

تاريخ القبول: 2021/10/17

تاريخ الإرسال: 2021/09/01

الطب الشرعي الرقمي: إطلالة على مفهومه وأهميته في نظام العدالة الجنائية

Digital Forensics: An overview of its concept and its importance in the Criminal Justice System.

مخلوف داودي¹¹جامعة غرداية (الجزائر)، daoudi.makhlouf@univ-ghardaia.dz

المخلص:

تتمثل الأهداف الرئيسية لهذا البحث في إلقاء الضوء على الطب الشرعي الرقمي الناشئ الذي يقوم على أسس علمية في سياق التحقيقات الجنائية بجمع الأدلة الرقمية ودراساتها، ونقلها، وتخزينها، وتحليلها، وتفسيرها، وإعادة بنائها؛ لضمان المقبولية القانونية لدى المحاكم.

لقد خلص البحث إلى نتائج كثيرة، ولعل أهمها أن الطب الشرعي الرقمي صار علما راسخا في التحقيقات الجنائية بما يملكه من أدوات، وتقنيات، وعمليات قياسية، ودراسة افتراضية مكنته من إدارة الأدلة الرقمية في مسرح الجريمة وصولا بها إلى أروقة المحاكم، إلا أن هناك تحديات تعترض سبيل ذلك، ولعل أهمها تلك الفجوة المعرفية التي قد يفرضها التطور السريع في تقنيات التكنولوجيا الرقمية.

الكلمات المفتاحية: الطب الشرعي الرقمي، الدليل الرقمي، الكمبيوتر، التحقيقات الجنائية، التكنولوجيا الرقمية.

Abstract:

The main objectives of this research are to shed light on the emerging science-based digital forensics in the context of criminal investigations by collecting and studying digital evidence, transmitting, storing, analyzing, interpreting, and reconstructing to ensure legal admissibility before the courts.

*المؤلف المرسل

The research has concluded many results and perhaps the most important of them is that digital forensics has become a well-established science in criminal investigations with its tools, techniques, standard processes, and hypothetical knowledge that enabled it to manage digital evidence at crime scenes and bring it to the corridors of courts. However, there are challenges facing the way to do this, and perhaps the most important of which is the knowledge gap that may be imposed by the rapid development of digital technology techniques.

Keywords: digital forensics, digital evidence, computer, criminal investigations, digital technology.

مقدمة:

الحمد لله والصلاة والسلام على أشرف المرسلين، وعلى آله وصحبه أجمعين وبعد: نفذت التكنولوجيا الرقمية بشكل نشط ومتسارع في إدارة جل أنماط مناحي الحياة فالأفراد صاروا يعتمدون عليها بكفاءة لإدارة شؤونهم المالية والشخصية، وفي عمليات التسوق، وحجز الفنادق، وجدولة النقل، والتواصل المعرفي وغير ذلك من الأنشطة الأخرى. كما تعتمد الأعمال التي تقوم بها المؤسسات والشركات على مختلف أنواعها الآن بشكل شبه كامل على التكنولوجيا الرقمية كجزء أساسي من أنشطتها. فبدون الأنظمة الرقمية المسؤولة عن قبول الطلبات ومعالجتها، والتحكم في الهياكل التنظيمية الداخلية وإصدار الفواتير، وإدارة المعاملات المالية والإدارية،..ستبدأ معظم الشركات والمؤسسات في ظرف وجيز من المعاناة من أزمة تكدس الأعمال الإدارية والمالية. لقد وفّرت التكنولوجيا الرقمية بأقل التكلفة، وربما بفرص متساوية للجميع استخدام تقنياتها لجعل الحياة أسهل، والتواصل أسرع، إلى حد يمكن القول أن المجتمع البشري اليوم تطوّر إلى مجتمع رقمي؛ حيث تأثير اعتماده الرقمي متزايد وملاحظ في العديد من المجالات.

إن استخدامنا المكثف للتكنولوجيا الرقمية لم يبق -للأسف الشديد- في المجالات المشروعة بل استغلها البعض لاستخدامها في دعم أنشطته الإجرامية؛ وكنتيجة لذلك تطورت الظاهرة الإجرامية بفعل التكنولوجيا الرقمية التي أحدثت فيها انقلابا ليس فقط

في المفاهيم النظرية بل وفي الأساليب والتقنيات إلى حد أنه من السائع القول: لا توجد جريمة ليس لها بعد رقمي.

فالمجرمون يستخدمون منتجات التكنولوجيا الرقمية؛ لتنفيذ جرائمهم مما أوجد حالة من التحديات للعدالة الجنائية في ملاحقتهم واعتقالهم. فمسرّح الجريمة لم يعد يقتصر على الواقع المادي، بل صارت أكثر الجرائم ترتكب داخل الفضاء الرقمي.

لقد تورطت أجهزة الكمبيوتر المحمولة وغير المحمولة والهواتف المحمولة وأجهزة Pad والإنترنت،..في الجرائم. وبما أنه لا جريمة بدون آثار تدل على الجناة ظهر نوع جديد من الأدلة يدعى الأدلة الرقمية "digital evidence". يمثل هذا الشكل الجديد من الأدلة بعض التحديات المهمة جدا لنظامنا القانوني. فهذه الأدلة تختلف اختلافا كبيرا في طبيعتها عن الأدلة الجنائية المعروفة في الواقع المادي ولا يمكن التعامل معها بنفس الطريقة.

من هنا، أدت الحاجة إلى ظهور ما يسمى بالطب الشرعي الرقمي "digital forensics" الذي يختلف عن معظم علوم الطب الشرعي الأخرى؛ نظرا لطبيعة المادة قيد الفحص التي ليس لها أي بنية بيولوجية، أو فيزيائية، بل ذات طبيعة خاصة فرضتها التكنولوجيا الرقمية.

إن الطب الشرعي الرقمي صار يقدم مساهمة عظيمة لنظام العدالة الجنائية في الكشف عن الأنشطة الإجرامية التي تتم على مستوى الأنظمة الرقمية من خلال تتبع الأدلة الجنائية الرقمية، وتوثيقها وفهمها وتحليلها بما يمكن من بناء تصور كامل للكشف عن الجريمة، وإدانة مرتكبيها.

الإشكالية:

لقد أوجد الطب الشرعي الرقمي حالة من الجدل حول توحيد المعايير في كيفية التعامل مع الأدلة الرقمية، وتحديد جرائم الأجهزة الرقمية وغير ذلك من المسائل بسبب عدم الاتفاق حول مصطلحه والمصطلحات الأساسية الدارجة فيه. وبما أن الطب الشرعي الرقمي يستخدم البيانات التي تم إنشاؤها بواسطة الأجهزة الرقمية كمصدر له، فإن مع التطورات الحاصلة في التكنولوجيا الرقمية قد تشكّل عامل تحد كبير على قدرته في

الاستيعاب، والتحليل، وقيمتها الإثباتية أمام العدالة الجنائية...، من هنا، تبرز الإشكالية التالية:

ما هي الإشكالات المعرفية في تحديد مصطلح الطب الشرعي الرقمي؟ وما أهمية دوره في التحاليل والتحقيقات الجنائية المتعلقة بجرائم الأجهزة الرقمية؟ وما هي متطلبات المقبولية القانونية للأدلة الرقمية؟

الفرضيات:

تمكننا الفرضيات من إعطاء رأي مبدئي، ومن وضع استنتاجات استباقية التي ستواجه فيما بعد بالحقائق:

1- إن احتضان المجتمع للتكنولوجيا الرقمية في جميع الأنشطة ومنها الأنشطة الإجرامية أدى إلى التغير السريع في مشهد الأدلة للظاهرة الإجرامية، وهو ما انعكس على تقنيات التحقيقات الجنائية وعلى عمل المحاكم التي بدأت في تعديل طبيعة أدلة الإثبات.

2- إن كثرة الاعتماد على الطب الشرعي الرقمي في عمليات التحقيقات الجنائية في الجرائم الرقمية ستدفع به خطوات إلى أن يكون علما جنائيا راسخا؛ نظرا لما يوفره من سمة مميزة من المبادئ، والمناهج، وأدوات خاصة، والدراية الافتراضية..

أهداف البحث:

إن حسن إدارة الأدلة الرقمية في مسرح الجريمة ذات أهمية حيوية للتحقيق الجنائي؛ فالدليل الرقمي يفقد قيمته الإثباتية أمام المحاكم إذا لم تتم إدارته بطريقة منهجية وعلمية متخصصة. تهدف هذه الدراسة إلى إظهار تقنيات الطب الشرعي الرقمي ومنهجيته وعملياته القياسية في التعامل مع الأدلة الرقمية؛ لضمان المقبولية القانونية، والتحديات التي يواجهها في سبيل تحقيق ذلك.

منهج البحث:

تمّ استخدام المنهج الوصفي التحليلي للتعرف أكثر على ماهية علم الطب الشرعي الرقمي، وتفاعل تقنياته في سياق التحقيقات الجنائية مع المعطيات الفعلية للأدلة الرقمية.

الخطة :

تأتي هذه الدراسة البحثية لدراسة المصطلحات الأساسية للطب الشرعي الرقمي والتعريفات ومناقشتها، كما تروم أيضا إعطاء نبذة مختصرة عن تاريخ ظهوره، وبيان نطاق بحثه، ودور تقنياته في التحقيقات الجنائية، والتحديات التي تواجهها الأدلة الرقمية للوصول بها للمقبولية القانونية على مستوى المحاكم، وذلك وفق خطة اعتمدت فيها النموذج الثنائي؛ لأن الموضوع محل الدراسة تطلب أولا إلقاء نظرة عامة على الطب الشرعي الرقمي، وثانيا الكلام عن إجراءاته وإمكانياته الإثباتية في القضاء الجنائي.

1. نظرة عامة على الطب الشرعي الرقمي

تزايد الوعي المجتمعي في الآونة الأخيرة بأهمية الطب الشرعي الرقمي وعظيم مساهمته في خدمة نظام العدالة الجنائية، أو أي نظام آخر كالدفاع الوطني، وهذا كنتيجة عاكسة لتزايد خطورة ونطاق الجرائم التي تتم بواسطة أجهزة الكمبيوتر أو أي جهاز رقمي آخر.

لقد أثار هذا الاهتمام والحاجة المتزايدة للطب الشرعي الرقمي نقاشات حول المصطلحات والتعريفات والمعايير، والعديد من الجوانب الأساسية الأخرى لهذا المجال النامي مقارنة بعلوم الطب الشرعي التقليدية الأخرى.

1.1 . تعريف الطب الشرعي الرقمي وتاريخ ظهوره**1.1.1. تعريفه**

لقد وردت طرق عديدة لتعريف الطب الشرعي الرقمي؛ ففي مجلة الطب الشرعي Forensic Magazine، عرّف كين زاتيكو "Ken Zatyko" الطب الشرعي الرقمي بهذه الطريقة: "هو تطبيق علوم الكمبيوتر وإجراءات التحقيق لغرض قانوني يتضمن تحليل الأدلة الرقمية بعد عملية البحث المناسبة، وسلسلة العهدة chain of custody¹، والتحقق من الصحة باستخدام الرياضيات، واستخدام الأدوات التي تم التحقق من صحتها، والتكرار وإعداد التقارير، والعرض التقديمي المقدم من طرف الخبراء".²

يلاحظ أن هذه الطريقة في التعريف هي أقرب إلى أن تكون بياناً لإجراءات الطب الشرعي من كونها تعريفاً.

كما تم تعريف الطب الشرعي الرقمي بتعريف بسيط بأنه: "تطبيق العلم والهندسة على المشكلة القانونية للأدلة الرقمية".³ فالطب الشرعي الرقمي، إذن، هو علم جمع وحفظ وفحص وتحليل وتقديم الأدلة الرقمية ذات الصلة لاستخدامها في الإجراءات القضائية⁴ من هنا، يختلف الطب الشرعي الرقمي، عن معظم علوم الطب الشرعية الأخرى؛ لأن طبيعة المادة قيد الفحص يتم تحديدها، إلى حد كبير، بالفكر الافتراضي المبدع؛ فبدلاً من البحث عن آثار المواد المودعة من قبل الكيانات الفيزيائية أو البيولوجية، والتي تميل إلى التطور البطيء، إلا أننا نتعامل مع التكنولوجيا الرقمية التي يتم تحديثها وتحسينها وحتى إنشاؤها بمعدل متسارع ينذر بوجود كثير من التحديات التي تعترض عمل الطب الشرعي الرقمي في التحقيقات الجنائية.

2.1.1. مصطلح الطب الشرعي الرقمي

أصبح التحرك نحو توحيد المعايير في كيفية التعامل مع الأدلة الرقمية وجرائم الكمبيوتر أكثر صعوبة بسبب عدم وجود اتفاق على المصطلحات الأساسية. وسنقتصر على دراسة مصطلح الطب الشرعي الرقمي الذي له عدة تسميات: الطب الشرعي الحاسوبي computer forensics، والطب الشرعي السيبراني cyber forensics، والتحقيقات الرقمية digital investigations وما إلى ذلك.⁵

يشير الطب الشرعي للكمبيوتر computer forensics عادة إلى فحص الطب الشرعي لمكونات الكمبيوتر ومحتوياتها، مثل محركات الأقراص الثابتة والأقراص المدمجة والطابعات. ومع ذلك، يستخدم المصطلح أحياناً بشكل فضفاض لوصف التحقيق الجنائي لجميع أشكال الأدلة الرقمية، بما في ذلك البيانات التي تنتقل عبر الشبكات (المعروف أيضاً باسم الطب الشرعي للشبكة (a.k.a. network forensics)).⁶

وزيادة في الإرباك، تم اعتماد مصطلح الطب الشرعي الحاسوبي computer forensics من قبل مجتمع أمن المعلومات the information security community لوصف

مجموعة واسعة من الأنشطة التي تتعلق بحماية أنظمة الكمبيوتر أكثر من جمع الأدلة الرقمية.

لكن ونظرا لتطور المجال في العديد من التخصصات الفرعية المتميزة، بما في ذلك التحليلات الجنائية للبرامج الضارة والطب الشرعي للأجهزة المحمولة، فقد أصبح المصطلح الأكثر عمومية واستخداما على نطاق واسع لوصف المجال ككل هو مصطلح الطب الشرعي الرقمي digital forensics.⁷

3.1.1. تاريخ ظهور الطب الشرعي الرقمي

تاريخ الطب الشرعي الرقمي قصير مقارنة بتاريخ التخصصات العلمية الأخرى؛ حيث بدأ أقدم عمل للطب الشرعي المرتبط بالحاسوب خلال الثمانينيات، ففي عام 1984 طور مكتب التحقيقات الفيدرالي FBI برنامجا رائدا لتحليل أدلة الكمبيوتر. بالإضافة إلى ذلك، أدت الزيادة في إساءة استخدام الإنترنت إلى إنشاء فريق الاستجابة للطوارئ الحاسوبية (CERT) عام 1988، والذي تمّ تشكيله من قبل وكالة مشاريع الأبحاث الدفاعية المتقدمة (DARPA) ويقع مقره في جامعة كارنيجي ميلون Carnegie Mellon في بيتسبرغ Pittsburgh.⁸

أما فترة التسعينات فقد شهدت نموا كبيرا في استعمال الإنترنت، وأصبحت أجهزة الكمبيوتر الشخصية شائعة في المنازل. خلال هذا الوقت، كان الطب الشرعي الحاسوبي computer forensics موضوعا رئيسيا بين وكالات إنفاذ القانون. ففي عام 1993، استضاف مكتب التحقيقات الفيدرالي FBI أول المؤتمرات الدولية المتعددة حول أدلة الكمبيوتر ومساهمتها في إنفاذ القانون، وفي عام 1995، تم تشكيل المنظمة الدولية لأدلة الكمبيوتر (IOCE) وبدأت في تقديم توصيات بشأن المعايير المتعلقة بهذا العلم الجديد.⁹

وبعد مطلع الألفية، أدت جملة من العوامل التي أنتجها التطور السريع للتكنولوجيا الرقمية، كعمليات الاختيال عبر الإنترنت، والقرصنة الالكترونية والهجمات بالبرامج الضارة وإساءة الاستخدام وغيرها من الحوادث إلى زيادة الطلب على الطب الشرعي

الرقمي، وتوسيع تركيز نطاق بحثه؛ ليشمل ليس فقط فحص الأدلة الرقمية من أجهزة الكمبيوتر بل مجالات التقاط حركة مرور الشبكة وتحليلها لصالح التحقيقات الجنائية.¹⁰

2.1. مجال بحث الطب الشرعي الرقمي

مجال بحث الطب الشرعي الرقمي هو فحص الأدلة الرقمية من مصادرها الكثيرة كأجهزة الكمبيوتر، أو الأجهزة المحمولة، أو الشبكات أو غير ذلك من الأجهزة والأنظمة التي تدخل إلى حد كبير في نطاق تخصصه. ينصب تركيزنا في هذا الجزء من البحث على تعريف الدليل الرقمي، وكيفية إنشائه، ومصادره.

1.2.1. تعريف الدليل الرقمي

عرّف الباحث الأمريكي كيسي Casey الدليل الرقمي Digital Evidence على أنه: "أي بيانات مخزنة أو مرسلّة باستخدام جهاز كمبيوتر تدعم أو تدحض نظرية لكيفية حدوث جريمة أو تعالج العناصر الحاسمة للجريمة مثل النية أو الذريعة".¹¹ يمكن طرح العديد من التعريفات المماثلة للأدلة الرقمية، ولكن من أجل الفهم العام، تم قبول التعريف الوارد أعلاه؛ لكن يُعتقد أن الاستثناء الوحيد في التعريف ليكون جامعاً هو تغيير كلمة "كمبيوتر" "computer" إلى "نظام الجهاز الرقمي" "digital device-system" لمسيرة نطاق الطب الشرعي الرقمي الذي صار مؤخراً يغطي تقنيات وأجهزة وأنظمة أوسع.¹²

يتضح من خلال التعريف اختلاف طبيعة الأدلة الرقمية عن طبيعة الأدلة التقليدية؛ فالأدلة الرقمية تفتقد إلى البنية البيولوجية أو الفيزيائية، فلا يمكن لمسها أو تشكيلها لكونها تنتمي إلى السجل الإلكتروني، وموجات الراديو المخزنة في الأجهزة؛ وبالتالي هذه الأدلة لا يمكن رؤيتها بأعيننا، لذلك تعيّن على خبراء الطب الشرعي الرقمي تحويلها إلى محتويات مُشكّلة يمكن قراءتها وفهمها.¹³

2.2.1. كيفية إنشاء الأدلة الرقمية

كما أسلفنا في التعريف يبدأ الدليل الرقمي كبيانات إلكترونية، إما في شكل معاملة أو مستند أو نوع من الوسائط مثل تسجيل صوتي أو فيديو.

تشمل المعاملات المالية أو غير المالية ميدانا خصبا لإنشاء الأدلة الرقمية؛ فعملية الشراء ودفع الفاتورة وسحب النقود وحتى كتابة شيك ورقي، قد يبدو أن كتابة الشيك طريقة قديمة وليست رقمية أو إلكترونية بطبيعتها، إلا أن معالجة هذا الشيك المكتوب تكون إلكترونية ويتم تخزينها في البنك أو شركة بطاقة الائتمان التي تتعامل معها. وبالمحصلة يتم في النهاية تحويل كل نوع من المعاملات اليوم رقميا وفي نهاية المطاف إلى دليل رقمي: زيارات الطبيب، ومشاريع البناء، وتعبئة الوصفات الطبية، وتسجيل طفل في المدرسة...¹⁴.

في عالم اليوم ، يكاد يكون من المستحيل أن تكون خارج الإنترنت تماما " off the net"; بحيث لا تنشئ أنشطتك شكلا من أشكال السجلات الإلكترونية؛ بل أدى انفجار مواقع التواصل الاجتماعي إلى إنشاء مجال جديد تماما من الأدلة الإلكترونية المنتشرة والمستمرة. فمثلا صار تقريبا كل فرد منا يشارك الناس اليوم وسائل التواصل الاجتماعي مثل Twitter و Facebook أنشطتهم اليومية وأفكارهم وصورهم الشخصية وحتى مواقعهم. أضف إلى ذلك انفجار عالم المدونات، حيث ينشر الأفراد كصحفيين أو مواطنين منشورات في مدونات ذاتية على الإنترنت تعكس آرائهم السياسية، إلى مدونات عائلاتهم الشخصية مع صور لأطفالهم وحيواناتهم الأليفة.¹⁵

فعندما ينشئ شخص ما بريدا إلكترونيا، أو يكتب مستندا باستخدام برنامج Notepad أو برنامج معالجة النصوص، أو يأخذ سيارته في جولة مع تشغيل وحدة تحديد المواقع العالمية (GPS) ، أو يدفع فاتورة عبر الإنترنت، فإنهم ينشئون دليلا رقميا. تشغيل جهاز الكمبيوتر الخاص بك، أو تصفح الإنترنت، أو إجراء مكالمة هاتفية على هاتفك الخليوي - كل ذلك - ينشأ دليلا رقميا. الكاميرات الرقمية، وكاميرات الفيديو الرقمية وكاميرات الويب، ومسجلات الصوت الرقمي كلها تنشأ أدلة رقمية. فهذه هي الأشكال الأكثر شهرة للأدلة الرقمية.

ومع ذلك، من السهل التغاضي عن الطرق العديدة التي تنشأ بها الأدلة الرقمية دون أن ندرك أننا نقوم بذلك. فإذا كنت تلعب ألعابا عبر الإنترنت مع لاعبين آخرين، أو تشاهد مقاطع فيديو من الإنترنت، أو تتسوق في أحد آلاف المتاجر عبر الإنترنت أو حتى

ترسل بطاقة تهنئة عبر موقع Hallmark عبر الإنترنت، فأنت تقوم بإنشاء دليل رقمي.¹⁶

ففي هذه الأيام، من المستحيل تقريبا قضاء يوم دون إنشاء شكل من أشكال البصمة الرقمية. حتى ولو كنت "خارج الشبكة" تماما، ولا تستخدم جهاز كمبيوتر أو هاتفًا خلويًا، وكمثال على ذلك أن تشغيل الرادار حيث توجد كاميرا لمراقبة حركة المرور يمكن أن تلتقط رقم لوحة السيارة الخاصة بك، مع الإشارة إلى موقعك، وبالطبع تحرير مخالفة في حالة تجاوز السرعة المسموح بها، وإنشاء سجل رقمي بكل هذه المعلومات.

3.2.1. مصادر الأدلة الرقمية

هذه الأنواع المختلفة من البيانات الرقمية مفيدة في عملية التحقيق. يمكن تقسيم مصادر البيانات الرقمية إلى ثلاث فئات:¹⁷

أ- أنظمة الكمبيوتر المفتوحة Open computer systems:

هي أنظمة الكمبيوتر التي يعرفها غالبية الناس مثل أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر المكتبية والخوادم. تضمن زيادة مساحة التخزين في أنظمة الكمبيوتر الحصول على كمية كبيرة من الأدلة الرقمية (على سبيل المثال ، يمكن أن يحتوي ملف واحد على كمية كبيرة من البيانات الرقمية).

ب-أنظمة الاتصالات Communication systems:

تعد أنظمة الهاتف التقليدية وأنظمة الاتصالات اللاسلكية المتقدمة والإنترنت مصادر غنية للأدلة الرقمية .

ج-أنظمة الكمبيوتر المدمجة: Embedded computer systems

يمكن أن تحتوي العديد من أنظمة الكمبيوتر المدمجة، مثل الأجهزة المحمولة وأنظمة الملاحة وأنظمة أخرى على العديد من الأدلة الرقمية القيمة في التحقيق الجنائي.

2. إجراءات الطب الشرعي الرقمي وإمكاناته الإثباتية في القضاء الجنائي

هذا الجزء من البحث يغطي إجراءات الطب الشرعي الرقمي من خلال بيان الممارسات الأساسية السليمة من الناحية الجنائية التي يمكن استخدامها لجمع الأدلة الرقمية ودراساتها ونقلها وتخزينها، وتحليلها، وتفسيرها، وإعادة بنائها. كما يتناول

إمكانيات الطب الشرعي الرقمي الإثباتية من خلال تفاعل تقنياته مع الأدلة الرقمية للوصول بها إلى المقبولة القانونية والتحديات التي تعترض سبيل ذلك، وهو الأمر الذي يعدّ شرطا أساسيا لدراسة الطب الشرعي الرقمي.

1.2. إجراءات الطب الشرعي الرقمي

يمكن تقسيم عملية الطب الشرعي الرقمي إلى ثلاث فئات من الأنشطة: الاستحواذ

acquisition ، والتحليل analysis، والعرض التقديمي presentation .

1.1.2. الاستحواذ acquisition: تشير عملية الاستحواذ إلى فحص مجموعة من الوسائط الرقمية digital media. اعتمادا على نوع الفحص، يمكن أن تكون محركات أقراص صلبة مادية أو وسائط ضوئية أو بطاقات تخزين من الكاميرات الرقمية أو الهواتف المحمولة أو شرائح من الأجهزة المدمجة أو حتى ملفات مستندات فردية في أي حال، يجب التعامل مع الوسائط التي سيتم فحصها بدقة. كحد أدنى ، يجب أن تتكون عملية الاستحواذ من إنشاء ملف لنسخ مكررة من الوسائط الأصلية (نسخة العمل)، بالإضافة إلى الاحتفاظ بسجلات جيدة لجميع الإجراءات التي تم اتخاذها باستخدام الوسائط الأصلية.¹⁸

2.1.2. التحليل analysis: تشير عملية التحليل إلى فحص الوسائط الرقمية digital media من خلال تحديد المواد ذات الأهمية الموجودة في الوسائط المعنية، ثم يتم إخضاعها للتحليل المناسب من قبيل تحليل نظام الملفات، أو فحص محتوى الملف، أو تحليل السجل، أو التحليل الإحصائي، أو أي عدد من أنواع المراجعة الأخرى.¹⁹ أخيرا، يستخدم ممارسو الطب الشرعي الرقمي مهاراتهم وخبراتهم وأدواتهم في عملية التحليل التي تعتمد على الحقائق ومراعاة الملبسات التي تحيط بظروف التحقيق .على سبيل المثال، يمكن أن يشمل التحليل ما يلي:²⁰

- ربط بعض الأنشطة بحساب مستخدم معين،
- وضع جدول زمني للأحداث،
- تحديد ما إذا كان قد تم توصيل جهاز USB بالجهاز،
- كسر التشفير،

- تحديد العلاقات أو الصلات بين الأفراد (أي بين المشتبه بهم و الضحية)،
- تحديد المواقع التي تم زيارتها،
- تحديد ما إذا تم فتح ملفات معينة أو تنزيلها،..

3.1.2. العرض التقديمي presentation : يشير العرض التقديمي إلى العملية التي يقوم بها ممارس الطب الشرعي الرقمي والتي تتمثل في اطلاع الطرف أو الأطراف المعنية بنتائج مرحلة التحليل من خلال كتابة تقرير واف بكل الإجراءات التي اتخذها والمواد التي تم الكشف عنها، والمعاني التي تؤدي إليها تلك المواد في سياق التحقيق. كما يمكن أن تشمل مرحلة العرض أيضا دفوعاته وإجاباته إزاء الاعتراضات والتحديات التي قد تشكك في مصداقية النتائج المتوصل إليها.²¹

يتضح مما سبق أن النتائج المستخلصة من مرحلة التحليل يمكن أن تؤدي إلى عمليات استحواذ إضافية، كل منها سيحتاج إلى تحليلات إضافية أخرى؛ وهذا نظرا لطبيعة بيئة التحقيق وخصوصيتها، وهو ما قد يستلزم في بعض الحالات تحقيق جنائي طويل الأمد.

2.2. إمكانيات الطب الشرعي الرقمي الإثباتية في القضاء الجنائي

الطب الشرعي الرقمي الذي يبحث في مجال الأدلة الرقمية هو مثال لدمج العلم مع القانون لحل مشكلة قانونية، وعلى هذا الأساس لا يمكن أن يتخلف أحدهما عن الآخر في التطبيق. فأفضل دليل علمي رقمي في العالم لا قيمة له من الناحية الإثباتية إذا كان غير مقبول في القضاء. لذلك تعترض الأدلة الرقمية كثير من العقبات والتحديات للوصول بها إلى أروقة المحاكم.

1.2.2. أهمية الطب الشرعي الرقمي في التحقيقات الجنائية

البيانات الرقمية في كل مكان حولنا ويجب جمعها بشكل روتيني في أي تحقيق. يمكن أن تكون الأدلة الرقمية مفيدة في مجموعة واسعة من التحقيقات الجنائية بما في ذلك جرائم القتل، والجرائم الجنسية، والمفقودين، وإساءة معاملة الأطفال، والاتجار بالمخدرات، والاحتيال وسرقة المعلومات الشخصية. أيضا، يمكن أن تتوقف القضايا المدنية على الأدلة الرقمية، وأصبح الاكتشاف الإلكتروني جزءا روتينيا من النزاعات

المدينة. يمكن أن تساعد السجلات المُحوسبة في تحديد وقت وقوع الأحداث، وأين كان الضحايا والمشتبه بهم، والأشخاص الذين تواصلوا معهم، وقد تظهر أيضا نية المشتبه بهم في ارتكاب جريمة.²²

وكمثال على ذلك أظهر تاريخ متصفح الويب لروبرت دورال Robert Durall's أنه بحث عن مصطلحات مثل "قتل + الزوج" و "حادث + وفيات" و "خنق" و "قتل" قبل قتل زوجته. تم استخدام عمليات البحث هذه لإثبات سبق الإصرار والترصد وزيادة التهمة إلى القتل العمد من الدرجة الأولى. في بعض الأحيان تكون المعلومات المخزنة على جهاز الكمبيوتر هي الدليل الوحيد في التحقيق. في إحدى الحالات، كانت رسائل البريد الإلكتروني هي الرابط الاستقصائي الوحيد بين القاتل وضحيته.²³

ومما تجدر الإشارة إليه أنه حتى ولو كانت البيانات الرقمية لا توفر صلة بين جريمة وضحيته أو جريمة ومرتكبها، إلا أنها يمكن أن تكون مفيدة في التحقيق الجنائي. فمثلا يمكن للأدلة الرقمية أن تكشف عن كيفية ارتكاب جريمة ما، أو تدحض أو تدعم إفادات الشهود، أو تحدد المشتبه بهم المحتملين.²⁴

2.2.2. تحديات الطب الشرعي الرقمي

أحد التحديات الكبرى اليوم ليس ما إذا كان الدليل الرقمي موجودا، ولكن مكان تخزين الأدلة، والوصول إلى هذا التخزين، وأخيرا، استعادة ومعالجة تلك الأدلة الرقمية من أجل ملاءمتها في ضوء دعوى مدنية أو جنائية ويمكن إجمال أهم التحديات ضمن النقاط الرئيسية التالية :

أ- الطبيعة الصعبة للأدلة الرقمية:

مثل الأدلة المادية، يواجه الدليل الرقمي العديد من التحديات، وهذه التحديات نابعة من خصائصه وطبيعته الخاصة:²⁵

- الدليل الرقمي هو نوع من الأدلة التي يصعب التعامل معها. على سبيل المثال يحتوي محرك الأقراص الثابتة على العديد من الأطباق، ويتكون كل منها من قدر كبير من البيانات الفوضوية والمضطربة، ومن الصعب جدا استخراج البيانات المتاحة منه.

- الدليل الرقمي هو تجريد لبعض الأشياء أو الأحداث الرقمية. على سبيل المثال، إذا تمّ استخدام الكمبيوتر لأداء بعض المهام، فلن تبقى جميع آثار هذه المهام، إلا أن القليل منها فقط يمنحنا عرضاً جزئياً لما حدث.
- الأدلة الرقمية عادة ما تكون ظرفية.
- إحدى المشكلات التي يواجهها المحققون هي أنه يمكن تغيير الأدلة الرقمية، أو حجبها، أو حذفها من قبل الجناة، أو حتى -بدون قصد- من قبل المحققين أثناء عملية التحقيق.

ب-التحديات المتعلقة بالتحقيق والمحققين الجنائيين :

- اتساع الفجوة بين مطوري التكنولوجيا والمحققين: المحققون والفاحصون وموظفو الاستجابة للحوادث والخبراء يميلون إلى الدخول في هذا المجال بخلفية في العلوم الاجتماعية، بينما يميل مطورو التكنولوجيا الرقمية إلى امتلاك خلفيات في علوم الكمبيوتر والهندسة؛ مما يؤدي ذلك إلى اختلاف نمط التفكير والنهج لحل المشكلات المعترضة في المجال الرقمي.²⁶

- تكلفة وتوافر الأدوات الجديدة: في الماضي ، كان المحققون يحملون معهم فقط حفنة من الأجهزة وأدوات البرمجيات لاستخراج الأدلة الرقمية والحفاظ عليها. اليوم لمعالجة مجموعة واسعة من الحالات التي قد يواجهونها ، قد يكون ما بين 30-40 منتجاً برمجياً software products ضرورياً لمجرد فقط إجراء عملية الاستحواذ perform acquisition والتحليل الأولي rudimentary analysis للمحتوى الرقمي لمسرح الجريمة. بالطبع هذه مجرد بداية لعملية التحقيق ويستمر عدد وتنوع الأدوات التحليلية في الازدياد. يمكن أن تكون التكلفة الحقيقية لامتلاك هذه التقنيات مذهلة، خاصة عندما نضع في الاعتبار التعليم والتدريب.²⁷

- عدم وجود بيئة للتعاون: يتمتع مجرمو الإنترنت بميزة التعاون غير المقيد فيما بينهم، إلى جانب الوصول إلى الموارد التي تساعدهم في تنفيذ الهجمات الضارة وقيامهم بأنشطة الجرائم الإلكترونية المعقدة. يحتاج المحققون ومطورو الأساليب والتقنيات الجديدة إلى نفس الميزة. وعلى ضوء ما سبق يتطلب الأمر منصة للتعاون

والتطوير المشترك والوصول إلى الابتكارات الجديدة التي يمكن تطبيقها مباشرة على الوضع الحالي²⁸.

ج-تحديات قانونية:

أحد العوائق الأساسية التي تحول دون حصول ممارسي الطب الشرعي الرقمي على الأدلة الرقمية خاصة من مواقع التواصل الاجتماعي، هو بعض القوانين. وكمثال على ذلك قانون the Stored Communications Act الذي يمنع الكشف عن المعلومات أو البريد الإلكتروني المخزن من قبل مزود خدمة الإنترنت.²⁹

خاتمة:

لقد خلاص هذا البحث إلى عدة نتائج، وعدة توصيات:

أولاً: أهم النتائج:

يساهم الطب الشرعي الرقمي بفعالية في خدمة نظام العدالة الجنائية لمواجهة الجرائم الرقمية، أو أي نظام آخر مثل الدفاع الوطني؛ لفهم الأدلة الرقمية، ومعالجتها من أجل ملاءمتها في ضوء دعوى مدنية أو جنائية.

- تاريخ الطب الشرعي الرقمي قصير مقارنة بتاريخ التخصصات العلمية الأخرى.
- الطب الشرعي الرقمي صار علماً راسخاً في التحقيقات الجنائية بما يملكه من أدوات وتقنيات، مكنته من حسن إدارة الأدلة الرقمية في مسرح الجريمة، وصولاً بها إلى المقبولة القانونية.

- يختلف الطب الشرعي الرقمي عن معظم علوم الطب الشرعي الأخرى؛ نظراً لطبيعة الأدلة الرقمية مجال بحثه، التي ليس لمادتها أي بنية بيولوجية أو فزيائية كما هو الشأن في الأدلة المادية الأخرى، بل ذات طبيعة خاصة فرضتها التكنولوجيا الرقمية.

- هناك فجوة معرفية هائلة في نظامنا القانوني والقضائي اليوم عندما يتعلق الأمر بالمسائل المتعلقة بالأدلة الرقمية. وللتدليل على ذلك أن معظم المشتغلين في المجال الرقمي من محققين ومحامين وقضاة... لهم خلفيات علوم اجتماعية دون أن يكون لهم إحاطة معرفية فنية متخصصة بعلوم الكمبيوتر والهندسة.

-تواجه فاعلية الطب الشرعي الرقمي الناشئ كثير من التحديات معظمها لها أساس علمي؛ أي: ناجمة عن التطورات في نطاق ووتيرة تكنولوجيا المعلومات. والبعض الآخر ذو طبيعة هندسية وهو ما يتطلب إنشاء برامج وأجهزة جديدة؛ لتمكين المحققين من جمع الأدلة الرقمية المحتملة والاحتفاظ بها وفحصها ومعالجتها من أجل ملاءمتها في ضوء دعوى مدنية أو جنائية. وبعض التحديات تتعلق بممارسي الطب وخلفيتهم الاجتماعية وكل هذه التحديات تؤثر على المقبولية القانونية، والقيمة الإثباتية لنتائج الطب الشرعي الرقمي.

ثانيا: أهم التوصيات:

-إن ضمان جودة إدارة الأدلة الرقمية في مسرح الجريمة ذات أهمية حيوية في التحقيق الجنائي. وهو ما يتطلب الاهتمام بهذا المجال في الدراسات الأكاديمية للمساهمة في إضاءة النقاش العام وتدعيم التفكير العلمي؛ لضمان المقبولية القانونية للأدلة الرقمية وانتاجيتها في تحقيق العدالة.

إن هذا لا يتأتى إلا من خلال رسم لافئة علمية لكل المعنيين؛ لجذب الأفضل والأدكى إلى وظيفة التحقيق في الجرائم الرقمية، فهذه السلالات الجديدة من الأدلة الرقمية لا تحتاج في معالجتها إلى الأدوات والتكنولوجيا فحسب، بل إلى وجود فكر رقمي-إن صح التعبير-له القدرة على البحث والاستحواذ والتحديد والتحليل والتقييم...كما يملك القابلية على مسايرة التطورات في مجال التكنولوجيا الرقمية، بل أكثر من ذلك يتمتع بميزة الافتراض التي تجعله مستشرفا لكل القضايا الرقمية.

- تواجه وكالات العدالة الجنائية في جميع أنحاء العالم حاجة متزايدة للتحقيق في الجرائم المرتكبة جزئيا أو كليا عبر الإنترنت أو وسائل الإعلام الإلكترونية الأخرى. وبالتالي، هناك حاجة متزايدة لتدعيم ممارسي الطب الشرعي الرقمي بموارد وأدوات جديدة للبحث الفعال عن جميع أنواع الأدلة الإلكترونية، وتحديد مكانها وحفظها ومعالجتها.

- ضرورة إنشاء منصة للتعاون الدولي المشترك لممارسي الطب الشرعي الرقمي من أجل تبادل الخبرات والتقنيات، والوصول إلى الابتكارات الجديدة التي يمكن تطبيقها مباشرة على الوضع الحالي الذي يشهد تطورات متسارعة في مجال الجرائم الرقمية.

الهوامش والمراجع:

- (1) تشير عبارة Chain of custody "سلسلة العهدة أو الاحتجاز أو الحراسة" إلى الطريقة التي تم بموجبها التعامل مع عناصر الأدلة التي يمكن استخدامها لأغراض قانونية. والغرض من الشهادة المتعلقة بسلسلة الاحتجاز هو إثبات أن الدليل لم يتم تغييره خلال جميع المراحل، لذا يجب أن تتضمن مسارا توثيقا بشكل صحيح لكيفية جمع الأدلة ونقلها وتحليلها وتقديمها إلى المحاكم.
- asmin Cosic and Zoran Cosic, Chain of Custody and Life Cycle of Digital Evidence, Computer Technology and Application, 3 (2012) p126.
- (2) John Sammons, The Basics of Digital Forensics- The Primer for Getting Started in Digital Forensics-,Elsevier, USA, Second Edition,2015,p2.
- (3) Martin S. Olivier ,Sujeet Shenoi, ADVANCES IN DIGITAL FORENSICS II, Springer, New York, USA,p68.
- (4) Ibid, p68.
- (5) Ibid, p4.
- (6) Eoghan Casey, Digital evidence and computer crime : forensic science, computers and the internet, Elsevier, USA, 3rd ed,2011,p xxv.
- (7) Ibid, p xxv.
- (8) Bruce Nikkel, Practical Forensic imaging: securing Digital Evidence with Linux Tools, No Starch Press, San Francisco, 2016,p1.
- (9) Ibid, p3.
- (10) Ibid, p4.
- (11) Eoghan Casey,p7.
- (12) Halil Ibrahim Bulbul, H. Guclu Yavuzcan, Mesut Ozel, Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM), Forensic Science International 233 (2013),p245.

- (13) Han-Chieh Chao, Shih-Hao Peng, Research of Digital Evidence Forensics Standard Operating Procedure with, Comparison and Analysis based on Smart Phone, International Conference on Broadband and Wireless Computing, Communication and Applications, 2011, p387.
- (14) Larry E. Daniel, Lars E. Danie, Digital Forensics for Legal Professionals- Understanding Digital Evidence From the Warrant to the Courtroom-, Elsevier, USA, p4.
- (15) Ibid, p4.
- (16) Ibid, p5.
- (17) Safiia Mohammed, AN INTRODUCTION TO DIGITAL CRIMES, International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.5, No.3, May 2015, p15.
- (18) Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Elsevier, USA, 2011, p3.
- (19) Ibid, p3.
- (20) John Sammons, The Basics of Digital, Forensics: The Primer for Getting Started in Digital Forensics, p8.
- (21) Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, p4
- (22) Eoghan Casey, p6.
- (23) Ibid, p6.
- (24) Ibid, p6.
- (25) Safiia Mohammed, p15.
- (26) Chet Hosmer, Python Forensics A Workbench for Inventing and Sharing Digital Forensic Technology, Elsevier, USA, p2.
- (27) Ibid, p2.
- (28) Ibid, pp4-6.
- (29) Larry E. Daniel, Lars E. Danie, p139.