات في المواد المدنية والتجارية، دار النهضة العربية، ١٩٩٨، ص ٨.

الحصول عليها أو من حيث سلامة الاستنتاج المستخلص منها.¹⁷² ويترتب على ذلك أن الميتاداتا، رغم أهميتها، قد تواجه صعوبات عملية في القبول أمام القضاء في ظل هذا النظام، ما لم يتدخل المشرع أو القضاء لتقنينها صراحة ضمن الأدلة الرقمية المقبولة.

٣- الميتاداتا في النظام المختلط:

يتخذ النظام المختلط موقفاً وسطاً، فيقر من حيث المبدأ بجواز الاستعانة بالميتاداتا كدليل رقمي، مع إخضاعها لضوابط تشريعية عامة، وترك تقدير قيمتها الإقناعية للقاضي الجنائي.^{١٧٣} ففي هذا النظام، قد يُحدّد المشرع إطاراً عاماً للأدلة الرقمية، دون أن يفرض قالباً جامداً على القاضي في كيفية تقييمها.¹⁷⁴ ويُتيح هذا النظام للقاضي أن يُعول على الميتاداتا بوصفها قرينة تقنية قوية، وقد ترتقي - في بعض الحالات - إلى دليل مباشر، متى ثبتت أصالتها وسلامة إجراءات ضبطها وفحصها. كما يسمح بإدماج الميتاداتا ضمن منظومة الأدلة، إلى جانب الشهادة والقرائن والخبرة الفنية، بما يحقق قدرًا معقولاً من التوازن بين الضبط التشريعي وحرية الاقتناع القضائي. وبالنظر إلى الأساسين النظريين اللذين تقوم عليهما نظم الإثبات، يتضح أن الميتاداتا تتأثر بكلا العنصرين:

- من حيث تحديد الدليل: يختلف النظم في مدى الاعتراف الصريح بالميتاداتا كدليل، فبينما يُقبل ضمناً في نظام الإثبات الحر، قد يحتاج إلى نص أو اجتهاد قضائي في النظام المقيد.

- ومن حيث تقدير القيمة الإقناعية: تتراوح الميتاداتا بين كونها مجرد قرينة تقنية تُساند غيرها من الأدلة، وبين كونها دليلاً ذا قوة مباشرة، بحسب سلامتها الفنية واتساقها مع باقي عناصر الدعوى.

١٧٢ د. رؤوف عبيد: الإجراءات الجنائية في القانون المصري، بدون دار نشر، ١٩٧٦ ص ٦٧٢

١٧٣ د. محمد الجمال: مرجع سابق، ص ١٣

١٧٤ ا. محمود صالح محمد اليسير: الأدلة العلمية الحديثة وأثرها في الأحكام الجنائية، رسالة ماجستير، كلية الحقوق، جامعة المنصورة، ٢٠١٧، ص ٢٧

الخاتمة

خلص هذا البحث إلى أن الميَّادات لم تعد مجرد معطيات تقنية محايدة تُستخدم لأغراض تشغيلية أو تنظيمية، بل أضحت - في ظل التحليل الرقمي التجميعي والتطور التكنولوجي المتسارع - أداة قادرة على الكشف العميق عن الحياة الخاصة للأفراد، من خلال إعادة بناء تحركاتهم، وأنماط تواصلهم، وشبكات علاقاتهم الاجتماعية، دون الحاجة إلى الاطلاع على محتوى الاتصالات ذاته. وهو ما يُحدث تحولاً جوهرياً في طبيعتها القانونية، وينزع عنها الوصف التقليدي الذي كان يُقلل من خطورتها على الخصوصية.

وقد بيّن البحث أن التمييز الشكلي بين محتوى الاتصال والبيانات غير المحتوائية لم يعد معياراً صالحاً لتحديد نطاق الحماية القانونية، سواء على مستوى التشريع أو القضاء، إذ كشفت التطبيقات القضائية المقارنة - ولا سيما الأوروبية والأمريكية - عن اتجاه متزايد نحو اعتماد معيار وظيفي موضوعي، يربط مشروعية جمع الميَّادات واستخدامها بمدى أثرها الكاشف وقدرتها الفعلية على المساس بالحق في الخصوصية وسرية الاتصالات. وبذلك، انتقل مركز الثقل من طبيعة البيانات في ذاتها إلى نتائج استخدامها وتحليلها. كما أظهر البحث أن غياب تنظيم تشريعي صريح ومتكامل للميَّادات، ولا سيما في بعض التشريعات العربية، يفتح الباب أمام توسع غير منضبط في سلطات المراقبة وجمع البيانات، ويُفضي إلى تفاوت في التطبيقات القضائية، بما يهدد مبدأ الأمن القانوني ويُضعف ضمانات المحاكمة العادلة. ولا يمكن تدارك هذا القصور باللجوء إلى التفسير الموسع للنصوص التقليدية وحده، لما ينطوي عليه ذلك من تعارض مع مبدأ الشرعية الجنائية وضيق التفسير في مجال القيود على الحقوق والحريات.

ومن ثمّ، يخلص البحث إلى أن إدراج الميَّادات ضمن نطاق الحماية القانونية المشددة لا يُعد ترفاً تشريعياً أو استجابة ظرفية، بل هو نتيجة منطقية لمسار فقهي وقضائي متكامل، يهدف إلى إعادة التوازن بين مقتضيات الأمن الجنائي وضرورة صون الحقوق والحريات الأساسية في البيئة الرقمية. ويقتضي هذا المسار اعتماد تنظيم قانوني واضح يُخضع جمع الميَّادات وتحليلها لمبادئ الشرعية، والضرورة، والتناسب، والتحديد الدقيق للغرض، مع رقابة قضائية فعّالة، تضمن عدم تحولها من أداة لكشف الحقيقة إلى وسيلة للمراقبة الشاملة. وقد أسفرت هذه الدراسة عن جملة من النتائج، نوردتها فيما يلي ثم نعقبها ببعض التوصيات:

أولاً: أهم النتائج:

١. أن الميتادات لم تعد مجرد بيانات تقنية محايدة، بل تحولت في الواقع الرقمي المعاصر إلى أداة كاشفة قادرة على إعادة بناء السلوك الرقمي للفرد، وتتبع نشاطه الزمني والمكاني، وربط الأفعال الرقمية بأشخاص وأجهزة محددة، بما يمنحها خطورة قانونية لا تقل عن خطورة محتوى البيانات ذاته.

٢. الميتادات تتمتع بطبيعة إثباتية مرنة ومتدرجة، فلا تُعدّ دليلاً مباشراً على إطلاقه، ولا مجرد قرينة ضعيفة، وإنما تمثل في الأصل قرينة تقنية قوية، قد ترتقي إلى مرتبة الدليل الرقمي المباشر متى ثبتت أصالتها، وسلامة سلسلة حيازتها، واتساقها مع باقي عناصر الإثبات.

٣. هناك قصور واضح في العديد من التشريعات العربية في تنظيم الميتادات، سواء من حيث تعريفها، أو تحديد طبيعتها القانونية، أو ضبط شروط جمعها وتحليلها واستخدامها في التحقيق الجنائي، وهو ما أدى إلى اضطراب التطبيق القضائي وغياب الأمن القانوني.

٤. أن الاتجاه الأوروبي يتبنّى معياراً وظيفياً متقدماً، يُخضع الميتادات للحماية القانونية متى كان من شأنها الكشف عن الهوية أو السلوك أو نمط الحياة، بصرف النظر عن كونها بيانات محتوى أو بيانات غير محتوى.

٥. أن التمييز الشكلي بين محتوى الاتصال والميتادات لم يعد صالحاً في ضوء التحليل التجميعي الحديث، إذ قد تؤدي الميتادات - وحدها - إلى انتهاك فعلي لسرية الاتصالات والحياة الخاصة دون الحاجة إلى الاطلاع على مضمون الاتصال.

٦. الطابع الزمني وسجلات النظام تمثل العمود الفقري للإثبات الرقمي، لما لها من قدرة على إعادة بناء التسلسل الزمني للأحداث الرقمية، غير أن حجيتها تظل مرهونة بسلامة البيئة التقنية وعدم العبث بإعدادات النظام.

٧. إدماج تقنيات الذكاء الاصطناعي في تحليل الميتادات عزّز من فعاليتها الإثباتية، لكنه في المقابل أفرز مخاطر قانونية جسيمة، أبرزها غموض الخوارزميات، وصعوبة الطعن الفني، والانحياز الخوارزمي، بما قد يهدد ضمانات المحاكمة العادلة.

٨. الميتادات تمثل امتداداً تقنياً معاصراً لفكرة القرينة القضائية، مع فارق جوهري يتمثل في كونها نتاجاً آلياً للنظام الرقمي، لا ثمرة للاستنباط الذهني البحت، وهو ما يمنحها درجة أعلى من الموضوعية التقنية دون أن يجعلها بمنأى عن الطعن.

ثانيا : التوصيات:

١. نوصي بتدخل تشريعي صريح لتنظيم الميادات، من خلال إدراج تعريف قانوني واضح لها في قوانين حماية البيانات الشخصية أو قانون مكافحة جرائم تقنية المعلومات وقانون الإجراءات الجنائية، ويجب أن يراعي طبيعتها الوظيفية لا وصفها التقني المجرد.
٢. ضرورة التمييز التشريعي الدقيق بين البيانات الأصلية، وبيانات الاتصالات، والميادات، مع إخضاع كل فئة لنظام إجرائي يتناسب مع درجة مساسها بالخصوصية، منعاً للخلط الذي يؤدي إلى إهدار الأدلة أو انتهاك الحقوق.
٣. إخضاع الميادات لنظام حماية خاص متدرج، بحيث تخضع الميادات الكاشفة للسلوك أو الموقع أو نمط الحياة لإذن قضائي مسبق. ويُسمح بجمع الميادات ذات الطابع الفني البحت بضوابط أخف، مع رقابة لاحقة.
٤. وضع إطار تشريعي منظم لاستخدام الذكاء الاصطناعي في التحقيق الجنائي الرقمي، يفرض قابلية تفسير الخوارزميات، ويكفل حق الدفاع في مناقشة نتائجها، ويمنع الاعتماد عليها كدليل وحيد للإدانة.
٥. دعوة القضاء إلى تبني معيار وظيفي مرن عند تقدير حجية الميادات، يقوم على أثرها الكاشف في الواقع العملي، لا على تصنيفها الشكلي بوصفها بيانات غير محتوى.
٦. عدم التعويل على الميادات منفردة في بناء الحكم الجنائي، إلا إذا تعززت بعناصر فنية وإثباتية أخرى، وثبتت سلامة سلسلة حيازتها وعدم العبث بها.
٧. تعزيز دور الخبرة الفنية المتخصصة في مناقشة الميادات، وعدم الاكتفاء بالتقارير الفنية المجمل، مع تمكين الدفاع من مناقشة الخبراء مناقشة فعّالة.
٨. إلزام جهات الضبط والتحقيق باحترام بروتوكولات صارمة لسلسلة الحيازة الرقمية (Chain of Custody)، وتوثيق كل مرحلة من مراحل التعامل مع الميادات، باعتبار ذلك شرطاً جوهرياً لقبولها أمام القضاء.
٩. تدريب القضاة وأعضاء النيابة على الجوانب التقنية للميادات، بما يتيح فهم دلالاتها وحدودها، ويمنع الانبهار غير النقدي بالدليل الرقمي.
١٠. إنشاء وحدات متخصصة في الأدلة الرقمية داخل جهات التحقيق، تضم خبراء قانونيين وتقنيين، لضمان التكامل بين الفهم القانوني والتحليل الفني.

قائمة المراجع

أولا : المراجع العربية:

- د. أحمد حسام طه تمام: الحماية الجنائية لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربية، ٢٠٠٣.
- د. أحمد ضياء الدين خليل: مشروعية الدليل الجنائي في المواد الجنائية، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ١٩٨٣.
- د. أحمد عبد اللاه المراغي: دور الدلائل الكافية في مباشرة الإجراءات الجنائية ، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، المجلد ٥٨، ع ٣، ٢٠٢٢.
- د. أحمد عوض بلال: قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة ، دار النهضة العربية، ٢٠١٣.
- د. احمد محمد علي الخديم: الحماية الجنائية للبيانات الشخصية في ظل مكافحة الجرائم الالكترونية، دراسة مقارنته، رسالة دكتوراه، كلية الحقوق، جامعته المنصورة، ٢٠٢٥.
- د. أروي نصار المليبي: تطويع الميتادات كدليل مساند ضمن عمليات التحقيق الجنائي الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، ع ٣، ٢٠٢١.
- د. أسامه أحمد شوقي المليجي: القواعد الإجرائية للاثبات في المواد المدنية والتجارية، دار النهضة العربية، ١٩٩٨.
- د. أشرف توفيق شمس الدين: شرح قانون الإجراءات الجنائية، طبعه مزيدة ومنقحة لأحدث التعديلات التشريعية ونصوص دستور ٢٠١٤، بدون دار نشر، بدون سنه نشر.
- د. امال عبد الرحيم عثمان: شرح قانون الإجراءات الجنائية، الهيئة المصرية للكتاب، بدون تاريخ نشر.
- د. أيمن عبد الله فكري: الشاهد الالكتروني في الاثبات الجنائي، مجلة الشريعة والقانون، كليه الشريعة والقانون بالقاهرة، جامعة القاهرة، ع ٤٤، نوفمبر ٢٠٢٤.
- د. تامر محمد صالح: التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية، المجلد ١١، العدد ١ - الرقم المسلسل للعدد ١، عدد خاص بالمؤتمر الدولي السنوي العشرون الجوانب القانونية والاقتصادية للذكاء

- الاصطناعي وتكنولوجيا المعلومات، أغسطس ٢٠٢١.
- د. جلال ثروت: الإجراءات الجنائية (الخصومة الجنائية) ، بدون دار نشر، ٢٠٠٢.
- د. جميل الشرقاوي: الإثبات في المواد المدنية، دار النهضة العربية، ١٩٩٠.
- د. جميل عبد الباقي الصغير: أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ٢٠٠٢.
- د. حسام توكل موسى: حجية الأدلة في الإثبات الجنائي دراسة في ضوء القانون ١٥٧ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ،دار البحوث والدراسات القانونية، ٢٠٢٤.
- د. خالد ممدوح إبراهيم: فن التحقيق في الجرائم الالكترونية، دار الفكر الجامعي، ٢٠١٠.
- د. رامي متولي القاضي: الدليل الجنائي الرقمي في التشريع المصري في ضوء أحكام القانون رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية والتشريعات المقارنة، مجلة القانون والتكنولوجيا، كلية القانون الجامعة البريطانية بمصر، المجلد ٢، ع ١٤، أبريل ٢٠٢٢.
- د. رهاب عمر سالم: محاولات التخفيف من نطاق البطلان، في ضوء الغرضين النفعي والمعنوي للإجراء الجنائي ،مجلة القانون والاقتصاد ،كلية الحقوق، جامعة القاهرة، ع ٩٤، يوليو ٢٠٢١.
- د. روب كيتشن ترجمة د.محمد بن أحمد غروي: ثورة البيانات البيانات الكبيرة والبيانات المفتوحة والبنية التحتية للبيانات والنتائج المترتبة عنها، مركز البحوث والدراسات، معهد الإدارة العامة، المملكة العربية السعودية، ٢٠١٨.
- د. سعود عبد القادر الشاعر: دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، المجلد ١٣، العدد ٨٣ - الرقم المسلسل للعدد ٨٣، مارس ٢٠٢٣.
- د. شيماء سيد عبد الرحمن الشقيري، ”مدى حجية الأدلة الرقمية في إثبات الجرائم التقليدية: دراسة فقهية“، مجلة الشريعة والقانون بالقاهرة ٤١، عدد ٤١، أبريل ٢٠٢٣.
- د. طه أحمد متولي: الدليل العلمي وأثره في الإثبات الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠٠٧.

- د. مأمون محمد سلامة: الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، ١٩٩٢.
- د. مبروك محمد علام مهران: الحد من آثار البطالان في قانون الإجراءات الجنائية والفقه الإسلامي، دراسته مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٢٥.
- د. محمد سعيد القرعة: المواجهة الجنائية للمعالجة والاستغلال غير المشروع للبيانات الشخصية علي ضوء القانون رقم ١٥١ لسنة ٢٠٢٠ ، المجلة القانونية، كلية الحقوق، جامعة القاهرة - فرع الخرطوم، المجلد ١٨، ع ٣، نوفمبر ٢٠٢٣.
- د. محمد سيد الجمال: الدليل العلمي وحجيته الجنائية ،دراسة مقارنة بين القانونين المصري والامريكي ، رسالة دكتوراه ، كلية الحقوق، جامعة طنطا ، ٢٠١٢.
- د. محمد صالح جاد المولي: الدليل الرقمي وحجيته في اثبات جرائم المعلومات ،رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠١٨.
- د. محمد عبد الحميد عرفه: مدي حجية الأدلة الالكترونية الرقمية في الإثبات في المواد الجنائية، دراسة تحليلية تطبيقية مقارنة، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الإسكندرية، ع ١، ٢٠١٨.
- د. محمد عبد الحميد مكي: شرح قانون الإجراءات الجنائية، بدون دار نشر، ٢٠٢٤.
- د. محمد عبد الفتاح عبد المقصود: القواعد الإجرائية للجرائم التي تقع عبر شبكات الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠١٥.
- د. محمود أحمد طه: التحقيق الجنائي العملي، بدون دار نشر، بدون سنة نشر.
- د. محمود أحمد طه: التعدي علي حق الانسان في سرية اتصالاته الشخصية بين التجريم والمشروعية، دار الكتب القانونية، ٢٠١٢.
- د. محمود أحمد طه: الموسوعة الفقهية والقضائية شرح قانون الإجراءات الجنائية، ج ٣، دار الكتب القانونية، ٢٠١٣.
- د. محمود حسين سيد أبو سيف: الأدلة الرقمية أمام المحكمة الجنائية الدولية، مجلة القانون والتكنولوجيا، كلية القانون، الجامعة البريطانية بمصر، مجلد ٤، ع ١، أبريل ٢٠٢٤.

- د. محمود سلامة الشريف: الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيتها، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي ، جامعة نايف الأمنية، السعودية، مج ٢، ع ٣، بدون سنة نشر.
- د. محمود عبد الحكيم: الشك في مجال الإجراءات الجنائية ،دراسة مقارنة، كلية الحقوق جامعة حلوان ، رسالة دكتوراة، ٢٠٢٣.
- د. محمود محمد سويف: دور بصمة المخ في الاثبات الجنائي ، دار الجامعة الجديد، ٢٠٢٢.
- د. محمود محمد سويف: سرية التحقيق الابتدائي بين اعتبارات تحقيق المصلحة العامة ومتطلبات الحق في الاعلام دراسة مقارنة، دار الجامعة الجديدة ، ٢٠٢١.
- د. محمود نحيب حسني: شرح قانون الإجراءات الجنائية، دار النهضة العربية، المجلد الثاني، الطبعة الخامسة، ٢٠١٦.
- د. مسعود بن حميد المعمري: الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، ملحق خاص، ع ٣، ج ٢ ، أكتوبر ٢٠١٨.
- د. مصطفى إبراهيم العربي: دور الدليل الرقمي في الإثبات الجنائي ، مجلة البحوث القانونية، المجلد ٦، ع ٧، ٢٠١٩.
- د. ممدوح حسن مانع: المسؤولية الجنائية عن أفعال الذكاء الاصطناعي غير المشروعة ، مجلة دراسات علوم الشريعة والقانون، الأردن، المجلد ٤٨، ع ٤، ٢٠٢١.
- د. وفاء محمد أبو المعاطي صقر: دور الحشرات في الإثبات الجنائي، دار الجامعة الجديدة، ٢٠٢٤.
- د. وفاء محمد صقر: المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، ٩٦٤، أكتوبر ٢٠٢١.
- د. يوسف بن سعيد الكلباني: الحماية الجزائية للبيانات الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعه عين شمس، ٢٠١٦.

ثانياً: المراجع باللغة الأجنبية:

- Abbas Karimi et al., "Cybercrime Detection Using Semi-Supervised Neural Network," Computer Science Journal of Moldova 29, no. 2 (86) (2021).
- ALbeladi SS, Othman FA: The effective role of big data in supporting the telecommunications sector – an analytical study. Journal of Information Studies & Technology 2023:1.5. <https://doi.org/10.5339/jist.2023>.
- Andrew D. Selbst, "A Due Process Theory for Algorithmic Discrimination," California Law Review 108 (2020):
- BACA, Murtha (ed.). Introduction to metadata. Getty Publications, 2016
- Brian Carrier, File System Forensic Analysis –Addison-Wesley, 2005–.
- CARRIER, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.
- Céline Vanini, Christopher J. Hargreaves, Harm Beek, and Frank Breiting, "Was the Clock Correct? Exploring Timestamp Interpretation through Time Anchors for Digital Forensic Event Reconstruction," Forensic Science International: Digital Investigation 49 – 2024.
<https://doi.org/10.1016/j.fsidi.2024.301759>.
- Christopher Hargreaves, Alex Nelson, and Eoghan Casey, "An Abstract Model for Digital Forensic Analysis Tools – A Foundation for Systematic Error Mitigation Analysis," Forensic Science International: Digital Investigation 48, Supplement (2024): Article 301679, <https://doi.org/10.1016/j.fsidi.2023.301679>.
- Christopher Kuner, Lee A. Bygrave & Christopher Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, 2020.

- Christopher T. Anglim, ed: Privacy Rights in the Digital Age, 1st ed. (Amenia, NY: Grey House Publishing, 2015).
- Christopher T. Timko, "Metadata and the Fourth Amendment," Boston University Law Review 97 (2017).
- Daniel J. Solove, "Digital Metadata and Privacy: The Privacy Interest in Metadata," Minnesota Law Review 102 (2017): p 1445
- Daniel J. Solove: Understanding Privacy- Harvard University Press, 2008.
- David Anderson QC, A Question of Trust: Report of the Investigatory Powers Review (2015), Independent Reviewer of Terrorism Legislation.
- Dong Bin Oh et al: GPT: Evaluation on Triaging Ransomware Process in Memory Forensics with Large Language Model," Forensic Science International: Digital Investigation 49, Supplement- 2024, Article 301756,
<https://doi.org/10.1016/j.fsidi.2024.301756>.
- Eoghan Casey, Digital Evidence and Computer Crime, 4th ed. (2020).
- Eoghan Casey, Digital Evidence and Computer Crime (4th ed., Academic Press, 2020)
- Eoghan Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. , Academic Press, 2011.
- Eoghan Casey :Handbook of Digital Forensics and Investigation -Academic Press, 2010 .
- G. Ramirez, "The Erosion of Smith v. Maryland," Case Western Reserve Law Review (2019), Case Western Reserve University School of Law Scholarly Commons, p. 493 accessed (19 December 2025).

- G. Ramirez, "What Carpenter Tells Us About When a Fourth Amendment Search Is Required," Case West. Reserve Law Rev. (2019) (unpaginated), Case Western Reserve Law Review, (accessed 19 December 2025)

<https://scholarlycommons.law.case.edu/caselrev/vol71/iss3/>.

- GARTNER, Richard: Metadata. Springer, ٢٠١٦
- GILLILAND, Anne J. Setting the stage. Introduction to metadata, 2008, 3
 - Hany Farid :Photo Forensics (MIT Press, 2016),
 - Haynes, David. Metadata for Information Management and Retrieval: Understanding Metadata and Its Use. 2nd ed. London: Facet Publishing, 2018,
 - Jacob Leon Kröger, Recognizing Information Inferred about Individuals as Personal Data (Technische Universität Berlin, 2022), SSRN Electronic Journal, posted February 8, 2023, p243 (accessed 18 December 2025 at 12:28AM, <https://papers.ssrn.com/abstract=4349200>).
 - Jan-Niclas Hilgert, Axel Mahr, and Martin Lambertz, "Forensic Implications of Stacked File Systems," in DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, Forensic Science International: Digital Investigation 48, Supplement (2024): Article 301678, <https://doi.org/10.1016/j.fsidi.2023.301678>.)
 - John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 3rd ed. (Charles River Media, 2005)
 - Lilian Edwards, "From DRIPA to IPA: The UK's Journey Towards Privacy-Compliant Surveillance," International Journal of Law and Information Technology 26 (2018)
 - Lisa M. Dreier et al: Beyond Timestamps: Integrating Implicit Timing Information into Digital Forensic Timelines," Forensic Science International: Digital Investigation 49 – 2024,

Article 301755.

<https://doi.org/10.1016/j.fsidi.2024.301755>.

- Lucie Cluzel-Métayer et Émilie Debaets : Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *Revue française de droit administratif*, no 6 (novembre-décembre 2018) .
- Mark L. Krotoski: “Effectively Using Electronic Evidence Before and at Trial,” *United States Attorneys’ Bulletin* 59, no. 6 , November 2011.
- MILLER, Steven Jack. Metadata for digital collections. American Library Association, 2022.
- NIST Guidelines on Digital Evidence, Special Publication 800-86 (2006).
- Orla Lynskey, “After Watson: Mandatory Data Retention and the CJEU,” *European Data Protection Law Review* 3 (2017).
- Paul M. Schwartz & Karl-Nikolaus Peifer, “Transatlantic Data Privacy Law,” *Georgetown Law Journal* 106 (2017).
- Rebecca Wexler, “Life, Liberty, and Algorithmic Detection of Recidivism,” *Supreme Court Review* 70 (2020).
- Recognizing Information Inferred about Individuals as Personal Data”, SSRN Working Paper (2023).
- Sandra Wachter et al.: “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,” SSRN Working Paper”, 2018.
- Sarah Larson, Surya Mattu, Lauren Kirchner, and Julia Angwin, “How We Analyzed the COMPAS Recidivism Algorithm,” *ProPublica*, May 23, 2016, archived at Perma.cc, <https://perma.cc/8BXL-NU4D> (accessed 9 May 2025).
- Sarah Morrissey, “Geolocation Metadata in Mobile Fo-

rensics,” Journal of Digital Forensics, Security and Law 15, no. 2 (2020).

- Serge Slama, “Données de connexion et vie privée,” Revue française de droit constitutionnel 168 (2021).
- Shahzad Saleem, Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics (PhD diss., Stockholm University, 2015).
- Sheri B. Pan, “Get to Know Me: Protecting Privacy and Autonomy Under Big Data’s Penetrating Gaze”, Harvard Journal of Law & Technology 30, no. 1 (Fall 2016) p.244, accessed: <https://jolt.law.harvard.edu/assets/articlePDFs/v30/30Harv-JLTech239.pdf>.
- Simon Caqué: Le régime juridique des données publiques numériques (thèse de doctorat, Université de Rennes 1, 2020), dirigée par Hélène Muscat, soutenue le 10 septembre 2020.
- Simson Garfinkel & Alex Schatz, “Quantifying Forensability,” Journal of Digital Investigation 8 (2011).
- Simson L. Garfinkel: Digital Forensics Research: The Next 10 Years– Digital Investigation 7, 2010.
- Siwei Lyu et al., “A Review of Deep Learning Methods for Detecting Deepfakes,” IEEE Transactions on Information Forensics and Security 16 (2021).
- Siwei Lyu et al., “Metadata-Assisted Deepfake Detection: EXIF and Encoding Analysis,” IEEE Transactions on Information Forensics and Security 17 (2022).
- Souradip Nath et al., “Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics,” in Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (Washington, DC, USA, 28–31 October 2024): 11–20.

<https://doi.org/10.1109/TPS-ISA62245.2024.00012>.

- Stephen Mason & Daniel Seng, Electronic Evidence (5th ed., 2021), p. 456 & George L. Paul, Foundations of Digital Evidence (ABA Book Publishing, 2019).
- Stephen Mason, Electronic Evidence (5th ed., 2021).
- Taha Gharaibeh, Ibrahim Baggili, and Anas Mahmoud: On Enhancing Memory Forensics with FAME: Framework for Advanced Monitoring and Execution– Forensic Science International: Digital Investigation 49, Supplement ,2024. <https://doi.org/10.1016/j.fsidi.2024.301757>.
- Xiaoyu Du and Mark Scanlon: “Methodology for the Automated Metadata–Based Classification of Incriminating Digital Forensic Artefacts,” in Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES ’19) (Canterbury, UK: ACM, 2019 <https://doi.org/10.1145/3339252.3340517>.
- Yan Zhao: Metadata Management for Data Lake Governance. PhD diss., Université Toulouse 1 Capitole, 2021.
- ZENG, Marcia Lei; QIN, Jian. Metadata. American Library Association, 2020.