إجراءات استخراج الدليل الإلكتروني

Procedures for extracting electronic evidence

https://aif-doi.org/AJHSS/108005

الباحث/ حسن بن علي قاسم شبعاني*

*طالب دكتوراه في قسم الأنظمة
كلية الأنظمة والدراسات القضائية
الجامعة الإسلامية بالمدينة المنورة

ملخص البحث

يهدف هذا البحث إلى التعرف على الإجراءات التقليدية للحصول على الدليل الإلكتروني، وكذلك بيان الإجراءات المستحدثة للحصول على الدليل الإلكتروني، ويعتمد البحث على المنهج الوصفي التحليلي، وذلك بجمع المعلومات المتعلقة بموضوع البحث، ووصفها، وتحليلها، وتشخيصها من مُختلف جوانبها وأبعادها المختلفة، بهدف التوصل إلى نظرة واضحة عن الآليات والقواعد الإجرائية المُلائمة لاستخراج الدليل الإلكتروني من الجرائم الإلكترونية بوصفها ظاهرة إجرامية مُستحدثة.

ولقد خلص البحث إلى مجموعة من النتائج أبرزها ضرورة مواكبة التطور التقني، وذلك بإدخال وسائل وطرق حديثة للكشف عن الجرائم والحصول على الأدلة التي تتناسب وطبيعتها، وهو ما عملت عليه أجهزة البحث والتحقيق من خلال الاستعانة بالوسائل الحديثة في إثبات الجرائم، مما أحدث ثورة علمية في مجال الإثبات الجنائي على نحو يصبح استخدام هذه الوسائل الحديثة أمراً ضرورياً ليقوم رجال البحث والتحري بمهامهم على أكمل وجه.

الكلمات المفتاحية: دليل إلكتروني، المعاينة، التفتيش، المراقبة الإلكترونية، الذكاء الاصطناعي

ISSN : 2410-1818

Abstract

This research aims to identify the traditional procedures for obtaining electronic evidence, as well as to explain the new procedures for obtaining electronic evidence. The researcher relies on the descriptive and analytical method, by collecting information related to the subject of the research, describing it, analyzing it, and diagnosing it from its various aspects and dimensions, with the aim of arriving at A clear view of the appropriate mechanisms and procedural rules for extracting electronic evidence from cybercrime as a new criminal phenomenon.

The research concluded with a set of results, the most prominent of which is the necessity of keeping pace with technical development, by introducing modern means and methods to detect crimes and obtain evidence that is appropriate to their nature, which is what the research and investigation agencies worked on by using modern means to prove crimes, which created a scientific revolution in the field. Criminal proof in such a way that the use of these modern methods becomes necessary for research and investigation personnel to carry out their tasks to the fullest extent.

Keywords: electronic evidence, inspection, inspection, electronic monitoring, artificial intelligence.

مقدمة البحث

شكلت الجرائم الإلكترونية تحديات واضحة على الصعيدين الدولي والوطني، بسبب الفراغ التشريعي الذي تعانيه غالبية دول العالم؛ لأن التشريعات العقابية القائمة وجدت لمواجهة الجرائم التقليدية المعروفة، وهو ما يصعب تطبيقه على الجرائم المعلوماتية التي تتصف بخصائص تختلف عن هذه الجرائم، من حيث آلية ارتكابها والوسط التي تتم فيه ونوعية مرتكبيه، وأولى هذه التحديات هي الإشكالية المتعلقة بقبول الدليل الإلكتروني، إذ يلعب الدليل في المجال الجنائي أهمية كبيرة؛ لأنه هو الذي يناصر ويظهر الحقيقة، ويبين مرتكب الجريمة، وهو الذي يحول الشك إلى يقين.

أمام عجز وقصور الإجراءات التقليدية في البحث والتحري عن الجريمة المعلوماتية، واستخلاص الدليل الإلكتروني كان لزامًا على مختلف التشريعات الحديثة أن تبحث عن وسائل أكثر ملائمة مع الطبيعة الخاصة للجريمة الإلكترونية حتى تتحقق تلك النتيجة المرجوة من التحقيق. فقد أصبح من الضروري مواكبة التطور التقني، وذلك بإدخال وسائل وطرق حديثة للكشف عن الجرائم والحصول على الأدلة التي تتناسب وطبيعتها، وهو ما عملت عليه أجهزة البحث والتحقيق من

ISSN : 2410-1818

خلال الاستعانة بالوسائل الحديثة في إثبات الجرائم، مما أحدث ثورة علمية في مجال الإثبات الجزائي على نحو يصبح معه استخدام هذه الوسائل الحديثة أمرًا ضروريًا ليقوم رجال البحث والتحري بمهامهم على أكمل وجه.

فكان من الطبيعي أن تتطور بالمقابل أساليب البحث والتحري وجمع الأدلة، فظهرت المراقبة الإلكترونية كإجراء ووسيلة حديثة للبحث والتحري عن الجرائم والمجرمين وكشف الأدلة الإلكترونية في إطار الجرائم الإلكترونية. كما يُعد الذكاء الاصطناعي كذلك أحد أهم الميادين الحديثة التي تستقطب اهتمام كافة المجتمعات، والتي تشهد تطورات مستمرة، ومن المتوقع أن يكون للذكاء الاصطناعي دور مهم في مستقبل البشرية.

أولًا: موضوع البحث:

تنقسم الأدلة الجنائية – عمومًا- إلى تقسيمات كثيرة، وتصنيفات متعددة، غير إنه نظرًا للتطور العلمي، وانتشار التقنية المعلوماتية في التعاملات اليومية، فقد أدى ذلك إلى استغلال الجناة هذه التقنية بوصفها وسيلة لارتكاب الجرائم، وبذلك اختلف الوسط الذي ترتكب فيه الجريمة من وسط مادي إلى وسط معنوي، أو ما يُعرف بالوسط الافتراضي، وهو ما استتبع ظهور طائفة جديدة من الأدلة تتفق وطبيعة الوسط الذي ترتكب فيه الجريمة، وهي ما يُسمى بالأدلة الإلكترونية أو المعلوماتية، وهي أدلة من نوع خاص تستمد خصوصيتها من الجريمة الإلكترونية النابعة منها [1].

ويُعرِّف الدليل الإلكتروني بأنه:" مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة في شكل حروف أو أرقام أو أشكال خاصة تُوصف أو تمثل فكرة أو موضوعًا أو هدفًا أو شرطًا أو أية عوامل أخرى، وتمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات، فالبيانات تُعد مصطلحًا عامًا لكل الحقائق والأرقام والرموز والحروف فهي معطيات أولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات".[2]

وقد يكون الدليل الإلكتروني من الوضوح، حينما يتخذ صور معينة، مثل: مطبوعات رسائل البريد الإلكتروني المتوفرة بسهولة التي يرسلها مرتكب الجريمة، أو سجلات اتصال بروتوكول الإنترنت التي يبلغ عنها مباشرة من قبل موفر خدمة الإنترنت، وقد يتطلب في أحوال أخرى استعمال تقنيات متطورة من أجل التوصل إليه عن طريق استخدام تقنيات أو أدوات لاستعادة الآثار أو البيانات التي يتم الحصول عليها من الحاسب الآلي والنظم المعلوماتية والشبكات والتي من شأنها أن تقدم أدلة

(1) لطفي، إبراهيم الشحات(2018م)، الحبس الاحتياطي وأهميته في الحفاظ على أدلة الجريمة: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ص314.

(2) المري، بهاء (2017م)، الوسيط في جرائم المخدرات والإنترنت وحجية الدليل الإلكتروني في الإثبات، طبعة نادي القضاة، القاهرة، ص443.

ISSN : 2410-1818

على وقوع جرم ما، ومن ثم يأتي دور خبراء وتقنيات الأدلة الجنائية الرقمية في استعادة وتحليل المواد التي تم الحصول عليها من أجهزة الحاسب والشبكات والنظم المعلوماتية، والاستفادة من قابلية الحواسب لتخزين وتسجيل وحفظ البيانات عن أغلب أنشطة مستخدميها، في جمع وتعقب الآثار الرقمية[3]. وبالتالي يثير هذا النوع من الأدلة عدة إشكاليات نظرًا لحداثته، حيث إن إثبات هذا النوع من الجرائم يُعتبر من المستجدات التي لا يقدر المحقق أو القاضي أن يصل إليها بنفسه، بل لابد من الاستعانة بالخبراء لاستخلاص أدلتها وتحريزها [4]؛ الأمر الذي يدعونا للبحث عن إجراءات استخراج الأدلة الإلكترونية في الجرائم المعلوماتية، وهذا ما يهتم به هذا البحث.

ثانيًا: أهمية البحث:

ترجع أهمية البحث إلى الطبيعة الخاصة لجرائم تقنية المعلومات كجريمة عبر وطنية، تتطلب تحقيقات سريعة تتسم بالخبرة، وهو ما يتطلب ضرورة تعاون أجهزة إنفاذ القانون بصورة سريعة وفعالة، كما تكمن الأهمية النظرية للبحث في تناوله لظاهرة مستحدثة في عصر يُكنى بعصر الثورة المعلوماتية. فرغم المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة، وفي شتى ميادين الحياة المعاصرة؛ فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة، والانحراف عن الأغراض المتوخاة منها، تمثلت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي: ظاهرة الإجرام المعلوماتي.

ثالثًا: إشكالية البحث:

تبرز مشكلة الدراسة من خلال البحث عن الإجراءات الحديثة اللازمة لاستخلاص الدليل الإلكتروني في الجرائم المعلوماتية، حيث جاءت تلك الوسائل لكي تلاءم التطورات التكنولوجية والتقنية التي تطور معها الفكر الإجرامي المعلوماتي، مما ألقى على عاتق القائمين على مكافحة الجريمة في الدول عبئًا كبيراً ومهامًا جسامًا تفوق القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث الجنائي والإثبات الجنائي التقليدية، نظرًا لعدم كفاية وعدم ملاءمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحية القانونية أو التقنية.

(3) القاضي، رامي متولي(2021م)،، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018م، مقارنًا بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 75، مارس، ص1283.

(4) الغني، محمود (2019م)، دور الدليل الإلكتروني في الإثبات الجنائي: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ص174.

ISSN : 2410-1818

رابعًا: منهج البحث:

اعتمد الباحث على المنهج الوصفي التحليلي، وذلك بجمع المعلومات المتعلقة بموضوع البحث، ووصفها، وتحليلها، وتشخيصها من مُختلف جوانبها وأبعادها المختلفة، بهدف التوصل إلى نظرة واضحة عن الآليات والقواعد الإجرائية المُلائمة لاستخراج الدليل الإلكتروني من الجرائم الإلكترونية بوصفها ظاهرة إجرامية مُستحدثة.

خامسًا: خطة البحث:

المبحث الأول: الإجراءات التقليدية للحصول على الدليل الإلكتروني.
المبحث الثاني: الإجراءات المستحدثة للحصول على الدليل الإلكتروني.

المبحث الأول

الإجراءات التقليدية للحصول على الدليل الإلكتروني

تمهيد وتقسيم:

رغم وجود تشابه كبير بين التحقيق في الجرائم الإلكترونية وبين التحقيق في الجرائم الأخرى؛ فهي جميعًا تحتاج إلى إجراءات تتشابه في عمومها، مثل: المعاينة والتفتيش والشهادة والخبرة، وتُعد هذه الإجراءات أحد وسائل جمع الأدلة، ولكل منها قواعده الخاصة التي يجب اتباعها للحصول على الدليل الإلكتروني، وهو ما نتعرف عليه من خلال التقسيم التالي:

المطلب الأول: المعاينة والتفتيش في الجرائم الإلكترونية.
المطلب الثاني: الخبرة والشهادة في الجرائم الإلكترونية.

المطلب الأول

المعاينة والتفتيش في الجرائم الإلكترونية

تمهيد وتقسيم:

بمجرد العلم بوقوع الجريمة، فإن أول خطوة يقوم بها رجل الضبط القضائي هو الانتقال إلى مسرح الجريمة، ومعاينته والتفتيش فيه بحثًا عن الأدلة والآثار في المكان، أي الأشياء التي تُعد في ذاتها الدليل على الجريمة، أو يمكن أن يظهر منها الدليل، وقد تكون هذه الأشياء هي ما استعمل في ارتكاب الجريمة، وقد تكون هذه الأشياء السبب الذي ارتكبت لأجله الجريمة؛ فقد يقع التفتيش على المكونات المادية للحاسب الآلي، وبرامجه، وقد يكون التفتيش من أجل الجرائم التي تُرتكب عبر شبكة الإنترنت، وهذا ما نوضحه من خلال التقسيم التالي:

الفرع الأول: المعاينة في الجرائم الإلكترونية.
الفرع الثاني: التفتيش في الجرائم الإلكترونية.

ISSN : 2410-1818

الفرع الأول

المعاينة في الجرائم الإلكترونية

تأتي المعاينة لغة بمعنى النظر، وعاين الشيء، رآه بعينه ودلالتها في اللغة تشير بمعناها الواسع إلى الرؤية والمشاهدة، ودلالتها القانونية وخاصة في المجال الجنائي، هي التي تعتمد على حاسة البصر، وتبعًا لذلك تعني المعاينة رؤية أماكن ارتكاب الوقائع الجنائية.[5]

ويرى البعض من الشراح[6] النظر للمعاينة بصورة أكثر شمولية، باعتبارها رؤية بالعين لمكان أو شخص، أو شيء لإثبات حالته، وضبط كل ما يلزم لكشف الحقيقة، بينما ينظر جانب آخر من الشراح للمعاينة من خلال ما تقتضيه من الانتقال إلى مكان الجريمة، حيث تم وصفها طبقًا لذلك، بأنها إجراء ينتقل بمقتضاه المحقق، إلى مكان وقوع الجريمة ليشاهد بنفسه كيفية وقوعها، ويجمع الآثار التي تفيد في كشف الحقيقة[7]. أما المعاينة لمسرح الجريمة المعلوماتية فُيقصد بها المشاهدة والرؤية بالعين لمكان أو شخص أو شيء له علاقة بالجريمة، لإثبات حالته والآثار المادية التي خلفها ارتكاب الجريمة المعلوماتية، وضبط كل ما يلزم من الأشياء لكشف الحقيقة عن الجريمة ومرتكبيها، بهدف المحافظة على الأدلة التقنية من التلف أو المحو أو التعديل[8]، ويقوم بالمعاينة في العالم الافتراضي رجل الضبط الجنائي في المراحل الأولى للتحقيق، وهو ما اصطلح عليه بمرحلة الاستدلال من خلال الانتقال المباشر للعالم المادي، وقد تكون المعاينة عن طريق الانتقال إلى الوسط الإلكتروني.

وما تجب الإشارة إليه أنه لا تتمتع المعاينة في مجال كشف الجريمة الإلكترونية بالدرجة نفسها من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك إلى اعتبارين: الأول: إن الجرائم التي تقع على نظم المعلومات قلما يترتب على ارتكابها آثار مادية، والثاني: أن عددًا كبيرًا من الأشخاص قد يتردد على مكان، أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها، مما يهيئ الفرصة لحدوث تغيير، أو إتلاف، أو عبث بالآثار المادية.[9]

(5) الرازي، محمد بن أبي بكر عبد القادر(1951م)، مختار الصحاح، ترتيب محمود خاطر، ط6، القاهرة، ص467؛ عاشور، محمد أنور(1978م)، الموسوعة في التحقيق الجنائي العملي، عالم الكتب، القاهرة، ص114.

(6) أبو عامر، محمد زكي (1990م)، الإجراءات الجنائية، الطبعة الرابعة، دار النهضة العربية، القاهرة، ص604.

(7) سلامة، مأمون (2010م)، قانون الإجراءات الجنائية معلقًا عليه بالفقه وأحكام النقض طبقًا لأحدث التعديلات والأحكام، الطبعة الثالثة، دار طيبة للطباعة، الجيزة، ص347.

(8) الخشاشنة، توفيق، (2016م)، معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص77.

(9) إبراهيم، الشحات(2011م)، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ص195.

ISSN : 2410-1818

والأصل أن للمعاينة ضوابط إجرائية يجب على رجل الضبط الجنائي التقيد بها، حيث يحب عليه في حالة التلبس بجريمة أن ينتقل فورًا لمحل الواقعة، ويعاين الآثار المادية للجريمة، والالتزام بقواعد المحافظة على مسرح الجريمة، ومنع الأشخاص من الدخول إليه قبل ضياع الأدلة واختفائها، مع عدم السماح لنفسه، أو من برفقته بلمس الأشياء أو تحريكها قبل وصول الخبراء المختصين[10]، وعليه أن يحترس في كل خطوة يخطوها داخله حتى لا يضيف أو يزيل أثرًا ماديًا[11].كذلك يُعد الانتقال المادي للمحقق في المراحل الأولى من التحقيق ومرحلة الاستدلال من الموضوعات المهمة في كشف الجرائم المعلوماتية، وبالتالي فإن معاينة هذه الجرائم مفيد في التحقيق في هذه المرحلة، لأنها تهدف إلى كشف أسلوب ارتكاب الجريمة، والوسائل المستخدمة فيها ومرتكبيها.

وتكمن أهمية الانتقال كذلك في ضبط كل ما يمكن أن يؤدي إلى إظهار الحقيقة، وإثبات حالة الأماكن والأشخاص، وكل ما يفيد في كشف الحقيقة، وأن يعرض الأشياء المضبوطة على الأشخاص المشتبه بهم للتعرف عليها، وكذا إخطار النيابة العامة فورًا بانتقاله، لكي تنتقل بدورها إلى محل الجريمة في حالة الجناية المتلبس بها.[12]

ولضمان القيام بمعاينة أجهزة الحاسوب، وبشكل أكثر دقة لا بد من القيام ببعض الإجراءات قبل إجراء المعاينة، ومنها: توفير معلومات مسبقة عن مكان الجريمة، وكذا تحديد نوع الأجهزة المحتمل استخدامها في الجريمة، وكذلك مواقع الأجهزة والملفات[13]، ويجب الاستعانة بأجهزة التنصت لمراقبة الاتصالات السلكية واللاسلكية والتصوير الإلكتروني في الضوء والظلام، والتصوير التلفزيوني، وتحديد الاتجاهات والمواقع، وتحليل المعلومات بغرض التنسيق والتفسير[14]. أما في حالة معاينة جرائم شبكة الإنترنت؛ فإنه يتم الاستعانة بوسائل تصوير شاشة الحاسوب، سواء بواسطة آلة تصوير تقليدية، أو عن طريق استخدام برمجية حاسوب متخصصة في أخذ صور لما يظهر على الشاشة، أو عن طريق حفظ الموقع باستخدام خاصية الحفظ المتوفرة في أنظمة التشغيل المختلفة.[15]

(10) المادة التاسعة والسبعون من نظام الإجراءات الجزائية السعودي.
(11) العازمي، فهد (2012م)، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص267.
(12) المادة 55 من اللائحة التنفيذية لنظام الإجراءات الجزائية.
(13) الخشاشنة، توفيق، المرجع السابق، ص84.
(14) إبراهيم، خالد ممدوح (2009م)، فن التحقيق في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، ص157، 158.
(15) بن يونس، عمر محمد أبو بكر (2004م)، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، الطبعة الأولى، دار النهضة العربية، القاهرة، ص859.

ISSN : 2410-1818

وفي إطار الحديث عن معاينة مسرح الجريمة الإلكترونية؛ فإنه تجب التفرقة بين حالتين على النحو الآتي:[16]

أولًا: مسرح الجريمة التقليدي: ويقع خارج بيئة الحاسوب، ويتكون-بشكل رئيس-من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، وقد يترك فيها الجاني آثارًا عدة، مثل: البصمات وغيرها، وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه، وفي هذه الحالة ليست هناك صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات للمعاينة من قبل رجل الضبط الجنائي، والتحفظ على الأشياء التي تعد أدلة مادية علي ارتكاب الجريمة، ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة، والتحفظ عليها، مع إخطار النيابة العامة بذلك، والسبب في سهولة المعاينة في هذه الحالة أنها تتم علي عناصر مادية ملموسة كانت محلًا للجريمة، أو تخلفت عنها عكس المعاينة التي تتم عقب وقوع الجريمة، بواسطة مكونات غير مادية.

ثانيًا: مسرح الجريمة الافتراضي: ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكة الإنترنت، وفي ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن يتم على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.

ويثار التساؤل حول مدى صلاحية مسرح الجرائم الإلكترونية لمعاينته، وفي هذا الإطار يجب التفرقة بين الجرائم الواقعة على المكونات المادية للحاسب والجرائم الواقعة على المكونات المعنوية أو بواسطتها:

الحالة الأولى: الجرائم الواقعة على المكونات المادية للحاسب: وهذه الجرائم مثل: جرائم الاعتداء على أشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومكونات الحاسب نفسه ولوحة المفاتيح والأقراص وغيرها من مكونات الحاسب ذات الطابع المادي الملموس، والأمر هنا لا يثير صعوبة للتقرير بصلاحية مسرح الجريمة الذي يحوي هذه المكونات لمعاينته من قبل مأموري الضبط والتحفظ على الأشياء التي تعد أدلة مادية تدل على ارتكاب الجريمة ونسبتها لشخص معين وكذا

(16) المزروعي، سعيد سالم المزروعي وآخرون(2018م)، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الإماراتي، بحث منشور في مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث غزة، المجلد الثاني، العدد الثالث عشر، أكتوبر، ص117 وما بعدها، السرحاني، محمد بن نصير محمد(2004م)، مهارات التحقيق الجنائي في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ص77.

ISSN : 2410-1818

وضع الأختام في الأماكن التي تمت فها معاينة وضبط كل ما استعمل في ارتكاب الجريمة مع إخطار النيابة بذلك .[17]

الحالة الثانية: الجرائم الواقعة على المكونات المعنوية أو بواسطتها: وهي الجرائم الواقعة على برامج الحاسب وبياناته أو بواسطتها، وهنا تظهر صعوبات عدة تحول دون فاعلية المعاينة أو فائدتها، ويمكن تلخيص هذه الصعوبات في عاملين رئيسين هما: قلة الآثار المادية التي تتخلف عن الجرائم التي تقع على برامج الحاسب وبياناته أو بواسطتها، وكذلك الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبًا ما تكون طويلة نسبيًا وذلك ما بين اقتراف الجريمة والكشف عنها الأمر الذي يمنح فرصة لحدوث تغيير أو تلفيق أو عبث بالآثار المادية، أو زوال بعضها وهو ما يلقي ظلالًا من الشك على الدليل المستقى من المعاينة .[18]

نخلص مما تقدم أن إجراء المعاينة في الجريمة الإلكترونية يتقيد بعدة ضوابط، وإجراءات فنية يتعين مراعاتها، وتتمثل هذه الإجراءات فيما يلي:[19]

1. تصوير الحاسب الآلي، والأجهزة الطرفية المتصلة به، والمحتويات والأوضاع العامة بمكانه، مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحساب وملحقاته، ويُراعى تسجيل وقت وتاريخ ومكان التقاط كل صورة.
2. العناية بملاحظة الطريقة التي تم بها إعداد النظام.
3. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.
4. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب الآلي من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.
5. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.
6. التحفظ على محتويات سلة المهملات، من الأوراق الملقاة، أو الممزقة وأوراق الكربون المستعملة، والشرائط والأقراص المغنطة غير السليمة أو المحطمة، وفحصها ورفع البصمات التي قد تكون على علاقة بالجريمة المقترفة.

(17) عبد المطلب، سعد عاطف(2019م)، دور الشرطة في مكافحة الجرائم السيبرانية: المستحدثة وتحقيق الأمن المعلوماتي، مجلة بحوث كلية الآداب، جامعة المنوفية، المجلد 30، ع 118، يوليو، ص511.

(18) عبد المطلب، سعد عاطف، المرجع السابق، ص512.

(19) الخشاشنة، توفيق، المرجع السابق، ص85 وما بعدها.

ISSN : 2410-1818

7. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

الفرع الثاني

التفتيش في الجرائم الإلكترونية

يُعد التفتيش في الجرائم الإلكترونية من أهم وأخطر المراحل الجزائية على صعيد الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية، لأنه غالبًا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم، والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تساعد في ظهور الحقيقة، ونتيجة لذلك يُعد التفتيش في الجرائم الإلكترونية من أخطر المراحل الإجرائية التي تتخذ في مسرح الجريمة الإلكترونية إزاء مرتكب هذه الجريمة.

ويُعرف التفتيش الإلكتروني بأنه:" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل جهاز الحاسب الآلي أو أنظمة أو شبكة الإنترنت"[20]. كما عرف المجلس الأوروبي التفتيش المعلوماتي بأنه:" إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني".[21]

ويهدف التفتيش في نظم وشبكات الحاسب الآلي إلى حفظ الوسائط الإلكترونية التي سجلت عليها هذه البيانات لجمعها وتخزينها، كالأسطوانات والأقراص المغنطة ومخرجات الحاسوب، والتي تتعلق بالجريمة المعلوماتية وتفيد في كشف الحقيقة، أي أن محل التفتيش هو البيانات المعالجة آليًا، أما الضبط فهو وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة الإلكترونية، والتي تفيد في كشف الحقيقة عنها وعن مرتكبها، واستخدام البرامج الهامة من أجل الولوج للبيانات المراد ضبطها، إلى جانب وضع اليد على تلك الدعائم المادية.[22]

فالتفتيش الإلكتروني إذن هو إجراء تحقيقي يستهدف ضبط أدلة الجريمة الإلكترونية، مثل البرامج غير المشروعة والملفات المخزنة في الحواسيب الآلية والمعطيات المعلوماتية والاتصالات الإلكترونية، كما يشمل المحل الذي ينصب عليه التفتيش الإلكتروني إلى جانب المكونات المادية لجهاز الحاسب الآلي مكونات أخرى معنوية كشبكة المعلومات الدولية بسائر مكوناتها، ويخضع

(20) أحمد، هلالي عبد اللاه (1997م)، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي: دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ص47.

(21) عربوز، فاطمة الزهراء العلمي(2019م)، التفتيش الإلكتروني كإجراء للتحقيق في الجرائم المعلوماتية، بحث منشور في مجلة الأبحاث القانونية المعمقة، العدد 34، يوليو، ص106.

(22) الخشاشنة، توفيق، المرجع السابق، ص145.

ISSN : 2410-1818

التفتيش الإلكتروني للقواعد العامة في البطلان، من حيث أسبابه، وحالاته وأحكامه، وشروطه، فجميع القواعد المتعلقة بالتفتيش هي من القواعد الجوهرية التي يترتب على مخالفتها البطلان.

ويُشترط لمشروعية التفتيش الإلكتروني عدة شروط يمكن تقسيمها إلى شروط موضوعية، وأخرى شكلية، ويُقصد بالشروط الموضوعية بصفة عامة أي القواعد اللازمة لإجراء تفتيش صحيح، ويمكن حصرها في ثلاث شروط، وذلك على النحو التالي:

1. أن يكون هناك سبب للتفتيش في البيئة الإلكترونية، وهذا يقتضي وقوع جريمة إلكترونية بالفعل سواء كانت جناية أو جنحة، وأن يكون إجراء التفتيش بقصد ضبط أشياء تتعلق بالجريمة، أو تفيد في كشف الحقيقة[23]، وأن تتوفر في حق الشخص المراد تفتيشه– أي تفتيش شخصه أو تفتيش مسكنه -دلائل كافية تدعو للاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية.[24]

2. محل التفتيش في الجرائم المعلوماتية، وهذ يقتضي تحديد محل التفتيش في الجرائم الإلكترونية[25]، ويجوز تفتيش شخص المتهم أو شخص غيره إذا اتضح من أمارات قوية أنه يخفي أشياء تفيد في كشف الحقيقة، ويدخل في ذلك جهاز الحاسب الآلي خاصته أو المعدات ووسائل التقنية الإلكترونية الحديثة الأخرى [26]، كما يجوز لعضو النيابة العامة تفتيش منزل المتهم بناءً على تهمة موجهة إليه بارتكاب جريمة أو باشتراكه في ارتكابها[27]، ويحصل تفتيش منزل المتهم بحضوره أو حضور من ينوب عنه كلما أمكن ذلك، وإذا حصل تفتيش في منزل غير منزل المتهم يُدعى صاحبه إلى الحضور بنفسه أو بوساطة من ينيبه كلما أمكن ذلك .[28]

3. إسناد مهمة التفتيش إلى السلطة المختصة به قانونًا. فالأصل أن تقوم سلطة التحقيق الأصلية بتفتيش النظم المعلوماتية والإلكترونية بنفسها أو ندب رجل الضبط الجنائي للقيام بذلك وفقًا للقواعد الإجرائية المنصوص عليها في نظام الإجراءات الجزائية .[29]

(23) الزيودي، خالد راشد علي(2020م)، إجراءات تفتيش وضبط جرائم تقنية المعلومات في التشريع الإماراتي، بحث منشور في مجلة الأبحاث والدراسات القانونية، المركز العربي للدراسات والاستشارات القانونية وحل المنازعات، المغرب، العدد السابع عشر، ص241.

(24) المادة 4/28 من اللائحة التنفيذية لنظام الإجراءات الجزائية.

(25) بن يونس، عمر محمد أبو بكر، المرجع السابق، ص864، 865.

(26) المادة 45 من نظام الإجراءات الجزائية.

(27) المادة 44 من نظام الإجراءات الجزائية.

(28) المادة 47 من نظام الإجراءات الجزائية.

(29) المادة 42 من نظام الإجراءات الجزائية.

ISSN : 2410-1818

أما الشروط الشكلية للتفتيش في مسرح الجريمة المعلوماتي؛ فإنها تتمثل فيما يلي:

1. أن يشتمل بالإضافة على البيانات العامة اللازمة في أوامر الندب بأن يحدد المنزل المراد تفتيشه تحديدًا نافيًا للجهالة، ولا يشترط تسبيب الأمر بالتفتيش[30] ، وقد تقوم النيابة العامة بذلك بنفسها، وقد يقوم به رجل الضبط الجنائي في أحوال التلبس والندب.
2. إعداد محضر تفتيش خاص بالجرائم الإلكترونية: ولم يتطلب المنظم شكلًا خاصًا في محضر التفتيش، ولا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحضر عمومًا، وينبغي أن يكون هناك شخص متخصص في أمور المعلوماتية والحوسبة والإنترنت يرافق رجل الضبط الجنائي القائم بالتفتيش، للاستعانة به في مجال الخبرة الفنية الضرورية وفي صياغة مسودة محضر التفتيش.
3. الميقات الزمني للتفتيش: لم تضع غالبية التشريعات الجزائية قيدًا يوجب تمام التفتيش في وقت معين، فيجوز إجراء التفتيش في أي وقت ليلًا أو نهارًا، والتي من بينها الجرائم الإلكترونية محل البحث[31] . بخلاف المنظم السعودي الذي اشترط ضرورة أن يكون التفتيش نهارًا من شروق الشمس إلى غروبها في حدود السلطة التي يخولها النظام، ويمكن أن يستمر التفتيش إلى الليل ما دام إجراؤه متصلًا .[32]

وتجدر الإشارة إلى أن خضوع المكونات المادية للحاسب الآلي بمختلف أشكالها، وأنواعها للتفتيش في مسرح الجريمة الإلكترونية لا تثير أية إشكالية، فلا خلاف لدى الشراح[33] حول إمكانية خضوعها لنظرية التفتيش في حالة وقوع جريمة معلوماتية على اختلاف أشكالها[34]، فيخضع تفتيش الحاسب الآلي إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز. فإذا كان الحاسب الآلي مودعًا في مكان خاص، كمسكن المتهم أو أحد ملحقاته، فتأخذ حكم المسكن، وبالتالي لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم، وبذات الضمانات المقررة في نظام الإجراءات الجزائية. فإذا كانت مكونات الحاسب الآلي المراد تفتيشه في المسكن غير متصلة بنهايات طرفية موجودة في مكان آخر، فلا يوجد خلاف بشأن تفتيشها.

(30) المادة 29 من اللائحة التنفيذية لنظام الإجراءات الجزائية.
(31) كالمشرعين المصري والإماراتي مثلًا.
(32) المادة 52 من نظام الإجراءات الجزائية.
(33) إبراهيم، خالد ممدوح(2009م)، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، ص195 وما بعدها.
(34) العبيدي، أسامة بن غانم(2013م)، التفتيش عن الدليل في الجرائم المعلوماتية، بحث منشور في المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، ديسمبر، ص89.

ISSN : 2410-1818

وإذا كانت تلك النهايات مرتبطة في مكان آخر، وتطلبت دواعي التفتيش الوصول إليها وتفتيشها، فيجب مراعاة الضمانات والاشتراطات التي يتطلبها المنظم لتفتيش تلك الأماكن. أما بالنسبة للأماكن العامة، فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية، أو كان حائزًا لها أو مسيطرًا عليها؛ فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها قانونًا.[35]

أما الجرائم التي تقع على الكيان المعنوي للحاسب الآلي؛ فإنه يصعب اكتشافها إذا ظلت على صورتها المعنوية في شكل نبضات أو ذبذبات، أما إذا تحولت هذه الكيانات إلى مستخرجات أو مستندات أو سجلات فإنه يسهل الوصول إلى الجرائم التي ترتكب عليها، غير إنه قد أثار تفتيش المكونات المعنوية للحاسب الآلي خلافًا كبيرًا في الفقه بشأن جواز تفتيشها من عدمه ما بين معارض ومؤيد، فقد أثار أصحاب الرأي الأول الشكوك حول صحة عد البحث والتفتيش عن الأدلة في برامج وبيانات الحاسب الآلي والشبكات الإلكترونية من قبيل التفتيش بمعناه القانوني، واستطرد أصحاب هذا الرأي إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي بوصفه وسيلة للإثبات المادي؛ لأن ذلك يهدف إلى ضبط أدلة مادية تتعلق بالجريمة، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي.[36]

كما يبرر أنصار هذا الاتجاه بعدم إمكانية مواءمة أحكام التفتيش التي نص عليها القانون الإجرائي، مع ما قد يتطلبه كشف الحقيقة عن جرائم نظم المعلومات من بحث وتنقيب عن الأدلة الخاصة بهذه الجرائم خصوصًا وأن هناك بعضًا من التشريعات الإجرائية قد حددت مسبقًا هدف وغاية التفتيش في البحث عن شيء معين بذاته، ومن ثم ضبطه [37]، ويقترح أنصار هذا الاتجاه - لمواجهة القصور التشريعي- ضرورة النص صراحة على أن يُضاف إلى هذه الغاية التقليدية عبارة الأدلة الإلكترونية المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن أدلة المادة الإلكترونية.[38]

(35) العبيدي، أسامة بن غانم، المرجع السابق، ص89.

(36) طاهر، مصطفى(2002م)، المواجهة التشريعية لظاهرة غسيل الأموال المتحصلة من جرائم المخدرات، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، ص322.

(37) المادة 46 من نظام الإجراءات الجزائية؛ المادة 31 من اللائحة التنفيذية لنظام الإجراءات الجزائية؛ ومن بين تلك التشريعات الإجرائية التي أوردت عبارات أشياء أو الشيء: المواد 41، 44، 84 من قانون الإجراءات الجنائية المصري؛ المواد 46، 80، من قانون الإجراءات الجزائية العُماني؛ المواد 75، 78، 82، 92 من قانون الإجراءات الجنائية الليبي؛ المواد 61، 102، 105 من القانون الجنائي المغربي؛ المواد 93، 97، 99، 100 من مجلة الإجراءات الجزائية التونسي.

(38) عبد الناصر، حمد حسين موسى(2016م)، المواجهة الجنائية لجرائم الاعتداء على حقوق الملكية الأدبية والفنية عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة أسيوط، ص346.

ISSN : 2410-1818

بينما يتجه أنصار الاتجاه المؤيد [39]إلى اعتبار تفتيش الأنظمة والشبكات الإلكترونية من قُبيل التفتيش القانوني، ويرون أنه ولو كانت الطبيعة المادية للبيانات الإلكترونية، أو المعالجة آليًا مجرد نبضات أو ذبذبات إلكترونية، أو موجات كهرومغناطيسية، ما دام أنها قابلة لأن تسجل، وتخزن على وسائط أو على أوعية مادية؛ كالأسطوانات، والأقراص والأشرطة الممغنطة ومخرجات الحاسب الآلي، وأنه يمكن نقلها وبثها وحجبها، واستغلالها وإعادة إنتاجها، فهذا يعني إنها ليست شيئًا معنويًا؛ كالحقوق والآراء والأفكار، بل هي أشياء محسوسة ومادية، ولها وجود غير منكر في العالم الخارجي، وبالتالي فإنه يصح قانونًا أن يقع التفتيش عليها، وقد تم تأييد هذا الرأي بالعديد من القرارات القضائية .[40]

وبالتالي فإنه متى ما وجد القاضي الجنائي اطمئنانًا إلى الدليل الرقمي من خلال الفحص الفني أو أقوال الخبير الذي أعده ووجده وثيق الصلة بالجريمة المرتكبة، وكان واضحًا في دلالته نحو إثبات العلاقة بين الجاني والمجني عليه، ومن ثم؛ وقوع الجريمة فإنه يكون مقبولًا لديه وحجة في إدانة المتهم لا سيما أن الأدلة الرقمية عادة ما يدعمها رأي الخبراء المختصين في هذا المجال .[41]

وإذا كان المنظم السعودي لم ينص صراحة على مدى خضوع المكونات المنطقية للحاسب الآلي للتفتيش، إلا أنه قد أكد ذلك في نظام الإجراءات الجزائية، حيث أشار نص المادة 80 من نظام الإجراءات الجزائية السعودي إلى وقوع التفتيش على الأشياء المتعلقة بالجريمة أو التي تكون لازمة للتحقيق فيها، وأن للمحقق أن يفتش أي مكان ويضبط كل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج منها، وكل ما يفيد في كشف الحقيقة بما في ذلك الأوراق والأسلحة.

ويؤيد الباحث ما ذهب إليه أنصار الاتجاه الأخير المؤيد لفكرة جواز التفتيش الواقع على الكيان المعنوي للأنظمة والشبكات المعلوماتية للعثور على الدليل الإلكتروني الجاري البحث عنه وتحريزه، ولمواجهة القصور التشريعي في ذلك الأمر، نأمل من المنظم السعودي تعديل النصوص

(39) عبد الرحمن، خالد حمدي(1998م)، الحماية القانونية للكيانات المنطقي: برامج المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص72.

(40) ما قضت به المحكمة الجزائية بالأحساء في القضية رقم 3426314 لعام 1435هـ بسجن المتهم الأول ستة أشهر والمتهم الثاني أربعة أشهر لإدانتهما بالدخول غير المشروع لأحد المواقع الإلكترونية وتغيير بياناته الخاصة وإتلافه، مستندة في قضائها التقرير المعد من قبل المجموعة المتخصصة لتقديم الخدمات الإلكترونية للشبكة العنكبوتية وإفادة الجهة الأمنية المختصة المتضمنة أنه تم إخضاع الملقم للمعالجة الفنية وتبين أنه استخدم بالدخول على شبكة الإنترنت من خلال الهاتف المسجل باسم المتهم الأول وباستجواب المتهم الثاني أقر بأنه مشترك مع المتهم الأول باستخدام شبكة الإنترنت، وهو ما يثبت صدور هذا الفعل من الآي بي الخاص بالمتهمين، وقد تم تأييد الحكم من محكمة الاستئناف.

(41) المري، بهاء، المرجع السابق، ص449.

ISSN : 2410-1818

الخاصة بالتفتيش، وذلك بإضافة نصوص خاصة إلى نظام الإجراءات الجزائية السعودي تنظم هذا النوع من التفتيش، وجعل التفتيش يشمل المكونات المعنوية.

المطلب الثاني

الخبرة والشهادة في الجرائم الإلكترونية

تمهيد وتقسيم:

من المسلم به أن إجراءات جمع الأدلة والاستدلالات التقنية ذات طبيعة خاصة، وتحتاج لمتطلبات فنية، وخبرات معلوماتية معينة تساعد في التوصل لكشف الحقيقة، فكان من المتعين أن يعهد بهذه المهمة الحساسة والدقيقة لأشخاص يتم اختيارهم من بين أفضل العناصر الموجودة من الباحثين والمحققين الذين تتوفر لديهم الكفاءة العلمية، والخبرة الفنية في مجال علوم التقنية، وبرمجة الشبكات، ونظم المعلومات، وبالإضافة إلى الخبرة تُعد الشهادة في الجرائم الإلكترونية أحد الإجراءات المهمة في استخلاص الدليل الإلكتروني.

الفرع الأول: الخبرة في الجرائم الإلكترونية.

الفرع الثاني: الشهادة في الجرائم الإلكترونية.

الفرع الأول

الخبرة في الجرائم الإلكترونية.

يُقصد بالخبرة إبداء رأي فني من شخص مُختص فنيًا في شأن واقعة ذات أهمية في الدعوى؛ فهي وسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، وهي في حقيقتها ليست دليلًا مستقلًا عن الدليل القولي أو المادي، وإنما هي تقييم فني لهذا الدليل [(42)]، ويقوم الخبير التقني في سبيل التحري لبلوغ الحقيقة بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله، عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه، وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها مسببًا بشكل منطقي وإلا تعرض حكمها للنقض

وتستعين أجهزة العدالة الجنائية بأصحاب الخبرة الفنية المُتميزة في مجال تكنولوجيا المعلومات بُغية كشف غموض هذه الجرائم، وتجميع أدلتها والتحفظ عليها، ومُساعدة المُحققين فيها، واستجلاء غموضها خاصة في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق، فهذه

(42) فرج، محمد عبد اللطيف(2011م)، شرح قانون الإجراءات الجنائي وفقًا لأحدث التعديلات التشريعية، الجزء الأول، الطبعة الثالثة، بدون دار أو مكان نشر، ص277 وما بعدها.

ISSN : 2410-1818

الطائفة من الجرائم تتعلق بمسائل فنية غاية في التعقيد، فضلًا عن التطور السريع والمُتلاحق في وسائل ارتكابها، وهو ما يتطلب وجود خُبراء على درجة عالية من التخصص والخبرة.[43]

وهناك أسلوبان لعمل الخبير التقني، فالأسلوب الأول: يتمثل في القيام بتجميع وتحصيل لمجموعة المواقع التي تُشكل جريمة إلكترونية، ثم القيام بعملية تحليل فني لها بمعرفة كيفية إعدادها البرمجي، ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها وكيف تم التوصل إلى معرفتها، ومن ثم التوصل في النهاية إلى معرفة عناصر برتوكول الإنترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذا الموقع .[44]أما الأسلوب الثاني: القيام بتجميع وتحصيل لمجموعة من المواقع التي يشكل موضوعها جريمة في ذاته، وتؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم، كما هو الحال في المواقع التي تساعد الغير على التعرف على كيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها.[45]

ويلاحظ أنهُ يُعتبر رأي الخبير رأيًا استشاريًا لا يلزم المحكمة، فلها أن تأخذ به أو تطرحه، ولها أن تأخذ برأي الخبير ولو لم يكن جازمًا في المسألة التي طلب فيها الرأي منه، ولها أن تأخذ ببعض ما جاء في تقرير الخبير الذي ندبته سلطة التحقيق الابتدائي، وتطرح تقرير الخبير الذي هي ندبته أثناء المحاكمة، لذلك يذهب جانب من الشراح [46] إلى أن القاضي يظل هو الخبير الأعلى، حتى ولو كانت المسالة الفنية في مجال الإنترنت قد تعرض لها خبير الإنترنت، وأخذ القاضي برأيه، بل إنه حتى في حالة رفض الأخذ برأي الخبير فإن القاضي ليس ملزمًا بسلوك محدد؛ كالاستعانة بخبير آخر يقدم تقريرًا فنيًا، ومثل هذا المنطق لا يجعل الخبير في مستوى عمل القاضي، بل يظل دور القاضي قائمًا في المفاضلة بين التقارير الفنية المقدمة إليه.

ويثار التساؤل حول طبيعة التزام الخبير في الجرائم الإلكترونية؟، هل هو التزام ببذل عناية؟ أم بتحقيق نتيجة؟، وللإجابة عن هذا التساؤل نجد أن البعض من الشراح قد ذهب إلى أن التزام الخبير يكون ببذل عناية، فلا يُسأل إذا لم يصل إلى النتيجة المطلوبة نتيجة ضعف خبرته أو بسبب العقبات

(43) عقيدة، محمد أبو العلا(2003م)، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث منشور ضمن أعمال المؤتمر العلمي الأول حول: الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، في الفترة من 26–28 أبريل المنعقد في دبي، دولة الإمارات العربية المتحدة، ص6.

(44) الصغير، جميل عبد الباقي(2007م)، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، البصمة الوراثية : دراسة مقارنة، بحث منشور في مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد 49، العدد 2، يوليو، ص149.

(45) Patrick S. Chen,"An Automaic System for Collecting Crime Information on the Internet",Refereed article published on 31 October 2000, The Journal of Information, Law and Technology (JILT), 2000,on the following website: https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/chen/ Accessed 05/08/2023 at 01.15 Pm.

(46) عطا الله، شيماء (2005م)، الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظامين اللاتيني والأنجلوأمريكي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ص435.

ISSN : 2410-1818

التي واجهته أثناء مُباشرته لمُهمته، ويمكن أن تنشأ مسئوليته الجنائية إذا رفض القيام بالمُهمة المُكلف بها، أو أتلف عمدًا البيانات المطلوب منه التعامل معها أو حفظها، هذا إلى جانب التزام الخبير بالمُحافظة على السر المهني، فإذا أفشى الخبير أية معلومة أو بيان مُتعلق بالجريمة المُكلف بالعمل فيها، فإنه يعاقب بالعقوبة المُقررة لهذه الجريمة.(47)

ومما تجب الإشارة إليه في هذا الصدد أن المنظم السعودي قد أورد وسائل الإثبات على سبيل المثال لا الحصر، وذلك بهدف تمكين القائم على التحقيق من إذابة ما يوجهه من عقبات يمكن أن تظهر أثناء مباشرة التحقيق، كما أن المحقق غير ملزم باتباع ترتيب معين عند مباشرته للتحقيق، بل إنه غير ملزم من الأصل بمباشرة كافة الوسائل، وإنما يباشر منها ما تمليه عليه مصلحة التحقيق، وظروفه، وترتيبها وفقًا لما تقتضيه ظروف التحقيق.(48)

ويرى الباحث أنه لا يوجد-بلا شك-اختلاف لهذه القواعد بين الجرائم التقليدية والجرائم الإلكترونية، رغم الطابع الخاص الذي تتميز به الأخيرة المتمثل في كون محلها أو موضوعها غير مادي، رغم ما تثيره مسألة الإثبات في مجال الوسط الإلكتروني أو الافتراضي من صعوبات كبيرة أمام القائمين على التحقيق، والتي تتمثل في صعوبة اكتشاف هذه الجرائم بحسب أنها جرائم فنية تتطلب تقنية معُينة في مجال الحاسبات الآلية والإنترنت.

وحسنًا فعل المنظم المصري باستحداث سجلين للخبراء الذين يمكن لجهات التحقيق والمحاكمة الاستعانة بهم في الجرائم المعلوماتية، حيث يجوز للمحكمة وجهات التحقيق أن تندب أحد خبراء الجهاز القومي لتنظيم الاتصالات أو أحد خبراء المعلوماتية ممن هم مشهود لهم بالكفاءة والخبرة في هذا المجال المستحدث، وبما يواجه مشكلة عدم توافر العدد المناسب من الخبراء لدى الجهاز القومي لتنظيم الاتصالات في ضوء ضخامة الأعداد المتوقع نظرها من هذه القضايا أمام القضاء الجنائي (49)، وفيما يتعلق بالمنظم السعودي نجد أنه لم ينظم أية أحكام للخبرة أو الشهادة في نظام مكافحة جرائم المعلوماتية، تاركًا الأمر للقواعد العامة في نظام الإجراءات الجزائية، بخلاف المنظم المصري الذي أفرد لها أحكامًا مستقلة بموجب اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018م بموجب قرار مجلس الوزراء رقم 1699 لسنة 2020م.

(47) القاضي، رامي متولي، المرجع السابق، ص1269.

(48) فقد أورد المنظم السعوي تلك الوسائل في المادة 79 وما بعدها من نظام الإجراءات الجزائية.

(49) المادة العاشرة من القانون المصري رقم 175 لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات، والمادتين 5، 6 من اللائحة التنفيذية للقانون الصادرة بقرار رئيس مجلس الوزراء رقم 1699 لسنة 2020م.

ISSN : 2410-1818

الفرع الثاني

الشهادة في الجرائم الإلكترونية

يُلاحظ أن الشاهد في الجرائم الإلكترونية قد يكون ممن لديه الخبرة والتخصص الكافي في تقنية علوم الحاسب، حيث يكون لديه معلومات جوهرية لازمة للولوج إلى نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، وهذا ما يُعرف بالشاهد المعلوماتي، وذلك تمييزًا عن الشاهد التقليدي.(50)

ويميز الشراح في هذا الإطار بين كل من الخبرة والشهادة من حيث إن الأولى ترتكز على الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات على خلاف الثانية، ومن ثم كانت الخبرة وقفًا على الأخصائيين من أهل العلم والتكنولوجيا لا بناءً على مجرد مُشاهدتهم أو سماعهم، فالشاهد يدلي بأقواله عن الواقعة كما حدثت في مادياتها، أما الخبير فشهادته فنية؛ أي تنصرف إلى تقييمه الفني للواقعة محل الخبرة(51). لذلك أجاز الفقه الجزائي استبدال الخبير في الدعوى بغيره من الخبراء، وهو أمر غير مُتصور بالنسبة للشاهد لأن دوره في الدعوى قاصر عليه وحده. فالشاهد يقدم إلى القاضي معلومات حصلها بالملاحظة الحسية، أما الخبير فيقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية أو أصول فنية، ومع ذلك قد يجمع الشخص بين صفتي الشاهد والخبير، كطبيب شهد ارتكاب جريمة قتل وحاول إسعاف المجني عليه قبل وفاته، فأتيح له بذلك معرفة أسباب وفاته.

ويُلاحظ أنه إذا كانت الشهادة تنصب على ما رآه الشاهد بعينه أو عاصره بإحدى حواسه فإنه يكون من الصعب أن نطلب منه أن يقدم مساعدته للكشف عن الدليل أو الوصول إليه، فلا يجوز مثلًا إجبار العامل الفني لأحد الأنظمة المعلوماتية أن يقوم- لحساب البوليس- بطباعة أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات، فهذا البحث يدخل في اختصاص الخبير القضائي.(52)

وبالتالي فإنه ليس من واجب الشاهد وفقًا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الفقه الألماني، إذ يرى عدم التزام الشاهد بطبع البيانات المخزونة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على

(50) أحمد، هلالي عبد الاله (1997م)، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ص35.
(51) القاضي، رامي متولي، المرجع السابق، ص1269.
(52) الصغير، جميل عبد الباقي(2011م)، الحاسب الآلي كوسيلة لإثبات الجريمة، ندوة بعنوان: الواقع الأمني مسؤوليات- إنجازات- التي نظمها مركز بحوث الشرطة، القاهرة، المنعقدة في التاسع من يناير، ص20.

ISSN : 2410-1818

الإفصاح عن كلمات المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة [53]. بينما يتجه البعض الآخر إلى أن من بين الالتزامات التي يتحمل الشاهد بها القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، إذ يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطاتها في مجال الإجراءات المعلوماتية (54)، ومن ثم؛ يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم.[55]

ولا شك أن قيام الشاهد الذي يحوز كلمات المرور والشفرات الخاصة بأنظمة حاسوبية معينة بغية دخول سلطات التحقيق إليها للوصول إلى حقيقة واقعة إجرامية معينة أمر ضروري ومؤثر في الوصول إلى الدليل الإلكتروني، ولا شك أن ذلك الأمر يحتاج إلى إلزام، والإلزام لا يكون إلا بنص تشريعي، لذلك يرى الباحث أنه يتعين على المنظم السعودي المسارعة في تقنين ذلك الأمر لوضع حل تشريعي لهذه الإشكالية، وإن كان الأمر كذلك فيما يتعلق بالكشف والإفصاح عن كلمات المرور السرية، والشفرات الخاصة بالأنظمة الحاسوبية؛ فإنه في المقابل نجد أن الشاهد يلتزم بأداء الشهادة، أي التصريح بما لديه من معلومات تخص الواقعة محل الشهادة، وإن كان هناك بعض الأشخاص يسمح لهم القانون بعدم التصريح لما لديهم من معلومات لأنهم أمناء على هذه المعلومات، ومن أمثلة ذلك: الأطباء المحامون وغيرهم .[56]

ويجب أن يكون الشاهد لديه الخبرة والتخصص الكافي في تقنية علوم الحاسب، حيث يكون لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، وهذا ما يُعرف بالشاهد المعلوماتي، وذلك تمييزًا عن الشاهد التقليدي [57]، ويشمل الشاهد المعلوماتي بهذا الوصف ما يلي:[58]

1. المبرمجون: وهم الأشخاص الذين يقومون بتحليل الخطوات، وتجميع بيانات نظام معين، ودراسة هذه البيانات، ثم تحليل النظام إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات. كما يقوموا بتتبع البيانات داخل النظام عن طريق ما يُسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

(53) طاهر، أنسام سمير(2013م)،الحماية الجنائية لتكنولوجيا المعلومات، رسالة ماجستير، كلية القانون، جامعة كربلاء، العراق، ص37.

(54) علي، عبد الله حسين(2006م)،سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، القاهرة، ص383.

(55) المواد 62، 109، 138 من قانون الإجراءات الجنائية الفرنسي.

(56) الغني، محمود، المرجع السابق، ص180 وما بعدها.

(57) أحمد، هلالي عبد اللاه، المرجع السابق، ص35.

(58) حجازي، عبد الفتاح بيومي(2007م)، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ص38.

ISSN : 2410-1818

2. مشغل الحاسب: أي عامل تشغيل الحاسب وهو الشخص المسؤول عن تشغيل هذا الجهاز والمعدات المتصلة به، ويجب أن تكون لديه خبرة كبيرة في استخدام الجهاز ومكوناته، ومعلومات عن قواعد كتابة البرامج.
3. مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المعلقة به.
4. مديروا النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.
5. مقدموا الخدمات الوسطية في مجال المعلوماتية والإنترنت، وكذلك متعهدوا الوصول، ومتعهدوا الإيواء، ومسؤولوا المنتج، ومسؤولوا ناقل المعلومات، ومسؤولوا متعهد الخدمات، وكذلك مورد الخدمات، كذلك مورد المعلومات ومؤلف الرسالة.

كما قد يوجد عدد من الأشخاص بحكم وظيفتهم وخبرتهم واتصال عملهم بالتقنية والنظم المعلوماتية يمكن اعتبارهم كشهود معلوماتيون، بحيث يقع تحت بصرهم أو علمهم بعض المعلومات والأخبار التي تتصل بارتكاب جرائم معلوماتية، كمدخل البيانات، ومخطط البرامج والنظم المعلوماتية(59) .كما يوجد أيضًا محلل البيانات والنظم المعلوماتية، وهو من يقوم بتحليل الخطوات وتجميع بيانات نظام معين، ودراستها ثم تحليل النظام بتقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات، وتتبع البيانات داخل النظام، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب، وكل هؤلاء الأشخاص لابد أن يكون لديهم الخبرة والدراية الكافية في استخدام الحاسب الآلي والأجهزة التقنية، كذلك يجب أن يتوفر لديهم كم من المعلومات المناسبة عن استخدام الحاسب الآلي والنظم المعلوماتية .[60]

المبحث الثاني

الإجراءات المستحدثة للحصول على الدليل الإلكتروني

تمهيد وتقسيم:

أمام عجز وقصور الإجراءات التقليدية في البحث والتحري عن الجريمة المعلوماتية، واستخلاص الدليل الإلكتروني كان لزامًا على مختلف التشريعات الحديثة أن تبحث عن وسائل أكثر ملائمة مع الطبيعة الخاصة للجريمة الإلكترونية حتى تتحقق تلك النتيجة المرجوة من التحقيق، ومن هذه الإجراءات إجراء المراقبة الإلكترونية.

كما ساهمت تكنولوجيا الذكاء الاصطناعي إلى تعزيز الأمن والسلامة العامة في المجتمع، فقد ساهم استخدام تقنيات الذكاء الاصطناعي في مجال عمل الأدلة الجنائية وعلم الجريمة أيضًا في

(59)القاضي، رامي متولي، المرجع السابق، ص1268.
(60) أحمد، هلالي عبد اللاه، المرجع السابق، ذات الموضع.

ISSN : 2410-1818

تقديم أدلة دامغة إلى الجهات القضائية حول الجرائم، إلى جانب توفير معلومات ودلائل إلى الأجهزة الشرطية لفك ألغاز الجرائم المعقدة.

وبناءً عليه سوف يُقسم الباحث هذا المبحث إلى مطلبين نتعرف من خلالهما على دور كل من المراقبة الإلكترونية وكذلك تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية، وذلك من خلا التقسيم التالي:

المطلب الأول: دور المراقبة الإلكترونية في الكشف عن الأدلة الإلكترونية.

المطلب الثاني: دور الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية.

المطلب الأول

دور المراقبة الإلكترونية في الكشف عن الأدلة الإلكترونية

تمهيد وتقسيم:

تجدر الإشارة إلى أن المنظم السعودي مثله في ذلك مثل بقية التشريعات الأخرى لم يحدد الوسائل والطرق التي يتبعها رجل الضبط الجنائي في جمع الاستدلالات، فكل وسيلة مشروعة من شأنها الكشف عن الجريمة ومرتكبها يمكن أن يلجأ إليها رجل الضبط الجنائي طالما تحقق غاية الاستدلال، فليس هناك حدود معينة بالنسبة لقدر أو نوع المعلومات التي يتعين عليه أن يقوم بتحصيلها للوصول إلى الحقيقة، ومن الوسائل الحديثة في ذلك ما يعرف بالمراقبة الإلكترونية كأسلوب أو طريقة حديثة يسلكها الباحث الجنائي في استخلاص الدليل الإلكتروني.

الفرع الأول: مفهوم المراقبة الإلكترونية.

الفرع الثاني: ضوابط استخدام المراقبة الإلكترونية.

الفرع الأول

مفهوم المراقبة الإلكترونية

تُعرف المراقبة – عمومًا- على أنها:"وضع أشخاص أو أشياء أو أماكن تحت المراقبة السرية أو المكشوفة باستخدام الوسائل المشروعة، وبالطرق والمعايير الفنية، بغرض جمع أكبر قدر من المعلومات التي تفيد في منع الجرائم أو كشفها وضبط فاعليها"[(61)]. كما تُعرف كذلك بأنها:" وضع شخص أو مكان أو آلية تحت الملاحظة لتسجيل كل ما يحدث من تصرفات بطريقة غير محسوسة، وفي جو من السرية والحذر والكتمان على النحو الذي لا يمكن معه الإحساس بوجود هذه

(61) ناجي، يعقوب، وآخرين(2010م)، البحث والتحري الجنائي بواسطة الطرق التقليدية، بحث منشور في مجلة الدراسات الحقوقية، جامعة سعيدة الدكتور مولاي الطاهر، كلية الحقوق والعلوم السياسية، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية وواقعها في الجزائر، المجلد السابع، العدد الثاني، يونيو، ص536.

ISSN : 2410-1818

المراقبة[62]. أما المراقبة الإلكترونية فإنه يمكن تعريفها على أنها:" مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع البيانات والمعلومات عن المشتبه به، سواء أكان شخصًا أم مكانًا أو شيئًا حسب طبيعته لتحقيق غرض أمني أو لأي هدف آخر.[63]

وتُعتبر أنظمة المراقبة – عمومًا- من أهم وسائل جمع المعلومات وركيزة من ركائز التحري، تستمد أهميتها بأنها تُعطي رجل الضبط الجنائي منظور خاص حول القضية التي هو بصددها بحيث يبني خططه على أساس متين ومعلومات مؤكدة تختلف عن المعلومات التي استقاها من المرشدين، والذي يتطلب الأمر التثبت مما أورده لمعرفة مدى مصداقيته[64]. كما تُعتبر المراقبة الإلكترونية كذلك وسيلة من وسائل جمع المعلومات والبيانات عن المُشتبه بهم، يقوم بها مراقب إلكتروني وهو رجل الضبط الجنائي، يكون ذو كفاءة عالية في استخدام التقنيات الحديثة التي تتماشى مع نوع الجريمة، التي يتعامل معها مستخدمًا التقنية الإلكترونية.[65]

ومن أمثلة المراقبة الإلكترونية في الواقع الميداني: المراقبة في المطارات، والمراقبة عن طريق الأقمار الصناعية للمنافذ الحدودية، والمراقبة الإلكترونية للعديد من الأماكن الهامة، وهذا ما برز بشكل كبير في كشف غموض بعض القضايا الكبرى التي اعتمدت فيها التحريات على المراقبة الإلكترونية مثل: قضية سوزان تميم، وقضية قتل المبحوح بإمارة دبي، حيث سهلت المراقبة الإلكترونية الوصول للجاني. كما تبرز أهمية المراقبة الإلكترونية في الجرائم المنظمة كجرائم الاتجار بالبشر وجرائم غسل الأموال، وجرائم المخدرات.[66]

ومن الأمثلة على أهمية المراقبة الإلكترونية بنظام الفحص الإلكتروني في كشف غموض الجرائم المعلوماتية، ما قامت به وكالة التحقيقات الفيدرالية الأمريكية في تعقب مطلوبين والقبض عليهم عبر تحويل هواتفهم النقالة عن بعد إلى أداة للتجسس عليهم، وتقوم الفكرة على تلغيم جهاز الشخص المطلوب ببرنامج خاص، يقوم بتحويل عدد من القطع الإلكترونية الداخلية للجهاز على أدوات تسجيل وبث خاصة، ويمكن لمستخدم الهاتف النقال أن يشك إذا لاحظ سخونة دائمة على

(62) العصيمي، جزاء غازي(2002م)، إسهام البحث الجنائي في الكشف عن الجرائم المقيدة ضد مجهول، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ص103.

(63) موسى، مصطفى(2005م)، المراقبة الإلكترونية عبر شبكة الإنترنت: دراسة مقارنة، دار الكتب القانونية، المحة الكبرى، مصر، ص192.

(64) العصيمي، جزاء غازي، المرجع السابق، ص103.

(65) هروال، نبيلة هبة (2006م)، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ص199.

(66) النعيمي، سلطان عبيد(2017م)، التحري والاستدلال بواسطة الدوائر التليفزيونية، أكاديمية العلوم الشرطية، الشارقة، دولة الإمارات، ص59.

ISSN : 2410-1818

جهاز الهاتف أو استنزاف لشحن البطارية غير معتاد، أو صوت مكالمة عند تقريب الهاتف من سماعات جهاز ما كصوت زنّة معينة، فحينئذ قد يكون الجهاز مراقبًا.(67)

كما حققت تقنية برنامج كارنيفور نجاحات كبيرة في تعقب المجرمين والتحري عنهم، حيث أصدر مكتب التحقيقات الفيدراليF.B.I في يناير 2000م، أوامره بنصب هذا البرنامج للتنصت على مواقع المقامرة وغسيل الأموال، وقد نجح المكتب في هذه العملية، وتمكن من الحصول على أرقام الحسابات المستخدمة لإخفاء الأموال. كما تمكن من اعتقال أحد الأشخاص الفارين من الخدمة العسكرية، وكذلك تمكن مكتب التحقيقات وبفضل هذه التقنية من تقديم قرائن أدانت ميليشيات كانت تستخدم الإنترنت للتراسل، وللتخطيط للدخول لمنشآت عسكرية لسرقة متفجرات وتفجير محطات الطاقة الموجودة جنوب شرق الولايات المتحدة الأمريكية.(68)

كما تُعتبر المراقبة الإلكترونية من أهم مصادر التحري التي يستعين بها المحقق الجنائي في البحث والتقصي عن الجرائم عامة، وعن المشتبه بهم في الجرائم الإلكترونية وخاصة جرائم الإنترنت، إذ تعتبر أقصر الطرق لكشف الجرائم، إذ يجوز لمأمور الضبط القضائي اتخاذ أسلوب المراقبة الإلكترونية لجمع البيانات والمعلومات عن المُشتبه فيه في العالم الافتراضي عبر حلقات النقاش ومواقع الدردشة(69)، واستخلاص الأدلة الإلكترونية.

ومن الأمثلة أو النماذج على المراقبة الإلكترونية في الجرائم الإلكترونية، ما يلي:

1. نظام الفحص الإلكتروني: وهو تتبع حركة مسار الإنترنت الذي يطلق عليه علم البصمات المعاصر في الأساليب المتبعة في تتبع الحركة العكسية لمسار الإنترنت، الذي يمكن استخدامه من قبل المحقق الجنائي الإلكتروني في ملاحقة المشتبه بهم عبر الشبكة العنكبوتية.(70)
2. تقنية برنامج كارنيفور: وهي تعتبر من النماذج الخاصة بالمراقبة الإلكترونية التي طورتها إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي F.B.Iوذلك من أجل تعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بتوفير خدمات الإنترنت، ويشتبه أن تيار الرسائل المار عبر خدماتها يحمل معلومات عن جرائم أو أفعال

(67) الخشاشنة، توفيق، المرجع السابق، ص244.
(68) هروال، نبيلة هبة، المرجع السابق، ص202.
(69) الخشاشنة، توفيق، المرجع السابق، ص243.
(70) بدوي، أميرة محمود(2013م)، الإثبات الجنائي للجرائم المرتبكة عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ص293وما بعدها.

ISSN : 2410-1818

جنائية، ولا تتم عملية الفحص والتعقب إلا بعد استئذان المحكمة المختصة بوضع الشركة الموفرة للخدمة وأجهزتها تحت المراقبة.(71)

3. تقنية تعقب المواقع الإباحية: وهو برنامج يبحث عن الصور الجنسية المخلة بالآداب على أنظمة الكمبيوتر التي تعمل ببرامج ويندوز الحديث، فيقوم بإبلاغ الهيئات الحكومية عنها، وذلك من أجل تطهير الشبكة من المواقع الجنسية والإباحية، وهو ما يسمى ببرنامج "نوبد شرطي الإنترنت". فالبرنامج يصل على هيئة دورة إلكترونية ملحقه مع رسالة إلكترونية بعنوان "ساعدونا لإنهاء المواقع الإباحية، وقد بدأت المراقبة الإلكترونية لمواقع الإنترنت من خلال مراقبة المواقع الإباحية وحجبها عن المستخدمين في بعض الدول التي ترى ضرورة ذلك.(72)

وفي جميع الأحوال؛ فإن رجل الضبط الجنائي يهدف من المراقبة إلى الحصول على معلومات أو نتائج معينة، ومنها: الحصول على معلومات متصلة بوقائع جريمة وقعت بالفعل مثل مكان الجريمة أي مسرح الجريمة، ووقت وقوع الجريمة، وأسلوب ووسائل ارتكاب الجريمة، وأسبابها، والأدوات التي استخدمت في ارتكابها، والظروف المحيطة بالجريمة، وكذا أشخاصها، كما تهدف المراقبة إلى منع جريمة أو ضبط مرتكبيها متلبسين، مثل مراقبة شخص مهدد بالقتل لوجود معلومات عن احتمال قتله.كما تهدف المراقبة كذلك إلى الوقوف على نشاط شخص معين كمراقبة ذوي السمعة السيئة أو المفرج عنهم لمعرفة نشاطهم الإجرامي، كعملاء الاتجار في الأشياء المسروقة، وتجار الأسلحة غير المرخصة، كما تهدف إلى حماية أشخاص أو متابعة عمليات سرية كحراسة وتأمين أشخاص ذوي مكانة خاصة أثناء تواجدهم في مكان معين بدون الحراسة اللصيقة.(73)

وتأسيساً على ما سبق يتضح للباحث أن إجراء المراقبة الإلكترونية هو إجراء يقع أيضًا في إطار الإجراءات الوقائية ضد الجرائم التي يمكن أن ترتكب عبر شبكة المعلوماتية. بالإضافة إلى إمكانية إجراء مراقبة الاتصالات الإلكترونية في إطار التحقيقات للوصول إلى أدلة لم يكن من الممكن الوصول إليها لولا استخدام هذه الطريقة، بالإضافة إلى إمكانية استغلال هذه التقنية في البيئة الرقابية من أجل منع احتمال ارتكاب الجرائم الخطيرة عبر الشبكة المعلوماتية، لا سيما الجرائم التي من شأنها أن تهدد كيان الدولة والنظام العام.

(71) موسى، مصطفى محمد، المرجع السابق، ص209.
(72) النعيمي، سلطان عبيد، المرجع السابق، ص54.
(73) فوزي، محمد، (2019م)، عمليات البحث الجنائي، حكومة الشارقة، أكاديمية العلوم الشرطية، دولة الإمارات العربية المتحدة، ص82.

ISSN : 2410-1818

الفرع الثاني

ضوابط استخدام المراقبة الإلكترونية

إذا كانت الوسائل المستحدثة وعلى رأسها إجراء المراقبة الإلكترونية قد ساهمت بشكل كبير في ملاحقة مجرمي المعلوماتية، وكشف جرائمهم، إلا أنها قد أبرزت جانبًا خطيرًا آخر، وهو الاعتداء على حرمة الحياة الخاصة، وسرية الاتصالات والمراسلات باعتبار أن المراقبة الإلكترونية تقوم على التجسس والتنصت، حيث تتم المراقبة الإلكترونية سرًا دون موافقة وعلم الشخص المعني، حفاظًا على سرية وخصوصية المحادثات والمراسلات من جهة، ولضمان تنفيذ القانون من جهة أخرى.

فالمراقبة الإلكترونية في الغالب تنصب على المراسلات الإلكترونية مهما كان نوعها أو البرنامج الذي تمت بواسطته، حيث يهتم القائمون بعملية المراقبة بإخضاع كل المراسلات الإلكترونية لعملية الاعتراض والمراقبة، فالمراسلات تُعتبر مصدرًا غنيًا لتحصيل أدلة إثبات الجريمة الإلكترونية، ومن بين أنواع المراسلات التي يتم مراقبتها في الوقت الحالي المراسلات التي تتم عبر البريد الإلكتروني وعبر برنامج الفيسبوك أو برنامج الماسنجر أو الفايبر والسكايب، وغيرها العديد من برامج التواصل الإلكتروني، كون تلك البرامج من أكثر الوسائل الحديثة استخدامًا للاتصال عبر الإنترنت، وتعتبر مجالًا خصبًا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة وبدون حواجز.(74)

كما أن أغلب أنظمة التواصل الإلكتروني- حاليًا- والتي تكون محلاً للمراقبة الإلكترونية- تعتمد نظام للتراسل باستخدام شبكات الحاسب والذي يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميًا في صندوق خاص وشخصي للمستخدم، ولا يمكن الدخول إليه إلا عن طريق كلمة مرور، كما تأخذ المراسلات الإلكترونية أيضًا شكل محادثات فورية، وهي نوع من المحادثات التي تتم عبر شبكة الإنترنت، وتبعًا لذلك تأخذ الاتصالات الإلكترونية شكل المراسلات المكتوبة أو المحادثات الشفوية.

ولما كان إجراء المراقبة الإلكترونية إجراءً خطيرًا جدًا باعتباره ينتهك أهم الحقوق المكفولة دستوريًا، وهي سرية المراسلات والاتصالات، لذلك يلزم توافر الأسباب الجدية والكافية لمباشرة المراقبة الإلكترونية، وعدم اكتفائها بإساءة استعمال السلطة أو التعسف فيها أو الانحراف بها، وإلا خرجت عن غرضها المشروع وأضحت مجرد إجراء تعسفي لا يسانده القانون، وعلى ذلك فإنه يلزم لمباشرة المراقبة الإلكترونية - كقاعدة عامة - وجود أفعال قد بدت منها عناصر إجرامية معينة، أي

(74) براهيمي، جمال، (2018م)، التحقيق الجنائي في المراقبة الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، ص90.

ISSN : 2410-1818

توافرت إحدى الحالات المنذرة بالخطر أو أن يكون هذا الخطر قد تحول فعلًا إلى ضرر، وجدية المراقبة موضوع مستقل في تقديره عن نتيجتها.[75]

ولما كان الهدف الرئيس الذي يسعى إليه المحقق الجنائي من وراء اتخاذ مثل هذا الإجراء هو الحصول على دليل يساهم في كشف غموض الجرائم الإلكترونية، وتأكيد الأدلة المستخلصة من البحث والتحقيق حتى يتم إسناد الجريمة المرتكبة في الفضاء السيبيراني للمتهم، فإنه يتعين لإجراء المراقبة الإلكترونية أن يكون هناك إذن مكتوب[76]، فلا يجوز إجراء عمليات المراقبة للحصول على الدليل الإلكتروني إلا بإذن مكتوب من السلطة المختصة بالتحقيق.

وإذا كان المنظم قد خول لرجل الضبط الجنائي اتخاذ أسلوب المراقبة الإلكترونية لجمع البيانات والمعلومات عن المُشتبه فيه في العالم الافتراضي عبر حلقات النقاش ومواقع الدردشة، فإنه لا يجوز اللجوء لمراقبة الأحاديث الخاصة في البحث عن الأدلة إلا إذا توفرت لدى المحقق أدلة جادة تحتاج لتدعيم بإجراء هذه المراقبة[77] لذلك يتعين تجريم مراقبة الحوارات الخاصة لاعتدائها على حرمة الحياة الخاصة، إلا في الحالات الاستثنائية التي يخولها النظام.[78]

المطلب الثاني

دور الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية

تمهيد وتقسيم:

تُعتبر تقنيات الذكاء الاصطناعي من أهم ضروريات العصر والتي يجب دمجها داخل المجتمع، حيث تسهل الكثير من الأمور المتعلقة بالحياة البشرية اليومية، وتساعد في إنجاز العديد من المهام التي يصعب على الإنسان القيام بها وبكفاءة أعلى من الكفاءة البشرية، كما أنها تُعد التكنولوجيا الأكثر تطورًا في السوق الآن. فقد تم استخدام تطبيقات وتقنيات الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية واستخلاصها، وهو ما نوضحه من خلال ما يلي:

الفرع الأول: ماهية الذكاء الاصطناعي.

الفرع الثاني: فعالية تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية.

(75) النعيمي، سلطان عبيد، المرجع السابق، ص53، 54.

(76) سرور، أحمد فتحي، (1993م)، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ص583، 584.

(77) وهو ما قرره المشرع الجزائري في نص المادة 04 فقرة 06 من القانون رقم04/09، لسنة 2009.

(78) المادة 40 من النظام الأساسي للحكم في المملكة العربية السعودية.

ISSN : 2410-1818

الفرع الأول

ماهية الذكاء الاصطناعي

نظرًا لتعدد المفاهيم والتعريفات للذكاء الاصطناعي في وقتنا الحالي أدى إلى اختلاف الباحثين على وضع تعريف دقيق للذكاء الاصطناعي، فمنهم من نادى بأن تكون سلوكيات أنظمة الذكاء الاصطناعي تتماشى مع الذكاء البشري وتحاكيه، وفريق آخر يقول أنه ليس من الضروري أن تعتمد الأنظمة على نفس الطرق، والآليات التي يستخدمها البشر لسلوك معين، ورغم هذه الاختلافات في شرح ووصف الذكاء الاصطناعي، إلا أنهم يجتمعون في نقطة واحدة، وهي بناء نظام ذكي يتفوق على العوائق التي تواجه الذكاء البشري أو تباطؤه.[79]

ولقد عرّف البعض الذكاء الاصطناعي بأنه:" علم وهندسة صنع آلات ذكية، وخاصة برامج الكمبيوتر الذكية، وهي مرتبطة بالمهمة المتمثلة في استخدام أجهزة الكمبيوتر في أنشطة تعتمد علي فهم الذكاء البشري"[80]. بينما عرفه البعض الآخر بأنه:" أحد أفرع علوم الكمبيوتر المعنية بكيفية محاكاة الآلات لسلوك البشر، فهو علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بالطريقة نفسها التي يعمل بها الدماغ البشري، تتعلم مثلما نتعلم، وتقرر كما نقرر، وتتصرف كما نتصرف".[81]

نخلص من التعريفات آنفة الذكر أن الذكاء الاصطناعي ما هو إلا محاكاة لعمليات الذكاء البشري بواسطة الآلات، وخاصة أنظمة الكمبيوتر، وتشمل التطبيقات المحددة للذكاء الاصطناعي من أنظمة الخبرة وتقنيات معالجة اللغة الطبيعية، وتقنيات التعرف على الكلام، وتقنيات الرؤية الآلية لدي الأنظمة الحاسوبية، ويلعب الذكاء الاصطناعي دورًا مهمًا في مستقبل البشرية، ويقوم الحاسب الآلي بفضل الذكاء الاصطناعي بحل المسائل والمشاكل، والقيام بالأعمال الصناعية، والمجالات الهندسية والطبية، والعسكرية، والتعليمية، والأمنية.

وعلى هذا؛ يختلف الذكاء الاصطناعي عن البرامج الإلكترونية من حيث قدرته على العمل بدون سيطرة الإنسان أو تدخله المباشر، بحسبان أن المشتغلين بهذه التقنية يحدوهم الأمل في إكساب برامج الآلة الذكية قدرة على الوعي تسمح لها بالتعامل مع غيرها من البرامج أو الاشخاص، وقدرة على رد الفعل واتخاذ المبادرات استقلالًا ودون الحاجة إلى الرجوع إلى من قام ببرمجتها أو تشغيلها،

(79) سعيد، وليد سعد الدين محمد(2022م)، المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، بحث منشور في مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد 64، العدد 2، ص9.

(80) الغني، محمود(2021م)، الاتجاهات الحديثة في المسؤولية الجنائية للكيانات التي تعمل بتقنيات الذكاء الاصطناعي، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مصر، العدد 53، مايو، ص498.

(81) الفلاسي، عبد الله أحمد مطر (2021م)، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، بحث منشور في المجلة القانونية، كلية الحقوق، جامعة القاهرة فرع الخرطوم، المجلد التاسع، العدد الثامن، ص2844.

ISSN : 2410-1818

وهذا الوعي الاصطناعي ليس في منظور علماءه إلا مرتبطًا باعتقادهم أن الوعي الإنساني ليس إلا زيادة في عدد الشبكات العصبية التي تسمح بالقيام بعمليات عقلية معقدة، وأنه عند بلوغ أنظمة الذكاء الاصطناعي هذا الحد من التعقيد، فحتما تبلغ قدرًا عاليًا من الوعي مماثلًا لما يتمتع به الإنسان، ويمكنها أن تقوم بالتصرفات الذاتية.[82]

وتتعدد الطرق والتصنيفات المختلفة من أجل تصنيف أنواع الذكاء الاصطناعي، ومن هذه التصنيفات التصنيف وفقًا للمعيار الأساسي حيث ميز البعض من الفقه[83] بين نوعين من الذكاء الاصطناعي، وهما:

النوع الأول: الذكاء الاصطناعي الصناعي، وهو الذي يتم الاستعانة به في مجال التصنيع الآلي في المصانع، مثل: صناعة السيارات خاصة السيارات ذاتية القيادة، وصناعة الحاسب الآلي، وصناعة شاشات التليفزيون الذكية (سمارت) وغيرها من الصناعات المعقدة والتي تحتاج إلى عمليات عالية الدقة والتعقيد في إنشائها.

النوع الثاني: الذكاء الاصطناعي الخدمي أي الذكاء الاصطناعي الذي يتم تجسيده في شكل جسم الإنسان، والذي يملك قدرة التفاعل مع الغير، مثل: الروبوتات، ويتمتع هذا النوع من الذكاء الاصطناعي بالوعي العاطفي أي يتمتع بالقدرة على إجراء التفاعلات العاطفية من مشاعر الحب والكراهية والغضب؛ الأمر الذي يثير الكثير من التساؤلات القانونية حول ما إذا ارتكب السلوك الإجرامي المكون للجريمة، وما مدى إمكانية نسب هذا السلوك الإجرامي إلى الذكاء الاصطناعي، وبالتالي تحمله المسئولية الجنائية عن هذه الأفعال الإجرامية.

كما ميز البعض الآخر[84] بين ثلاث صور للذكاء الاصطناعي، النوع الأول: ذكاء اصطناعي متخصص: ويقصد به أنظمة الذكاء الاصطناعي التي تستطيع القيام بمهام محددة وواضحة؛ كالسيارات ذاتية القيادة، أو حتى برامج التعرف على الكلام أو الصور، أو لعبة الشطرنج الموجودة على الأجهزة الذكية، ويُعتبر هذا النوع من الذكاء الاصطناعي أكثر الأنواع شيوعًا وتوفرًا في وقتنا الحالي. بينما النوع الثاني: ذكاء اصطناعي عام: وهو النوع الذي يمكن أن يعمل بقدرة تشابه قدرة الإنسان من حيث التفكير، إذ يركز على جعل الآلة قادرة على التفكير والتخطيط من

(82) السيد، أحمد لطفي (2022م)، انعكاسات تقنية الذكاء الاصطناعي على نظرية المسؤولية الجنائية: دراسة تأصيلية مقارنة، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 80، ص257 وما بعدها.

(83) اللمعي، ياسر محمد، (2021م)، المسؤولية الجنائية عن أعمال الذكاء الاصطناعي ما بين الواقع والمأمول: دراسة تحليلية استشرافية، مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، الفترة من 23-24 مايو، ص831.

(84) القاضي، رامي متولي (2021م)، نحو إقرار قواعد للمسؤولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي، مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، الفترة من 23-24 مايو، ص883.

ISSN : 2410-1818

تلقاء نفسها، وبشكل مشابه للتفكير البشري، إلا أنه لا يوجد أي أمثلة عملية على هذا النوع، فكل ما يوجد حتى الآن مجرد دراسات بحثية تحتاج للكثير من الجهد لتطويرها وتحويلها إلى واقع. أما النوع الثالث: ذكاء اصطناعي فائق: وهو الذي قد يفوق مستوى ذكاء البشر، ويستطيع القيام بالمهام بشكل أفضل مما يقوم به الإنسان المتخصص وذو المعرفة، ولهذا النوع العديد من الخصائص التي لا بد أن يتضمنها؛ كالقدرة على التعلم، والتخطيط، والتواصل التلقائي، وإصدار الأحكام، إلا أن مفهوم الذكاء الاصطناعي الفائق يُعتبر مفهومًا افتراضيًا ليس له أي وجود في عصرنا الحالي، ويبرز أهمية تناول الأنواع الثلاثة الأخيرة من الذكاء الاصطناعي إلى تصور الاحتمالات التي قد تصل إليها تطبيقات الذكاء الاصطناعي في المستقبل، ومدى تصور انطباق قواعد القانون الجنائي عليها.

ولا شك أن تجهيز وتحفيز البنية النظامية لمواكبة تحديات تقنيات الذكاء الاصطناعي أصبحت ملحة لما لتلك الأخيرة من تأثير اقتصادي كبير، بحسبان ما سوف يؤدي إليه إدخال إنترنت الأشياء من تبعات على مستوى التوظيف والاستهلاك، مما قد يجلب العديد من المخاطر الاقتصادية بشأن التسريح الجماعي للموظفين ذوي المؤهلات المنخفضة. كما ستفتح هذه التقنيات مجالاً تنافسيًا رهيبًا بين الشركات الصناعية، بحكم ما سوف تسمح به تقنية التسجيل الموزعة أو الكتل المتسلسلة من تخزين ومعالجة للمعلومات بالنسبة لجميع أنواع القطاعات ومواقع الإنترنت، وما ستوفره من توسع في مجموعة متنوعة من الخدمات الإلكترونية، في مجالات اقتصادية واجتماعية عديدة.[85]

الفرع الثاني

فعالية تطبيقات الذكاء الاصطناعي في الكشف عن الأدلة الإلكترونية

لقد توسعت الأنشطة الإجرامية في الآونة الأخيرة إلى حد بعيد، وذلك من خلال اعتمادها على التكنولوجيا الحديثة والذكاء الاصطناعي على نحو مخيف من جرائم إرهابية وقرصنة وابتزاز، وسرقة إلكترونية، وغيرها، ومما يبعث الأمل أن تلك التكنولوجيا التي تعتمد عليها العصابات الإجرامية هي نفسها التي توفر فرص هائلة أمام مؤسسات الأمن للتصدي لهذه الجرائم ومواجهتها[86]، وهذا يدفعنا للتأكيد على ضرورة أن تتضمن استراتيجيات الأجهزة الأمنية اعتماد الذكاء الاصطناعي؛ كأحد الدعائم الرئيسة لمواجهة الجرائم الإلكترونية المستقبلية من أجل مواجهتها والقضاء عليها.

ويمكن للأجهزة الأمنية أن تطور من قدراتها من خلال استخدام تقنيات الذكاء الاصطناعي في كشف الجرائم لا سيما المعلوماتية منها، حيث يُستخدم الذكاء الاصطناعي في مجموعة واسعة

(85) السيد، أحمد لطفي (2022م)، المرجع السابق، ص250.

(86) إبراهيم، علي أحمد(2021م)، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، بحث منشور في المجلة القانونية، كلية الحقوق، جامعة القاهرة فرع الخرطوم، المجلد التاسع، العدد 8، ص2824.

ISSN : 2410-1818

من المهام الأمنية، ففي مجال البحث الجنائي والطب الشرعي يتم استخدام خوارزميات الذكاء الاصطناعي لتفسير صور الأشعة الطبية التي يمكن أن يكون لها آثار مهمة للعدالة الجنائية والفاحص الطبي عند تحديد سبب وطريقة الموت، كما تم استكشاف خوارزميات الذكاء الاصطناعي في مختلف التخصصات في علم الطب الشرعي، بما في ذلك تحليل الحمض النووي.[87]

كما يتم توظيف أنظمة الذكاء الصناعي في الكشف عن الجريمة، وهو ما يُعرف بالشرطة التنبؤية التي تعني جمع حلول التنبؤ[88]، والوقاية من الجريمة باستخدام تقنيات المعلومات المختلفة، وأنظمة الذكاء الاصطناعي بإمكانات تحليلية قوية ومجموعة غنية من البيانات المتكاملة المستمدة من تطبيقات نظم المعلومات، وتقوم فكرة هذه الأنظمة على تزويد الأجهزة الأمنية بالوسائل التكنولوجية والذكية بتحقيق أفضل استخدام للأشخاص والمعلومات المتوفرة لمراقبة اتجاهات الجريمة وقياسها والتنبؤ بها .[89]

ومن المرجح أن تشكل هذه التحليلات الدقيقة وفق نظام تنبؤ الجريمة إلى جانب تنبؤات ضباط الشرطة من ذوي الخبرة، قوة هائلة لردع الجريمة، ولا يخفى علينا إمكانية تغذية برامج الذكاء الاصطناعي المتطورة-سواء المتمثلة في ربوتات أو في أية تطبيقات ذكية أخرى قد تعتمد عليها الأجهزة الأمنية- بمجموعة من البيانات الخاصة بعدد من القضايا الأمنية والجرائم السابقة ومزيد من البيانات عن مرتكبيها ليبحث النظام الحاسوبي في برنامج الذكاء الاصطناعي الأنماط السائدة في الجرائم، ويقوم بتصنيفها ما يمكنه من التنبؤ بإمكانية وقوعها في المستقبل عند تكرار نفس الظروف والملابسات .[90]

ومن أحدث التقنيات العالمية للتنبؤ بالجريمة خاصية التعرف التلقائي على الوجه، المعروف باسم Facial recognition system، ويعمل هذا النظام من خلال تحليل ميزات الوجه الرئيسية، وإنشاء تمثيل رياضي لها، ثم مقارنتها مع الوجوه المعروفة في قاعدة البيانات داخل الأنظمة الأمنية، لتحديد التطابقات المحتملة، وأصبحت هذه الخاصية مألوفة بشكل متزايد للجمهور من خلال استخدامه في المطارات للمساعدة في إدارة عمليات فحص جوازات السفر وغيرها .[91]

---

(87) الغني، محمود، المرجع السابق، ص503.

(80)Strom ,Kevin,(2016),Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report, NCJ 251140,Affiliation: National Institute of Justice, May 2016,P.48, on the following website https://content.govdelivery.com/accounts/USDOJOJP/bulletins/1c9d005,Accessed 12/08/2023 at 01.00 Pm.

(89) البابلي، عمار ياسر(2019م)، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، بحث منشور في مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد 28، العدد 110، يوليو، ص61.

(90) إبراهيم، علي أحمد، المرجع السابق، ص2829.

(91) البابلي، عمار ياسر، المرجع السابق، ص62.

ISSN : 2410-1818

وهذا ما تم التأكيد عليه في الخطة الاستراتيجية الوطنية لبحوث تطوير الذكاء الاصطناعي في الولايات المتحدة الأمريكية عام ٢٠١٦م، حيث تم الاعتماد على تقنيات التعرف علي صور الوجه للمساعدة في تحديد هوية الفرد ومكان وجوده، حيث يعد فحص الحجم الهائل للصور ومقاطع الفيديو ذات الصلة المحتملة بطريقة دقيقة، وفي الوقت المناسب مهمة شاقة تستغرق وقتًا طويلًا، مع احتمال حدوث خطأ بشري بسبب الإرهاق، وغير ذلك من عوامل على عكس البشر، فالآلات لا تتعب، كما يقوم المحللون بإجراء تجارب علي استخدام الخوارزميات في التمييز بين مختلف الاشخاص باستخدام ملامح الوجه بنفس طريقة المحللين البشريين[92]. كما توجد هناك حالات مختلفة لاستخدامات أنظمة وتقنيات الذكاء الاصطناعي في العمل الشرطي والأمني، وهذا غالبًا ما يندرج تحت استراتيجية المدن الذكية، والتي من ضمن أهدافها استخدام التقنيات المتطورة، مثل: الذكاء الاصطناعي لضمان أمن وسلامة السكان في المدينة، ويمكن وصف المدينة الذكية بأنها مبادرة تقنية طويلة المدى، فعلى الرغم من وجود التقنية في كل ما يحيط بنا، إلا أنها تتحول على نحو متزايد إلى عنصر يعمل في الظل بهدف توفير بيئة مستدامة عالية الجودة للمواطنين.[93]

ولا شك أن مواكبة التقدم التكنولوجي الهائل في وسائل ارتكاب الجريمة لا تعني فقط تطوير الأجهزة الأمنية دون رفع كفاءة رجال الشرطة للتعامل مع هذه الأجهزة، حيث يتطلب الأمر تمتع رجال الشرطة بالمهارات الرقمية والتكنولوجية اللازمة من خلال وضع استراتيجية تدريب من قبل وزارة الداخلية لسد فجوة المهارات الرقمية في مجال العمل الشرطي، فالجرائم المعلوماتية والتهديدات الإرهابية والجريمة المنظمة آخذة في النمو متخذة أشكالًا غير متوقعة وجديدة حيث تستفيد المنظمات الإرهابية والإجرامية من المزايا التكنولوجية المقدمة عبر الإنترنت وتلك التي تعتمد على الذكاء الاصطناعي [94]. لذلك يجب على أجهزة الشرطة والأجهزة الأمنية أن تزيد من قدراتها بالاعتماد على تقنيات الذكاء الاصطناعي- والتي يعتمد عليها المجرمون في ارتكاب جرائمهم ومستمرون في تطوير تلك التقنيات- حيث أصبح توفر المعلومات والتكنولوجيا الجديدة للأجهزة الأمنية في غاية الأهمية لإحداث ما يشبه الثورة في العمل الجنائي من حيث التنبؤ بالجرائم واستباقها ومواجهتها بكل قوة.

وتقوم بعض الجهات الشرطية الرائدة حاليًا باستخدام الذكاء الاصطناعي، وتقنياته المختلفة في محاربة الجريمة[95]. حيث يتم استخدامه في مراقبة أنماط حركة المرور للتنبؤ بدقة كبيرة جدًا

(92) الغني، محمود، المرجع السابق، ص502، 503.

(93) بن عودة، حسكر مراد (2022م)، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، بحث منشور في مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد الخامس عشر، العدد الأول، أبريل، ص193.

(94) إبراهيم، علي أحمد، المرجع السابق، ص2825.

(95) وأفضل مثال: على ذلك ما قامت به شرطة مدينة نيويورك في إنشاء مركز إدارة الجريمة الذي يستخدم تقنيات تحليل البيانات والتنبؤ التحليلي، حيث يحتوي المركز على مستودع معلومات الجرائم التي تحدث في المدينة، ويقوم النظام بتحليل كمية كبيرة

ISSN : 2410-1818

بالاصطدامات، وتفاديها، وذلك لاستخدام هذه التقنيات في السيارات ذاتية القيادة، ويتم أيضًا استخدام تقنيات تعلم الآلة والذكاء الاصطناعي في مكافحة حالات التزوير والغش والاحتيال، وفي استخدام لنظام واطسن الذي طورته شركة IBM، تم تغذيته ببيانات شرطة مدينة نيويورك بين عام 2013م إلى عام 2015م لفهم العلاقة بين الحوادث والإصابات المصاحبة لها والوفيات، وبدأت هذه التطبيقات في اقتحام المجال الصناعي، ونجحت في القيام بالمهام الروتينية التي يقوم بها البشر في المصانع والمكاتب، بل ونجحت في القيام بالوظائف التي لا يمكن أن يقوم بها البشر كاستكشاف الفضاء أو أعماق المحيطات .[96]

كما يُعد التتبع الجغرافي للمتهم بواسطة GPS أحد مظاهر الرقمنة الجغرافية الجديدة لتحديد الموقع الجغرافي للأفراد والأشياء[97]، ويتمثل ذلك في تحديد الموقع الجغرافي في رصد تحركات الشخص، أو أي شيء سواء بعلم الشخص المعني أو دون علمه[98]، ويتم ذلك من خلال إجراء "تتبع ديناميكي" عن طريق الهاتف المحمول، أو قطعة GPS الموضوعة على سيارة، أو في كمبيوتر محمول، أو حقيبة، أو ملابس. ويتم نقل بيانات الموقع الذي ترسله الأقمار الصناعية إلى الهاتف بواسطة الأخير إلى هوائي الترحيل الذي يرسلها بدوره إلى مشغلي الاتصالات، وهي: شركات خطوط المحمول حيث يمكن نقلهم إلى خادم شرطة قبل ظهورهم أخيرًا في محطة عمل ضباط الشرطة.[99]

وبالإضافة إلى ما سبق بيانه تم استخدام التقنيات الذكية التي تعمل بالذكاء الاصطناعي في عملية التحليل الجنائي، والبحث عن الأدلة والسمات الحيوية، كبصمة الوجه والإصبع والعين والصوت، فقد تم استخدام نظام AFIS كنظام آلي للتعرف على بصمات الأصابع باستخدام الخوارزميات، حيث يقوم هذا النظام بتخزين البصمات وتصنيفها، والبحث فيها ومعالجها بسرعة

من بيانات الجرائم: الاتصال، والحوادث، والقبض، والمخالفات، والمخاطر المحتملة، وذلك للتنبؤ باحتمال وقوع الجرائم والاستعداد لها وتحسين زمن الاستجابة من خلال تكثيف وتوزيع الدوريات في الأماكن الأكثر عرضة لحدوث الجرائم.

(96) بن عودة، حسكر مراد، المرجع السابق، ص193.

(97)Alruily,Meshrif and Others (2010),Using Self Organizing Map to Cluster Arabic Crime Documents,Proceedings of the International Multiconference on Computer Science and Information Technology, Published 1 October 2010, P.357 on the following website: https://www.researchgate.net/publication/220947974_Using_Self_Organizing_Map_to_Cluster_Arabic_Crime_Documents, Accessed 11/08/2023 at 01.00 am.

(98)Al-Bastaki,Yousif A.Latif(2006), GIS Image Compression and Restoration: A Neural Network Approach. Information Technology Journal, 5: 88-93.

(99) صالح، تامر محمد(2021م)، التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية: دراسة مقارنة، بحث مُقدم إلى مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، المنعقد في الفترة من 23–24 مايو، ص7 وما بعدها.

ISSN : 2410-1818

ودقة عالية، كما تم استخدام نظام بصمة العين المعروف باسم Iris Scan، بالإضافة إلى ما يُعرف ببصمة المخ للتعرف على الجناة في الجرائم التي يتم ارتكابها.[100]

وإذا كان للذكاء الاصطناعي أهمية كبرى في آليات اكتشاف ورصد الجريمة وهوية مرتكبيها، وتخزين البيانات والأدلة التي يتم الحصول عليها من مسرح الجريمة خلال فترة زمنية محددة[101]، وذلك باستخدام الكاميرات الذكية لرصد مرتكبي الجرائم والتعرف عليهم وتحليل البيانات المسجلة للتعرف على سمات معينة، لتتبع والقبض على المجرمين أو الهاربين من العدالة. غير إنه يُخشى من إساءة استخدام واستغلال هذه البيانات الشخصية في التنميط الإلكتروني. بالإضافة إلى خاصية توقع ارتكاب الجرائم في المستقبل للوقاية من الجرائم باستخدام الذكاء الاصطناعي، وبالتالي الوقاية من الخطورة الإجرامية واحتمال ارتكاب جريمة في المستقبل.[102]

فرغم أن الذكاء الاصطناعي يُعد صورة من صور التطور التكنولوجي، وأعلاها منزلة في العصر الراهن، إلا أن الاعتماد عليه في كافة النشاطات، وما يترب عليه من آثار قانونية قد يكون محفوفًا بالمخاطر بسبب الأخطاء التي قد تنجم عن كيانات الذكاء الاصطناعي، ومن ثم يؤدي إلى الإضرار بالمتعاملين، مما يستلزم ضرورة البحث عن التكييف القانوني الذي يتناسب مع معطيات العصر، والنظر إلى المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي من منظور جديد يتناسب مع التطور التكنولوجي المذهل في كافة المجالات.[103]

وفي ظل ما أوضحنا من حتمية الاعتماد على أنظمة وتقنيات الذكاء الاصطناعي في المجالات الأمنية وخدمة العدالة، وأهمية ذلك في الحد من الجرائم المعلوماتية ومكافحتها، يثار التساؤل المهم حول النظام (القانون) الذي سوف تخضع له هذه الروبوتات أو الأجهزة الذكية التي سوف تعتمد عليها الأجهزة الأمنية في مكافحة الإجرام المعلوماتي، وهل سيكون المسؤول عن الخطأ المطور أم المبرمج أم المسير في ظل عدم وجود تشريع يحدد ذلك؟

لذلك أثار ظهور كيانات الذكاء الاصطناعي تساؤلات عديدة حول تحديد المسؤولية عن الجرائم التي يرتكبها الذكاء الاصطناعي، ويرجع ذلك أساسًا إلى أن الذكاء الاصطناعي يعمل على نحو مستقل مع سيطرة محدودة من البشر؛ الأمر الذي يدفع الباحثين للعمل في هذا المجال الهام،

(100)Rughani, Parag(2017),Artificial Intelligence Based Digital Forensics Framework, in:Gujarat Forensic Sciences University Gandhinagar,International Journal of Advanced Research in Computer Science, Vol.8, No.8, P.11.

(101)Karimi, Abbas and Others(2021),Cybercrime Detection Using Semi-Supervised Neural Network, in:Computer Science Journal of Moldova" (CSJM), Vol.29, No.2(86), P. 156.

(102) اللمعي، ياسر محمد، المرجع السابق، ص8.

(103) العدوان، ممدوح حسن مانع (2021م)، المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، بحث منشور في مجلة دراسات، علوم الشريعة والقانون، عمادة البحث العلمي، الأردن، المجلد 48، العدد الرابع، ص150.

ISSN : 2410-1818

في محاولة للإجابة على الإشكاليات القانونية الناتجة عن هذه التصرفات، ومنها مدى إمكانية المسئولية القانونية عن أعمال الذكاء الاصطناعي.

وفي هذا الإطار يقترح الباحث على المنظم السعودي أن يضع قانون خاص ينظم الاعتماد على تقنيات الذكاء الاصطناعي، ويضمن كذلك استخداماً آمناً لهذه التقنيات، بما يسمح بالاعتماد عليها بشكل آمن وأكثر فاعلية، مع ضرورة الالتزام بحماية خصوصية البيانات الشخصية الإلكترونية، بحيث لا يكون الوصول إليها متاحًا لأي شخص حماية لخصوصية هذه البيانات الشخصية من كافة صور الاعتداء عليها.

ISSN : 2410-1818

الخاتمة

في نهاية هذا البحث يمكن القول أن من الضروري تطوير أساليب البحث الجنائي على نحو يواكب على الأقل تطور الأساليب الإجرامية المنظمة، وذلك عن طريق رصد ظواهر الجريمة وتحليلها، وأساليب ارتكابها، وخطورتها الإجرامية، بتوظيف العلم والتكنولوجيا المتقدمة في تحليل تلك الظواهر، والاستفادة من نتائج هذا التحليل في تفعيل أعمال مكافحة الجريمة، مما يتطلب تزويد الأجهزة الأمنية بالوسائل والمعدات الحديثة التي تدعم قدرتها على التدريب لرجل البحث الجنائي.

ولقد خلص هذا البحث إلى مجموعة من النتائج والتوصيات نوردها فيما يلي:

أولًا: نتائج البحث:

1. لقد أصبح من الضروري مواكبة التطور التقني، وذلك بإدخال وسائل وطرق حديثة للكشف عن الجرائم والحصول على الأدلة التي تتناسب وطبيعتها، وهو ما عملت عليه أجهزة البحث والتحقيق من خلال الاستعانة بالوسائل الحديثة في إثبات الجرائم، مما أحدث ثورة علمية في مجال الإثبات الجزائي على نحو يصبح استخدام هذه الوسائل الحديثة أمرًا ضروريًا ليقوم رجال البحث والتحري بمهامهم على أكمل وجه.
2. يسعى المحقق الجنائي المختص بجرائم تكنولوجيا المعلومات بكل الوسائل التي تمكنه من التوصل للدليل، وفي هذا الإطار يكون من الضروري الاعتماد على تقنية تكنولوجيا المعلومات في جمع الدليل الإلكتروني، وذلك من أجل المساعدة في تجميع الدليل بالوسائل التقنية الحديثة، وكذلك اللجوء لإجراءات حديثة مستقلة بذاتها، فهناك بعض التقنيات التي تساهم في جمع الأدلة الإلكترونية، وبالتالي مساعدة المختصين بالأمن الإلكتروني الرقمي من مزاولة عملهم.
3. لما كان التفتيش والضبط عن بُعد في مسرح الجرائم المعلوماتية يتطلب استحداث أحكام إجرائية جديدة لمواجهة هذه الجرائم والتعامل معها، حيث إن اللجوء للقواعد التقليدية للقانون الجزائي غير مجد، بالإضافة إلى أن تطبيق النصوص التقليدية على تفتيش الجرائم المتعلقة بالإنترنت يخلق مشاكل تتعلق بالاختصاص والسيادة وغيرها، فكان من الطبيعي أن تتطور بالمقابل أساليب البحث والتحري وجمع الأدلة، فظهرت المراقبة الإلكترونية كإجراء ووسيلة حديثة للبحث والتحري عن الجرائم والمجرمين في إطار الجرائم الإلكترونية. كما يُعد الذكاء الاصطناعي من الميادين الحديثة التي تستقطب اهتمام كافة المجتمعات، والتي تشهد تطورات مستمرة، ومن المتوقع أن يكون للذكاء الاصطناعي دور مهم في مستقبل البشرية.

ISSN : 2410-1818

ثانيًا: توصيات البحث:

1. يقترح الباحث قيام المنظم السعودي بإضافة نصوص خاصة إلى نظام الإجراءات الجزائية السعودي تنظم مسألة التفتيش الواقع على الكيان المعنوي للأنظمة والشبكات الإلكترونية من أجل العثور على الدليل الإلكتروني الجاري البحث عنه، واستخراجه، وذلك بتعديل النصوص النظامية الخاصة بالتفتيش، وجعل التفتيش يشمل المكونات المعنوية، وذلك من أجل مسايرة ومواجهة التطورات العلمية.

2. يوصي الباحث المنظم السعودي اعتماد إجراء المراقبة الإلكترونية؛ كإجراء خاص واستثنائي ضمن أساليب البحث والتحقيق في كشف الجرائم الإلكترونية، وذلك بإدراج هذا الإجراء في صلب نظام الإجراءات الجزائية، مع النص على الضوابط النظامية والشرعية المقررة واللازمة لاستخدامه، لما له من دور كبير في مكافحة الجرائم المعلوماتية، بالإضافة إلى مساهمته- إلى حد كبير -في الحد من خطورتها، وقدرة الأجهزة المكلفة بالتحقيق الجنائي على ضبط بعض الجرائم وإحباط ارتكابها قبل وقوعها.

3. يقترح الباحث على المنظم السعودي أن يضع قانون خاص- أو من إدخال تعديلات نظامية على نظام الإجراءات الجزائية- ينظم من خلاله الاعتماد على تقنيات الذكاء الاصطناعي، ويضمن كذلك استخدام آمن لهذه التقنيات، بما يسمح بالاعتماد عليها بشكل آمن وأكثر فاعلية، مع ضرورة الالتزام بحماية خصوصية البيانات الشخصية الإلكترونية، بحيث لا يكون الوصول إليها متاحًا لأي شخص حماية لخصوصية هذه البيانات الشخصية من كافة صور الاعتداء عليها، مع تحديد المسئولية الجزائية لكيانات الذكاء الاصطناعي من حيث طبيعة الركن المادي والمعنوي للجرائم التي تقع من هذه الكيانات، وأحكام المسئولية، وأسباب امتناعها وغير ذلك من الجوانب ذات الصلة، مع تفريد المسؤولية الجزائية لكل من المصنع، والمالك، والتقنية نفسها، وكذلك المستخدم بصورة لا تقبل اللبس، حتى يمكن تحديد المسؤول جزائيًا، وإيقاع العقوبة عليه.

ISSN : 2410-1818

قائمة المراجع

أولًا: الكتب باللغة العربية:

1. إبراهيم، خالد ممدوح(2009م)، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية.
2. إبراهيم، خالد ممدوح (2009م)، فن التحقيق في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية
3. إبراهيم، الشحات(2011م)، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية.
4. أحمد، هلالي عبد اللاه (1997م)، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي: دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة.
5. أحمد، هلالي عبد اللاه (1997م)، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دار النهضة العربية، القاهرة.
6. حجازي، عبد الفتاح بيومي(2007م)، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.
7. سرور، أحمد فتحي، (1993م)، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة.
8. سلامة، مأمون (2010م)، قانون الإجراءات الجنائية معلقًا عليه بالفقه وأحكام النقض طبقًا لأحدث التعديلات والأحكام، الطبعة الثالثة، دار طيبة للطباعة، الجيزة، مصر.
9. أبو عامر، محمد زكي (1990م)، الإجراءات الجنائية، الطبعة الرابعة، دار النهضة العربية، القاهرة.
10. العصيمي، جزاء غازي(2002م)، إسهام البحث الجنائي في الكشف عن الجرائم المقيدة ضد مجهول، الطبعة الأولى، أكاديمية نايف العربية للعلوم الأمنية، الرياض.
11. علي، عبد الله حسين(2006م)، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الرابعة، دار النهضة العربية، القاهرة.
12. الغني، محمود (2019م)، دور الدليل الإلكتروني في الإثبات الجنائي: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية.
13. فرج، محمد عبد اللطيف(2011م)، شرح قانون الإجراءات الجنائي وفقًا لأحدث التعديلات التشريعية، الجزء الأول، الطبعة الثالثة، بدون دار أو مكان نشر.
14. فوزي، محمد، (2019م)، عمليات البحث الجنائي، حكومة الشارقة، أكاديمية العلوم الشرطية، دولة الإمارات العربية المتحدة.

ISSN : 2410-1818

15. المري، بهاء (2017م)، الوسيط في جرائم المخدرات والإنترنت وحجية الدليل الإلكتروني في الإثبات، طبعة نادي القضاة، القاهرة.
16. موسى، مصطفى(2005م)، المراقبة الإلكترونية عبر شبكة الإنترنت: دراسة مقارنة، دار الكتب القانونية، المحة الكبرى، مصر.
17. النعيمي، سلطان عبيد(2017م)، التحري والاستدلال بواسطة الدوائر التليفزيونية، أكاديمية العلوم الشرطية، الشارقة، دولة الإمارات، ص59.
18. هروال، نبيلة هبة (2006م)، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات: دراسة مقارنة، دار الفكر الجامعي، الإسكندرية.
19. بن يونس، عمر محمد أبو بكر (2004م)، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، الطبعة الأولى، دار النهضة العربية، القاهرة.

ثانيًا: الأبحاث والدراسات العربية:

1. إبراهيم، علي أحمد(2021م)، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، بحث منشور في المجلة القانونية، كلية الحقوق، جامعة القاهرة فرع الخرطوم، المجلد التاسع، العدد 8.
2. البابلي، عمار ياسر(2019م)، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، بحث منشور في مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد 28، العدد 110، يوليو.
3. بدوي، أميرة محمود(2013م)، الإثبات الجنائي للجرائم المرتبكة عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
4. براهيمي، جمال، (2018م)، التحقيق الجنائي في المراقبة الإلكترونية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر.
5. الخشاشنة، توفيق، (2016م)، معاينة مسرح الجريمة من خلال شبكة المعلومات الدولية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
6. الزيودي، خالد راشد علي(2020م)، إجراءات تفتيش وضبط جرائم تقنية المعلومات في التشريع الإماراتي، بحث منشور في مجلة الأبحاث والدراسات القانونية، المركز العربي للدراسات والاستشارات القانونية وحل المنازعات، المغرب، العدد السابع عشر.
7. السرحاني، محمد بن نصير محمد(2004م)، مهارات التحقيق الجنائي في جرائم الحاسوب والإنترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.

ISSN : 2410-1818

8. سعيد، وليد سعد الدين محمد(2022م)، المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، بحث منشور في مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد 64، العدد 2.
9. السيد، أحمد لطفي (2022م)، انعكاسات تقنية الذكاء الاصطناعي على نظرية المسؤولية الجنائية: دراسة تأصيلية مقارنة، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 80.
10. صالح، تامر محمد(2021م)، التتبع الجغرافي للمتهم بواسطة تقنية GPS والحق في الخصوصية: دراسة مقارنة، بحث مُقدم إلى مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، المنعقد في الفترة من 23-24 مايو.
11. الصغير، جميل عبد الباقي(2007م)، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، البصمة الوراثية: دراسة مقارنة، بحث منشور في مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد 49، العدد 2، يوليو.
12. الصغير، جميل عبد الباقي(2011م)، الحاسب الآلي كوسيلة لإثبات الجريمة، ندوة بعنوان: الواقع الأمني مسؤوليات- إنجازات- التي نظمها مركز بحوث الشرطة، القاهرة، المنعقدة في التاسع من يناير.
13. طاهر، أنسام سمير(2013م)، الحماية الجنائية لتكنولوجيا المعلومات، رسالة ماجستير، كلية القانون، جامعة كربلاء، العراق.
14. العازمي، فهد (2012م)، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
15. عبد الرحمن، خالد حمدي(1998م)، الحماية القانونية للكيانات المنطقي: برامج المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.
16. عبد الناصر، حمد حسين موسى(2016م)، المواجهة الجنائية لجرائم الاعتداء على حقوق الملكية الأدبية والفنية عبر الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة أسيوط.
17. العبيدي، أسامة بن غانم(2013م)، التفتيش عن الدليل في الجرائم المعلوماتية، بحث منشور في المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، ديسمبر.
18. العدوان، ممدوح حسن مانع (2021م)، المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، بحث منشور في مجلة دراسات، علوم الشريعة والقانون، عمادة البحث العلمي، الأردن، المجلد 48، العدد الرابع.

ISSN : 2410-1818

19. بن عودة، حسكر مراد (2022م)، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، بحث منشور في مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، المجلد الخامس عشر، العدد الأول، أبريل.
20. الغني، محمود(2021م)، الاتجاهات الحديثة في المسؤولية الجنائية للكيانات التي تعمل بتقنيات الذكاء الاصطناعي، بحث منشور في مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنوفية، مصر، العدد 53، مايو.
21. الفلاسي، عبد الله أحمد مطر (2021م)، المسؤولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي، بحث منشور في المجلة القانونية، كلية الحقوق، جامعة القاهرة فرع الخرطوم، المجلد التاسع، العدد الثامن.
22. القاضي، رامي متولي (2021م)، نحو إقرار قواعد للمسؤولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي، مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، الفترة من 23-24 مايو.
23. القاضي، رامي متولي(2021م)، ، المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون 175 لسنة 2018م، مقارنًا بالمواثيق الدولية والتشريعات المقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد 75، مارس.
24. لطفي، إبراهيم الشحات(2018م)، الحبس الاحتياطي وأهميته في الحفاظ على أدلة الجريمة: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة.
25. اللمعي، ياسر محمد، (2021م)، المسؤولية الجنائية عن أعمال الذكاء الاصطناعي ما بين الواقع والمأمول: دراسة تحليلية استشرافية، مؤتمر: الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، مصر، الفترة من 23-24 مايو.
26. المزروعي، سعيد سالم المزروعي وآخرون(2018م)، إجراءات التحقيق الجنائي في جرائم تقنية المعلومات وفقًا للتشريع الإماراتي، بحث منشور في مجلة العلوم الاقتصادية والإدارية والقانونية، المركز القومي للبحوث غزة، المجلد الثاني، العدد الثالث عشر، أكتوبر
27. ناجي، يعقوب، وآخرين(2010م)، البحث والتحري الجنائي بواسطة الطرق التقليدية، بحث منشور في مجلة الدراسات الحقوقية، جامعة سعيدة الدكتور مولاي الطاهر، كلية الحقوق والعلوم السياسية، مخبر حماية حقوق الإنسان بين النصوص الدولية والنصوص الوطنية وواقعها في الجزائر، المجلد السابع، العدد الثاني، يونيو.

ISSN : 2410-1818

ثالثًا: الأبحاث باللغة الإنجليزية:

1. Al-Bastaki,Yousif A.Latif(2006), GIS Image Compression and Restoration: A Neural Network Approach. Information Technology Journal, 5: 88-93.
2. Alruily,Meshrif and Others (2010),Using Self Organizing Map to Cluster Arabic Crime Documents,Proceedings of the International Multiconference on Computer Science and Information Technology, Published 1 October 2010, P.357 on the following website: https://www.researchgate.net/publication/220947974_Using_Self_Organizing_Map_to_Cluster_Arabic_Crime_Documents, Accessed 11/08/2023 at 01.00 am.
3. Karimi, Abbas and Others(2021),Cybercrime Detection Using Semi-Supervised Neural Network, in:Computer Science Journal of Moldova" (CSJM), Vol.29, No.2(86).
4. Patrick S. Chen,"An Automaic System for Collecting Crime Information on the Internet",Refereed article published on 31 October 2000, The Journal of Information, Law and Technology (JILT), 2000,on the following website: https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/chen/ Accessed 05/08/2023 at 01.15 Pm.
5. Rughani, Parag(2017),Artificial Intelligence Based Digital Forensics Framework, in:Gujarat Forensic Sciences University Gandhinagar,International Journal of Advanced Research in Computer Science, Vol.8, No.8, P.11.
6. Strom ,Kevin,(2016),Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report, NCJ 251140,Affiliation: National Institute of Justice, May 2016,P.48, on the following website https://content.govdelivery.com/accounts/USDOJOJP/bulletins/1c9d005,Accessed 12/08/2023 at 01.00 Pm.