دور التحليل الرقمي في مكافحة الجرائم.

The role of digital analysis in combating crimes.

أ.م.د عبد الخالق عبد الحسين سلمان- جامعة كربلاء/كلية القانون
abdulkhaleq.a@uokerbala.edu.iq
م . كاظم خضير محمد – جامِعة بابل / كلية القانون

الخلاصة.

صاحب التقدم التقني ظهور جرائم ألكترونية ومعلوماتية وبشكل مستمر فضلاً عن الجرائم التقليدية التي أصبحت ترتكب بالوسائل الألكترونية كذلك ، الأمر الذي يتطلب مواجهة جنائية تقنية أيضاً لكن هذا يحتاج إلى إمكانية تقنية وفنية بشأن اكتشاف الجرائم أوالحيلولة دون أرتكابها عن طريق تتبعها بالتحليل الرقمي ، فتقنيات التحليل الرقمي توفر أدوات سريعة ودقيقة لتحليل البيانات ، وهو ما يسهم في النهاية من تعزيز القناعة لدى الجهات التحقيقية والقضائية بشأن الأدلة الرقمية الناتجة عن طريق تحليل البيانات الرقمية بعد جمعها وحصرها وتوثيقها من قبل الجهات المختصة ووفقاً للقواعد القانونية والأوامر القضائية مع مراعاة الخصوصية والحرمة الشخصية لإصحاب هذه المحتويات خصوصاً بعد توسع الشبكة المعلوماتية ومنافسة العالم الرقمي للعالم التقليدي ، وهناك العديد من الأدوات والأنظمة الألكترونية التي تعين الجهات التحقيقية والقضائية في الوصول إلى مبتغاها وهذا يتطلب التحديث المستمر لخبرات هذه الجهات عن طريق الدورات والورش لمواكبة التطور العلمي فضلاً عن تشريع النصوص القانونية سواء أكانت موضوعية أم إجرائية للإستعانة بها في تحليل البيانات الرقمية وتعزيز القناعة القضائية بشأن مخرجات النتائج المتحققة من خلال تحليل البيانات والمعلومات الرقمية وهذا ماكان موضوعاً للبحث الذي تم التوصل في نهاية خاتمته إلى عددٍ من الاستنتاجات والمقترحات التي عسى أن تكون نافعة في المجال العلمي.

الكلمات المفتاحية: التحليل الرقمي . البيانات الرقمية . الذكاء الأصطناعي . الدليل الرقمي.

Abstract.

With the rapid technological advancements, electronic and cybercrime are continuously on the rise, in addition to traditional crimes being committed through electronic means as well. This necessitates a technological criminal response that relies on technical and technological capabilities to detect these crimes or prevent them through tracking using digital analysis . Digital analysis techniques provide fast and precise tools for data analysis, ultimately enhancing the confidence of investigative and judicial authorities regarding the digital evidence collected, documented, and authenticated by the relevant authorities in accordance with legal regulations and court orders. However, the privacy and personal rights of individuals must be considered, especially with the expansion of the information network and the increasing competition between the digital and traditional worldsSome numerous electronic tools and systems assist investigative and judicial authorities in achieving their goals, requiring continuous updating of the expertise of these entities through training courses and workshops to keep pace with scientific developments, as well as updating the legislation, whether substantive or procedural, for use in digital data analysis and enhancing judicial confidence in the results obtained. The research has addressed these points and concluded with findings and suggestions that may be beneficial in the scientific field.

Keywords: Digital analysis, Digital data, Artificial intelligence, Digital evidence.

المقدمة.

أولاً / فكرة البحث.

يتناول موضوع البحث تحليل البيانات والمعلومات الرقمية وما ينتج عنها من حجية تسهم في التصدي للأفعال والسلوكيات الاجرامية ، إذ يلعب التحليل الرقمي دورًا هامًا في مكافحة الجرائم من خلال توفير أدوات وتقنيات متطورة لتحليل البيانات التي تقود لكشف ومكافحة جرائم معلوماتية رقمية أو جرائم تقليدية عادية ، ومن ضمن هذه الوسائل والأدوات ، البيانات الموجودة على الهواتف المحمولة والذكية وأجهزة الحاسب الآلي ، والتي يمكن أن تساعد في فهم سلوك المتهمين من خلال تحليل البيانات الرقمية لفهم أنماط سلوكياتهم وتوقعاتهم . وقبل ذلك تحديد هوياتهم عن طريق تحليل السجلات التي تتضمن بياناتهم الشخصية وقوائم اتصالاتهم ، والرسائل النصية ، فضلاً عن النشاط على الشبكة المعلوماتية ، ومن هذه الإجراءات يتم جمع الأدلة واستخراج البيانات من الأجهزة الإلكترونية، مثل الصور ومقاطع الفيديو، لتقديم أدلة ذات حجية قوية لإثبات الأفعال الإجرامية عن طريق ربط الأدلة الرقمية بالمشتبه بهم ، ومن يقوم بأداء هذه الإجراءات يفترض فيه أن يكون على دراية عالية ومهارة فنية معرفية بتقنية المعلومات والإجهزة الرقمية فكيفية جمع وضبط البيانات الرقمية وما ينتج عنها من أدلة ألكترونية يُعد من الموضوعات المبتكره في بلدان العالم ، كما أن طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق ومحاكم الموضوع تعد من الموضوعات المهمة القانونية والعملية .

ثانياً / أهمية البحث .

للتحليل الرقمي دور مهم وأساسي في التعرض للأدلة عن الجرائم المرتكبة ، لكن لا تقف أهميته عند هذا الحد ، بل يساهم في منع ارتكاب الجرائم والأحتياط لذلك ، إذ يمكن استخدام تقنيات التحليل الرقمي للتنبؤ بالجرائم المحتملة ومنعها قبل وقوعها . أما عن مجالات أستخدام التحليل الرقمي ، فهو لا يقتصر على جرائم محددة وإن كان دوره يتسع ويضيق حسب نوع الجرائم ، ولكن بالأمكان أن يجد له حيزاً من التطبيق والفاعلية في جرائم عديدة كالتحقيق في الجرائم المعلوماتية منها الاحتيال الإلكتروني وسرقة البريد الألكتروني . كذلك تحليل المعلومات التي تُعد أدلة جنائية في الجرائم المالية ، ومنها جرائم غسيل الأموال وتمويل الإرهاب ، فضلاً عن الجرائم الجنائية العادية ، كجرائم القتل وجرائم الإيذاء. فهناك فوائد عديدة للتحليل الرقمي والذي يسهم في مكافحة الجرائم منها ، ضمان دقة التحقيق سواء أكان تحقيقاً أبتدائياً أم قضائياً والذي يسهم في تحقيق العدالة الجنائية . كما توفر تقنيات التحليل الرقمي أدوات سريعة ودقيقة لتحليل البيانات ، وهو ما يسهم في النهاية من تعزيز القناعة لدى الجهات التحقيقية والقضائية من إرتكاب الفعل الجرمي من عدمه وإصدار الاحكام والقرارات الجزائية المبنية على ثوابت رصينة .

ثالثاً / إشكالية البحث.

لابد من القول بأن التقدم التقني ينتج وبشكل مستمر جرائم جديدة تحتاج إلى إمكانية تقنية وفنية بشأن اكتشافها والحيلولة دون أرتكابها عن طريق تتبعها بالتحليل الرقمي ، وما يرافق ذلك من قصور تشريعي يقف عائقاً أمام المساحة المتوفرة للجهات التحقيقية والقضائية لأخذ دورها في مكافحة الجريمة وخصوصاً المعلوماتية منها ، ناهيك عن عدم وضوح الرؤيا كاملة بشأن حجية النتائج التي تستقى من تحليل البيانات الرقمية والمعلومات التي تنتجها الأجهزة الألكترونية ، فضلاً عن ذلك هناك العديد من التحديات التي تواجه استخدام التحليل الرقمي في مكافحة الجرائم ومنها حق الخصوصية ، إذ يجب مراعاة وحماية حق الخصوصية عند جمع وتحليل البيانات الرقمية ، والتحدي الأخر هو حجم البيانات والمعلومات التي تتطلب تقنيات التحليل الرقمي وهي بيانات بكميات هائلة ، مما قد يشكل عبئاً على أنظمة تكنولوجيا المعلومات. فضلاً عن ذلك أن التحليل الرقمي للبيانات يتطلب مهارات وخبرات شخصية يتمكن من خلالها الخبير الاستعمال الأمثل يتطلب للتقنيات التي يستلزمها التحليل الرقمي ، وما ينتج عنه من مخرجات تسهم في أثبات صدور الأفعال الإجرامية أو نفيها .

رابعاً/ منهجية البحث.

سيتم أتباع المنهج الإستقرائي للوقوف على ما يتم تبنيه وأتباعه من قبل الجهات المختصة في ضوء تتبع البيانات والمعلومات الرقمية للحصول على الدليل الرقمي ومدى حجيته في الإثبات في ضوء

القصور التشريعي مقارنة بالتطور التقني المتلاحق الذي يشهده العالم الرقمي مع الإستعانة بالمنهج الوصفي للوصول إلى حلول ناجعة يستعين بها القائمين بالتحقيق الإبتدائي والقضائي .

خامساً / خطة البحث.

لما تقدم سيتم تقسيم موضوع البحث على مبحثين ، يتناول المبحث الأول التعريف بدور التحليل الرقمي في مكافحة الجرائم إذ سيقسم على مطلبين يتطرق المطلب الأول إلى مفهوم التحليل الرقمي ، أما المطلب الثاني فسيتناول ادوات التحليل الرقمي ، أما المبحث الثاني فسيكون على مطلبين ، يتناول المطلب الأول فوائد ومعوقات التحليل الرقمي ، أما المطلب الثاني فسيترك لحجية الدليل الرقمي في الإثبات الجنائي .

المبحث الأول/ التعريف بدور التحليل الرقمي في مكافحة الجرائم.

يتمثل التحليل الرقمي في إستخدام الأدوات المادية والرقمية والإستفادة من التكنولوجيا الحديثة لجمع ودراسة الأدلة الرقمية ومن ثم الاستفادة منها في إثبات مختلف الجرائم أو نفيها .فيمكن للأجهزة الأمنية المعنية الحصول على البيانات الرقمية المطلوبة في تتبع الجرائم المرتكبة من خلال التحري والاستدلال عنها ، فضلاً عن ذلك أن التحقيق الجنائي الرقمي سواء أكان أبتدائي أم قضائي يمكن له الإستفادة من معلومات وبيانات أجهزة الحاسب الألي والهواتف المحمولة والبريد الإلكتروني وكافة الملفات الرقمية الأخرى في الحصول على الدليل الرقمي ، ولما تقدم سيقسم هذا المبحث على مطلبين ، يتناول الأول مفهوم التحليل الرقمي ، فيما يتطرق الأخر لادوات التحليل الرقمي .

المطلب الأول/ ماهية التحليل الرقمي في مكافحة الجرائم.

بعد التطورات الكبيرة التي تحققت في المجال التقني وظهور جرائم مستحدثة كثيرة بسبب هذا التقدم التكنلوجي وما تمتلكه الأجهزة الألكترونية من قدرة عالية في معالجة البيانات وسعة تخزين كبيرة للمعلومات فضلاً عن تصميم العديد من البرامج لمعالجة الكثير المسائل وبمختلف المجالات وهنا دخل العالم الرقمي كقوة فاعلة أخذت حيزاً لا يستهان به مقارنة بالعالم التقليدي ولضخامة المعلومات والبيانات وما يرتكب عن طريقها من أفعال جرمية برزت أهمية التحليل الرقمي لهذه المنظومة المعلوماتية ، ولما تقدم سيقسم هذا المطلب على فرعين يكون الأول منهما لتعريف التحليل الرقمي فيما يترك الثاني لدور التحليل الرقمي في العلوم الجنائية .

الفرع الأول/ مفهوم التحليل الرقمي في مكافحة الجرائم.

تعد تقنية المعلومات من أبرز الابتكارات التي غيرت وجه العالم بشكل جذري في السنوات الأخيرة [1] . ومع تزايد استخدام التكنولوجيا في جميع جوانب الحياة، فإنها لم تترك القانون الجنائي دون أثر من جانبه الإجرائي فكان للتحليل الرقمي دوراً في أكتشاف الجرائم أو توفير الأدلة الرقمية لإثباتها أو نفيها . وعرف التحليل الرقمي هو العملية التي يتم من خلالها تقييم المعلومات الواردة في فيديو، أو صورة، أو مستند ، أو بيان للتأكد من صحتها وصدقها [2] . فالتحليل الرقمي هو عملية استخراج ومعالجة البيانات الرقمية الموجودة في الأجهزة الإلكترونية للكشف عن الأدلة والمعلومات المهمة في التحقيق الإبتدائي أو القضائي [3] ، إذ يسهم التحليل الرقمي في ترشيح البيانات الموجودة في الأجهزة الرقمية مثل الحاسب الآلي والهواتف المحمولة ، ووسائط التخزين الأخرى فيتم ترشيح البيانات بعد فهرستها ، وهذا الحال ينطبق حتى على المعلومات المحذوفة أو المخفية بعد استرجاعها ومن ثم تحويلها إلى بيانات قابلة للفهرسة والتحليل . إذاً التحليل الرقمي وهو عملية جمع وفرز وترشيح للبيانات الرقمية الموجودة على الأجهزة الإلكترونية والحواسيب والشبكات والهواتف الذكية وغيرها، ويتم ذلك باستخدام الأدوات الخاصة بالتحليل الرقمي ، فضلاً عن تحليل البيانات المستخرجة لتحديد الأدلة المتعلقة بالجرائم ويتمثل ذلك في تحليل الصور ومقاطع الفيديو، والرسائل النصية والبريد الإلكتروني، وسجلات المكالمات، والتنقيب عن البيانات، واستخلاص المعلومات الرقمية الهامة [4] .إضافة إلى التحقق من الأدلة الرقمية [5] ، إذ يتم التحقق من صحة وموثوقية الأدلة الرقمية المستخرجة لضمان قبولها كأدلة قانونية في المحاكم ، الأمر الذي يتطلب القدرة على تقييم صحة البيانات وتحليلها والتأكد من أنها لم تتم تزييفها أو تعديلها.

ولتحقيق النتائج المرجوة من التحليل الرقمي لابد من التعاون المشترك بين المحققين الرقميين وخبراء الأمن السيبراني وعلماء الحوسبة الرقمية يتعاونون معاً لتحليل البيانات وتفسيرها واستنتاج النتائج المهمة.

وباستخدام التحليل الرقمي، يتم تعزيز فعالية التحقيقات الجنائية وتحسين جودة الأدلة المقدمة ، بالإضافة إلى ذلك يستخدم المحقق الرقمي تقنيات مخصصة لإسترداد البيانات لجمع الأدلة ومن ثم تحليلها ، إذ يهدف التحليل الجنائي الرقمي إلى جمع البيانات الرقمية وترتيبها وفرزها لتأكيد أو نفي وجود الجريمة [6] . وهنا تتاح الفرصة للجهات التحقيقية ومن خلال خوارزميات التصنيف وخوارزميات التنبؤ (التنبؤ بالجريمة) في تحديد المشتبه بهم والمسؤولين عنها [7] . بعبارة أخرى فإن ما يميز التقنيات الحديثة في هذا المجال هو قدرتها على تحليل وفهم البيانات الرقمية بشكل أسرع وأكثر فعالية .

الفرع الثاني/ علاقة التحليل الرقمي بالعلوم الجنائية.

توجد العديد من العلوم الجنائية التي تعرضت لدراسة أسباب أرتكاب الجريمة كظاهرة أجتماعية ودراسة شخصية مرتكب الفعل الإجرامي ، فضلاً عن أبتكار الوسائل التي تحد من الجريمة أو تقلل نسب الإجرام ومن ما تقدم لابد من تناول علاقة التحليل الرقمي ببعض العلوم الجنائية .

أولاً- علاقة التحليل الرقمي بعلم النفس الجنائي.

لاشك فأن هناك علاقة وثيقة بين علم النفس الجنائي والتحليل الرقمي [8] ، إذ يمكن استخدام علم النفس لتحليل البيانات الرقمية ومن ثم الحصول على الأدلة الرقمية ويكون ذلك بعدة طرق. وهي من خلال دراسة السلوك البشري والعمليات المعرفية ، مثل رسائل البريد الإلكتروني ومنشورات وسائل التواصل الاجتماعي والنشاط عبر الإنترنت، أن توفر نظرة ثاقبة لسلوك الشخص وأفكاره وعواطفه. ومن خلال تحليل هذه البيانات الرقمية باستخدام المبادئ النفسية ، يمكن للمحققين الحصول على فهم أفضل للحالة العقلية للشخص وربما تحديد علامات الخداع أو المشكلات النفسية الأخرى ، بالإضافة إلى ذلك يمكن استخدام التقنيات النفسية مثل تحليل المحتوى وتحليل المشاعر . ويمكن استخدام علم النفس الشرعي لتحليل البيانات الرقمية من خلال فحص سلوك ودوافع الأفراد الذين يتفاعلون مع الأجهزة الرقمية ، إذ يمكن أن يشمل ذلك تحليل أنماط الاتصال الرقمي والنشاط عبر الإنترنت وملفات تعريف الوسائط الاجتماعية لتحديد المشتبه بهم المحتملين أو مرتكبي الأنشطة الإجرامية . ويمكن لخبراء النفس الشرعي استخدام البيانات الرقمية لتقييم مصداقية الشهود والضحايا، وكذلك لفهم الدوافع النفسية وراء الجرائم الإلكترونية والسلوك الإجرامي الآخر [9] . بالإضافة إلى ذلك، يمكن لعلماء النفس الشرعي المساعدة في تطوير بروتوكولات جمع وتحليل المعلومات والبيانات الرقمية [10].

ويدور تساؤل عن كيفية استخدام علم النفس في تحليل البيانات الجنائية الرقمية ؟ .

لابد من القول أن استخدام علم النفس في تحليل الطب الشرعي الرقمي بعدة طرق [11]. ومن ضمن ذلك أنه يساعد في فهم سلوك الأفراد الذين يتركون بصمات رقمية ، مثل أفعالهم ودوافعهم وعمليات تفكيرهم . ويكون مفيدًا في تحديد المشتبه بهم المحتملين، وتتبع تحركاتهم عبر الإنترنت، وتحليل أنماط اتصالاتهم الرقمية. فضلاً عن ذلك يمكن استخدام علم النفس لتحليل الحالة النفسية للأفراد الذين يتركون أدلة رقمية ، مثل حالتهم العاطفية ، وقدراتهم المعرفية ، وسماتهم الشخصية . ويمكن أن يساعد هذا في تحديد مصداقية الأدلة الرقمية، فضلاً عن احتمال تورط الفرد بإرتكاب أفعال إجرامية .

ثانياً- علاقة التحليل الرقمي بعلم الاجرام .

علم الجريمة هو دراسة أسباب الجريمة وتفهم مصادرها والدوافع إليها والعمل على مكافحتها [12] ، ويمكن استخدامه لتحليل البيانات الرقمية من خلال فحص أنماط ودوافع وسلوكيات المجرمين الذين يستخدمون التكنولوجيا لارتكاب الجرائم ، ويمكن أن يشمل ذلك فحص البيانات مثل الاتصالات الإلكترونية ونشاط وسائل التواصل الاجتماعي والنشاط عبر الإنترنت لتحديد السلوك والأنماط الإجرامية. فضلاً عن تحليل المعلومات الرقمية باستخدام طرق مختلفة مثل استخراج البيانات ، والتعرف على الأنماط ، وخوارزميات التعلم الآلي لتحديد وتتبع النشاط الإجرامي . بالإضافة إلى ذلك ، يستفاد من علم الجريمة لتطوير استراتيجيات لمنع ومكافحة الجرائم السيبرانية .

ثالثاً- علاقة علم البصمات بالتحليل الرقمي.

هناك رابطة وثيقة بين علم البصمات بالتحليل الرقمي [13] ، إذ تساعد التكنولوجيا في تعريف البصمات الرقمية [14] ، والتي تعتبر أنماطًا فريدة من نوعها يتركها الأفراد أثناء استخدامهم للتكنولوجيا الرقمية. إذ يمكن استخدام البصمات الرقمية في تتبع الأنشطة على الإنترنت وربطها بالمشتبه بهم ، ومن ثم تسهم التقنية في تحديد هوية المشتبه بهم وربطهم بأنشطة جنائية محتملة. ويعمل القضاء على توظيف هذه التقنية لتعزيز الكشف عن الجرائم وتحقيق العدالة. ومن ضمن أنماط البصمات بصمات الأصابع ، إذ تستخدم لتحليل البيانات الرقمية من خلال تحديد الخصائص الفريدة لجزء معين من المعلومات الرقمية أو الملفات الألكترونية . وتتضمن هذه التقنية مقارنة الأنماط أو الخصائص الفريدة ضمن الأدلة الرقمية لتحديد أصلها أو مصدر البيانات . ويمكن إجراء بصمات الأصابع على أنواع مختلفة من البيانات الرقمية بما في ذلك رسائل البريد الإلكتروني والمستندات والبرامج . وتُستخدم هذه التقنية غالبًا لتتبع مصدر جزء من الأدلة الرقمية ، أو إثبات صحة مستند ما ، أو التعرف على أصل برنامج حاسوبي .

رابعاً- علاقة التحليل الرقمي بعلم وظائف الأعضاء.

وتتمثل بالعديد من الأنماط ومنها الكشف عن الجناة وتتضمن هذه الطريقة تحليل الخصائص الفسيولوجية للشخص [15] ، مثل صوته أو وجهه أو أنماط كتابته ، لتحديد ما إذا كان شخصًا حقيقيًا أو روبوت دردشة يعمل بالذكاء الاصطناعي [16] ، والأخرى ديناميكيات ضغطة المفاتيح ، وتتضمن تحليل التوقيت والضغط المطبق عند الكتابة على لوحة المفاتيح لاكتشاف التناقضات أو الشذوذات المحتملة في سلوك الكتابة. والنمط المهم الأخر تحليل التوقيع ، ويتضمن هذا الطريق تحليل الخصائص الجسدية لخط يد الشخص أو توقيعه للتحقق من هويته ، والوسيلة اللأحقة تتبع حركة العين: وتتضمن هذه الطريقة تحليل حركة العين ، فالتقنيات الحديثة لها القدرة على تحليل العينين لتحديد ما إذا كان الشخص الموجود في الفيديو حقيقياً أم لا .

المطلب الثاني/ ادوات التحليل الرقمي.

عند الكشف على محل الحادث والأطلاع على مسرح الجريمة يواجه المحقق الجنائي عدداً من العلامات البصرية والأشياء التي قد تفيد التحقيق والوصول على مرتكبي السلوك الإجرامي ، وتتولد على الأقل معلومات أولية عن الفعل الإجرامي ، وهنا تدخل التحليل الرقمي في الوقت الحاضر للتعرف على محتويات ما يلتقطه القائم بالإجراءات التحقيقية من صور أثناء معاينة مسرح الجريمة أو تحليل للمواد والأشياء التي عثر عليها والتي قد تقود إلى كشف الحقيقة وهذا في العالم الواقعي كذلك الحال في العالم الأفتراضي عبر الإجهزة الألكترونية والشبكة المعلوماتية برزت الأهمية الكبيرة للتحليل الرقمي من خلال التعرض للبيانات والمعلومات الألكترونية . فالتحليل الرقمي أداة فعالة في مكافحة الجريمة من خلال مساعدة القائم بالتحقيق في الكشف عن الأنماط والروابط بين المعلومات المسجلة في قواعد بيانات الأجهزة الامنية المخولة باتخاذها والحصول عليها ، ولما تقدم سيتم تناول ممهدات التحليل الرقمي وأدواته كلاً بفرع مستقل .

الفرع الاول/ ممهدات التحليل الرقمي.

تشير أدوات تحليل البيانات الرقمية في علم الجريمة إلى البرامج المستخدمة لفحص ومعالجة [17] وتحليل هذه البيانات الرقمية المجدية في التحقيقات الجنائية ، ويمكن لهذه الأدوات استرداد البيانات وتحليلها من الأجهزة الرقمية مثل أجهزة الحاسوب والهواتف المحمولة والأجهزة الإلكترونية الأخرى [18] وقبل تحليل البيانات والأنشطة لابد من تهيئة وتوفير الممهدات لتحليل البيانات والمعلومات ومن ثم المرور عبرها وهي عبارة عن مراحل أو إجراءات لابد من تجاوزها للحصول على الأدلة الرقمية .

أولاً :- جمع المعلومات الداعمة لاثبات او نفي الجريمة وتعد من اهم الاجراءات التي تخص جمع المعلومات والادلة من الاجهزة الرقمية باساليب متفق عليها مسبقاً لضمان سلامة الادلة من خلال إجراء التفتيش [19]، ولغرض جمع المعلومات لابد ابتداءً من أتخاذ الأتي :

1- البحث عن الجدوى من هذا الجمع [20] ، وفيما إذا كان للعنصر الرقمي المعني صلة ظاهرة بتحقيق معين. وتعتمد جدوى أي عنصر على محتواه ومصدره وعلى أهداف التحقيق والعناصر المعروفة عن

الوضع . وفي مراحل التحقيق المبكرة، قد يصعب معرفة العناصر المجدية ، وهو أمر قد يدفع المحققين إلى الافراط في جمع المعلومات بيد أن المحققين المتخصصين في المصادر المشروعة ينبغي أن يكونوا قادرين على إيضاح السبب الذي يحملهم على الاعتقاد بأن العنصر المعني قد يكون مفيداً وتسجيل هذا التقييم .

2– الموثوقية

ينبغي على المحققين المتخصصين أن يوثقوا البيانات الرقمية بمحاضر إجراءات قبل عملية الفحص والتحليل له وكذا توثيق طريقة ضبطها والوسيلة المستخدمة في ذلك ومكان حفظها وما تتصف به [21] ، وأن يحددوا إن كانت المعلومات أو الادعاءات المذكورة في المحتوى أولى باستعراض المحتوى الرقمي تبدو موثوقة للوهلة الإولى عن المعلومات السياقية الواردة في الملف وتقييمه ، ويمكن أن يشمل ذلك التحقق من البيانات الوصفية المضمنة ، وينبغي أن تتضمن هذه والمعلومات المرتبطة والمصدر أصلي، وهو أمر يقتضي العملية محاولة لتحديد مصدر المادة التي تتبع مصدر البيانات المنشورة على الانترنت، أو الجهة التي قامت بتحميلها أو مؤلفها.

3– الازالة

يجدر بالمحققين المتخصصين في ضبط البيانات وتوثيقها أن يضعوا احتمال إزالة البيانات الرقمية من الانترنت . وحين تكون إزالة المحتوى محتملة، يجب أن يبين في محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزمHash 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 [22] ، مع جمع أوثق صيغة معروفة من المحتوى حتى أثناء إجراء مزيد من التحقيق في صيغ سابقة أو أفضل. ويمكن تقييم احتمال إزالة المحتوى باستخدام عدة عوامل من بينها هوية المصدر وموقع المحتوى وتوافق المحتوى مع شروط خدمة مقدم الخدمة .

4- سلامة الموقع الألكتروني

ينبغي على المحققين المتخصصين في المصادر المفتوحة أن يحددوا إن كان جمع العنصر الرقمي آمناً أو يستدعي اتخاذ احتياطات إضافية ، ويرجح أن يثير جمع البيانات مخاوف إن تم من موقع شبكي قد يحتوي على عناصر تم افسادها من شأنها أن تلحق الضرر بالنظام الداخلي ومن صوره البحث في السجلات الألكترونية ، ويعني ذلك البحث عن السجلات العامة و الحكومية والتجارية المتعلقة بالمستخدم ، والبحث عن المعلومات الموجودة على المواقع الإلكترونية ومنصات التواصل الاجتماعي. إضافة إلى ذلك التصوير والفيديو: فالتقنيات المتقدمة للتصوير والتسجيل تعتبر أدوات قوية في عمليات التحقيق الجنائي والقانوني [23] ، فالتسجيلات المصورة ومقاطع الفيديو يمكن أن تكون أدلة قوية في حالات الجرائم، وتوفر دلائل فيديو واضحة وموثوقة بفضل التكنولوجيا المتقدمة، يمكن تحسين جودة الصور والفيديوهات واستخلاص التفاصيل الدقيقة التي يمكن أن تدعم التحقيقات وتثبت الحقائق .

ولما تقدم وعلى سبيل المثال عندما يدور سؤال عن ماهية الأدلة الرقمية التي يمكن الحصول عليها في قضايا الاختلاس ، فهنا لابد من البحث عن رسائل البريد الإلكتروني والبيانات المصرفية وسجلات الحاسب وسجلات المعاملات لإثبات سرقة الأموال ، ويمكن أن تظهر هذه السجلات تحويل الأموال، ووقت وتاريخ المعاملات ، وهوية الأفراد المعنيين. بالإضافة إلى ذلك يمكن أيضًا استخدام البصمات الرقمية مثل ، منشورات وسائل التواصل الاجتماعي وعمليات البحث عبر الإنترنت وبيانات الموقع لدعم الحالة من المهم ملاحظة أن الأدلة الرقمية المحددة المطلوبة في قضية الاختلاس قد تختلف اعتمادًا على وقائع القضية وظروفها.

ثانياً:- الوسائل المتاحة لجمع البيانات والمعلومات الرقمية : وتشمل بعض الأساليب الشائعة منها :

1- تصوير الطب الشرعي: يتضمن ذلك إنشاء نسخة طبق الأصل من وحدة تخزين الجهاز الرقمي للحفاظ على الأدلة الأصلية.

2- التسجيل: يتضمن ذلك تسجيل نشاط النظام والأحداث التي تحدث على جهاز رقمي ، فمثلاً السوار الإلكتروني يسمح لجهة التحقيق تحديد تفاصيل الزمان والمكان الذي يجب أن يكون فيها المتهم ، ومن خلال ذلك، يتم ضمان تحفظ حقوق المتهم بشكل محدود وفقًا للقانون. ويُتاح للمتهم الحرية المشروطة بارتداء السوار الإلكتروني بدلاً من البقاء في الحبس المؤقت، مما يسمح له بالتنقل بحرية محددة في أوقات محددة وفقًا للشروط المحددة في القانون ، وتعد هذه التقنية إجراءً مبتكرًا يستفيد من تكنولوجيا الإعلام والاتصال لتحسين إجراءات التحقيق الجنائي وتطبيق العدالة ، ويعد استخدام السوار الإلكتروني بديلاً للحبس المؤقت بمثابة خطوة نحو تحقيق توازن بين حماية المجتمع وحقوق المتهمين [24] .

أما المحادثة المرئية : فبالأمكان استخدامها عن بعد في مرحلة التحقيق الجنائي ، إذ يُسمح لجهات التحقيق استخدامها في حالات توفر مقتضيات حسن سير العدالة، أو الحفاظ على الأمن أو الصحة العامة، أو أثناء الكوارث الطبيعية، أو لاحترام مبدأ الأجال المعقولة، مع احترام الحقوق والقواعد التنظيمية .

يعطي هذا الإجراء جهات التحقيق القدرة على إجراء المحادثات والاستجوابات عن بُعد باستخدام تكنولوجيا المحادثة المرئية، مما يوفر مرونة أكبر وتوفير للوقت والجهد في إجراءات التحقيق الجنائي. ويساهم استخدام المحادثة المرئية عن بعد في تيسير التواصل مع المشتبه بهم والشهود المحتملين وتسهيل جمع الأدلة اللازمة للتحقيق.

3- إزالة التكرار: يتضمن ذلك مقارنة البيانات من مصادر متعددة لتحديد المعلومات المتداخلة أو المكررة التي يمكن استخدامها كدليل.

4- أصبح التصوير والفيديو من العناصر المهمة في عمليات التحقيق الجنائي والقانوني ، إذ يتم استخدام التصوير والفيديو لجمع الأدلة في مواقع الجرائم والمشاهد القانونية الأخرى. ويمكن توثيق الأدلة المادية، مثل الآثار والأشياء المعنية بالجريمة، من خلال التصوير الفوتوغرافي . كما يمكن تسجيل الفيديو للشهود والمشتبه بهم والأحداث المرتبطة بالجريمة.

ثالثاً : فحص المعلومات والبيانات التي تم جمعها تمهيداً لتحليلها لاحقاً. فمثلاً البصمات الرقمية تعتبر أنماطًا فريدة من نوعها تتركها الأفراد أثناء استخدامهم للتكنولوجيا الرقمية ، وعن طريقها يتم :

1- التحقق من الهوية : تستخدم البصمات الرقمية لتحديد الهوية الرقمية للمتهم ، إذ يتم تخزين بصمات الأصابع أو الوجه أو بصمات العين في قواعد البيانات الرقمية للمقارنة والتحقق من هويته فضلاً عن الأفراد الأخرين .

2- ربط الأنشطة الرقمية : يمكن استخدام البصمات الرقمية لربط أنشطة الأفراد على الإنترنت وتتبعها. على سبيل المثال يمكن ربط بصمة الأصبع بالأنشطة التي تمت على الهاتف الذكي مثل الرسائل النصية أو المكالمات الهاتفية .

3- التحقيق الأبتدائي : فيمكن استخدام البصمات الرقمية كأدلة في التحقيقات الجنائية ،عندما يتم العثور على آثار بصمات رقمية على جهاز أو في موقع جريمة، يمكن استخدامها لتحديد المشتبه بهم وربطهم بالجرائم المحتملة.

4- حماية البيانات الشخصية : يعد استخدام البصمات الرقمية كطريقة للتحقق والوصول إلى الأنظمة والأجهزة والحسابات الشخصية أكثر أمانًا من كلمات المرور التقليدية ، فهي تعزز حماية البيانات الشخصية وتقلل من فرص الاختراق والاستخدام غير المصرح به.

5- تحليل الفيديو: يتطلب التحقيق الجنائي تحليل الفيديو لاستخراج المعلومات المهمة كتحديد الأشخاص والأنشطة والتوقيتات المرتبطة بالجرائم ويستخدم الخبراء أدوات وتقنيات مثل ، تحليل الحركة وتحليل الوجوه وتحسين الصورة لاستخلاص المعلومات القيمة.

الفرع الثاني/ التقنيات المستخدمة في التحليل الرقمي.

تعرف أنظمة التحليل الرقمي في مجالها الجنائي (Digital Forensics): بإنها عملية يتم بها الربط بين العلم الجنائي وعلوم الحاسوب والشبكات من خلال أجهزة الحاسب والشبكات وانترنت الأشياء والوسائط الرقمية ينتج على أثرها أدلة رقمية لوقائع إجرامية وقعت [25] ، ويستخدم في هذه العملية جميع البيانات المتوفرة لدى جهات إنفاذ القانون كقوائم الأشخاص المشتبه بهم أو الإرهابيين أو المبلغ عنهم في

قضايا أخرى والجهات الأخرى كالصحية والاجتماعية ، ويهدف التحليل الجنائي الرقمي للحفاظ على الأدلة الرقمية وتحديدها والحصول عليها وتوثيقها لاستخدامها في المحاكم . وحتى يمكن الحصول على نتائج مرضية ودقيقة كأدلة رقمية واجراء التحقيق في تلك الجرائم لابد من القيام بعدة عمليات وهي حفظ البيانات، استخراجها، تحديدها وتشخيصها بدقة، ومن ثم تحليلها، وانتهاءً بكتابة التقرير النهائي ولتنفيذ تلك الخطوات او العمليات يستوجب وجود ادوات فعالة لتسهيل مهام الجهات التحقيقية والقضائية ومن هذه الادوات :-

أولاً: ProDiscover Pro : تعمل تلك الاداة على جمع البيانات ومعلومات الاتصال بمنصات التواصل الاجتماعي باستخدام (RemoteAgent™) ، فضلاً عن تحديد الملفات والأقسام المخفية فهي أداة مهمة في مراحل الدعوى الجزائية من خلال مراحل الالتقاط والحفظ والتحليل وإعداد التقارير[26].

ثانياً : Autopsy Sleuth Kit: تمتلك هذه الأداة العديد من المهام منها تحليل السجلات والبريد الالكتروني ولها امكانية دعم انظمة الاندرويد ، ويمكن دمجها مع المكتبة الرقمية لطيف واسع من أدوات الطب الشرعي والاستخدام المباشر وإصدار الأوامر للعثور على الأدلة الثبوتية التي تتعلق بالجريمة ، فضلاً عن تحليل صور القرص واستعادة مميزات الملفات كما توفر للمحقق امكانية تحليل كمية كبيرة من بيانات النظام ، ويتم استخدامه على نطاق واسع من قبل وكالات إنفاذ القانون، الفاحصين العسكريين وكذلك الشركات تسمح هذه الاداة بدمج وحدات إضافية لتحليل الملفات ومعرفة المحتويات وبناء الأنظمة الآلية[27].

ثالثاً: Magnet Axiom: تتميز هذه الأداة بامكانية فحص البيانات مفتوحة المصدر وبيانات حساب المستخدم من المصادر السحابية مثل (WhatsApp) (Google) ، وما الى ذلك من تطبيقات التواصل الاجتماعي وقدرة الاكتشاف تلقائيًا للصور المحتملة ان تكون محتوى غير مشروع وفق جداول زمنية محددة لضمان سرعة التحقيق مثل ، إساءة معاملة الأطفال والمخدرات والأسلحة باستخدام أدوات التعلم الآلي والذكاء الاصطناعي ، كما تمتلك هذه القدرة على استرداد وتحليل البيانات الخاصة بأي قضية تحتاج الى التحقق في مكان واحد ، فضلاً عن قدرتها على فحص البيانات الرقمية من مصادر متعددة مثل الهاتف المحمول والسحابة والحواسيب والمركبات الذكية، جنبًا إلى جنب مع عمليات الاستخراج التابعة لجهات خارجية، كل ذلك في ملف حالة واحد ، كما يمتلك القدرة على كشف التاريخ الكامل لملف أو اي دليل اخر لبناء القضية وإثبات النية وتوفير الدعم الفني لأحدث الأجهزة والمصادر[28].

رابعاً: Belkasoft Evidence Center X : من مزايا هذه الاداة لها القدرة في الحصول على البيانات الرقمية المتنوعة بطريقة مشروعة من الناحية الجنائية من مجموعة واسعة من الأجهزة المحمولة وأجهزة الحاسوب وتحليلها، تشغيل مهام تحليلية متنوعة، إجراء عمليات بحث على مستوى الحالة ، وضع علامات مرجعية على العناصر، وانتهاءً بإنشاء التقارير[29].

خامساً: Redline: يمكن لـ (Redline) إجراء التدقيق وجمع الادلة الخاصة بالعمليات المشغلة وبرامج التشغيل بمختلف انواعها من الذاكرة ، نظام الملفات البيانات التعريفية، بيانات التسجيل، سجلات الأحداث، معلومات الشبكة، الخدمات والمهام وسجل الويب ، فهي عبارة عن مجموعة أدوات توفر إمكانات الجهات الأمنية والتحقيقية للعثور على علامات النشاط الضار من خلال تحليل الذاكرة والملفات وتطوير ملف تعريف لتقييم التهديدات ، كما تدعم هذه الاداة العديد من اصدارات انظمة التشغيل مثل ويندوز XP، ويندوز فيستا، ويندوز 7، ويندوز 8 (32 بت و64 بت)، وويندوز10 [30].

سادساً: FTK: تتميز بسرعتها في البحث والتقصي عن اي معلومة تتعلق بالتحقيق في الأفعال الإجرامية ، وهناك العديد من مكاتب المحامات والهيئات الادارية تستخدم هذه الاداة علماً ان هذه الأداة أُنشأت من قبل (Access Data Group) كوسيلة لتسهيل مهمة التحقيق ، وتتركز مهامها في فحص أجهزة الحاسوب والشبكات والهواتف المحمولة ، كما تمتاز ايضاً بالعديد من المزايا الأخرى منها (توفير بيانات الشبكات، نقل البيانات، الكشف عن الادلة، النسخ الصوري للقرص الصلب، استعادة كلمات المرور).

سابعاً: X-Ways Forensics : تعد بيئة عمل متقدمة لجهات التحقيق في الجرائم المعلوماتية والألكترونية ، وتمتاز هذه الاداة بقابلية الوصول الى الاقراص الصلبة والسرعة لاكتشاف الملفات

المحذوفة ، فهي تعتمد على قواعد بيانات بسيطة وسهلة التعامل . كما تمتلك العديد من المميزات الأخرى منها استعادة كلمات المرور وسهولة الوصول إلى الصور والبصمات ومعلومات الفايلات، فضلاً عن استنساخ الاقراص الصلبة .

ثامناً: EnCase: تعد هذه الاداة من الادوات المهمة بالتحقيق في الجرائم الالكترونية وتستخدم من قبل الجهات التحقيقية والقضائية بنسبة 90 بالمائة لقدرتها على اعادة بناء البيانات وتحليل القرص واستعادة كلمات المرور - للتاكد من دقة الادلة - بالاضافة امتلاكها واجهة برمجة التطبيقات (API) الكاملة التي تتيح أتمتة مهام التحقيق ورفع قدرة الجهات التحقيقية ، كما تتميز بتحليل البيانات وللعديد من الاجهزة بشكل أسرع بنسبة تصل إلى 75 بالمائة من الادوات المنافسة ، وهو ما تم إثباته في الاختبارات العملية للباحثين باستخدام ملفات الأدلة الواقعية [31].

تاسعاً : نظام بيس ، طور الباحثين عملية تقييم عدد المشاركين في الجريمة من خلال العينات المأخوذة في مكان الحادث ، ويعتمد هذا النظام على خوارزميات تمكنت بعد معالجة آلاف العينات التي تحتوي على بصمات وراثية، من تمييز العينة التي تحتوي على بصمتين وراثيتين لشخصين وبين غيرها التي تحتوي على ثلاث بصمات وراثية [32] . وفي السياق ذاته قد تساعد آثار حبوب اللقاح أو الطلقات النارية المأخوذة من نعل الحذاء في إثبات وجود المشتبه به في مسرح الجريمة ، وعندما يبحث رجال الشرطة عن مفقودين أو قتلى، قد يعثرون في بعض الأحيان على شظايا عظام، وربما لا يتمكنون من مضاهاتها بعينة الحمض النووي ، لتحديد هوية الأشخاص هي تقنيات التعرف على الوجوه والتي قد تقود في الوصول إلى مرتكب الفعل الإجرامي .

ويقول أحد أساتذة التفاعل بين البشر والحاسب الآلي ، إن الخوارزميات يمكنها أيضا العثور على روابط محتملة بين القضايا الجنائية من خلال البحث السريع في قواعد بيانات الأجهزة التحقيقية ، وبهذا تنبه عناصر الأمن المعنية إلى أنماط ارتكاب الجرائم أو تشابه الأدلة أو أطراف الجريمة [33] .

عاشراً- نظام فالكري، إذ تم تطوير التحليل البصري في مجال البحث الجنائي ، وهذا النظام يستخدم الآن في تحليل بيانات فعلية من قاعدة بيانات الأجهزة الأمنية في أوروبا ، وقد يساعد في كشف ملابسات جرائم حقيقية بعد شهور من الآن . وقد عكف على تطوير نظام لتحليل الصور بإمكانه حصر عدد الجسيمات المجهرية التي عُثر عليها في نعل حذاء المشبه به ، مثل بقايا طلق ناري أو حبوب لقاح ، لتحديد الفترة التي كان فيها المشتبه به موجودا في منطقة معينة ، لكن البعض يرى أنه لن يكون من السهل التثبت من استنتاجات الذكاء الاصطناعي، إما لأنه ملك خاص لشركات بعينها قد لا ترغب في إفشاء أسرارها، أو لأن الجهاز معقد إلى حد يستحيل معه إثبات استنتاجاته ، وهذا قد يعوق استخدام هذه التقنيات على نطاق واسع [34].

وفي مجال الطب الشرعي، قد تغير هذه الآثار الدقيقة مجرى التحقيقات تماما، حيث يكون لتحليل الحمض النووي على سبيل المثال أثر كبير في مجال التحقيقات الجنائية .

احدى عشر –نظام تحديد هوية الجمجمة .

لقد طور أحد الباحثين ، نظاما يجري مسحاً ثلاثي الأبعاد لبضعة شظايا من الجمجمة ويجمعها رقميا فيما يشبه تجميع قطع الأحجية غير المكتملة. وقد تدرب النظام، بعد معالجة عدة جماجم بشرية مختلفة الأشكال والأبعاد، على ملء الفراغات بمستوى معقول من الدقة ، كما طور ذات الباحث خوارزمية عالجت صور آلاف الأشخاص للعثور على الوجه الأقرب لشكل الجمجمة التي أعاد النظام تشكيلها ، إذ يقوم النظام بتركيب آلاف النماذج ثلاثية الأبعاد لكل جمجمة مجهولة الهوية، ثم يختار من بينها النموذج الذي يطابق شكل الجمجمة تماما. وفي حالة وجود اختلاف بين النموذج ثلاثي الأبعاد للوجه وبين الجمجمة، يصحح النظام الفوارق ويعدل النموذج حتى يطابق ملامح وجه المجني عليه المحتمل . قد يكون من الصعب التعرف على هوية الجثة من شظايا العظام، لكن ثمة طرقا جديدة تعتمد على الذكاء الاصطناعي لإعادة تشكيل وجه الضحية من بقايا جمجمته [35] . ولا تزال هناك تساؤلات حول مدى دقة هذه التقنيات على المدى الطويل. صحيح أن الأنظمة المبنية على الذكاء الاصطناعي أثبتت أنها أسرع من الطرق التقليدية وأكثر كفاءة منها في التجارب محدودة النطاق ، لكنها ستواجه اختبارا فعليا عند استخدامها

في القضايا الحقيقية. إذ سيكون على الأجهزة الأمنية إثبات مدى مطابقتها للمعايير القانونية والأخلاقية قبل الإشادة بفوائدها في مجال التحقيقات الجنائية.

اثنا عشر: نظام ماركوف .

يتمثل في عملية تحكم عشوائية ذات وقت منفصل تستخدم لنمذجة صنع القرار في مشاكل التحسين عند عدم التيقن، فتقنيات اتخاذ القرارات (Decision Making Techniques): هي نموذج يعزز من القدرة على اتخاذ القرارات الحاسمة والتعامل الأمثل مع الأمور الغامضة في وقت قصير وقياسي ، وذلك من خلال تحليل العمليات الحسابية المكثفة التي توافرت لدى التقنية من خلال مواقف مختلفة سابقة وما النتائج التي ترتبت على تلك المواقف لتقديم قرارات الأفضل وأدق وتقليل نسبة الخطأ في نتائج هذه القرارات، وهناك العديد من التطبيقات التي تؤثر وتساعد الذكاء الاصطناعي على اتخاذ القرارات منها النظم الخبيرة والشبكات العصبية ، وهذه التطبيقات تتميز بقدرتها على معالجة البيانات والاشارات وتقديم الحلول التقنية المبنية على الخبرات السابقة والدمج بين المشاركة التقنية والمشاركة الإنسانية المتمثلة في الخبرات السابقة في مكان واحد مما يعود بالأثر على القرارات التي يتم اتخاذها، وكذلك تراقب جودة المخرجات للقرارات الصادرة من التقنية، والقدرة على التنبؤ بالمتغيرات التي قد تحدث في مجالات عديدة [36] .

المبحث الثاني/ الأطار الموضوعي للتحليل الرقمي.

يعد التحليل الرقمي أمرًا بالغ الأهمية في علم الجريمة ، لأنه يساعد في تحديد المجرمين وتعقبهم من خلال بصماتهم الرقمية. وتزايدت هذه الأهمية مع تطور التكنولوجيا والاتصالات الرقمية ، فغالبًا ما يترك المجرمون وراءهم سلسلة من البيانات الرقمية التي يمكن تحليلها واستخدامها لكشف الجرائم المرتكبة ، إذ يساعد تحليل البيانات الرقمية في تأكيد الأعذار ، وتقديم الأدلة للمحاكم ، ويمكن استخدامه أيضًا لمنع إرتكاب الجرائم واكتشافها من خلال مراقبة النشاط الرقمي للأنماط والاتجاهات إلا أن ذلك لا يخلو من صعوبات وتحديات . ولما تقدم سيتم تناول هذا المبحث على مطلبين يتناول الأول فوائد ومعوقات التحليل الرقمي ، فيما يتطرق الثاني لحجية نتائج التحليل الرقمي .

المطلب الأول/ فوائد ومعوقات التحليل الرقمي.

بعد التوسع الذي شهده العالم الأفتراضي والرقمي وإلغاء الحدود التقليدية المعروفة بسبب ظهور الشبكة المعلوماتية وتوسعها وتطورها المستمر وما رافق ذلك من ظهور جرائم جديدة ترتكب في العالم الإفتراضي فضلاً عن أرتكاب الجرائم التقليدية بالوسائل التقنية أصبح من الواجب واللأزم على الجهات التحقيقية والقضائية أن تواكب هذا التطور التكنلوجي ومواجهة الجرائم بذات الوسائل التي ترتكب بها أو أكثر تطوراً ، وهنا برزت الأهمية البالغة في التعرض للبيانات الرقمية وتحليلها للوصول مرتكبي الجريمة أو الحيلولة دون تنفيذ الفعل الإجرامي المشروع ، ولكن تبرز في ضوء ذلك تحديات كبيرة قد تعرقل الوصول إلى نتائج مرضية أو تؤخر الحصول عليها ، وهذا ماسيبحث على فرعين .

الفرع الأول/ فوائد التحليل الرقمي.

للتحليل الرقمي فوائد عديدة يمكن تناولها على شكل فقرات :

أولاً: تحليل العادي للبيانات مهما كان حجمها فمن مزايا التحليل الرقمي اداء عمليات المعالجة والتحليل المجراة على البيانات الضخمة [37] بشكل فعال في الجرائم الرقمية مما يساعد في اكتشاف الأنماط والاتجاهات غير الطبيعية والتي يمكن أن تكون مفيدة في التحقيق .

ثانياً: التحليل التنبؤي : إن قدرة التنبؤ الكبيرة التي تقدمها التقنيات الحديثة سوف تكون مساندة في اتخاذ القرار المرتبط بإعادة بناء مسرح الجريمة ، فقد تم تطوير نموذج الشبكة البايزية (أو شبكة القرار) Bayesian networks للتنبؤ بنوع القضية من خلال المدخلات (البيانات والمعلومات الرقمية)، وذلك للمساعدة في حل قضية ما . ويُعرف نموذج الشبكة البايزية بأنه نموذج رسومي احتمالي يمثل مجموعة من المتغيرات وتبعياتها الشرطية عبر رسم بياني دوري موجه، وهو نموذج مثالي للتنبؤ بالاحتمالات. فعلى سبيل المثال، يمكن للشبكة أن تمثل العلاقات الاحتمالية بين الأمراض والأعراض، وكذلك العلاقات الاحتمالية بين الأدلة ونوع الجريمة. ويتكون النموذج المطور من ثلاث طبقات، وهي الفرضية

والسيناريو والأدلة . فضلاً عن القدرة على استخدام نماذج التعلم الآلي لتحليل السلوكيات الرقمية يساعد في توقع الأنشطة المستقبلية واكتشاف الأنماط المشبوهة ، الامر الذي يساعد المؤسسات وشركات استشارات الطب الشرعي الرقمي والشركات الخاصة بتحديد مدى التزام المؤسسات بسياسات الامن السيبراني في اداء مهامها وابداء المشورة بشكل دقيق [38] .ويمثل الذكاء الاصطناعي هنا وظيفة تنظيم وترتيب العمل الأمني وتحليل البيانات والمعلومات ومعالجتها والقيام بالبحث والتقصي في مخازن البيانات في العالم الرقمي وأنظمة المعلومات بناء على الآلية التي تم تحديدها له والتقنية المحددة له في مجاله الأمني، والخروج بتوصيات لاتخاذ قرار صائب بنسبة كبيرة ودقيقة من خلال تقديم المعلومات للجهات الأمنية وكلما كان المجال التقني والأمني للجهة متطوراً بشكل كبير مع تطور التقنيات التكنولوجية كإنترنت الأشياء، كلما أثمر ذلك في القرارات والنتائج التي يقدمها الذكاء الاصطناعي لأفراد الجهات الأمنية مما يساهم في الحد من الجرائم ومكافحتها، فقد أثبتت التجارب على أن هذه التقنيات تقدم خدمات كبيرة وتساهم أيضا بمكافحة الجرائم وتقلل من الوقت المهدر للجهود البشرية في البحث والتحليل والتقصي عن الأدلة [39] .ولكون البيانات الضخمة بالعالم الرقمي تحمل في جنباتها أدلة رقمية ستبقى آثارها مهما حاول إتلافها ، ولكن ذلك لا يمكن اكتشافه مع تأخر الجهات الأمنية في تطوير أساليبه التقنية والاستفادة منها في مكافحة الجرائم وذلك من خلال ربط التقنية بين أعمال مكافحة الجرائم والبيانات الضخمة وجعلها من أبواب البحث عن أدلة رقمية للجرائم المرتكبة ، تكون هذه العملية منذُ بداية مرحلة البلاغ وإتاحت خيار تقديمه إلكترونياً وعبر تطبيقات تابعة وتحت جهات إنفاذ القانون ويتم تطويرها وتحديثها بشكل دوري ويتم بعد ذلك مرور البلاغ في مراحل تدقيق وتصفية لتأكد من صحته وعدم كونه بلاغاً كيدياً ، وبعدها في حال التثبت تتم مرحلة البحث والاستدلال عن معلومات البلاغ والمشتبه بهم ومقدم البلاغ وجمع أكبر قدر ممكن من المعلومات والبيانات عنهم وتتم على أثرها مرحلة المقارنة والتنقيب والتحليل وجمع الأدلة الرقمية وفحصها من قبل الذكاء الاصطناعي مما يساهم في تسريع وتيرة إنجاز البلاغات بأوقات قصيرة والبدء في مراحل التحقيق والمواجهة مع توفر الأدلة الرقمية والمعلومات المهمة عن الواقعة الإجرامية والمشتبه بهم ومحل الاشتباه، وجميع هذه المراحل تكون في فترة زمنية أقصر من الفترة الزمنية التي يستغرقها العنصر البشري في جمع كافة هذه المعلومات [40] .

ثانياً: التعرف على الصورة والصوت: بالامكان استخدام تقنيات التعرف على الصور والصوت التي تعتمد على الذكاء الاصطناعي في عمليات البحث والتحقق في الادلة (متعددة الوسائط) وهذا يمكن أن يساعد في تحليل الملفات كالصور ومقاطع الفيديو والصوت، ومن ثم توفير معلومات ذات قيمة قانونية تخدم الجانب التحقيقي وقد تدمج هذه التقنيات مع التطبيقات ومنصات الطب الشرعي الرقمي لزيادة فاعليتها.

رابعاً: التحليل اللغوي: يمكن للذكاء الاصطناعي فهم وتحليل اللغة الطبيعية، مما يساعد في فحص الرسائل الإلكترونية، وسجلات المحادثات، ووسائل التواصل الاجتماعي لاكتشاف أدلة قد تكون ذات صلة بالجريمة الالكترونية .

خامساً: الروبوتات الذكية: يمكن استخدام الروبوتات الذكية لتنفيذ المهام البسيطة والمتكررة في التحقيقات الجنائية الرقمية بشكل اوتوماتيكي مما يساعد في تحرير المحققين للعمل على مهام أكثر تعقيدًا.

سادساً: أمان البيانات: الذكاء الاصطناعي يمكن استخدامه لتعزيز أمان البيانات وحمايتها من التلاعب، والوصول غير المصرح به، وهو أمر حيوي للحفاظ على صحة وسلامة الأدلة الرقمية.

سابعاً: تسريع التحقيقات: باستخدام تكنولوجيا الذكاء الاصطناعي، يمكن تسريع عمليات التحقيق بشكل كبير من خلال التحليل الذكي للبيانات وتحديد المعلومات الرئيسية بسرعة.

ثامناً: التعاون بين الأنظمة: يمكن للذكاء الاصطناعي تعزيز التفاعل بين مختلف أنظمة التحقيق الجنائي، مما يسهم في مشاركة البيانات مع الجهات ذات العلاقة وتحسين فعالية التحقيق.

الفرع الثاني/ معوقات التحليل الرقمي.

تواجه عمليات التحليل الرقمي تحديات ومخاطر وهذه بالإمكان أن يتطرق لها بفقرات كالأتي :

أولا: معوقات تتعلق بالبيانات والمعلومات الرقمية : وهذه تتمثل بتعقيد الأجهزة الرقمية وتشفير البيانات وتزايد حجم البيانات الرقمية الهائل. إذ أن هذا التضخم يجعل من الصعب على المحققين تجميع وتحليل

هذه البيانات بشكل فعال وفي وقت قصير وتزداد الصعوبات إذا صاحب ذلك حالات تلاعب في برامج الحاسبات [41] . وعن تزوير البيانات الرقمية. يجب على المحققين الرقميين أن يكونوا على دراية بأحدث التقنيات والأدوات والإجراءات القانونية للتعامل مع هذه التحديات.ولكون البيانات الضخمة بالعالم الرقمي تحمل في جنباتها أدلة رقمية ستبقى آثارها مهما حاول إتلافها ولكن ذلك لا يمكن اكتشافه مع تأخر الجهات الأمنية والتحقيقية في تطوير أساليبه التقنية والاستفادة منها في مكافحة الجرائم ، وتزداد الصعوبة في رؤية البيانات الرقمية فالجريمة المعلوماتية ترتكب في العالم الافتراضي ، والذي بدوره تكون فيه الأدلة عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية في شكل بيانات أو معلومات رقمية وهذا ما يثير إشكال جمع وتحليل الدليل الرقمي لعدم إمكانية رؤيته ومن ثم لابد من التعامل مع البيانات والمعلومات الرقمية بشكل صحيح وعدم التلاعب بها أثناء التجميع والنقل. إذ قد تتعرض إلى التغيير أثناء جمعها وتخزينها مع المحو والتدمير .

ثانياً : تجدر الإشارة إلى أنه من المعوقات التي تواجه الجهات التحقيقية هو ملاحقة مرتكبي الجرائم المعلوماتية لأنهم يلجؤون إلى إخفاء هوياتهم الخاصة عند استخدام شبكة الأنترنت من خلال استعمال العديد من البرامج والتطبيقات التي تعمل على إخفاء الهوية في شبكة الأنترنت .وهنا تبرز الحاجة الجادة والماسة إلى المعرفة المتخصصة والمعدات اللازمة للتجميع والتحليل ، واحتمال سوء تفسير أو سوء استخدام البيانات من قبل المحققين أو الخبراء . والأمر الذي قد يكون مكلفًا من الناحية المالية ، والحاجة إلى الصيانة المستمرة وصيانة أنظمة تخزين الأدلة الرقمية مع الحاجة إلى تدريب متخصص للعاملين في مجال إنفاذ القانون والقانون في مجال جمع البيانات الرقمية وتحليلها. فضلاً عن ذلك برزت تقنيات عديدة تشكل تحدياً كبيراً في العالم الرقمي ، وهنا هل يمكن للجهات المختصة في مجال التحقيق الرقمي مجابهتها ، ومن ضمن التقنيات الجديدة المثيرة للشبهة وهي تقنية التزييف العميق (deepfake) وتعرف هذه التقنية deepfake بأنها تطبيق من التطبيقات الحديثة في المجال الرقمي إذ تكمن خطورة هذه التقنية في قدرتها على صنع فيديوهات وصور مزيفة عبر تقنيات رقمية متطورة . إذ تقوم هذه التقنية على محاولة دمج عدد من الصور ومقاطع الفيديو لشخصية ما من أجل إنتاج مقطع فيديو جديد. وقد يبدو للوهلة الأولى أنه حقيقي للغاية لكنه في واقع الأمر مزيف حيث تعرض هذه الفيديوهات أشياء غير حقيقية ولم تحصل إطلاقا بطريقة مقنعة غير قابلة للشك [42] .ولكن رغم هذه القدرة على تزييف الحقائق إلا انه يمكن استخدام العديد من التقنيات لكشف الفوارق بين مقاطع الفيديو الحقيقية وتلك التي تم إنشاؤها باستخدام تقنية (deepfake). فالتقنيات الحديثة لها القدرة على تحليل الوجوه وحركات الفم والعينين وأيضاً الحركة العامة للجسم لتحديد ما إذا كان الشخص الموجود في الفيديو حقيقياً أم لا. فعن طريق بعض التقنيات مثل تحليل البيانات العصبية يمكن تحليل النمط العصبي في الصور والفيديوهات لتحديد ما إذا كانت تعاني من عمليات تلاعب. وأيضاً عن طريق بعض العيوب التي قد تتركها تقنية ال (deepfake) . على سبيل المثال يمكن أن تظهر بعض الخطوط غير الطبيعية أو الانحناءات في المناطق التي تم التلاعب بها إذ يمكن للذكاء الإصطناعي ملاحظة وكشف هذه العيوب [43] .

وبذلك يواجه التحقيق الجنائي في العالم الرقمي تحدي الابتكار التقني [44] ، إذ تشهد التكنولوجيا الرقمية تطوراً سريعاً يحتم على الجهات التحقيقية الجنائية الرقمية أن تبقى على إطلاع دائم على التطورات والإبتكارات التقنية الجديدة . وبذلك يجب أن تتوفر لدى المحققين والفنيين المهارة الكبيرة والدراية الكافية في التعامل مع هذا النوع من البيانات والمعلومات [45] ، وفي ذات السياق إن تنوع الأجهزة مع التطبيقات الهائل يعد أيضاً تحدياً للتحقيق الجنائي الرقمي ، إذ يعتمد هذا المجال على الوصول إلى مختلف أنواع الأجهزة والتطبيقات الرقمية . ومن ثم فإن التنوع الكبير لهذه الأجهزة والتطبيقات - مع تطور طرق إرتكاب الجرائم لتشمل التهديدات الإلكترونية المتقدمة التي تهدد الأفراد والمؤسسات على حد سواء- يزيد من صعوبة المهمة على عاتق المحقق الجنائي الرقمي . وهنا تبرز أهمية التقنيات الحديثة التي يمكن ان تكون حليفاً قوياً لهذا المجال ،فلها دور حاسم في إستمرارية عمل الجهات التحقيقية والقضائية في العالم الرقمي ونجاحها .

بالإضافة لما تقدم تبرز التحديات الأخلاقية ومدى أحترام الحق في الخصوصية أمام عمل الجهات المخولة والمكلفة في جمع وتتبع البيانات الرقمية ومن ثم تحليلها [46] ، فتطرح التقنيات الحديثة تساؤلات أخلاقية حول مشروعية استخدامها في التحقيقات الاستقصائية ، مثل مدى قانونية جمع البيانات واستخدامها بدون موافقة ، ومن ثم يجب أن يكون لدى الجهات المعنية معرفة كاملة في اخلاقيات استخدام أدوات التحليل الرقمي [47] .

ثالثاً: المعوقات الأخرى التي تعترض التحليل الرقمي ما يتعلق بالتشريع [48] . فعلى المستوى الدولي، فهو من أبرز المعوقات التي تواجه الدول في حصر وتنظيم موضوع الجرائم المعلوماتية هو القصور التشريعي [49] ، مما جعل هذه الدول تعمل على إعادة وتحديث منظومتها القانونية عن طريق تعديل قوانينها الإجرائية أو إصدار قوانين جديدة تتماشى مع التطور العلمي والتكنلوجي الحديث وما نتج عنه من جرائم معلوماتية يحتاج لإثباتها الحصول على البيانات الرقمية ومن ثم تحليلها للوصول إلى المتهمين بإرتكاب هذا النوع من الجرائم .

المطلب الثاني/ حجية نتائج التحليل الرقمي.

بعد تحليل البيانات والمعلومات الرقمية يمكن أن يستخلص من هذه العملية أدلة مهمة تساعد في منع أرتكاب الجرائم أو كشف أرتكابها ومعرفة مرتكبيها ، ولهذه الأدلة أهمية في مراحل الدعوى الجزائية وكما هو معلوم أن هذه المراحل مرتبطة بعضها مع بعض وتعد كل مرحلة مكملة للمرحلة التي تسبقها .

الفرع الأول/ دور نتائج التحليل الرقمي في مرحلة التحقيق.

لتكنولوجيا المعلومات دورًا حاسمًا في استخراج وتحليل النتائج الرقمية . فباستخدام التكنولوجيا، يتمكن المحققون من استخلاص البيانات من الأجهزة الرقمية مثل الهواتف الذكية والحواسيب ووسائط التخزين الأخرى والتي تُعد أدلة رقمية - كما عدتها قوانين بعض الدول [50] - كالبصمات الرقمية (عناوين IP والطوابع الزمنية والسجلات) ورسائل البريد الإلكتروني وتطبيقات المراسلة ومنشورات وأنشطة وسائل التواصل الاجتماعي بيانات الهاتف المحمول (سجلات المكالمات والرسائل النصية والموقع) ، لقطات الدوائر التلفزيونية المغلقة وتسجيلات كاميرات المراقبة و الطب الشرعي الرقمي (استعادة البيانات وتحليل الملفات والبيانات الوصفية) ، أدلة الأمن السيبراني (البرامج الضارة والفيروسات ومحاولات القرصنة) ، المستندات والملفات الإلكترونية (Word وPDF وExcel). فنتائج التحليل الرقمي ذو طبيعة تقنية ، إذ يتم التعامل معها من قبل مختصين في العالم الإفتراضي ومع توسع قاعدة التحليل الرقمي ، يمكن لهذا الأخير أن يشمل أنواعا متعددة من المعلومات والبيانات الرقمية والتي بدورها تصلح أن تكون دليل جنائيا على إحالة المتهم الى محكمة الموضوع بشرط أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه ، وفق لنطاق لصلاحية جهة التحقيق [51] ، مع عدم تغيير أو تحديث أو محو أو تحريف الكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة للمعلومات أو البرامج أو الدعامات الإلكترونية وغيرها. ويشمل ذلك استخدام تقنيات مثل Write Blocker وDigital Images Hash وغيرها من التقنيات المماثلة التي تحافظ على سلامة وثبات البيانات والمعلومات المستخرجة أو المأخوذة، بحيث لا يتم تغييرها أو تحديثها أو محوها أو تحريفها أو إتلافها [52] ، فالأدلة الرقمية هي نتاج لتزايد إستخدام تقنية المعلومات الرقمية [53] ، بعد أن أصبح كل من الحاسب الألي و شبكة الأنترنت يشكلان موطنا هاما للبيانات و المعلومات الرقمية ، وإن كانت البيانات والمعلومات الرقمية يصعب إتلافها أو التخلص منها ، ففي حالة محاولة إزالة ذلك فمن الممكن إعادة إظهاره من خلال ذاكرة الالة . والأمر المهم في نتائج التحليل الرقمي هو مشروعية استخلاصها . وهو شرط أساسي لقبول النتائج المتحققة كدليل إثبات ، ويقصد بمشروعية النتائج أن يكون الإجراء الذي تحصل منه المحققون عليها يتفق مع القواعد القانونية التي تحكمه [54] ، أو بمعنى آخر ضرورة اتفاق الإجراء الذي تم الحصول من خلاله على النتائج الرقمية مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع ، وبذلك فالحصول على النتائج الرقمية مختلف في البحث عنها عن الوسائل التقليدية ، لأن شرطها الأول هو مشروعية الحصول عليها أي أن تكون وسائل وأدوات الاستدلال والتفتيش بأنظمة الحاسب الآلي أو شبكة الأنترنت تمت بشكل مشروع ، والشرط الثاني هو ضمانة الحفاظ

عليها من التلاعب وهذا يكون من خلال الخبراء وأن المحافظة على ذلك تتطلب مهارة وكفاءة في التعامل مع عناصر الجريمة ، وأطرافها [55] . واستخلاصها دون إكراه كممارسة الإكراه المادي أو المعنوي من أجل فك شفرة الحاسوب الخاص به مثلا ، للوصول إلى ملف البيانات المخزنة، أو التزوير المعلوماتي أو التجسس المعلوماتي، وكذلك الاستخدام غير المصرح بالتنصت والمراقبة الإلكترونية [56] ، وإلا كانت غير مشروعة وعليه لا تصلح لتكوين قناعة محكمة التحقيق ومن ثم إحالة الدعوى لمحكمة الموضوع لغرض إجراء المحاكمة وإصدار الحكم .

الفرع الثاني/ دور نتائج التحليل الرقمي في مرحلة المحاكمة.

إذا أدت نتائج التحليل الرقمي إلى تكوين أدلة رقمية أقتنعت بها محكمة التحقيق يتم إحالة الدعوى على محكمة الموضوع لغرض إجراء المحاكمة وإتخاذ مايلزم لإصدار الحكم الجزائي . ومن المبادئ المهمة التي يجب على محكمة الموضوع الإلتزام بها هي بلوغ اقتناعها الى درجة اليقين. ومعناه ذلك أن يكون اقتناع المحكمة مبني على الجزم واليقين لا على الشك والاحتمال [57] ، وذلك لأن قرينة البراءة لا يمكن دحضها إلا عند بلوغ المحكمة درجة الجزم واليقين الذي لا يشترط فيه أن يكون مطلقا بل بصفة نسبية يتحقق معها تكوين المحكمة لعقيدتها التي يبني عليها حكمها القضائي [58] ، ولكن ليس المطلوب هنا الاقتناع الشخصي لمصدر الحكم فقط ، بل أيضا اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل في ذاتها معالم القوة في الاقناع ، ويتحقق هذا اليقين من خلال مناقشة النتائج الرقمية المستخلصة من البيانات والمعلومات التي يجب أن يكون لها أساس ثابت في أوراق الدعوى وتطرح للمناقشة أمام الأطراف كافة بعد أطلاعهم عليها [59] . وهنا لابد من معرفة سلطة محكمة الموضوع في قبول نتائج التحليل الرقمي ومن ثم حسم الدعوى الجزائية بناءً عليها . ابتداءً لابد من القول أن أحد المبادئ القانونية الثابتة هو القناعة القضائية والمتمثلة بحرية المحكمة في تقدير نتائج التحليل الرقمي التي تُعد أدلة علمية مستخلصة بوسائل تقنية ، فالمعطيات والتوجه القضائي يشير إلى أن دلائل الإثبات الرقمية يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي [60] ، إلا أن القناعة يجب أن تكون منطقية وغير مبناة على التصورات الشخصية للمحكمة سواء أكانت قاضي فرد أم هيأة ، ففي حالة اعتمادها على أساليب ينكرها المنطق السليم، فإنه يعرض حكمها للنقض. وعليه فقيمة النتائج الرقمية تخضع لمعيارين يتمثل الأول في أن تكون هذه النتائج يجيزها القانون أي يسمح للمحكمة أن تستند أليها في تكوين عقيدتها ، أما المعيار الثاني فهو أن تتوافر شروطها التي تضفي عليها المشروعية . وبذلك فأن مبدأ حرية المحكمة في قبول نتائج التحليل الرقمي وهي أدلة علمية هو أساس التبرير بالوسائل العلمية، بحيث يحق لها قبول أي نتائج رقمية مشروعة تكتسب يقينا، وإن كانت هذه النتائج مستمدا من الوسائل العلمية الحديثة ، وبالرغم من أن المحكمة حرة في اختيار أي دليل، فإن هذا لا يعني أنه قادرة على إصدار أحكام مطلقة ، بل هناك حدود يجب احترامها والضمانات التي يمنحها القانون ومنها تسبيب الأحكام وطرق الطعن أمام المحاكم العليا التي تُعد رقيباً على محكمة الموضوع . تمثل الأدلة الرقمية مصدرًا هامًا في عمليات التحقيق الجنائي الإبتدائي والقضائي وهذا ما حاز تأييد وثقة أغلب الفقه الجنائي لإعتمادها على قواعد علمية وحسابية دقيقة [61] ، فلتكنولوجيا المعلومات دورًا حاسمًا في استخراج وتحليل البيانات الرقمية نظراً لوضوحها ودقتها في إثبات أو نفي أرتكاب الفعل الإجرامي وعلاقته بالجاني أوعلاقة الجاني بالمجني [62] . فباستخدام التقنية الرقمية ، تتمكن الجهات المختصة من استخلاص البيانات من الأجهزة الرقمية مثل الهواتف الذكية والحواسيب ووسائط التخزين الأخرى. وبدوره تنتج الأدلة الرقمية التي لها كلمة الفصل في الدعوى الجزائية مع مراعاة الخصوصية وحرمة الشخصية بالتعامل معها بالسرية التامة وضمان عدم استغلالها أو تلاعبها بشكل غير قانوني [63] .

الخاتمة.

بعد الأنتهاء من تناول موضوع البحث الموسوم (دور التحليل الرقمي في مكافحة الجرائم) فقد تبين من ذلك عدداً من الأستنتاجات والمقترحات التي يمكن تلخيص أهمها بما يأتي :

أولا/ الإستنتاجات.

1- صاحب التطور التقني نشوء أفعال إجرامية بعضها مجرم قانوناً والأخر يحتاج إلى تشريعات خاصة فضلاً عن التعقيدات التي تصاحب الجرائم المعلوماتية والتي تتطلب من المشرع الجنائي تحديث النصوص القانونية لتتوافق مع التكنولوجيا الحديثة وتوفر الحماية اللازمة للأفراد في العالم الرقمي .

2- إستحالة عمل الجهات التحقيقية والقضائية إن لم يكن لها إلمام بالتقنيات الحديثة لفهم لغة اجهزة الحاسوب وطبيعة الجريمة والفرد الذي يتعامل معه ، وفهم ماينتج عنها من مخرجات لتحليلها والتي تشكل دليلاً رقمياً يتمتع الدليل الرقمي بمجموعة من الخصائص جعلته يتميز عن باقي الأدلة الجنائية .

3- هناك ثمة معوقات تكتنف التحليل الرقمي في المكونات الإلكترونية ، سواء من حيث طرق الحصول عليها أو من حيث طبيعتها ويحتاج لعمليات فنية وعلمية معقدة ، وطبيعتها قد تكون غير مرئية كالذبذبات والنبضات، إضافة إلى أنها من السهولة بمكان إخفائها بالتشفير وكلمات المرور السرية.علاوة على الجانب الأخلاقي وما يرتبط به من حماية حق الخصوصية وحرمتها .

4- هناك قصور في التشريعات الإجرائية فيما يخص إجراءات التحليل الرقمي وإقتصارها على القواعد العامة ومازال هناك الكثير يخضع للنصوص التقليدية مما يؤدي الى تزايد الصعوبات في الحصول على مخرجات التحليل .

5- الاثبات الجنائي مهم وتطور بالنسبة للجرائم المعلوماتية وعلا شأن الأدلة الرقمية في ضوء التقنيات الحديثة وما تشهده من تطور سريع ومستمر .

6- تمثل تقنيات تحليل البيانات مرحلة هامة من مراحل تطورنظم وتقنية المعلومات والاتصالات، والعبرة في أهمية هذه التقنيات هي الاستفادة منها من خلال توظيفها، في الحصول على نتائج إيجابية من تحليل البيانات التي يمكن الاعتماد عليها في اصدار الاحكام الجزائية .

7- تساعد تقنيات التحليل الرقمي على تحليل البيانات واستخلاص النتائج في تطوير وتحسين أداء الجهات التحقيقية والقضائية ، كما يساهم التحليل الجنائي الرقمي في استخلاص الادلة الرقمية والمحافظة عليها .

ثانياً / المقترحات.

1- ندعو لتخصص الجهات التي تتولى التحقيق والفصل خصوصاً في الجرائم المعلوماتية هذا يتأتى بعقد دورات وورش تدريبية لمنتسبي هذه الجهات وتحديداً المختصين بالتحري والتحقيق وفقاً للتقنيات الحديثة ومجال استخدامها في العالم الرقمي لتأهيلهم من الناحية الفنية التقنية.

2- من فائدة العملية والعلمية توثيق روابط التعاون بين الجهات التحقيقية والقضائية من جهة والجهات الأكاديمية التقنية من جهة أخرى في مجال تبادل الخبرات والمعلومات التكنلوجية لما للبيانات الرقمية من أهمية بالغة في إيجاد الأدلة الرقمية التي تجد لها مساحة في التطبيق ايضا في الجرائم التقليدية .

3- الإستعانة بقواعد إجرائية داعمة لأساليب التحري والتحقيق لإعداد الدليل الرقمي وعلى نحو يكفل توفير سلطات ملائمة وكافية لجهات المختصة مع كفالة احترام حقوق وحريات الافراد.

4- ضرورة النص صراحة في قانون الجرائم الألكترونية - عند تشريعه- على نتائج التحليل الرقمي وعدها أدلة رقمية تتمتع بالحجية القانونية في إثبات أو نفي أرتكاب الجريمة .

5- بعد تطور الوسائل والإجهزة التقنية أصبح من اللازم إنشاء قاعدة بيانات الأفراد تضم بيانات خاصة لكل فرد ومنه صور شخصية ، فصيلة الدم ، بصمة شحمة الأذن ، الحمض النووي مع وضع النصوص القانونية الكفيلة بعدم حيدة تلك البيانات عن أغراضها، وأن تكون سرية وألا تستخدم الا في الأغراض المحددة لها .

الهوامش.

([1]) عرفتها الإتفاقية العربية لمكافحة جرائم تقنية المعلومات في نص المادة الثانية من الاتفاقية بأنها " أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفق للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكي أو لاسلكي في نظام أوشبكة" .

([2]) الأمم المتحدة ، مكتب حقوق الأنسان ، بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة المصدر ، ص61

([3])Ira S. Rubinstein: Big Data: The End od Privacy or a New Beginning?., International Data Privacy Law. 2013, Vol. 3. No. 2, p. 74.

([4]) إن التحليل الرقمي قد يتعرض لتحليل المصدر ويتعلق المصدر بأصل شيء ما، أو بأول وجود معروف له. للتحقق من موثوقيته وصحته ، أما التحليل التقني فيشير إلى تحليل العنصر الرقمي نفسه، سواء أكان مستنداً، أو صورة، أو فيديو، وقد يكون مقارن أو تفسيري. بخلاف تحليل المحتوى الذي يتم من خلاله تقييم المعلومات الواردة في فيديو، أو صورة، أو مستند، أما التحليل الاستقصائي فهو ممارسة تتمثل في استعراض المعلومات الوقائعية وتفسيرها لاستخلاص نتائج جوهرية ذات صلة باتخاذ القرارات، أو إعداد القضايا . فضلا عن ذلك التحليل المكاني أو التحليل الجغرافي المكاني، الذي يتضمن تحليل المحتوى المرئي وتحليل البيانات الوصفية للعناصر التي تقدم حداثيات جغرافية أو أسماء أماكن للمزيد متاح على الموقع : www.orgnet.com/sna.html :. وعن تحليل الشبكات الاجتماعية فيتمثل تحليل الشبكات ألاجتماعية في رصد وقياس العلاقات بين الاشخاص والمجموعات والمنظمات والحواسيب والمحددات المنتظمة لموقع الموارد وغيرها ، الموقع الأتي :

Orgnet, "Social network analysis: an introduction" . تاريخ الزيارة 2024/6/25

([5]) عرف الدليل الرقمي :"الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب و شبكة الأنترنت، و الأجهزة الإلكترونية الملحقة والمتصلة به و شبكات الاتصال، من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة" .خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى،دار الثقافة للنشرو التوزيع، الأردن، 2011،ص 230. كما عرف أيضاً بأنه "الدليل المأخوذ من أجهزة الكمبيوتر و يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج و تكنولوجيا خاصة، و هي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور أوالأصوات أو الأشكال أو الرسوم و ذلك من أجل اعتماده أمام أجهزة تنفيذ وتطبيق القانون." . د. ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت ، دار الكتب القانونية ، مصر، 2006، ص 88.

([6]) يقصد بالتحليل الجنائي الرقمي : عملية استعادة وتحليل المحتويات الموجودة على الأجهزة الرقمية، مثل أجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة والأجهزة اللوحية، والهواتف الذكية، وما إلى ذلك؛ وبتعبير آخر يمكن القول بأنه : مجموعة الممارسات التي تجريها الأجهزة المختص بالأستدلال والتحقيق والتي يكون الغرض منها جمع البيانات الرقمية وتحليلها والأبلاغ عنها بطريقة مقبولة قانونا، وذلك بهدف الكشف عن الجريمة أو الوقاية منها . Jeetendra Pande and Ajay Prasad: DIGITAL FORENSICS,2016, Uttarakhand Open University, Haldwani, New Delhi, P.2, Downloaded from : https://www.researchgate.net/publication/300474145

([7]) يقصد بالتنبؤ بالجريمة: توقع حدوثها في المستقبل، أو هو الوقوف على سلوك مستقبلي ينطوي على خطورة إجرمية لدى بعض الأفراد يدفعهم الى ارتكاب الجريمة في المستقبل . د. رمضان السيد الألفي ، نظرية الخطورة الإجرامية، دار النهضة ، 1998 ،ص312 .

([8]) وهو العلم الذي يسعى الى تحري أسباب الجريمة عن طريق دراسة نفسية مرتكب الفعل الاجرامي وتحليل عقليته ومحاولة تفهم الافكار والخواطر والإحساسات والانفعالات التي انساق تحت تأثيرها الى الجريمة .

([9]) المادة (69-أ) من قانون اصول المحاكمات الجزائية العراقي رقم (23) لسنة 1973 المعدل – يجوز للقاضي او المحقق من تلقاء نفسه او بناء على طلب الخصوم ان يندب خبيرا أو اكثر لابداء الراي في ما له صلة بالجريمة التي يجرى التحقيق فيها .

([10]) هناك علاقة بين البيانات والمعلومات، فالبيانات هي : مجموعة من الحقائق أو المشاهدات، التي تكون عادة في شكل حرف أو أرقام أو أشكال خاصة، تُوصف أو تمثل فكرة أو موضوعًا أو هدفًا أوشرطًا أو أية عوامل أخرى وتمثل هذه البيانات المادة الخام التي يتم تجهيزها؛ للحصول على المعلومات. د. أسامة حسين محي الدين عبد العال ، حجية الدليل الرقمي للأثبات الجنائي في الجرائم المعلوماتية (دراسة مقارنة) ، مجلة البحوث القانونية والاقتصادية ، العدد (76) ، 2021 ، ص601 .

(11) عرف الطب العدلي (الشرعي) بأنه " فرع من الطب الخاص بمعالجة القضايا التي ينظرها رجال القانون من وجهة طبية) . د. وصفي محمد علي ، الوجيز في الطب العدلي ، دار المسلة للطباعة والنشر والتوزيع ، بغداد ، ص5

(12) د. علي حسين الخلف ود. سلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، المكتبة القانونية ، بغداد ، ص10 .

(13) هناك العديد من البصمات مثلاً بصمة الأصبع ، البصمة الوراثية ، بصمة العين ، بصمة الأذن ، بصمة الصوت ، بصمة الدم ، الشفاه ، الرئحة والعرق . للمزيد د. عبد الحميد بن صالح بن عبد الكريم الكراني الغامدي ، البصمات ومدى تأثيرها في النفي والإثبات وتطبيقها على حد المسكرات ، مجلة الدراسات الاسلامية والبحوث الاكاديمية ، العدد (82) ، ص108 ومابعدها .

(14) البصمة الرقمية – تسمى أحيانًا الظل الرقمي (a digital shadow) أو البصمة الإلكترونية (an electronic footprint)- تشير إلى أثر البيانات التي تتركها عند استخدام الإنترنت، وهي تشمل مواقع الويب التي تزورها، ورسائل البريد الإلكتروني التي ترسلها، والمعلومات التي ترسلها عبر الإنترنت، ويمكن استخدام البصمة الرقمية لتتبع أنشطة الشخص على الإنترنت وتتبع أجهزته، و ينشئ مستخدمو الإنترنت بصمتهم الرقمية إما بشكل نشط(active) أو سلبي (passive).

(15) علم الوظائف (الفسلجة) :- فرع من العلوم الحيوية يتعامل مع الوظائف الكاملة للأعضاء المختلفة للجسم ويؤكد على التغيرات التي تطرأ على الجسم بأكمله عند نشاط وعمل هذه الأعضاء عند قيامها بمهامها الاساسية والتحري عن سبب وكيفية أنجاز تلك الوظائف الحيوية الضرورية لإدامة حياة الكائن الحي .

(16) يُعرف الذكاء الاصطناعي من قبل JournalismAI في مركز أبحاث الصحافة بكلية لندن للاقتصاد والعلوم السياسية (LSE)، بأنه "مجموعة من الأفكار والتقنيات التي تتعلق بقدرة نظام الكمبيوتر على أداء المهام التي تتطلب عادةً ذكاءً بشرياً". الموقع الألكتروني : https://ijnet.org/ar/story/

(17) يقصد بها (عملية تقنية تتم بغرض كتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أواسترجاع أو استبدال للبيانات والمعلومات الالكترونية، ويتم ذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الألكترونية أو المغناطيسية أو الضوئية، أو ما يستحدث من تقنيات أو وسائط أخرى . د.أشرف توفيق شمس الدين: الدليل الجنائي الألكتروني- دراسة مقارنة، مطبعة أكتوبر الهندسية، ط1 .2021 ، ص32 .

(18) أسفرت التطوارت على مستوى نوع الجريمة وأساليب ارتكابها عن تعقد عمليات الكشف عن الجرائم الجديدة في ظل هذه الصعوبات المتعددة، واستتبع ذلك البحث عن سبل ملائمة للكشف عنها تمهيدا لملاحقتها، فظهرت بعض الوسائل المستحدثة كالتنصت على الهواتف وضبط المراسلات، تسجيل المكالمات الهاتفية، والاستعانة بالاجهزة الالكترونية كالهواتف المحمولة وأجهزة الكمبيوتر والانترنت وكاميرات المراقبة وغيرها . د. أشرف توفيق شمس الدين: الدليل الجنائي الالكتروني- دراسة مقارنة، مطبعة أكتوبر الهندسية، الطبعة الأولى ،2021 ، ص9 .

(19) نصت المادة (72 - ا) من قانون أصول المحاكمات الجزائية العراقي (لا يجوز تفتيش اي شخص او دخول او تفتيش منزله او اي محل تحت حيازته الا في الاحوال المبينة في القانون. ب – يقوم بالتفتيش قاضي التحقيق او المحقق او عضو الضبط القضائي بامر من القاضي او من يخوله القانون اجراءه) .

(20) الأمم المتحدة ، مكتب حقوق الأنسان ، بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة المصدر، ص56 .

(21) خالد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشروالتوزيع، عمان ،٢٠٠٠ ص ٦٣٤ .

(22) د. حسين محمود ، الوسائل العلمية الحديثة في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٨١، ص ٢٥ .

(23) عرف التحقيق الجنائي بأنه: "مجموعة من الاجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا رغبة لتمحيص الادلة والكشف عن الحقيقة قبل مرحلة المحاكمة " . د. مأمون محمد سلامة ،الاجراءات الجنائية في التشريع المصري"، الجزء الاول، دار النهضة العربية، القاهرة، 2008، ص 641 .

(24) ربح الله عفاف - بلخيري فايزة ، السوار الالكتروني كبديل للعقوبة السالبة للحرية ، رسالة ماجستير مقدمة لكلية القانون والعلوم السياسية - جامعة زيان عاشور -الجلفة- 2020 ، ص10 وما بعدها .

(25) تعرف بأنها "برنامج يهدف إلى إصدار أحكام منطقية أو تقديم المساعدة في مسألة معقدة، تكون فيها المها ارت البشرية قليلة أو نادرة، أو أنه برنامج مصمم لحل المشكلات على مستوى مشابه للخبير البشري في مجال معين، ويعمل من خلال توظيف المعرفة والاستنتاج " . Bryan S. Todd: AN INTRODUCTION TO EXOERT SYSTEMS, Oxford university Computing Laboratory, 1992, p.1. available at https://www.cs.ox.ac.uk .

(26) https://prodiscover.com/prodiscover-pro. (2024).

(2.) Debasis Giri, et all. (2021). Android forensics using sleuth kit autopsy. Springer Nature

(3) https://www.magnetforensics.com/products/magnet-axiom
(4)هي أداة رائدة من (Belkasoft) لأجهزة الكمبيوتر والأجهزة المحمولة وذاكرة الوصول العشوائي والطائرات بدون طيار وصور السيارات والسحابة. https://belkasoft.com/x (Brett Shavers, U. (2024).
(5) J. Kävrestad. (2020). Fundamentals of Digital Forensics . Springer.
6) Ambhire, V. R., & Meshram, B. B. (2012). Digital Forensic Tools, 2(3), 392–398. (Retrieved from www.iosrjen.org392|Page
(32) وهذا ما قام به الباحثان كل من مايكل مارسيانو وجوناثان أديلمان بمعهد الأمن القومي والطب الشرعي الأمريكي متاح على الموقع :https://www.bbc.com/arabic/vert-fut-47459695 - تاريخ الزيارة 2024/7/8 .
(33) متاح على الموقع : . https://www.bbc.com/arabic/vert-fut-47459695
(34) البصمة الوراثية لم تصبح أدلة يعتد بها في المحاكم حول العالم بين عشية وضحاها، إذ لم تعترف بها المحاكم الأمريكية كدليل إدانة إلا بعد تسع سنوات من اعتراف المحاكم البريطانية بها. قال روث مورغان إن الذكاء الاصطناعي قد يصور هذه الجسيمات ويعدّها في ساعات، في حين أن الطبيب الشرعي قد يعكف أسابيع أو شهورا على عدها متاح على الموقع : https://www.bbc.com/arabic/vert-fut-47459695.
(35) الباحث (زين لي) ، المتخصص في علوم الحاسوب بجامعة ولاية لويزيانا ، للمزيد متاح على الموقع : https://www.shorouknews.com/news/view.
(36) للمزيد متاح على الموقع : - https://fastercapital.com/arabpreneur تاريخ الزيارة 2024/6/29 .
(37) نظراً لحداثة فكرة البيانات الكبيرة أو الضخمة فلا يوجد تعريف موحد مقبول متفق عليه بين الأوساط العلمية والفقهية، لكن عرفتها بعض المؤسسات العاملة في مجال جمع وتحليل البيانات – مؤسسة Foundation TechAmerica - بأنها "مصطلح يصف
كميات كبيرة من البيانات عالية السرعة والتعقيد، كما أنها متغيرة باستمرار، وتتطلب أساليب وتقنيات متقدمة لتمكين استيعاب المعلومات وتخزينها وتوزيعها وإدارتها وتحليلها"، وتتميز البيانات الضخمة – على ذلك – بخصائص أربع : وهي السرعة والحجم والمصادقية والتنوع . كما وضع معهد ماكينزي العالمي تعريفا للبيانات الضخمة أنها "مجموعة البيانات بحجم يفوق قدرة قواعد البيانات التقليدية من التقاط وتخزين وإدارة وتحليل تلك البيانات المعقدة" . مركز الاحصاء بأبو ظبي – الامارات العربية المتحدة : مفاهيم عامة حول البيانات الكبيرة ، ص2، متاح على الموقع الألكتروني : https://www.scad.gov.ae
(38) د. فهيل عبدالباسط عبدالكريم ، دور الشرطة التنبؤية في التنبؤ برسم خريطة الجريمة الزمكانية ، متاح على الموقع : https://sjc.iq/view.74018/ تاريخ الزيارة 2024/6/15
(39) أدى استخدام أنظمة الشرطة التنبؤية في مراكز الشرطة في الولايات المتحدة الامريكية بولاية لوس أنجلوس بعام 2014م إلى انخفاض معدلات جرائم العنف إلى 21% وجرائم السرقة 33%، وفي بريطانيا ساهمت تقنية الشرطة التنبؤية إلى انخفاض معدلات الجريمة بنسبة 26% في عام 2011 ، دور تقنيات الذكاء الاصطناعي في مكافحة الجرائم ، متاح على الموقع https://www.bbc.com/arabic/vert-fut-47459695
(40) الجدير بالذكر أن هناك أمثلة في دولة الصين على تطوير وابتكار تقنيات مصممة للتنبؤ بالجريمة ومنع وقوعها من خلال تقنيات التعرف على الوجوه وتحليل المشتبه بهم وذلك تقنيات تحليل الحشود للكشف عن الأنماط المشبوهة بها وتتبع الأشخاص الذين لديهم سجلات إجرامية سابقة.
(41) د. محمد علي الكيك، السلطة التقديرية للقاضي الجنائي، دار المطبوعات الجامعية، مصر، عام ٢٠٠٧ ، ص.٢٩
(42) متاح على الموقع :https://www.arageek.com/-deepfake تاريخ الزيارة 2024/7/22
(43) متاح على الموقع : https://www.unite.ai/ar/what-are-deepfakes/ تاريخ الزيارة 2024/7/16
(44) عرف التحقيق الجنائي الرقمي بإنه "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الالكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لإقامة العدل " . د. مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الالكترونية "، ط1،مطابع الشرطه،القاهره،2009،ص 169 .
(45) د. ياسر محمد الكومي محمد أبو حطب، "الحماية الجنائية والامنية للتوقيع الالكتروني "، دراسه مقارنة، منشأة المعارف الاسكندرية ،2014 ، ص 391 .
(46) حق الخصوصية حق أساسي من حقوق الانسان مدرج في العديد من صكوك حقوق الانسان منها إلاعلان الامريكي لحقوق الانسان وواجباته ، المادة 5 ؛ ألاتفاقية الاوروبية لحقوق الانسان، المادة 8؛ الاتفاقية الامريكية لحقوق الانسان ، المادة 11 ؛ اتفاقية حقوق الطفل، المادة 16؛ الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم، المادة 14؛ الميثاق الافريقي لحقوق الطفل ورفاهيته، المادة 10 إ ؛ الميثاق العربي لحقوق الانسان، المادتان 16 و21 إ ؛ إعلان رابطة أمم جنوب شرق آسيا بشأن حقوق الانسان، المادة 21 : https://privacyinternational.org explainer/56/what-privacy.

(47) وقد قدم مركز بوليتزر، وكلية ميديل للصحافة والإعلام والاتصالات التسويقية المتكاملة بجامعة نورث وسترن مناقشة حول التحديات والإنجازات التي يواجهها الصحفيون خلال استخدام أدوات الذكاء التحليل الرقمي متاح على الموقع الألكتروني :.https://ijnet.org/ar/story تاريخ الزيارة 2024/6/27 .

(48) لم يشرع العراق قانون يتعلق بالجرائم المعلوماتية أو الإجراءات المتخذة بشأنها رغم قراءة المشروع أول قراءة عام 2011 وتلتها مناقشات وتعديلات عديدة طالت المشروع .عدلت فيها تسمية المشروع الى الجرائم الألكترونية .

(49) هناك معاهدات دولية عقدت بهذا الشأن ومنها معاهدة بودابست التي ألزمت الدول الأطراف عند تطبيق النصوص الإجرائية المتعلقة بالتحقيق في الجرائم الإلكترونية وجمع أدلتها بالخضوع للشروط والضمانات المتعلقة بحقوق الإنسان والحريات العامة، إلا أنها ألزمت الشخص المعني بالحفاظ على المعلومات الرقمية التي بحوزته ، والاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة 2010 والتي ألزمت الاتفاقية كل دولة بالمصادقة على تبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر، أو الحصول على الحفظ العاجل للمعلومات المخزنة .

(50) نصت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة2018 على أن الأدلة الإلكترونية المأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية والتي يمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، تعد معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة، وتشمل ما في حكمها ، كذلك المادة الثانية من قانون المعاملات والتجارة الالكترونية الإماراتي رقم ١ لعام 2006 .

(51) د. هلالى عبد الله أحمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٩٧، ص٢٥.

(52) د. أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي في الجرائم المعلوماتية، مصدر سابق ، ص660

(53) د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، ط3،١٩٩٨ ، ص766 .

(54) خالد علي نزال الشعار ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة دكتوراه ، جامعة المنصورة – كلية الحقوق ، ص37 .

(55) د. أسامة حسين محي الدين عبد العال ، المصدر السابق ، ص637 .

(56) د . جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجي الحديثة، دارالنهضة العربية ، القاهرة ، عام ٢٠٠٢،ص111 .

(57) د.علي عدنان، إجراءات التحري وجمع الأدلة والتحقق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية، مصر، ٢٠١٢، ص.٥٥

(58) د.علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة العلوم التطبيقية ، كلية الحقوق، البحرين، عام ٢٠٠٩، ص8.

(59) د.علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة ٢٠٠٣، ص436.

(60) د . هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، ١٩٩٧،ص ٤٢ .

(61) د. حسن ربيع ، الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية ، القاهرة ٢٠٠١ ، ص٧٢٠

(62) د . ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، المغرب، العدد ١٤٢٧،٣١ص1.

(63) قرار مجلس الوزراء رقم (434) لسنة 2019 في 2019/12/3 ، الذي تضمن سبع مواد، ونص على ما يأتي:

1- على أصحاب الشركات والمعامل والمصانع والمخازن والمحلات التجارية والصناعية والحرفية والفنادق والمطاعم والمقاهي والمسارح والنوادي والمنتجعات السياحية والمكاتب المهنية والمؤسسات الثقافية والرياضية والترفيهية والمستشفيات والعيادات الصحية ومراكز التسوق، تركيب كاميرات التصوير مع أجهزة التسجيل الفيديوية، وتحدد أماكن تثبيتها ومواصفاتها الفنية ومدة تسجيلها بموجب ضوابط يصدرها وزير الداخلية.

2- يقوم المذكورون في الفقرة (1) أنفأ بوضع لوحات مرئية للعيان توضح للمواطنين أن المكان مراقب بالكاميرات.

3- لا يجوز لأصحاب تلك المنشآت تزويد أي جهة بنسخة من التسجيل أو الاطلاع على التصوير الا بموافقة الجهة المختصة لأغراض تحقيقية أو بناء على قرار قضائي، وللجهة المختصة ربط عدد من كاميرات التصوير وأجهزة التسجيل بمنظومتها للضرورات التي يتطلبها العمل الأمني.

4- يحظر تركيب كاميرات التصوير في غرف النوم وغرف العلاج الطبيعي ودورات المياه والحمامات وغرف تغيير الملابس.

5- تخضع كاميرات التصوير للرقابة والتفتيش من الجهة المختصة حصرا للتحقق من مدى التزامها بضوابط وزارة الداخلية بما يحقق الأمن والنظام العام.

6- لوزير الداخلية إضافة أي منشآت الى الفقرة (1) انفا على ظروف الأمن ومقتضيات المصلحة العامة.

7- يعاقب المخالف للفقرات المذكورة آنفا فيما تقدم على وفق أحكام قانون العقوبات رقم 111 لسنة 1969 المعدل.
كتاب قيادة العمليات المشتركة (هيئة الاستخبارات) سري وشخصي 2/1/827 في 25 شباط 2024 المتضمن توجيهات رئيس مجلس الوزراء - القائد العام للقوات المسلحة خلال الاجتماع الأمني المنعقد بالساعة 2045 يوم 23 شباط 2024 في مقر وكالة الاستخبارات والتحقيقات الاتحادية وبالنظر لما تشكله كاميرات المراقبة من أهمية بالغة في كشف وتعقب مرتكبي الجرائم الجنائية ، الإرهابية، الحوادث الأخرى بمختلف اشكالها) ".

المصادر.

أولاً / الكتب.

1- أشرف توفيق شمس الدين: الدليل الجنائي الألكتروني- دراسة مقارنة، مطبعة أكتوبر الهندسية، ط1 .2021
2- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجي الحديثة، دارالنهضة العربية ، القاهرة ، عام .٢٠٠٢ .
3- حسن ربيع ، الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية ، القاهرة ،٢٠٠١ ،
4- حسين محمود ، الوسائل العلمية الحديثة في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٨١ .
5- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى،دار الثقافة للنشرو التوزيع، عمان ، الأردن، 2000
6- رمضان السيد الألفي ، نظرية الخطورة الإجرامية، دار النهضة ، 1998 .
7- علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة ،٢٠٠٣ .
8- علي حسن الطوالبة ، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، جامعة العلوم التطبيقية، كلية الحقوق، البحرين، عام ،٢٠٠٩ .
9- علي حسين الخلف ود. سلطان عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات ، المكتبة القانونية ، بغداد
10- علي عدنان، إجراءات التحري وجمع الأدلة والتحقق الابتدائي في الجريمة المعلوماتية، دار الكتب والوثائق القومية ، مصر، ٢٠١٢، .
11- مأمون محمد سلامة ،الاجراءات الجنائية في التشريع المصري"، الجزء الاول، دار النهضة العربية، القاهرة، 2008، .
12- محمد علي الكيك، السلطة التقديرية للقاضي الجنائي، دار المطبوعات الجامعية، مصر، عام .٢٠٠٧ .
13- محمود نجيب حسني، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، ط3،١٩٩٨ .
14- مصطفي محمد موسي، "التحقيق الجنائي في الجرائم الالكترونية "، ط1،مطابع الشرطة ، القاهره ،2009.
15- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر و الأنترنت ، دارالكتب القانونية ، مصر، ،2006
16- هلالى عبد الله أحمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٩٧،
17- وصفي محمد علي ، الوجيز في الطب العدلي ، دار المسلة للطباعة والنشر والتوزيع ، بغداد
18- ياسر محمد الكومي محمد أبو حطب، "الحماية الجنائية والامنية للتوقيع الالكتروني "، دراسه مقارنة، منشأة المعارف الاسكندرية ،2014 .

ثانياً / الأطاريح والرسائل الجامعية .

1- خالد علي نزال الشعار ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة دكتوراه ، جامعة المنصورة – كلية الحقوق
2- ربح الله عفاف - بلخيري فايزة ، السوار الالكتروني كبديل للعقوبة السالبة للحرية ، رسالة ماجستير مقدمة لكلية القانون والعلوم السياسية - جامعة زيان عاشور -الجلفة- 2020

ثالثاً / المجلات والوثائق .

1- أسامة حسين محي الدين عبد العال ، حجية الدليل الرقمي للأثبات الجنائي في الجرائم المعلوماتية (دراسة مقارنة) ، مجلة البحوث القانونية والاقتصادية ، العدد (76) ، 2021
2- عبد الحميد بن صالح بن عبد الكريم الكراني الغامدي ، البصمات ومدى تأثيرها في النفي والإثبات وتطبيقها على حد المسكرات ، مجلة الدراسات الاسلامية والبحوث الاكاديمية ، العدد (82)
3- ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، المغرب، العدد 4- ٣١،١٤٢٧
5- الأمم المتحدة ، مكتب حقوق الأنسان ، بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة .
6- قرار مجلس الوزراء العراقي رقم (434) لسنة 2019 في 2019/12/3

رابعاً / القوانين الوطنية والصكوك الدولية .

1- إلاعلان الامريكي لحقوق الانسان وواجباته ،
2- ألاتفاقية الاوروبية لحقوق الانسان

3- الاتفاقية الامريكية لحقوق الانسان ،
4- اتفاقية حقوق الطفل،
5- الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم،
6- الميثاق الافريقي لحقوق الطفل ورفاهيته
7- الميثاق العربي لحقوق الانسان،
8- إعلان رابطة أمم جنوب شرق آسيا بشأن حقوق الانسان،
9- والاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة 2010
10- قانون اصول المحاكمات الجزائية العراقي رقم 23 لسنة 1971
11- قانون المعاملات والتجارة الإلكترونية الإماراتي رقم ١ لعام 2006 .
12- قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة2018

خامساً / المواقع الألكترونية .

1- www.orgnet.com/sna.html .:
2- https://www.researchgate.net/publication/300474145
3- https://ijnet.org/ar/story/
4- https://prodiscover.com/prodiscover-pro. (2024 .
5- https://www.magnetforensics.com/products/magnet-axiom
6- https://www.bbc.com/arabic/vert-fut-47459695 Brett Shavers, U. (2024) -
7- https://www.bbc.com/arabic/vert-fut-47459695
8- مركز الاحصاء بأبو ظبي – الامارات العربية المتحدة : مفاهيم عامة حول البيانات الكبيرة الألكتروني : https://www.scad.gov.ae
9- فهيل عبدالباسط عبدالكريم ، دور الشرطة التنبؤية في التنبؤ برسم خريطة الجريمة الزمكانية ، متاح على الموقع : https://sjc.iq/view.74018

سادساً / المصادر الاجنبية .

1- Ira S. Rubinstein: Big Data: The End od Privacy or a New Beginning?., International Data Privacy Law. 2013, Vol. 3. No. 2.
2- Bryan S. Todd: AN INTRODUCTION TO EXOERT SYSTEMS, Oxford university Computing Laboratory, available at 1992 .
3- Jeetendra Pande and Ajay Prasad: DIGITAL FORENSICS,2016, Uttarakhand Open University, Haldwani, New Delhi .
4- Debasis Giri, et all. (2021). Android forensics using sleuth kit autopsy. Springer Nature .
5- J. Kävrestad. (2020). Fundamentals of Digital Forensics . Springer