دور الذكاء الاصطناعي في اثبات الجرائم السيبرانية

The Role of Artificial Intelligence in Proving Cybercrimes

أ.م.د. هدى عباس محمد رضا

كلية القانون – جامعة الكوفة

Hudaa. alshamaa@uokufa. edu. iq

تاريخ استلام البحث: ٢٠٢٦/٥/٨ تاريخ قبول النشر: ٢٠٢٦/٧/٣٠

الملخص:

يمثل الذكاء الاصطناعي احد اهم ما خلفته الثورة الصناعية الرابعة التي نقلت العالم الى العصر الرقمي لما انتجته من تقنيات تكنولوجية متطورة خاصة تقنيات الذكاء الاصطناعي، فالعصر الذي نعيشه الان يستحق ان نطلق عليه عصر الذكاء الاصطناعي الذي سيغير حياة البشر من خلال انشاء أجهزة وبرامج كومبيوتريه ذكية ومتطورة قادرة على التفكير والعمل بالطريقة ذاتها التي يعمل بها العقل البشري، وقد اثر هذا التطور بشكل ملحوظ على اشخاص ارتكاب الجريمة وأسلوب ارتكابها والذي يتمثل في استخدام اخر ما توصلت اليه العلوم التكنولوجية وتطويعها في خدمة الجريمة فأصبحت الجريمة تقع بواسطة الحاسب الالي او عليه او بواسطة شبكة الانترنت كما ان هذه الوسائل الرقمية الحديثة ساعدت في اثبات واكتشاف الجرائم اذ ان للذكاء الاصطناعي دور مهم في الوصول للحقيقة في اكثر أنواع الجرائم وخاصة الجرائم السيبرانية فهذا النوع من الجرائم ترتكب في بيئة تقنية المعلومات فالحاسوب والشبكات الرقمية الأداة الرئيسية في ارتكابها ومحلها المعلومات المخزنة في الحاسوب وشبكاته كما انها ترتكب اثناء احدى مراحل تشغيل نظام المعالجة الالية للمعلومات سواء في مرحلة الادخال او المعالجة او الإخراج كما ان الجريمة السيبرانية متعددة النطاق الجغرافي لان انتاج هذه الجريمة لا يقتصر على دولة دون دولة أخرى فالبشرية شريكة في الاستفادة من هذا النتاج الادبي الفني والى جانب ذلك فان الاستخدام غير المشروع لهذه الوسيلة والشبكة اتصف بالعالمية وسنسلط الضوء في بحثنا على دور الذكاء الاصطناعي بتقنياته المختلفة في اثبات الجرائم السيبرانية والتوصل الى معرفة مرتكبيها.

الكلمات المفتاحية: الذكاء الاصطناعي، جرائم سيبرانية، اثبات.

Abstract:

Artificial intelligence (AI) is one of the most significant outcomes of the Fourth Industrial Revolution, which ushered the world into the digital age. This revolution produced advanced technologies, particularly AI technologies. The era we live in now deserves to be called the age of artificial intelligence, which will transform human life by creating intelligent and sophisticated computer devices and programs capable of thinking and functioning in much the same way as the human mind. This

development has significantly impacted the perpetrators of crimes and the methods used to commit them. Crimes are now often committed using, on, or via computers or the internet. These modern digital tools have also aided in proving and detecting crimes, as AI plays a crucial role in uncovering the truth in most types of crimes, especially cybercrimes. Cybercrimes are committed within an information technology environment, where computers and digital networks are the primary tools. The information stored on the computer and its networks is the target. Cybercrimes are committed during any stage of an automated information processing system, whether input, processing, or output. Furthermore, cybercrime has a multi-faceted geographical scope, as its production is not limited to any one country. Humanity shares in the benefits of this technology. This artistic literary output, in addition to the illegal use of this medium and network, has been characterized by globalization. In our research, we will highlight the role of artificial intelligence with its various technologies in proving cybercrimes and identifying their perpetrators.

Keywords: Artificial intelligence, cybercrimes, proof.

المقدمة

أولاً: موضوع البحث: بالرغم من ان العديد من أنواع الجرائم الالكترونية تتطلب درجة عالية من التنظيم والتخصص الا انه لا توجد ادلة تجريبية كافية للتحقق مما اذا كانت الجرائم الالكترونية تهيمن عليها مجموعات الجريمة المنظمة وما هو الشكل او البنية التي تكون عليها هذه المجموعات لقد مكنت التكنولوجيا السيبرانية الافراد بشكل غير مسبوق فنجح المراهقون الذين يتصرفون بمفردهم في تعطيل أنظمة الحكم في الحركة الجوية واغلاق مواقع كبار التجار الالكترونيين وافساد التعامل مع الصفقات في البورصات العالمية، وما يمكن للأفراد القيام به يمكن أيضا للمؤسسات القيام به وغالبا ما يكون افضل لأنه يكون اكثر دقة وتنظيم ويتم بالتعاون مع المتخصصين تقنيا. وجدير بالذكر ان العديد من المنظمات الاجرامية قادرة على الانخراط في الجرائم السيبرانية فالإنترنت والتقنيات ذات الصلة تتناسب تماما مع التنسيق بين المناطق المتفرقة وبالتالي قد تكون مجموعة الجريمة المنظمة عصابة مافيا تقليدية عالية التنظيم او مشروع اجرامي قصير المدى تقوده مجموعة تقوم بجريمة محددة عبر الانترنت تستهدف مجموعة معينة.

أهمية البحث: تكمن أهمية البحث في تقييم مدى كفاية النصوص الجنائية الواردة في قانون أصول المحاكمات الجزائية العراقي في التعامل مع ادلة الذكاء الاصطناعي مع ضرورة سد الفراغ التشريعي كما ان أهمية البحث تتجسد في وضع معايير لقبول ادلة الذكاء الاصطناعي امام المحاكم وتحقيق التوازن بين تمكين سلطات التحقيق بالأدوات الفعالة وضمان حقوق الدفاع وتطوير اليات تعاون قضائي دولي منسجمة مع استخدام ادلة الذكاء الاصطناعي في الجرائم السيبرانية عابرة الحدود.

مشكلة البحث: تتمثل المشكلة البحثية في القدرة على توظيف الذكاء الاصطناعي في الاثبات الجنائي فالقوانين الجنائية في العراق لا تتضمن نصوصا صريحة تنظم معايير قبول او رفض الأدلة المستخلصة بالذكاء الاصطناعي مما يولد إشكالية في الشرعية الجزائية وموثوقية هذه الأدلة امام القضاء كما ان القضاء يعوزه تقييم مخرجات الخوارزميات المعقدة كما ان الجرائم السيبرانية عابرة للحدود وهذا يزيد من تعقيد نطاق الاختصاص القضائي.

هيكلية البحث: سنتناول موضوعنا الموسوم ب دور الذكاء الاصطناعي في اثبات الجرائم السيبرانية على مبحثين خصصنا الأول لماهية الذكاء الاصطناعي و الجرائم السيبرانية اما المبحث الثاني الاثبات بأدلة الذكاء الاصطناعي في الجرائم السيبرانية

خطة البحث:

المبحث الأول ماهية الذكاء الاصطناعي و الجرائم السيبرانية

المطلب الأول التعريف الذكاء الاصطناعي والجرائم السيبرانية

الفرع الأول تعريف الذكاء الاصطناعي وانواعه

الفرع الثاني التعريف بالجرائم السيبرانية وانواعها

المطلب الثاني جريمة الإرهاب السيبراني وصلتها بالذكاء الاصطناعي

الفرع الأول تعريف جريمة الإرهاب السيبراني

الفرع الثاني اهمية الذكاء الاصطناعي في ردع الإرهاب السيبراني

المبحث الثاني الاثبات بأدلة الذكاء الاصطناعي في الجرائم السيبرانية

المطلب الأول مفهوم الدليل السيبراني

المطلب الثاني الدليل السيبراني المستمد من الذكاء الاصطناعي

الفرع الأول اثبات الجرائم السيبرانية بواسطة الجيل الأول من الذكاء الاصطناعي

الفرع الثاني اثبات الجرائم السيبرانية بواسطة الجيل الثاني من الذكاء الاصطناعي

الفرع الثالث حجية الدليل السيبراني المستمد من الذكاء الاصطناعي

المبحث الأول: ماهية الذكاء الاصطناعي والجرائم السيبرانية

اتجه الانسان الى التفكير لابتكار طرق جديدة في حفظ المعلومات ونقل المعارف والخبرات من العنصر البشري وصولا الى شيء يحاكي العقل الإنساني ويصبح شريكا له في التفكير والتعلم فكان لابد من اللجوء الى أنظمة تكنولوجية وصناعية قادرة على استيعاب المعارف وتطويرها ومن هنا برزت فكرة الذكاء الاصطناعي كما ان تطور ثورة المعلومات والتكنولوجيا زاد معها التطور مما اثر على الجرائم ولذلك اصبحنا نرى صورا مستحدثة للجرائم ومنها الجرائم السيبرانية في التعدي على انتهاك المعلومات سواء اكانت على الفرد او الشركات او حتى على الدول والحكومات فهي جرائم عابرة للحدود، وسنتناول في هذا المبحث ماهية الذكاء الاصطناعي والجرائم السيبرانية وسنقسم المبحث الى مطلبين سنخصص

المطلب الأول لماهية الذكاء الاصطناعي والجرائم السيبرانية اما المطلب الثاني سنتناول فيه للتعريف بالجرائم السيبرانية اما المطلب الثاني سنتناول فيه جريمة الإرهاب السيبراني وصلتها بالذكاء الاصطناعي.

المطلب الأول: ماهية الذكاء الاصطناعي والجرائم السيبرانية

سنتناول في هذا المطلب التعريف بالذكاء الاصطناعي والجرائم السيبراني اذ سنقسمه الى فرعين خصصنا الفرع الأول للتعريف بالذكاء الاصطناعي اما الفرع الثاني للتعريف بالجرائم السيبرانية

الفرع الأول: التعريف بالذكاء الاصطناعي وانواعه

ان الذكاء الاصطناعي يوجد حاليا في كل مكان واصبح له دور لا يستطيع احد انكاره او تجاهله في مجالات الحياة المختلفة حتى في مجال الجرائم وخاصة الجرائم السيبرانية سنتناول تعريف الذكاء الاصطناعي في اللغة والاصطلاح وأنواع الذكاء الاصطناعي

أولا تعريف الذكاء الاصطناعي في اللغة والاصطلاح:

١. **تعريف الذكاء الاصطناعي في اللغة:** الذكاء في اللغة يعني حدة الفؤاد وسرعة الفطنة والذكاء مشتق من ذكا ذكي يذكى ذكا وذكى فهو ذكي وجمعها اذكياء ويقال رجل ذكي وفلان من الاذكياء يراد به المبالغة في الفطنة [١] اما الاصطناعي في اللغة اصلها منصنع واصطناع واصطنع [٢] وقال تعالى (وَاصْنَعِ الْفُلْكَ بِأَعْيُنِنَا) [٣] ويراد به أيضا هو ما كان مصنوعا وغير طبيعي[٤].

٢. تعريف الذكاء الاصطناعي في الاصطلاح سنتناول تعريف الذكاء الاصطناعي في التشريع والفقه والقضاء فعلى الصعيد التشريعي لم نجد تعريفا للذكاء الاصطناعي في قانون العقوبات العراقي اما بالنسبة الى مشروع مكافحة الجرائم الالكترونية في العراق لم يتطرق الى تعريف الذكاء الاصطناعي الا انه نص على الجرائم الالكترونية التي ترتكب باستخدام وسائل تقنية وتشمل تلك الوسائل الأجهزة الالكترونية والانترنت والشبكات.

اما بالنسبة للفقه فقد تعددت التعاريف المطروحة للذكاء الاصطناعي فعرفه راي بانه كل ما يهدف الى تطوير السلوكيات في الآلات الذكية في البيانات المعقدة[٥] وعرف بانه محاولة جمع الآلات الذكية التي تسلك سلوك الانسان المتسم بالذكاء والذي يتطلب التفكير والسمع والتفهم بأسلوب منطقي ومنظم للقيام بعمل معين او تنفيذ مهمة معينة مع منحها قدرا من الاستقلال والادراك [٦] وبراينا ان الذكاء الاصطناعي في مجال بحثنا يراد به مجموعة من الأنظمة البرمجية القائمة على الخوارزميات وتحليل البيانات التي تستخدم في كشف الأدلة الرقمية واستخراجها وربطها وتحليلها والتنبؤ بالأنماط الجرمية بما يعزز قدرة السلطات التحقيقية على اثبات الجرائم المرتكبة عبر الوسائل الالكترونية.

اما بالنسبة للقضاء لم يرد حكم من القضاء العراقي حسب اطلاعنا يعرف الذكاء الاصطناعي ويعتبر القضاء العراقي الاعمال التي يتم ارتكابها عبر تقنيات الذكاء الاصطناعي تدرج ضمن الجرائم الالكترونية او الجرائم التقليدية.

ثانيا أنواع الذكاء الاصطناعي: ان الذكاء الاصطناعي ليس نوعا واحدا وانما يتم تقسيمه بحسب القدرة المزود بها وينقسم الى ثلاثة أنواع:

١. الذكاء الاصطناعي المحدود وهو ابسط أنواع الذكاء الاصطناعي يبرمج للقيام بوظائف معينة لموضوع معين وهذا النوع قد يتفوق على ذكاء البشر في جوانب دون أخرى أي انه ذكاء اصطناعي متخصص في مجال واحد وهذا النوع من الذكاء الاصطناعي يدخل في اغلب جوانب الحياة فيعد اكثر الأنواع انتشارا وينتج عنه مشاكل قانونية فنجده في برمجة الصراف الالي والعاب الأجهزة الذكية وغيرها(٧)

٢. الذكاء الاصطناعي العام ويعمل هذا النوع من أنواع الذكاء الاصطناعي بقدرات مشابهة لقدرات الانسان في مختلف المجالات فيجمع البيانات ويحللها ويحولها الى معلومات تنتج من الخبرات والمواقف لبتي يكتسبها وتؤهله لاتخاذ قرارات ذاتية ومستقلة (٨)

٣. الذكاء الاصطناعي القوي وهنا قدرة الذكاء الاصطناعي تتجاوز قدرة ذكاء الانسان ثلاثة اضعاف كما ان المهمات التي يقوم بها تفوق المهمات التي يقوم بها الانسان المتخصص كالطبيب ورجل القانون اذ ان الذكاء الاصطناعي هنا اه القدرة على التخطيط والتعلم والتواصل وإصدار الاحكام والقرارات ولم يتوصل الخبراء حتى الان الى بلورة حقيقية متكاملة لهذا النوع من الذكاء (٩) وبراينا ان أنواع الذكاء الاصطناعي في اطار بحثنا تتجسد بأنظمة تحليلية تعنى بمعالجة البيانات الرقمية واستخلاص الأنماط الجرمية وأنظمة ادراكية تتوالى تحليل الصور والبيانات والاصوات وأنظمة تنبؤية تهدف الى استشراف السلوك الاجرامي المحتمل وجميعها تمثل وسائل تقنية داعمة لسلطة التحقيق دون ان تحل محل السلطة القضائية في تكوين قناعتها.

الفرع الثاني: التعريف بالجرائم السيبرانية وانواعها

ان مصطلح الجريمة السيبرانية هو احدى المصطلحات الحديثة والمستخدمة عن جرائم الانترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الاجرام المرتبط والمصل ببقية المعلومات، وسنتناول في هذا الفرع تعريف الجرائم السيبرانية قي اللغة والاصطلاح وانواعها.

أولا/ تعريف الجرائم السيبرانية في اللغة والاصطلاح:

١. **تعريف الجرائم السيبرانية في اللغة:** الجرائم السيبرانية تتألف من كلمتين هما الجريمة والسيبرانية، ويراد بالجريمة في اللغة الذنب ونقول اجرم وجرم واجترم والجريمة من الجناية بمعنى الذنب كقوله جرم اليهم وعليهم جريمة اجرم بمعنى جنى وجرم اذا عظم جرمه أي اذنب (١٠) اما السيبرانية ان اصل كلمة سيبرانية هي ترجمة المصطلح cybernetics والذي يعني القائد او الربان او الموجه وهي كلمة يونانية الأصل والسيبراني يتعلق بالعالم الافتراضي او الشبكات والحواسيب أي انه كل ما يتعلق بالعالم الرقمي وجدير بالذكر لا يوجد تعريف للسيبرانية في معاجم اللغة كونه مصطلح حديث، فالجريمة السيبرانية حاليا يراد بها الجريمة التي ترتكب باستخدام الحواسيب والشبكات.

٢. **تعريف الجرائم السيبرانية في الاصطلاح:** سنتناول تعريف الجرائم السيبرانية في التشريع والفقه والقضاء، فمن الناحية التشريعية لم يعرف قانون العقوبات العراقي النافذ الجريمة السيبرانية [١١] اما بالنسبة الى مشروع مكافحة الجرائم الالكترونية العراقي فقد تطرق الى الجرائم الالكترونية اذ عرف فيها النظام المعلوماتي والشبكة المعلوماتية والبيانات كذلك تناول الجرائم التي ترتكب ضد أنظمة المعلومات، الا ان هذا المشروع لم يتم اقراره لذا فأننا نحتاج الى إقرار تشريع متكامل لمكافحة الجرائم السيبرانية. اما على صعيد الفقه فقد تعددت التعاريف الفقهية المطروحة بشأن الجرائم السيبرانية فعرفها رأي في الفقه بانها السلوك غير المشروع او المنافي للأخلاق او غير المسموح به والمرتبط بالشبكات المعلوماتية العالمية [١٢] وعرفها راي اخر في الفقه بانها نشاط اجرامي تستخدم فيه تقنية الحاسب الالي بطريقة مباشرة او غير مباشرة كوسيلة او هدف لتحقيق الفعل الاجرامي المقصود [١٣] وعرفها اخر بانها الجرائم التي تتم بواسطة الكومبيوتر او احد وسائل التقنية الحديثة على كومبيوتر اخر او احد وسائل التقنية الحديثة مع ضرورة توفر شبكة اتصال بينهما [١٤] وبراينا نؤيد التعريف الذي يرى بان الجرائم السيبرانية اعمال غير قانونية يتم ارتكابها باستخدام الكومبيوتر كأداة او هدف او كليهما ويمكن ان تنطوي على أنشطة إجرامية تقليدية مثل السرقة والاحتيال او التشهير وتخضع لقانون العقوبات واحيانا تكون جرائم مستحدثة، وتصنف الجرائم السيبرانية حسب طريقة ارتكابها الى نوعين الأول جرائم استخدام الكومبيوتر كهدف حيث يستخدم الكومبيوتر للهجوم على أجهزة أخرى مثل القرصنة، هجمات الفايروسات، هجمات سحب الخدمة، اما النوع الثاني استخدام الكومبيوتر كسلاح حيث يستخدم الكومبيوتر في ارتكاب جرائم العالم الحقيقي مثال ذلك انتهاك حقوق الملكية الفكرية، الإرهاب السيبراني، الاحتيال في بطاقات الائتمان وعمليات الاحتيال عبر التحويل الالكتروني والمواد الإباحية [١٥]

اما بالنسبة للتعريف القضائي وبحسب اطلاعنا لم يتطرق القضاء العراقي الى تعريف الجرائم المعلوماتية ومنها الجرائم السيبرانية وترك ذلك للفقه.

ثانيا/ أنواع الجرائم السيبرانية: تتعدد أنواع الجرائم السيبرانية بحسب الهدف من ارتكابها وسنتناولها بالتفصيل:

١. **الاعتداء السيبراني على الامن:** ويتحقق من خلال انشاء موقع لمنظمات ارهابيه على الشبكة المعلوماتية ونشره لتسهيل الوصول لقيادة المنظمة او أعضاءها او الترويج لأفكارها او تمويلها او نشر الية تصنيع المتفجرات او أي أداة تستخدم في العمليات الإرهابية كذلك تتحقق من خلال الدخول غير المشروع الى نظام معلوماتي للحصول على بيانات تمس الامن الخارجي او الداخلي للدولة او اقتصادها الوطني [١٦]

٢. الاعتداء على معطيات الحاسب الالي كالتلاعب بالمعلومات المخزنة داخل الحاسب الالي واتلاف المعلومات والبيانات والبرامج

٣. الاعتداء السيبراني على حرمة الحياة الخاصة ويتحقق من خلال تشويه سمعة شخص او التشهير به او نشر صوره او صور خاصة لأفراد عائلته او الاستيلاء على العناصر الشخصية كالاسم والصورة والبيانات الشخصية المتصلة بالحياة الخاصة [١٧]

٤. الاحتيال والتغرير السيبراني ويتم الاحتيال عن طريق الاستيلاء لنفسه او لغيره على مال منقول او على سند او توقيعه عن طريق الاحتيال اما التغرير السيبراني فيتحقق من خلال بانتحال شخصية المواقع وذلك باختراق حاجز امني وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يحوله موقع بيني او يحاول اختراق موقع لاحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي الى توجه شخص الى موقعه بمجرد كتابة اسم الموقع المشهور [١٨]

٥. التنصت السيبراني ويراد به استخدام برنامج في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع الى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم ادخال هذا الملف الى جهاز الشخص المعتدى عليه عن طريق البريد الالكتروني او مواقع يزورها المعتدى عليه فيقوم بتنزيل عدة برامج ومنها برنامج التنصت او استخدام برنامج المحادثة فيقوم المجرم بإغراء الضحية بان هذا البرنامج يحتوي على العاب مثيرة او غير ذلك فيقوم الضحية باستقبال الملف [١٩]

٦. السطو السيبراني على اعمال البنوك ويتم ذاك عن طريق استخدام الجاني الحاسب الالي للدخول الى شبكة الانترنت والوصول غير المشروع الى البنوك والمصارف والمؤسسات المالية وتحويل الأموال من تلك الحسابات الخاصة بالعملاء الى حسابات أخرى وذلك بإدخال بيانات غير حقيقية او تعديل او مسح البيانات الموجودة بقصد اختلاس الأموال او نقلها او اتلافها وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جدا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال.

٧. الاعتداء السيبراني على الاخلاق والاتجار بالبشر وبالمخدرات ويتحقق ذلك بإنشاء موقع على الشبكة المعلوماتية او احد أجهزة الحاسب الالي او نشره للاتجار بالبشر او تسهيل التعامل به، او انشاء والمواد والبيانات المتعلقة بالشبكات الإباحية او الأنشطة المخلة بالآداب العامة او نشرها ويمكن ان يتحقق بإنشاء موقع على الشبكة المعلوماتية او احد أجهزة الحاسب الالي او نشره للاتجار بالمخدرات او المؤثرات العقلية او تسهيل التعامل بها او ترويجها او نشر الية تعاطيها[٢٠]

٨. الاعتداء السيبراني على حقوق الملكية الفكرية ويتحقق من خلال الاعتداء على العلامات التجارية وبراءات الاختراع ونسخ وتقليد البرامج وإعادة انتاجها وصنعها دون ترخيص فهو اعتداء على الحقوق المالية والحقوق الأدبية[٢١]

المطلب الثاني: جريمة الإرهاب السيبراني

تتميز الجريمة السيبرانية عن الجريمة التقليدية ان محلها هو الحاسوب وشبكة الانترنت العالمية مما يثير عدة صعوبات حول اثباتها ولعل اهم صور الجريمة السيبرانية الجريمة جريمة الإرهاب السيبراني وسنتناولها بالبحث تباعا اذ سنقسم المطلب الى فرعين خصصنا الفرع الأول للتعريف بجريمة الإرهاب السيبراني اما الفرع الثاني سنتناول فيه أهمية بالذكاء الاصطناعي في ردع الإرهاب السيبراني.

الفرع الأول: جريمة الارهاب السيبراني

ان الإرهاب يستخدم الانترنت كوسيلة لتبادل المعلومات لسهولة وسرعة التداول ولتوافر الحماية الأمنية اذ ارتكب الإرهاب العديد من الجرائم التي تميزت بجسامة اضرارها المادية والمعنوية مستغلا الانترنت على اعتبار ان ارتكاب الجرائم بواسطة الانترنت تحتاج وقت وجهد اقل واقل خطورة واكثر امن وسهولة.

والمقصود بجريمة الإرهاب السيبراني هو التقاء الفضاء السيبراني والإرهاب ويتم تنفيذه عبر الفضاء الالكتروني من قبل الافراد او الجماعات او المنظمات التي تتأثر بالحركات الإرهابية بدافع التأثير السياسي او الأيديولوجي وقد يؤدي الإرهاب السيبراني الى عنف جسدي وتداعيات نفسية للضحية بشكل مباشر [٢٢] وهناك صورتين للإرهاب السيبراني الهجين والخالص

أولا الإرهاب السيبراني الهجين وهو نوع من أنواع الإرهاب السيبراني يقوم على استخدام الانترنت للقيام بأنشطة إرهابية مثل الدعاية والتجنيد والتطرف وجمع الأموال واستخراج البيانات والاتصالات والتدريب والتخطيط للهجمات الإرهابية، اذ قد يستخدم الارهابيون الانترنت لنشر وإدارة دعاياتهم من خلال حرب المعلومات لنقل ايديولوجياتهم وإدارة الحرب النفسية و تجنيد أعضاء جدد من خلال المواقع الالكترونية الإرهابية ومختلف منصات التواصل الاجتماعي فيسبوك وإنستغرام ويوتيوب وتويتر كما استخدمت الجماعات الإرهابية الرسائل المشفرة وغرف الدردشة عبر الانترنت او إخفاء المعلومات عن المناقشات السرية والتخطيط والتنسيق لهجمات حقيقية والتخطيط لعمليات القرصنة كما ان جمع التبرعات لتمويل العمليات الإرهابية لم يتم فقط عن طريق المنظمات الخيرية بل اصبح يتم عن طريق منصات ومدونات الوسائط الاجتماعية واستخدام عملة البتكوين الرقمية كما يستخدم الارهابيون الانترنت لاستخراج البيانات وجمع المعلومات من أماكن وافراد معينين كهدف محتمل للتجنيد والهجمات [٢٣]

ثانيا الإرهاب السيبراني الخالص يعرف بانه نوع من أنواع الإرهاب السيبراني يقوم على استخدام الانترنت للهجوم المباشر على البنى التحتية للضحية لتحقيق اهداف سياسية ودينية وايديولوجية والإرهاب السيبراني الخالص اما يكون مدمر او تخريبي ويراد بالإرهاب السيبراني المدمر بانه التلاعب في وظائف نظام المعلومات وافساده لتدميره او تدمير الاصول الافتراضية المادية والسلاح الأكثر شعبية هو استخدام فايروسات الكومبيوتر والديدان وحصان طروادة اما الإرهاب السيبراني التخريبي وهو قرصنة مصممة لهدم المواقع الالكترونية وتعطيل نمط الحياة الطبيعي الذي يعتمد على البنى التحتية الحيوية التي تدعم المرافق الطبية والنقل والأنظمة المالية [٢٤] وقد نشطت عدة مجموعات من القراصنة المؤيدين لداعش في اختراق مواقع الويب لتشويه مواقع الانترنت ونشر الأفكار المتطرفة وفتح الحرب الكترونية على مواقع وسائل التواصل الاجتماعي ولتعزيز موقفهم في الفضاء الالكتروني تم دمج قدراتهم على الاختراق مثل دمج مجموعات بمسميات مثل قسم الخلافة الشبح وجيش أولاد الخلافة وجيش الخلافة الالكتروني والخلافة السيبرانية المتحدة وقد قاموا مجموعة من القراصنة المتحدين عبر الانترنت بنشر مقطع فديو يدعوا

القراصنة من المسلمين الى استخدام قدراتهم على الاختراق للمساعدة في معركة ضد الدول المعادية لتلك للتنظيمات من ذلك هجمات مجموعة الفلاجة التونسية وهي مجموعة قرصنة تونسية مرتبطة بداعش هاجمت العديد من المواقع الالكترونية التابعة لوزارة الصحة البريطانية من خلال هجوم تشويه صاحبه استبدال صفحات الويب بصور من الحرب في سوريا وشملت رسائل مثل أوقفوا القتل في سوريا [٢٥]

الفرع الثاني: أهمية الذكاء الاصطناعي في ردع الإرهاب السيبراني

عندما يتحقق هجوم الإرهاب السيبراني يترك اثارا تشير الى الجناة وهنا يبرز دور الذكاء الاصطناعي من خلال تعقب بصمات الاصابع الالكترونية او معلومات الشبكة والبرامج الأخرى الذكية من اجل اثبات الجريمة واسنادها للفاعل الذي شن الهجوم السيبراني وهنا يبرز دور الطب الشرعي السيبراني والذي يقوم عبر آليات الذكاء الاصطناعي بأثبات وتحليل مصدر الهجوم السيبراني ولكن الامر ليس بهذه السهولة بسبب استخدام الجناة لوسطاء الكترونيين او شن الهجوم من خلال عملاء مجهولين الهوية يخفون عنوان بروتكول الانترنت الخاص بهم لكن بالغالب تكون للذكاء الاصطناعي قدرة قوية ومعروفة بإثبات مصدر الهجوم السيبراني الى الجناة فقدرات الذكاء الاصطناعي ليست قاصرة على استخدام الجماعات الإرهابية لها فحسب ولكن من الممكن ان تقوم الدول والحكومات وأجهزة المخابرات باستخدام الذكاء الاصطناعي في التنبؤ والتعرف على الجماعات الإرهابية والقدرة على منعهم من العمليات الإرهابية من الأساس من خلال عدة أساليب:

أولا/ المساعدة في تقويض الأفكار المتطرفة: ان الجماعات الإرهابية تستخدم الذكاء الاصطناعي لعمل فيديوهات وصور تروج لأفكارها الإرهابية لجذب المستخدمين العاديين لذا يستخدم الذكاء الاصطناعي في التعرف على المحتوى الذي يحمل أفكارا إرهابية وتقوم بحجبه.

ثانيا/ المساعدة في تحديد وقت وموقع الهجمات الإرهابية: ويتم تحديد وقت ومكان الهجمات الإرهابية من خلال تتبع استخدام الجماعات الإرهابية للإنترنت وحجوزات الطيران الخاصة بهم كذلك معاملاتهم البنكية وغير ذلك من المعاملات الأخرى

ثالثا/ المساعدة في التعرف على وجه الإرهابيين: من الممكن استخدام الذكاء الاصطناعي من قبل الحكومات للتعرف على الإرهابيين المنتمين الى جماعات إرهابية فعلى سبيل المثال قامت الشرطة الفيدرالية الألمانية في ٢٠١٧ و٢٠١٨ بتركيب كاميرات تتضمن خاصية التعرف على الوجوه والتي تعتمد على الذكاء الاصطناعي في محطة قطار المانية تعتبر من اكثر المحطات ازدحاما بهدف التعرف على عناصر الجماعات الإرهابية المشتبه بهم لدى الحكومة الألمانية [٢٦]

المبحث الثاني: الاثبات بأدلة الذكاء الاصطناعي في الجرائم السيبرانية

ان تقنيات الذكاء الاصطناعي لديها بالفعل العديد من التطبيقات التي يمكن من خلالها اثبات الجرائم السيبرانية وتنفرد الجرائم السيبرانية ببعض الاحكام الإجرائية الخاصة ويعود ذلك لطبيعتها كجريمة عابرة للحدود الوطنية واختلفت الدول في مواجهة هذا النوع من الجرائم بالنسبة للمشرع العراقي في مشروع

قانون مكافحة الجرائم الالكترونية اسند القيام بإجراءات المكافحة الى سلطات الضبط القضائي وهو نفس موقف المشرع المصري في قانون مكافحة الجرائم الاليكترونية اذ جاءت المادة (٥) اذ جاء فيها (يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز او غيرهم ممن تحددهم جهات الامن القومي بالنسبة للجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأحكام وضائقهم) وسنتناول في هذا المبحث ماهية الدليل السيبراني في المطلب الأول اما المطلب الثاني سنتناول فيه الدليل السيبراني المستمد من الذكاء الاصطناعي.

المطلب الأول: ماهية الدليل السيبراني

ان تزايد جرائم تقنية المعلومات نتيجة الاستخدام المفرط لتقنية المعلومات أدى الى اتسلع نطاق الدليل فأصبحت الأجهزة الالكترونية وشبكات الانترنت مستودعا مهما للمعلومات والبيانات التي تدعم جهود رجال القضاء والعدالة وسنتناول في هذا المطلب التعريف بالدليل السيبراني وخصائصه في الفرع الأول اما الفرع الثاني سنتناول فيه انواع الدليل السيبراني.

الفرع الأول: التعريف بالدليل السيبراني وخصائصه

سنتناول تعريف الدليل السيبراني وخصائص الدليل السيبراني وعلى النحو التالي:

أولا/ تعريف الدليل السيبراني: سنتناول تعريف الدليل السيبراني في اللغة والاصطلاح، الدليل السيبراني في اللغة، الدليل من دل ويعني الارشاد والهداية والدليل هو المرشد وكل ما يستدل به فهو دليل [٢٧] اما السيبراني ان اصل كلمة سيبرانية هي ترجمة المصطلح cybernetics والذي يعني القائد او الربان او الموجه وهي كلمة يونانية الأصل والسيبراني يتعلق بالعالم الافتراضي او الشبكات والحواسيب أي انه كل ما يتعلق بالعالم الرقمي وجدير بالذكر لا يوجد تعريف للسيبرانية في معاجم اللغة كونه مصطلح حديث، فالدليل السيبراني حاليا يراد به الدليل المستمد من الحواسيب وأجهزة الهواتف الذكية والشبكات الرقمية.

اما الدليل السيبراني في الاصطلاح والذي يشمل التعريف به في التشريع والفقه والقضاء، فعلى صعيد التشريع نجد ان المشرع العراقي لم يعرف الدليل السيبراني لا في قانون العقوبات العراقي ولا في مشروع مكافحة الجرائم الالكترونية وكذلك الحال بالنسبة للمشرع المصري لم يعرف الدليل السيبراني اذ ان مهمة التعريف بالمصطلحات عادة يتركها المشرع للفقه.

اما على صعيد الفقه فان الدليل بصورة عامة هو الوسيلة التي يستعين بها القاضي لتكوين القضائية للوصول الى الحقيقة [٢٨] اما الدليل السيبراني هو الدليل الذي ستند الى العالم الافتراضي ويؤدي الى الكشف عن الجريمة [٢٩] وعرفه راي اخر بانه الدليل المأخوذ من أجهزة الكومبيوتر وهو يكون في شكل مجالات او نبضات مغناطيسية او كهربائية يمكن تجميعها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهو مكون رقمي في لتقديم معلومات في اشكال متنوعة مثل الصور والاصوات والرسوم وذلك من اجل اعتماده امام أجهزة انفاذ وتطبيق القانون [٣٠] وعرفه راي اخر في الفقه بانه الدليل المشتق النظم

البرمجية المعلوماتية الالكترونية كأجهزة ومعدات وأدوات الكومبيوتر او شبكات الاتصال من خلال إجراءات فنية وقانونية ثم تقديمها الى القضاء بعد تحليلها علميا او تفسيرها بشكل نصوص مكتوبة او رسومات او صور واشكال واصوات لإثبات وقوع الجريمة واثبات البراءة او الإدانة [٣١] وبراينا ان الدليل السيبراني هو الدليل الذي يستند الى العالم الافتراضي ويقود الى الجريمة.

اما في القضاء فان القضاء العراقي وكذلك المصري لم يعرف الدليل السيبراني من خلال اطلاعنا على القرارات القضائية الصادرة من الهيئات القضائية.

ثانيا/ خصائص الدليل السيبراني: يتميز الدليل السيبراني بعدد من الخصائص أهمها [٣٢]:

١. **الطبيعة غير مرئية:** أي ان الأدلة الرقمية يتم التوصل اليها من قبل المختصين ويمكن العثور عليها في مسرح الجريمة الالكتروني.

٢. **الطبيعة المتغيرة:** أي ان الدليل يتحول بمرور الوقت فأجزاء الدليل موجودة في الذاكرة العشوائية او اتصالات الشبكة وتختفي فور انقطاع التيار او إعادة التشغيل كما ان أنظمة التشغيل والبرامج تقوم باستمرار في تعديل الملفات وتحديث التوقيتات الزمنية وكتبة سجلات جديدة او حذف مؤقتات مجرد بقاء الجهاز قيد التشغيل يغير الأدلة كما ان أي خطا بسيط من المحقق مثل فتح ملف نصي قد يغير تاريخ الوصول للملف.

٣. **قابل للنسخ:** أي يمكن نسخ الدليل السيبراني نسخا مطابقا دون أي تغيير او فقدان للجودة بخلاف الأدلة المادية التي تتلف أحيانا اثناء عملية النسخ او النقل مثلا اثار الاقدام او طبعات الأصابع.

٤. **يحتاج الى متخصص للتعامل معه:** أي لا يمكن للشخص العادي جمع او تحليل الأدلة الرقمية بشكل صحيح يتطلب الامر خبيرا في الامن السيبراني لذا فان أي خطا من غير المختص قد يبطل الدليل قانونا ويجعله غير قابل للاستخدام.

٥. **قابل للاسترجاع:** ويراد بقابلية الاسترجاع انه يمكن استعادة أجزاء من الدليل حتى بعد محاولة اتلافها او حذفها فحذف ملف من النظام لا يزيل البيانات فعليا من القرص بل يشير اليها كمساحة قابلة للاستخدام.

الفرع الثاني: أنواع الدليل السيبراني

سنتناول أنواع الدليل السيبراني تبعا لمكوناته وتبعا لمكان وجوده ويوجد تقسيم اخر لوزارة العدل الامريكية سنتناوله بالبحث تباعا:

١. النوع الأول تبعا لمكوناته فهنا ينظر الى الدليل السيبراني من حيث شكله ومحتواه التقني فهناك ادلة على مستوى نظام التشغيل وتشمل الملفات (كالصور والمستندات والملفات المضغوطة) والميتاداتا كالتواقيت الزمنية والسجلات، وهناك ادلة على مستوى الذاكرة وادلة على مستوى الشبكة كسجلات الخادم والتواقيت والاستعلامات وأخيرا الأدلة على مستوى التطبيقات كرسائل لبريد الالكتروني ومحفوظات الدردشة [٣٣].

٢. النوع الثاني حسب مكان وجو الدليل السيبراني ويشمل ادلة داخلية توجد على جهاز الجاني كالقرص الصلب والذاكرة العشوائية والهاتف المحمول وادلة خارجية توجد في أجهزة قابلة للإزالة مثل الفلاش والقرص الخارجي والطابعات والماسح الضوئي وادلة شبكية وتوجد على أجهزة البنى التحتية كسجلات الراوتر والسيرفر وجدار الحماية، وادلة سحابية وتكون خارج نطاق السيطرة المادية كالخوادم و المايكروسوفت او خدمات الاستضافة وانها تحتاج الى امر قضائي للوصول اليها[٣٤].

٣. تقسيم وزارة العدل الامريكية لأنواع الدليل السيبراني: ويقسم الى السجلات المحفوظة بالحاسوب ويشمل الوثائق المكتوبة والمحفوظة كذلك البريد الالكتروني الصور التي تم تحميلها من كاميرا وتكتاز بالثبات نسبيا لا تتغير الا بالتعديل او الحذف اما قيمتها الاثباتية تعتمد على إمكانية اثبات ان المحتوى لم يعدل وان الشخص المعني هو من انشاه حقا اما النوع الثاني السجلات تم انشاؤها بواسطة الحاسوب وهذه السجلات يتم انشاها بشكل تلقائي بواسطة النظام او البرنامج دون تدخل بشري لحظة الانشاء مثل سجلات الخادم سجلات جدار الحماية بيانات تحديد الموقع المسجلة تلقائيا توقيت الخادم التلقائي للمعاملات وتمتاز بطبيعة متغيرة باستمرار كما انها موضوعية ومبرمجة مسبقا اما قيمتها الاثباتية فإنها تعتبر اكثر موضوعية وصدقا لكن يجب اثبات ان النظام كان يعمل بشكل صحيح عند توليدها اما النوع الثالث السجلات التي جزء منها تم حفظه بالإدخال وجزء اخر تم انشاه بواسطة الحاسوب مثالها معاملة بنكية عبر الانترنت اذ تتضمن ادخال بشري رقم الحساب المحول اليه والمبلغ المراد تحويله اما الانشاء الالي يتضمن رقم العملية والتوقيت الزمني ورقم جلسة العمل [٣٥].

نستنتج مما سبق ان الدليل السيبراني ليس نوعا واحدا لذا تتنوع وتتعدد وسائل الوصول اليه

المطلب الثاني: الدليل السيبراني المستمد من الذكاء الاصطناعي

ان تقنيات الذكاء الاصطناعي لديها العديد من التطبيقات التي تستطيع من خلالها اثبات الجرائم السيبرانية مثل تحليل المحادثات الالكترونية والتعرف على الوجوه والاصوات واكتشاف الحسابات الوهمية وتحليل البرمجيات الخبيثة والهجمات السيبرانية لتحديد مصدرها والية عملها كذلك كشف التزييف العميق وتحديد ما اذا كانت الصور او المقاطع معدلة بالذكاء الاصطناعي كذلك تطبيق تكنولوجيا الحدس والذي يعني المعرفة والمهارات التي تستخدم بعض الأساليب بتحديد وتحليل الرموز بذكاء لإثبات فايروس غير معروف بواسطة بعض القواعد اثناء المسح وسنتناول في هذا المطلب

اثبات الجرائم السيبرانية بواسطة الجيل الأول من الذكاء الاصطناعي والجيل الثاني وذلك في فرعين خصصنا الأول لإثبات الجرائم السيبرانية بواسطة الجيل الأول من الذكاء الاصطناعي اما الفرع الثاني سنتناول فيه اثبات الجرائم السيبرانية بواسطة الجيل الثاني من الذكاء الاصطناعي اما الفرع الثالث سنتناول فيه حجية الأدلة السيبرانية في الاثبات الجنائي وعلى النحو الاتي:

الفرع الأول: اثبات الجرائم السيبرانية بواسطة الجيل الأول من الذكاء الاصطناعي

ساهم الجيل الأول من الذكاء الاصطناعي في اثبات الجرائم السيبرانية من خلال الاعتماد على الأنظمة الخبيرة القائمة على قواعد منطقية محددة مسبقا لتحليل البيانات الرقمية وسجلات الأنظمة واكتشاف الأنماط الاجرامية المعروفة مما مكن جهات التحقيق من تحديد الأدلة الالكترونية وربطها بالواقعة الاجرامية الا ان دوره اقتصر على تحديد قواعد مبرمجة دون امتلاكه القدرة على التعلم الذاتي او استنتاج أنماط إجرامية جديدة ومن ابرز تقنيات اثبات الجرائم السيبرانية في الجيل الأول من الذكاء الاصطناعي الشبكات العصبية والعميل المحقق الذكي وستناولهما بالبحث تباعا:

أولا/ اثبات الجرائم السيبرانية بواسطة الشبكات العصبية: يمكن ان نعرف الشبكات العصبية بانها نماذج حاسوبية مستوحاة من طريقة عمل الدماغ البشري قادرة على التعلم من البيانات الرقمية واكتشاف الأنماط والعلاقات المعقدة بينها[٣٦]. وتعرف أيضا بانها الية الكترونية تحاكي الجوانب الهيكلية والوظيفية للشبكات العصبية الموجودة في النظم العصبية البايلوجية وهي مثالية في حالات التصنيف او التنبؤ او التحكم في البيانات السيبرانية الحيوية والمعقدة. وتتميز بانها ذات دقة عالية في التحليل وسرعة معالجة البيانات والقدرة على اكتشاف أنماط جديدة اما عن دورها في اثبات الجرائم السيبرانية فيتمثل في تحليل كم هائل من البيانات الرقمية في وقت قصير وكشف أنماط الاحتيال والاختراق الالكتروني والتعرف على الوجوه والاصوات في الأدلة الرقمية وكشف الصور والفيديوهات المزيفة وربط الأدلة الرقمية المتفرقة للوصول الى الجاني.

اما ابرز الإشكالات القانونية التي يثيرها الاثبات بواسطة الشبكات العصبية صعوبة تفسير بعض نتائجها واحتمال وجود تحيز او أخطاء خوارزمية وضرورة التحقق من سلامة البيانات المستخدمة في التدريب[٣٧].

ثانيا/ اثبات الجرائم السيبرانية بواسطة العميل المحقق الذكي: يمكن ان نعرف العميل المحقق الذكي بانه برنامج ذكي مستقل يعمل داخل البيئة الرقمية ويقوم بجمع الأدلة وتحليلها ومتابعة الأنشطة الالكترونية المشبوهة بصورة تلقائية لدعم التحقيق الجنائي[٣٨]. . ويمكن ان نعرفه بانه قوى مستقلة يولها الكومبيوتر وتتواصل وتتعاون مع بعضها البعض من اجل تخطيط وتنفيذ الاستجابات المناسبة في حالة وقوع احداث غير متوقعة وتعد هذه التقنية مناسبة جدا لإثبات ومكافحة الهجمات الالكترونية لقابليتها على الانتقال والقدرة على التكييف في البيئات التي يتم نشرها فيها بالإضافة الى طبيعتها التعاونية. واهم ما تميز به العميل المحقق الذكي العمل المستمر دون انقطاع وسرعة اكتشاف الجرائم الالكترونية وتقليل التدخل البشري في جمع الأدلة اما دوره في اثبات الجرائم السيبرانية فيتجسد في مراقبة الشبكات والأنظمة الالكترونية وجمع الأدلة الرقمية بصورة الية وتتبع مصدر الهجمات السيبرانية ورصد الحسابات الوهمية والأنشطة المشبوهة واعداد تقارير رقمية تساعد جهات التحقيق في اثبات الجريمة[٣٩] اما ابرز الإشكالات القانونية التي يمكن ان تثار على العميل المحقق الذكي مدى مشروعية المراقبة الالية وحماية الخصوصية والبيانات الشخصية وضرورة الرقابة الشرية على اعماله ومدى حجية التقارير التي يصدرها العميل المحقق الذكي امام القضاء.

الفرع الثاني: اثبات الجرائم السيبرانية بواسطة الجيل الثاني من الذكاء الاصطناعي

يعتمد الجيل الثاني من الذكاء الاصطناعي على التعلم من البيانات واستخلاص الأنماط والعلاقات بينها دون الاعتماد الكامل على قواعد مبرمجة مسبقا وسنتناول اثبات الجرائم السيبرانية بواسطة أنظمة المناعة الاصطناعية والخوارزمية الوراثية وعلى النحو الاتي:

أولا/ اثبات الجرائم السيبرانية بواسطة أنظمة المناعة الاصطناعية: يمكم ان نعرف أنظمة المناعة الاصطناعية بانها الأنظمة الذكية المستوحاة من الية عمل الجهاز المناعي في جسم الانسان والتي تتمتع بالقدرة على اكتشاف السلوكيات الشاذة والتهديدات الالكترونية وتمييزها عن الأنشطة الطبيعية داخل الأنظمة المعلوماتية. ويتم توظيف المناعة الاصطناعية مثل المناعة البايلوجية لدعم الاستقرار في بيئة متغيرة ويشمل اثبات الاختراق الالكتروني المستند الى المناعة الاصطناعية على تطور الخلايا المناعية واكتشاف المضادات في وقت واحد وينتج النظام المناعي الاصطناعي اجساما مضادة لمقاومة مسببات الجرائم ويمكن اثبات وتقدير كثافة الاقتحام الالكتروني الاجرامي باختلاف تركيز الجسم المضاد لذلك تلعب هذه الأنظمة دورا مهما في اثبات الجرائم السيبرانية. وتتجلى أهميتها في القدرة على التكييف مع التهديدات الجديدة واكتشاف الجرائم التي لا تتطابق مع الأنماط

المعروفة مسبقا وتعزيز دقة الدليل الرقمي وتقليل احتمالات الخطأ اما عن دورها في اثبات الجرائم السيبرانية فيتجسد في اكتشاف الاختراقات والهجمات الالكترونية غير المألوفة ورصد الانشطة المشبوهة داخل الشبكات وقواعد البيانات والتمييز بين السلوك المشروع والسلوك الاجرامي الكترونيا وتتبع الاثار الرقمية الناتجة عن الهجمات السيبرانية وتوفير مؤشرات وادلة رقمية تدعم اثبات الجريمة الالكترونية.

ثانيا/ اثبات الجرائم السيبرانية بواسطة الخوارزميات الوراثية: يمكن ان نعرف الخوارزميات الوراثية بانها تقنيات ذكاء اصطناعي مستوحاة من التطور والانتخاب الطبيعي وتعتمد على افضل الحلول من خلال عمليات الانتقاء والتكاثر والتحسين التدريجي ولها دور مهم في زيادة كفاءة الأدلة الرقمية والوصول الى نتائج دقيقة في البيئات المعلوماتية المعقدة والمساعدة في كشف الجرائم السيبرانية الغامضة كالاختراق الالكتروني الوراثي والتطفل الالكتروني والاقتحام الغامض اما عن دور الخوارزميات الوراثية في الاثبات الجنائي السيبراني يتجسد في تحليل كميات ضخمة من الأدلة الرقمية واختيار البيانات الأكثر ارتباطا في الجريمة وإعادة بناء مسار الهجوم الالكتروني وتحديد الالية الأكثر احتمالا لوقوعه والربط بين الأدلة الرقمية للوصول للجاني ودعم التحقيق الجنائي لاختيار افضل الأساليب انسجاما مع الوقائع الرقمية [٤٠].

الفرع الثالث: حجية الدليل السيبراني في الاثبات الجنائي

ان قبول الدليل الجنائي هو الخطوة الإجرائية الأولى التي يمارسها القاضي الجنائي قبل البدء في تقدير الدليل للتحقق من صلاحيته وملائمته لتحقيق ما قدم من اجله، وقبول القاضي الجنائي للدليل المستمد من الذكاء الاصطناعي لابد ان يستند على أساس وهذا الأساس يختلف حسب النظام اذا كان لاتينيا او انكلوامريكية، ففي نظام الاثبات الحر يكون للقاضي سلطة قبول كل الأدلة ويكون للقاضي

الجنائي دورا إيجابيا في الدعوى الجنائية كما تكون كل طرق الاثبات مقبولة مالم يستبعد المشرع بعضها صراحة وينظم الى هذه الفئة قانون الإجراءات الفرنسي (٤٢٧) والمادة (٣٠٢) من قانون الإجراءات الجنائية المصري والتي نصت على ان (يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته ومع ذلك لا يجوز ان يبني حكمه على أي دليل لم يطرح امامه في الجلسة) والمادة (٢١٣) من قانون أصول المحاكمات الجزائية العراقي والتي تنص على (أ . تحكم المحكمة في الدعوى بناء على اقتناعها الذب تكون لديها من الأدلة المقدمة في أي دور من أدوار التحقيق والمحاكمة).

اما النظام الاخر هو نظام الاثبات المقيد وهنا يحدد المشرع الأدلة التي يجوز للقاضي الجنائي قبولها وهنا يكون دور القاضي الجنائي سلبيا [٤١] اما نظام الاثبات المختلط فيه تقيد حرية الاثبات في مرحلة الفصل في مسألة الإدانة او البراءة اما في مرحلة تحديد العقوبة فيسود مبدأ حرية الاثبات وتأخذ بهذا النظام القوانين الانكلو امريكية[٤٢] والملاحظ على التشريعات اتي اخذت بنظام الاثبات الحر انها لم تورد نصوصا خاصة بقبول الدليل السيبراني على أساس ان هذه الدول تستند الى مبدأ حرية الاثبات في المسائل الجنائية، لكن هناك قيدا مهم على القاضي الجنائي عند الاخذ بالدليل السيبراني وهو قيد مشروعية الحصول على دليل الذكاء الاصطناعي، أي ان الدليل السيبراني بما يتضمنه من ادلة مستخرجة من وسائل الكترونية كالكومبيوتر مثلا لا يكون مشروعا ومن ثم مقبولا بالإثبات الا اذا جرت عملية البحث عنه والحصول عليه واقامته امام القضاء في اطار احكام القانون واحترام قيم العدالة واخلاقياتها التي يحرص على حمايتها[٤٣] فاذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة في شأن الجريمة وجمع ادلتها فان عمله مشروط في ان يتم في اطار الشرعية وذلك في اطار احترام حقوق الافراد وعدم المساس بها الا في الحدود التي يقررها القانون وفي حالة تجاوز هذه الحدود وجب طرح الدليل وعدم قبوله في الاثبات فاذا كانت طريقة الحصول على الدليل تتعارض مع القواعد العامة للإجراءات الجنائية والمبادئ القانونية العامة كالقواعد التي توجب احترام قيم العدالة واخلاقياتها واحترام حقوق الدفاع والنزاهة في الحصول على الأدلة [٤٤] ونلاحظ مما سبق ان هذا القيد هو مقابل لحرية القاضي الجنائي في قبول كل ادلة الاثبات بما في ذلك الأدلة التي لم ينظمها المشرع اذ ان المشرع أشار الى اهم وسائل الاثبات وترك الباب مفتوحا امام ما يستجد من وسائل أخرى. لكن القوة الاقناعية لدليل الذكاء الاصطناعي يجب ان تتأسس على دليل مقبول ويجب ان تكون القوة الاقناعية قائمة على ادلة وضعية:

أولا/ تأسيس القوة الاقناعية على دليل ذكاء اصطناعي مقبول وهنا يكون القاضي الجنائي حر في تقدير دليل الذكاء الاصطناعي المقبول في الدعوى أي ما تم الحصول عليه بطريق مشروع وتستبعد سائر الأدلة غير المقبولة لأنها لا تعد عنصرا من عناصر تقديره اذ ان مشروعية دليل الذكاء الاصطناعي ظمانا للحرية الفردية وللعدلة لان الغاية الأساسية هي تحقيق العدالة والكشف عن الحقيقة

ثانيا/ ان تكون القوة الاقناعية قائمة على ادلة وضعية[٤٥] أي لا يجوز للقاضي ان يبني حكمه على ادلة لم تطرح لمناقشة الخصوم في الجلسة أي يكون للدليل اصل ثابت في أوراق الدعوى ويتاح للخصوم فرصة الاطلاع عليه ومناقشته وهذا ما ايدته المادة (٣٠٢) من قانون الإجراءات الجنائية المصري والمادة (٢١٣) من قانون أصول المحاكمات الجزائية العراقي.

اما عن قيمة الدليل السيبراني المستمد من ادلة الذكاء الاصطناعي فقد أشار قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ الى ان (للأدلة المستمدة او المستخرجة من الأجهزة او المعدات او الوسائط او الدعامات الالكترونية او النظام المعلوماتي او من برنامج الحاسب او من أي وسيلة من تقنية المعلومات[٤٦] نفس قيمة وحجية الأدلة المادية في الاثبات الجنائي متى ما توافرت فيها الشروط الفنية الواردة باللائحة التنفيذية) اما في العراق فان مشروع قانون الجرائم المعلوماتية لم يذكر قيمة الدليل الالكتروني لذا نطالب المشرع العراقي بتضمين المشروع نص مشابه لما ورد بالتشريع المصري ويكون بالشكل التالي (يكون للأدلة المستمدة او المستخرجة من الأجهزة او المعدات او من برنامج الحاسب او من أي وسيلة من تقنية المعلومات نفس قيمة وحجية الأدلة المادية في الاثبات الجنائي متى ما توافرت فيها الشروط اللازمة لقبول الأدلة الالكترونية) ولكن بالرجوع الى المبادئ العامة يمكن عدها قرائن قضائية خاضعة للتجزئة والتقدير فأدلة الذكاء الاصطناعي مثل تحليل كاميرات المراقبة الذكية والتبوء الجنائي بسلوك النتهم والتقارير الفنية المستخرجة من خوارزميات الذكاء الاصطناعي لا تتمتع بحجية قانونية مطلقة بل تعامل كقرائن قضائية فللمحكمة ان تأخذ بها اذا اطمأنت لصحتها ولها ان تطرحها اذا ساورها الشك في دقتها [٤٧]. والجدير بالذكر ان ادلة الذكاء الاصطناعي تواجه تحديين أساسيين امام القاضي الجنائي المصري[٤٨] وكذلك العراقي أولهما التزييف العميق اذ ان مبدا الاثبات الحر يقابله التزام القاضي بان يكون الدليل نابعا من الحقيقة ومع قدرة التزييف على تغيير الأصوات والفيديوهات بدقة عالية اصبح القضاة في العراق يتعاملون بحذر شديد مع الأدلة الرقمية وغالبا ما يتم احالتها الى مديرية الأدلة الجنائية للتأكد من عدم التلاعب بها، اما الثاني وهو الخبرة الفنية فالقاضي هو الخبير الأعلى في الدعوى ولكنه لا الكفاءة التقنية لتفكيك خوارزميات الدليل الرقمي لذلك حجية هذا الدليل ترتبط بتقرير الخبير الفني المنتدب الذي يشرح للمحكمة مدى جدارة النظام المستخدم.

الخاتمة

بعد ان انتهينا من كتابة بحثنا الموسوم بـ (دور الذكاء الاصطناعي في اثبات الجرائم السيبرانية) توصلنا الى مجموعة من النتائج والمقترحات يمكن اجمالها بالاتي:

أولا: النتائج

١. توصلنا الى ان الذكاء الاصطناعي مجموعة من الأنظمة البرمجية القائمة على الخوارزميات وتحليل البيانات التي تستخدم في كشف الأدلة الرقمية واستخراجها وربطها وتحليلها والتنبؤ بالأنماط الجرمية بما يعزز قدرة السلطات التحقيقية على اثبات الجرائم المرتكبة عبر الوسائل الالكترونية.

٢. عرفنا الجرائم السيبرانية بانها اعمال غير قانونية يتم ارتكابها باستخدام الكومبيوتر كأداة او هدف او كليهما ويمكن ان تنطوي على أنشطة إجرامية تقليدية مثل السرقة والاحتيال او التشهير وتخضع لقانون العقوبات واحيانا تكون جرائم مستحدثة

٣. وتصنف الجرائم السيبرانية حسب طريقة ارتكابها الى نوعين الأول جرائم استخدام الكومبيوتر كهدف حيث يستخدم الكومبيوتر للهجوم على أجهزة أخرى مثل القرصنة، هجمات الفايروسات، هجمات سحب الخدمة، اما النوع الثاني استخدام الكومبيوتر كسلاح حيث يستخدم الكومبيوتر في ارتكاب جرائم العالم الحقيقي مثال ذلك انتهاك حقوق الملكية الفكرية، الإرهاب السيبراني، الاحتيال في بطاقات الائتمان وعمليات الاحتيال عبر التحويل الالكتروني والمواد الإباحية.

٤. عندما يتحقق هجوم الإرهاب السيبراني يترك اثارا تشير الى الجناة وهنا يبرز دور الذكاء الاصطناعي من خلال تعقب بصمات الاصابع الالكترونية او معلومات الشبكة والبرامج الأخرى الذكية من اجل اثبات الجريمة واسنادها للفاعل الذي شن الهجوم السيبراني وهنا يبرز دور الطب الشرعي السيبراني والذي يقوم عبر آليات الذكاء الاصطناعي بأثبات وتحليل مصدر الهجوم السيبراني ولكن الامر ليس بهذه السهولة بسبب استخدام الجناة لوسطاء الكترونيين او شن الهجوم من خلال عملاء مجهولين الهوية يخفون عنوان بروتكول الانترنت الخاص بهم لكن بالغالب تكون للذكاء الاصطناعي قدرة قوية ومعروفة بإثبات مصدر الهجوم السيبراني الى الجناة.

٥. من الممكن ان تقوم الدول والحكومات وأجهزة المخابرات باستخدام الذكاء الاصطناعي في التبؤ والتعرف على الجماعات الإرهابية والقدرة على منعهم من العمليات الإرهابية من الأساس من خلال عدة أساليب الدول والحكومات وأجهزة المخابرات باستخدام الذكاء الاصطناعي في التبؤ والتعرف على الجماعات الإرهابية والقدرة على منعهم من العمليات الإرهابية من الأساس من خلال عدة أساليب منها المساعدة في تقويض الأفكار المتطرفة، المساعدة في تحديد وقت وموقع الهجمات الإرهابية المساعدة في التعرف على وجه الإرهابيين

٦. الدليل السيبراني هو الدليل الذي يستند الى العالم الافتراضي ويقود الى الجريمة.

٧. ان دليل الذكاء الاصطناعي مقبول في الاثبات الجنائي شانه شان باقي الأدلة ف بصورة عامة وفي الجرائم السيبرانية بصفة خاصة بشرط احترام المشروعية فحرية الأطراف يجب ان تمارس في اطار ضوابط المشروعية وما تفرضه من قيود يستحيل مخالفتها والا ترتب على ذلك عدم مشروعية الدليل ومن ثم عدم قبوله وبطلانه.

٨. يخضع دليل الذكاء الاصطناعي للمبدأ العام في الاثبات الجنائي وهو حرية القاضي الجنائي في الاقتناع وله ان يقدر قيمة دليل الذكاء الاصطناعي بحسب قناعته الوجدانية.

ثانيا: المقترحات

١. ندعو المشرع العراقي الى إقرار مشروع قانون الجرائم المعلوماتية بالسرعة الممكنة وضرورة افراد نصوص خاصة بإجراءات التحقيق والتحري في الجرائم الالكترونية.

٢. ندعو المشرع العراقي بتضمين المشروع نص مشابه لما ورد بالتشريع المصري ويكون بالشكل التالي (يكون للأدلة المستمدة او المستخرجة من الأجهزة او المعدات او من برنامج الحاسب او من أي وسيلة من تقنية المعلومات نفس قيمة وحجية الأدلة المادية في الاثبات الجنائي متى ما توافرت فيها الشروط اللازمة لقبول الأدلة الالكترونية)

٣. توظيف محققين ذو كفاءة عالية بتقنيات الذكاء الاصطناعي كذلك اعداد الخبراء المتخصصين بمجال تقنيات الذكاء الاصطناعي وتعزيز دورهم في تقديم الأدلة اللازمة لإثبات الجرائم السيبرانية من خلال ادراجهم ضمن قائمة الخبراء المتخصصين.

٤. تشجيع الدول والحكومات على سن القوانين الدولية للتعاون الدولي لمواجهة الجرائم السيبرانية من خلال الاتفاقات الدولية وبروتكولات التعاون القضائية.

٥. عقد دورات بصورة مكثفة فيما يخص الجرائم السيبرانية وكيفية اثباتها وادراج ذلك في منهج التحقيق الجنائي.

الهوامش:

(١) احمد أبو حاقة، معجم النفائس الوسيط، ط٢، دار النفائس للطباعة والنشر، بيروت، ٢٠١١، ص٤٢٠.

(٢) د. احمد مختار معجم اللغة العربية المعاصر عالم الكتاب القاهرة ط١ ج٢، ١٤٢٩، ص ١٣٢٢.

(٣) سورة هود اية ٣٧.

(٤) القاموس المحيط للفيروز أبادي، مجد الدين بن يعقوب، مؤسسة الرسالة، بيروت لبنان، الطبعة السادسة عام ١٤١٩هـ، ص٥٥١.

(٥) د. احمد محمد غنيم الذكاء الاصطناعي ثورة جديدة في الإدارة المعاصرة المكتبة العصرية للتوزيع والنشر القاهرة ط١ ٢٠١٧، ص٢٥. د عائشة بنت بطيء بنت بشر، مبادئ وارشادات اخلاقيات الذكاء الاصطناعي، مكتب دبي، دبي ٢٠١١، ص٢٣

(٦) عادل عبد النور مخل الى علم الذكاء الاصطناعي مدينة الملك عبد العزيز السعودية ٢٠٠٥ ص١٢. د سلام العبلاني كيف تعمل الأشياء (الربوتات)، مؤسسة الكويت للتقدم العلمي الكويت، ٢٠١٧، ص١٢١

(٧) د. احمد محمد غنيم مصدر سابق ص٣٠.

(٨) د. ياسر محمد لمعي المسؤولية الجزائية عن اعمال الذكاء الاصطناعي جامعة طنطا مصر ٢٠٢٠، ص٢١

(٩) د. احمد ماجد الذكاء الاصطناعي بدولة الامارات العربية المتحدة، أبو ظبي ٢٠١٨ ص١٧.

(١٠) محمد بن ابي بكر الرازي بن عبد القادر الرازي، مختار الصحاح، ط١، دار الكتاب العربي، بيروت، ١٩٧٩، ص٦٨.

(١١) عرف الجريمة السيبرانية النظام السعودي لمكافحة الجرائم الالكترونية في المادة الأولى بانها: أي فعل يرتكب متضمنا استخدام الحاسب الالي او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

(١٢) د. صالح علي عبد الرحمن، الامن الرقمي وحماية المستخدم من جرائم الانترنت، دار النهضة العربية، القاهرة ٢٠١١، ص٨٥.

(١٣) د. محمود عمر محمود، الجرائم المعلوماتية والالكترونية، دار الكتاب العربي ط١، ٢٠١٥ص٦٨.

(١٤) محمود احمد القرعان، الجرائم الالكترونية، دار وائل للطباعة والنشر، عمان، ط١، ٢٠١٨، ص٢١.

(١٥) هدى طلب علي، استخدام وسائل الذكاء الاصطناعي في الاثبات الجنائي، دار النهضة العربية القاهرة، ٢٠٢٢، ص١٣٥.

(١٦) د. صالح علي عبد الرحمن، مصدر سابق، ص٩٥.

(١٧) علي نعمة جواد، الجريمة المعلوماتية الماسة بالحياة الخاصة، المكتب الجامعي الحديث، بدون ذكر سنة الطبع، ص٤٠

(١٨) د. صالح علي عبد الرحمن، مصدر سابق ص١٠٠.

(١٩) د. غانم مرتضى الشمري، الجرائم المعلوماتية، ، الدار العلمية الدولية، عمان ٢٠١٦، ص٥٥.

(٢٠) علي نعمة جواد، مصدر سابق، ص٩٨.

(٢١) د. صالح علي عبد الرحمن، مصدر سابق، ص٩٠.

(٢٢) د. سامح علي حامد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر العربي الإسكندرية ط١، ٢٠٠٥، ص٦٠.

(23) CHADHA, V. (2021) "Freedom oF Speech and expreSSion verSuS the gloriFication oF actS oF terroriSm, The Age of Human Rights Journal, p. 674.

(٢٤) علي نعمة جواد، مصدر سابق، ص١٠٢.

(٢٥) هدى طلب علي مصدر سابق، ص١٦٥.

(٢٦) د سامح راشد، الذكاء الاصطناعي في موجهة الإرهاب، دار الفكر العربي القاهرة بدون ذكر سنة الطبع ص٧٤

(٢٧) القاموس المحيط للفيروز أبادي، مجد الدين بن يعقوب، مؤسسة الرسالة، بيروت لبنان، الطبعة السادسة عام ١٤١٩ هـ، مادة سوس باب السين فصل السين، ص ٢٥١. محمد بن ابي بكر الرازي بن عبد القادر الرازي، مصدر سابق، ص٩٠.

(٢٨) احمد أبو القاسم الدليل الجنائي المادي ودوره في اثبات جرائم الحدود والقصاص المركز العربي للدراسات الرياض السعودية ط١، ٢٠٠٢، ص١٧٠.

(٢٩) محمد الأمين البشري التحقيق في جرائم الحاسب الالي والانترنت جامعة نايف الرياض السعودية ط١، ٢٠٠٤، ص٢٣٠.

(٣٠) جميل عبد الباقي الانترنت والقانون الجنائي دار النهضة العربية القاهرة ٢٠٠٢، ص٣٥.

(٣١) هدى طلب علي، مصدر سابق، ص١٦٦.

(٣٢) جون بندر اطار التدقيق الذكي للذكاء الاصطناعي، بدون ذكر نكان وسنة الطبع، ص١٣٥.

(٣٣) سامية شهيبي الذكاء الاصطناعي بين الواقع والمامول الجزائر ٢٠١٨ ص٣٢

(٣٤) د. ايمن محمد الاسيوطي الجوانب القانونية لتطبيق الذكاء الاصطناعي دار مصر للنشر والتوزيع القاهرة ط١، ٢٠٢٠، ص٢٧٥

(٣٥) حسنين المحمدي: الوسائل العلمية الحديثة في الاثبات الجنائي، الإسكندرية، ٢٠٠٥، ص١٠٨

(٣٦) اشرف عبد القادر قنديل الاثبات الجنائي في الجريمة الالكترونية دار الجامعة الجديدة الإسكندرية ٢٠٠١٨ص١٠٨

(٣٧) حسن عباس حميد: نحو اختصاص محكمة الكترونية خاصة بالجرائم المعلوماتية، دار النهضة العربية القاهرة، ٢٠٢١، ص٥٣

(٣٨) بكري يوسف بكري التفتيش عن المعلومات في الوسائل التقنية الحديثة، الإسكندرية، ٢٠٠٥، ص٦٥.

(٣٩) ديفد جيبرس عالم الروبوتات والذكاء الاصطناعي، دار الفاروق، مصر، ٢٠٠٨، ص٧٢.

(٤٠) عادل عبد النور: مدخل الى عالم الذكاء الاصطناعي، الرياض، ٢٠٠٥، ص٥٢.

(٤١) من ذلك نص المادة (٣٣٩) من قانون الإجراءات الجنائية الهولندي حيث نصت على (يعد ما يلي مقبولا بشكل حصري كوسيلة اثبات قانونية اول درجة: ملاحظات المحكمة الخاصة ثاني درجة: اقوال المتهم ثالث درجة: اقوال الشاهد رابع درجة: اقوال الشاهد الخبير خامس درجة المواد المكتوبة)

(٤٢) انتصار احميدة محمد، التحول في نظام الاثبات الجنائي، مركز الدراسات العربية، القاهرة، ٢٠١٧، ص١٣٥.

(٤٣) د عمر محمد بن يونس، الدليل الرقمي، دار النهضة العربية القاهرة ٢٠٠٦، ص٨٩، انتصار احميدة محمد: مرجع سابق، ص١٤٤. نقض ٤٠٢٣لسنة ٨٨ جلسة ٢٠٢١/٤/٥ (غير منشور)

(٤٤) ويمكن ان نظيف المصلحة الأولى بالرعاية وهنا يكون الدليل السيبراني غير المشروع كاثر للتعدي على الحياة الخاصة من جهة وفي نفس الوقت يعد وسيلة اثبات جرائم تهدد امن ونظام المجتمع الأخلاقي فاي المصلحتين أولى بالرعاية فاذا كان هناك من يشكك في مشروعية دليل الذكاء الاصطناعي باعتباره طريقة للتدخل في الحياة الخاصة للأفراد ولا سيما في مجال الجرائم الجنسية فالاستعانة بالوسائل الحديثة ونسر المحادثات الفاضحة يستهدف المصلحة العامة، د عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الفكر الجامعي القاهرة ٢٠٠٦، ص٢٧٢.

(٤٥) ويقوم شرط وضعية دليل الذكاء الاصطناعي على عنصرين الأول اتاحة الفرصة للخصوم للاطلاع على دليل الذكاء الاصطناعي والرد عليه والثاني ضرورة ان يكون للدليل السيبراني اصل بأوراق الدعوى حتى يكون اقتناع القاضي مبنيا على أساس. د خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية ٢٠٠٨ ص١٧٨.

(٤٦) نصت المادة (١٥) من قانون التوقيع الالكتروني المصري رقم ١٥ لسنة ٢٠٠٤على (ان للكتابة الالكترونية والمحررات الالكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في احكام قتنون الاثبات في المواد المدنية والتجارية متى استوفت الشروط المنصوص عليها في هذا القانون) اما المشرع العراقي فقد نص في المادة (٤/أولا) في قانون التوقيع الالكتروني رقم ٧٨ لسنة ٢٠١٢ على ان (يكون للتوقيع الالكتروني في اطار المعاملات المدنية والتجارية ذات الحجية المقررة للتوقيع الخطي اذا روعي في انشائه الشروط المنصوص عليها في المادة (٥) من هذا القانون)

(٤٧) اما عن دور ادلة الذكاء الاصطناعي في الدعوى الجنائية بموجب النظام اللاتيني المطبق في العراق: ففي مرحلة التحقيق تعد هذه الأدلة أداة بيد قاضي التحقيق والمحقق للوصول الى الأدلة التقليدية مثل تحديد مكان الجثة او معرفة هوية مشتبه به عبر بصمة الوجه الذكية وهنا دورها مساعد للتحقيق اما في مرحلة المحاكمة فهي دليل ساند اذ يستخدم مع غيره من الأدلة كالشهادة والاعتراف د ثامر محمد صالح، الحضور عن بعد في الدعوى الجزائية، دار الفكر والقانون للنشر والتوزيع المنصورة ٢٠٢١، ص٨٩

(٤٨) نقض ٤٤٠٦لسنة ١٣٥جلسة ٢٠٢٣/٩/٣ (غير منشور)

المصادر

أولا: القران الكريم

ثانيا: معاجم اللغة

١) احمد أبو حاقة، معجم النفائس الوسيط، ط٢، دار النفائس للطباعة والنشر، بيروت، ٢٠١١، .

٢) د احمد مختار معجم اللغة العربية المعاصر عالم الكتاب القاهرة ط١ ج٢، ١٤٢٩.

٣) المصباح المنير لأحمد بن محمد، تحقيق يوسف الشيخ محمد، المكتبة العصرية، بيروت لبنان، الطبعة الثالثة عام ١٤٢٠ هـ، مادة سوس، ص ١٥٤.

٤) القاموس المحيط للفيروز أبادي، مجد الدين بن يعقوب، مؤسسة الرسالة، بيروت لبنان، الطبعة السادسة عام ١٤١٩ هـ، مادة سوس باب السين فصل السين، ص ٥٥١.

٥) محمد بن ابي بكر الرازي بن عبد القادر الرازي، مختار الصحاح، ط١، دار الكتاب العربي، بيروت، ١٩٧٩.

ثالثا: الكتب القانونية

١) د. احمد محمد غنيم الذكاء الاصطناعي ثورة جديدة في الإدارة المعاصرة المكتبة العصرية للتوزيع والنشر القاهرة ط١ ٢٠١٧.

٢) د. احمد ماجد الذكاء الاصطناعي بدولة الامارات العربية المتحدة، أبو ظبي ٢٠١٨ ١٧.

٣) احمد أبو القاسم الدليل الجنائي المادي ودوره في اثبات جرائم الحدود والقصاص المركز العربي للدراسات الرياض السعودية ط١، ٢٠٠٢.

٤) اشرف عبد القادر قنديل، الاثبات الجنائي في الجريمة الالكترونية دار الجامعة الجديدة الإسكندرية ٢٠١٨.

٥) انتصار احميدة محمد، التحول في نظام الاثبات الجنائي، مركز الدراسات العربية، القاهرة، ٢٠١٧.

٦) د. ايمن محمد الاسيوطي الجوانب القانونية لتطبيق الذكاء الاصطناعي دار مصر للنشر والتوزيع القاهرة ط١، ٢٠٢٠، .

٧) بكري يوسف بكري التفتيش عن المعلومات في الوسائل التقنية الحديثة، الإسكندرية، ٢٠١٨

٨) د ثامر محمد صالح، الحضور عن بعد في الدعوى الجزائية، دار الفكر والقانون للنشر والتوزيع المنصورة ٢٠٢١، ص٨٩

٩) جميل عبد الباقي الانترنت والقانون الجنائي دار النهضة العربية القاهرة ٢٠٠٢.

١٠) جون بندر اطار التدقيق الذكي للذكاء الاصطناعي، بدون ذكر نكان وسنة الطبع.

١١) ديفد جيبرس عالم الروبوتات والذكاء الاصطناعي، دار الفاروق، مصر، ٢٠٠٨.

١٢) حسن عباس حميد: نحو اختصاص محكمة الكترونية خاصة بالجرائم المعلوماتية، دار النهضة العربية القاهرة، ٢٠٢١، .

١٣) حسنين المحمدي: الوسائل العلمية الحديثة في الاثبات الجنائي، الإسكندرية، ٢٠٠٥،

١٤) د خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية ٢٠٠٨.

١٥) د سامح علي حامد، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب، دار الفكر العربي الإسكندرية ط١، ٢٠٠٥.

١٦) د سامح راشد، الذكاء الاصطناعي في موجهة الإرهاب، دار الفكر العربي القاهرة بدون ذكر سنة الطبع

١٧) سامية شهيبي الذكاء الاصطناعي بين الواقع والمامول الجزائر ٢٠١٨.

١٨) د. سلام العبلاني كيف تعمل الأشياء (الربوتات)، مؤسسة الكويت للتقدم العلمي الكويت، ٢٠١٧.

١٩) د. صالح علي عبد الرحمن، الامن الرقمي وحماية المستخدم من جرائم الانترنت، دار النهضة العربية، القاهرة ٢٠١١.

٢٠) د. عائشة بنت بطيء بنت بشر، مبادئ وارشادات اخلاقيات الذكاء الاصطناعي، مكتب دبي، دبي ٢٠١١.

٢١) عادل عبد النور مخل الى علم الذكاء الاصطناعي مدينة الملك عبد العزيز السعودية ٢٠٠٥.

٢٢) د. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والانترنت، دار الفكر الجامعي القاهرة ٢٠٠٦، ص٢٧٢.
٢٣) علي نعمة جواد، الجريمة المعلوماتية الماسة بالحياة الخاصة، المكتب الجامعي الحديث، بدون ذكر سنة الطبع
٢٤) د. عمر محمد بن يونس، الدليل الرقمي، دار النهضة العربية القاهرة، ٢٠٠٦.
٢٥) د. غانم مرتضى الشمري، الجرائم المعلوماتية، ، الدار العلمية الدولية، عمان ٢٠١٦، .
٢٦) د. محمود عمر محمود، الجرائم المعلوماتية والالكترونية، دار الكتاب العربي ط١، ٢٠١٥
٢٧) محمود احمد القرعان، الجرائم الالكترونية، دار وائل للطباعة والنشر، عمان، ط١، ٢٠١٨،
٢٨) هدى طلب علي، استخدام وسائل الذكاء الاصطناعي في الاثبات الجنائي، دار النهضة العربية القاهرة، ٢٠٢٢،
٢٩) د. ياسر محمد لمعي المسؤولية الجزائية عن اعمال الذكاء الاصطناعي جامعة طنطا مصر ٢٠٢٠.

رابعا القوانين

١) قانون الإجراءات الجنائية المصري رقم ١٥٠ لسنة ١٩٥٠
٢) قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.
٣) قانون أصول المحاكمات الجزائية رقم ٢٣ لسنة ١٩٧٩.
٤) قانون التوقيع الالكتروني المصري رقم ١٥ لسنة ٢٠٠٤
٥) قانون مكافحة الارهاب رقم ١٣ لسنة ٢٠٠٥.
٦) قانون التوقيع الالكتروني العراقي رقم ٧٨ لسنة ٢٠١٢
٧) قانون تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨
٨) مشروع قانون مكافحة الجرائم المعلوماتية في العراق

خامسا القرارات القضائية

١) نقض ٢٠٢٣لسنة ٨٨ جلسة ٢٠٢١/٤/٥ (غير منشور)
٢) نقض ٤٤٠٦لسنة ١٣٥جلسة ٢٠٢٣/٩/٣ (غير منشور) نقض ٤٤٠٦لسنة ١٣٥جلسة ٢٠٢٣/٩/٣ (غير منشور)

سادسا المصادر الأجنبية

1) CHADHA, V. (2021) "Freedom oF Speech and expreSSion verSuS the gloriFication oF actS oF terroriSm, The Age of Human Rights Journal, p. 674.