URUK FOR HUMANITIES 2026;19:368–377

RESEARCH ARTICLE

The role of artificial intelligence in confronting cybercrime

[a*]Sarhan Naeem Al-Khafaji [b*]Adel Abdul Hadi Al-Nashi
[a]Al-Muthanna University College of Education for Human Sciences
[b]Ministry of Interior-Iraq

ABSTRACT

This study addresses the role of artificial intelligence in combating cybercrime, as this technology has become part of the modern and advanced daily lifestyle. Modern artificial intelligence programs help criminals create programs and excel in drawing and modifying images, facilitating the work of criminals more easily and smoothly. The ability to avoid detection and escape from the competent authorities. Artificial intelligence is one of the important technologies used in many fields and known skills, the use of which has developed in recent times in all fields and sectors, and has been used by weak-willed individuals, blackmailers, and hacking websites, accounts, and other things. Cyber threats are one of the most serious challenges facing the world. The use of modern technologies and artificial intelligence to combat cybercrimes and enhance information security infrastructure systems constitutes a heavy burden on the economies of countries due to the large sums and capabilities they require. Investing in information security is one of the most important priorities of countries, institutions and companies in various countries of the world. Moreover, cybercrimes and AI crimes are characterized by change and modernization with the advancement of modern technologies, the sophistication of criminals, and the globalization of crimes. The use of AI poses numerous threats to criminal activity. With the significant development of AI programs, criminals are developing new techniques for electronic blackmail and camouflage in the field of organized crime. Therefore, combating cybercrime requires building highly efficient systems to manage information security and artificial intelligence, make appropriate decisions, and detect espionage, manipulation, and other cybercrimes.

Keywords: Crimes, intelligence, electronic, confrontation, industrial.

مقالة بحثية

دور الذكاء الاصطناعي في مواجهة الجرائم الالكترونية

[1]سرحان نعيم الخفاجي [2]عادل عبد الهادي الناشي
جامعة المثنى-كلية التربية للعلوم الانسانية
وزارة الداخلية – العراق

الملخص:

تتناول هذه الدراسة دور الذكاء الاصطناعي، في مواجهة الجرائم الالكترونية، أذ باتت هذه التكنولوجيا جزءاً من نمط الحياه اليومية الحديثة والمتطورة ، أذ تساعد البرامج الحديثة للذكاء الاصطناعي المجرمين على انشاء برامج والتفنن في رسم وتعديل الصور وتسهيل عمل المجرمين بصورة اكثر سهولة ويسر ، والقدرة على عدم الاكتشاف والهروب من الجهات المختصة، ويعد الذكاء الاصطناعي من التقنيات المهمة التي تستخدم في العديد من المجالات والمهارات المعروفة والتي تطور استخدامها في الفترات الاخيرة في كافة المجالات والقطاعات، واخذت تستخدم من قبل ضعفاء النفوس والمبتزين واختراق المواقع والحسابات وغيرها . ان التهديدات الالكترونية تعد احد التحديات الخطيرة التي يواجهها العالم ، أذ ان استخدام تكنلوجيا التقنيات الحديثة والذكاء الاصطناعي في مواجهة الجرائم الالكترونية وتعزيز أنظمة البنية التحتية لأمن المعلومات يشكل عبئ كبير على اقتصاديات الدول لما تتطلبه من مبالغ وامكانيات كبيرة، ويمثل الاستثمار في أمن المعلومات، احد اهم اولويات الدول والمؤسسات والشركات في مختلف دول العالم، فضلاً عن ذلك أن الجرائم الالكترونية وجرائم الذكاء الاصطناعي تتسم بطابع التغير والحداثة مع تقدم التقنيات الحديثة وتفنن المجرمين واتخاذ الجرائم لطابع عالمي. وان استخدام الذكاء الاصطناعي يؤدي الى الكثير من التهديدات في مجال الجريمة ، اذ بات المجرمين ومن خلال التطور الكبير في برامج الذكاء الاصطناعي في تطوير تقنيات جديدة للابتزاز الالكتروني والتمويه في مجال الجرائم المنظمة ، ولذلك تتطلب مواجهة الجرائم الالكترونية بناء انظمة على درجة عالية من الكفاءة ، لإدارة امن المعلومات والذكاء الاصطناعي، واتخاذ القرارات المناسبة واكتشاف عمليات التجسس والتلاعب وغيرها من الجرائم الالكترونية.

الكلمات المفتاحية : الجرائم، الذكاء، الالكتروني، مواجهة، الصناعي.

Received 7/8/ 2025; accepted 14/9/ 2025. Available online 4/1/2026

* Corresponding author.
E-mail addresses: (**msc-sarhan@mu.edu.iq**).

https://doi.org/xx.xxxxx/2572-5440.1029

المقدمة:

أدى التطور السريع والمتلاحق لتقنية المعلومات إلى مضاعفة المخاطر والاعتداءات على الحريات الشخصية، وحرمة الحياة الخاصة، ونشر بعض العادات التي تمس المبادئ والقيم الاسرية، كما أنه يمكن من خلاله ارتكاب الجرائم التي تمس الامن القومي، والتجسس عن بعد وسرقة المعلومات، والارهاب والتحريض السياسي والتزوير والتزييف، مما يتطلب إعداد العدة لمواجهة سيل الجرائم الناتج من التقدم التقني (الدريني،2021).

أن اعتماد تقنيات الذكاء الاصطناعي لها دور جداً كبير في معرفة الجرائم الالكترونية ومعالجتها ، ولها دور ايضاً في معرفة المجرمين وكشفهم ومحاربة الجريمة. ان سبب استخدام تقنية الذكاء الاصطناعي في معرفة بالجريمة ومعالجتها، يرجع إلى أهمية تطوير مهارات قوى الامن والبحث الجنائي، نظراً مما تتميز به من سرعة ودقة الكشف عن الجريمة والمجرمين ، والمساهمة في تقديم الادلة الى الجهات المختصة ، أضافة الى تقديم معلومات مهمة ودلائل الى قوى الامن لكشف الجريمة ومرتكبيها.(9،ص11)، أن الجريمة الإلكترونية، هي فعل ينتهك القانون ويرتكب باستخدام تكنولوجيا المعلومات والاتصالات لاستهداف الشبكات والأنظمة والبيانات والمواقع الإلكترونية أو التكنولوجيا أو تسهيل ارتكاب جريمة. لقد سعى الباحثون في مجال الذكاء الاصطناعي الى خلق نظام يحاكي الجهاز العصبي البشري وبالأخص الخلايا العصبية (16،ص7)، وذلك من خلال بناء نماذج عصبية اصطناعية لها خواص مشابهة للخلايا العصبية الحية ، بهدف صنع اله ذكية قادرة على التعليم واكتساب المعرفة وحل المشكلات التي تواجهها في المستقبل بشكل تلقائي، ويعد ذلك من اهم الصعوبات التي تواجه الباحثين في مجال الذكاء الاصطناعي (12،ص17).

مشكلة الدراسة:

تكمن مشكلة الدراسة في سؤال رئيس وهو (هل للذكاء الاصطناعي دور في مواجهة الجرائم الالكترونية وأبراز خصائصها)، وهل توجد علاقة بين الذكاء الاصطناعي ومواجهة الجرائم الالكترونية ومكافحتها والحد منها.

فرضية الدراسة: يشير الجواب الرئيس للفرضية من (ان للذكاء الاصطناعي دور كبير وفعال في مواجهة الجرائم الالكترونية)، و للذكاء الاصطناعي دور محوري في الأمن السيبراني، أذ انه يساعد في مواجهة الأنشطة الاجرامية الالكترونية غير المشروعة ، من خلال تحديثه لأدوات واستراتيجيات جديدة .

هدف الدراسة:

تهدف هذه الدراسة إلى أبيان ماهية الذكاء الاصطناعي ودورة في مواجهة الجرائم الإلكترونية وتحليل هذه الجرائم من خلال تعريفها وايضاح خصائصها ودوافعها ومسبباتها ، وعن مدى وجود علاقة مشتركة بين الذكاء الاصطناعي من جهة والجرائم الإلكترونية من جهة أخرى.

اهمية الدراسة:

تكمن اهمية الدراسة، ان الذكاء الاصطناعي قد أضاف الكثير الى الجرائم السيبرانية ومسرحها، من خلال استثماره وتطويعه في الجريمة ، اضافة الى ان للذكاء الاصطناعي دور مهم ايضاً في الكشف عن الجريمة الالكترونية والقبض على مرتكبيها.

منهجية الدراسة:

اعتمدت الدراسة على المنهج الوصفي والتحليلي الذي يحدد ماهية الذكاء الاصطناعي وتصنيفه وانواع الجرائم الالكترونية وابيان دور أنظمة الذكاء الاصطناعي في الجرائم الالكترونية ومواجهتها.

1-مفهوم الذكاء الاصطناعي:

الذكاء الاصطناعي أداء تقوم به الآلات وفق برامج معدة من قبل الانسان ، بما يحاكي العقل البشري وقدراته ونمط عمله ، مثل القدرة على التعلم والادراك واستخلاص النتائج، واداء اعمال وردة فعل على أمور لم تبرمج في الآلة، أضافة الى صنع اجهزة حاسوب وعمل برامج قادرة على اتخاذ سلوك ذكي(8، ص12). يعرف أيضا بأن أحد فروع الحاسوب الذي من خلاله يمكن تصميم برامج الحاسوب التي تمشي اسلوب الذكاء الانساني.

2-مميزات الذكاء الاصطناعي:

يعد الذكاء الاصطناعي من التقنيات الحديثة والمعقدة التي لها عدة مميزات ودور كبير في مجالات عديدة (10،ص11) وهي كالاتي:

1- يستخدم الذكاء الاصطناعي في التعرف على الانشطة الارهابية والمواد غير المرخصة والسلع غير القانونية مثل المخدرات.

2- يستخدم الذكاء الاصطناعي في تحديد العملاء الذين يشترون كميات غير عادية من المواد الكيميائية التي تستخدم في الانشطة الارهابية .

3- يستخدم الذكاء الاصطناعي، وبالاعتماد على بيانات شركات ومؤسسات الشحن لمتابعة وتحديد الاتجار بالبشر.

4- الذكاء الاصطناعي يستخدم في الاحتيال ووسائل الدفع الإلكتروني والاستيلاء على الحسابات البنكية وغسيل الأموال وبطاقات الائتمان.

5- يستخدم الذكاء الاصطناعي، توسيع نطاق المراقبة بالكامرات للتعرف على الاشخاص ولوحات التراخيص ومن مسافات بعيدة .

6- يستخدم الذكاء الاصطناعي، بتنفيذ القانون بالاعتماد على المستشعرات الرقمية والبيومترية والتي تساعد على تنفيذ الاحكام.

7- يستخدم الذكاء الاصطناعي في تحديد الاراضي الزراعية التي تزرع بنباتات المخدرات، اضافة الى دوره في مراقبة الافراد من تجار المخدرات.

8- يستخدم الذكاء الاصطناعي في التعرف على الجثث مجهولة الهوية ومرتكبيها ودراسة وتفسير مسرح الجريمة من خلال البصمة الوراثية وبصمة الوجه والادلة الرقمية.

9- يستخدم الذكاء الاصطناعي في التهديد والابتزاز من خلال جرائم نقل البيانات والاستيلاء عليها بواسطة برامج ضارة.

3- مفهوم الجرائم الإلكترونية (الجرائم المعلوماتية):

ان المقصود بالجرائم المعلوماتية هي جرائم الانترنيت حيث يتم استخدام الحاسب الالي Computer- related crimes ، كوسيلة لتحقيق غايات واعمال غير قانونية مثل، عمليات النصب والاحتيال، او سرقة الملكية الفكرية (الدريني،2021)، وقد كان للتحولات الرقمية وثورتها الكبيرة التي يشهدها العالم وفي ظل التطور التكنلوجي الكبير ، ظهرت عصابات عابرة للحدود والامم باستطاعتها اختراق الحسابات الشخصية للافراد مستخدمي الإنترنت والهواتف ، وحسابات المؤسسات والشركات الحكومية والخاصة، لاغراض النصب واعمال اخرى ، وباتت الجرائم السيبرانية تشكل خطراً كبيراً بحكم التطور الكبير في التقنيات الحديثة اكثر من أي وقت مضى (6،ص9). والجريمة الإلكترونية: نوع من الجرائم التي يتم ارتكابها باستخدام الاجهزة الالكترونية وتمثل سلوك غير قانوني يهدف الى الاضرار بالأفراد أو المؤسسات او الحكومات وهي من الجرائم الحديثة التي تطورت مع تطور التكنلوجيا، (3،ص16).

في ظل التقدم التكنولوجي والتحول الرقمي، ظهرت نوعية جديدة من الجرائم يطلق عليها العديد من المسميات منها «الجريمة السيبرانية» حيث إنها تتم في الفضاء الإلكتروني، أو (الجريمة المعلوماتية) لأنها تتعلق بالمعلومات، وغيرها من المسميات أيضًا (الجريمة التكنولوجية)، ولكن يظل مفهومها هو أي استخدام غير مشروع وغير آمن للتقنيات التكنولوجية الحديثة وخاصة شبكة الانترنت ومواقع التواصل الاجتماعي، وتهدف إلى الإضرار بالغير لتحقيق منفعة مادية أو معنوية، فالجريمة المعلوماتية تتمتع بخصائص دولية، وليس هناك اتفاق حتى هذه اللحظة على تعريف دقيق لمعناها.(13،ص12)، وتتسم الجرائم الالكترونية وجرائم الذكاء الاصطناعي بانها جرائم عابرة بواسطة الشبكة العنكبوتية ، وان مرتكبيها يتسم بالذكاء المعلوماتي والمهارة المعرفية (18،ص11).

وتعرف الجريمة الالكترونية: في ضوء قانون مكافحة الجريمة الالكترونية العراقي لسنة 2019 بانها ، "هي كل فعل يرتكب باستعمال الحاسب الالي او شبكة المعلوماتية او غير ذلك من وسائل تقنية المعلومات ، معاقب عليها وفق احكام هذا القانون"(قانون مكافحة الجرائم الإلكترونية في العراق،2019).

4-التعريف الدولي للجريمة الإلكترونية:

هي أفعال غير قانونية تتم باستخدام التقنيات الحديثة ، من شبكات الاتصالات الإلكترونية وأنظمة المعلومات، بهدف تحقيق مكاسب شخصية أو مالية أو ضرر مثل سرقة الهوية، و الاحتيالي، وبرامج الفدية، وهجمات البرامج الضارة، والعديد من الأنشطة الأخرى،**(3،ص15)**.

5-الفئات التي تستهدفها الجرائم الإلكترونية:

يمكن تصنيف الفئات التي تستهدفها الجرائم الالكترونية الى الآتي(2،ص23):

1-جرائم موجهة للأفراد: هذه الجرائم تشمل مضايقة الافراد الكترونياً، ونشر محتوى غير اخلاقي ضدها، وكذلك تشمل جرائم الاحتيال على البطاقات الائتمانية، واختراق وتهكير الهوية الالكترونية ، والاستغلال ، والمساومة ، والتشهير، والاساءة.

2-جرائم ضد الممتلكات: هذه الجرائم هدفها اختراق اجهزة الحاسوب وسرقة محتوياتها، وانتهاك حقوق النشر والملكية وادخال فيروسات بهدف تخريبها .

3-الجرائم الموجهة ضد الحكومات: هذه الجرائم تستهدف سيادة الدولة وامنها من خلال اختراق معلومات سرية مهمة عنها ،وشن حرب ارهابية عليها.

6-انواع الجرائم الالكترونية(21،2023):

اولاً: جرائم تسبب الأذى للأفراد.

هذا النوع من الجرائم يستهدف فرد بشخصه او فئة من الافراد، لغرض الحصول على معلومات هامة تخص حسابه المصرفي او حسابه على الانترنيت ، وتشمل هذه الجرائم :

1-انتحال الشخصية : وفيها يقوم المجرم باستدراج ضحيته وينتزع منها معلومات بطريقة غير مباشرة، وكذلك استخدام صورة او حساب شخص اخر دون اذنه لأغراض غير قانونية.

2-الابتزاز الالكتروني : يقوم المجرم من خلاله بنشر صور او معلومات شخصية على مواقع التواصل، مقابل المال او اغراض

معينة.

3-تشويه السمعة : من خلالها يقوم المجرمين باستخدام البيانات المسروقة، واضافة لها بعض المعلومات المغلوطة الاخرى ، وارسالها عبر المواقع الاجتماعية او عبر البريد الإلكتروني للشخص لغرض تشويه السمعة ومحاربته نفسياً.

4-التحريض على الاعمال غير مشروعة : يقوم المجرم باعتماد البيانات المسروقة من الافراد واستغلالها بأمور تتعلق بالاستغلال الجنسي او المخدرات او غسيل الاموال وغيرها من الجرائم الالكترونية.

ثانيا: جرائم تسبب الأذى للمؤسسات،(قرصنة البرمجيات) ومنها ما يأتي:

1-هجمات رفض الخدمة: أشهر هذه الهجمات كانت في فبراير 2000م، على يد طفل يبلغ من العمر 15 عاماً، شلّت هذه الهجمات التجارة الإلكترونية آنذاك، فكان من ضمن المواقع المستهدفة أمازون وeBay،(مركز ذكاء، الجرائم الالكترونية ،**العربية السعودية،2024).**

2-الابتزاز الإلكتروني: وهو عبارة عن هجوم إلكتروني للمطالبة بالمال مقابل وقفه، ومن أبرز أشكاله: هجوم برنامج الفدية، حيث يقوم بتشفير مستندات وملفات مهمة للضحية ليستحيل الوصول إليها، حتى يتم دفع الفدية.

3-سرقة الهوية :سرقة المعلومات الشخصية للضحية من خلال الوصول إلى جهازه الإلكتروني، للتمكّن من الوصول إلى الحسابات البنكية وبطاقات الائتمان(مركز ذكاء، الجرائم الالكترونية ،**العربية السعودية،2024).**

4-أختراق الانظمة: وتتسبب الجرائم الإلكترونية بخسائر كبيرة للمؤسسات والشركات المتمثلة في الخسائر المادية والخسائر في النظم، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة في عملية الإدارة مما يسبب خسائر جسيمة للشركة أو المؤسسة.

5-كما يمكن سرقة المعلومات الخاصة بموظفين المؤسسات والشركات وتحريضهم وابتزازهم من أجل تدمير الأنظمة الداخلية للمؤسسات، وتثبيت أجهزة التجسس على الحسابات والأنظمة والسعي لاختراقها والسيطرة عليها لتحقيق مكاسب مادية وسياسية.

6-وتؤثر الجرائم الإلكترونية الخاصة باختراق الشبكات والحسابات والأنظمة بشكل سلبي على حالة الاقتصاد في البلاد، كما تتسبب في العديد من مشاكل تتعلق بتهديد الأمن القومي للبلاد إذا ما لم يتم السيطرة عليم ومكافحاتهم بكل جدارة، وتمثل نسبة الجرائم الإلكترونية والجرائم المعلوماتية حول العالم 170%، وتزداد النسبة يوم بعد يوم مما يجعلنا جميعاً في خطر محدق بسبب الانتهاكات واختراق الأنظمة والحسابات.

7-اختراق المواقع الإلكترونية والسيطرة عليها، ومن ثم توظيفها لتخدم مصالح كيانات خطيرة تهدف لزعزعة الأمن بالبلاد والسيطرة على عقول الشباب وتحريضهم للقيام بأعمال غير مشروعة.

8-تدمير النظم :

1-يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.

2- تدمير الخادم الرئيسي الذي يستخدمه جميع من بالمؤسسة من أجل تسهيل الأعمال، ويتم ذلك من خلال اختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة والدخول على الحسابات جميعاً في نفس ذات الوقت، ويتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره وبالتالي تعطل الأعمال بالشركات والمؤسسات.

ثالثا: جرائم الأموال، وتشمل ما يأتي:

1-جرائم الاحتيال والاعتداء والاستيلاء على حسابات البنوك والخدمات وأدوات الدفع الإلكترونية المتمثلة باختراق الحسابات المصرفية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات والشركات الخاصة،(20،ص23).

2-جرائم التعدي على حقوق الملكية الفكرية: وتشمل التعدي أو تسهيل التعدي على حقوق المؤلف أو براءات الاختراع، أو العلامات التجارية، أو الأسماء التجارية، أو الرسوم والنماذج الصناعية أو تصاميم الدوائر المتكاملة، التي يحميها القانون،(14،2024).

رابعا: **جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:**

تعد جريمة الاعتداء على الانظمة المعلوماتية الخاصة بالدولة احد صور الاعتداء على سلامة شبكات وانظمة وتقنيات المعلومات(الدريني،2021) ،أذ كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا

إلكتروني ا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها(20،ص12).ومن جرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة هي :

1-برامج التجسس: تنتشر العديد من برامج التجسس والمستخدمة في أسباب سياسية والتي تهدد أمن وسلامة الدولة، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات، فيقوم أعداء الوطن بهدم أنظمة النظام والاطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

2-استخدام المنظمات الإرهابية لأسلوب التضليل، ويعتمد الإرهابيون على استخدام وسائل الاتصال الحديثة وشبكة الإنترنت من أجل بث ونشر معلومات مغلوطة، والتي قد تؤدي لزعزعة الاستقرار في البلاد وإحداث الفوضى من أجل تنفيذ مصالح سياسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الانتفاع بمصالح شخصية.

3-جرائم المحتوى المعلوماتى : تشمل على كل من اعتمد استعمال تقنية معلوماتية أو برنامج معلوماتي في معالجة معطيات شخصية للغير لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه، ولربطها بمحتوى منافٍ للآداب العامة.

4-الجرائم المتعلقة بتصميم المواقع والحسابات الخاصة والبريد الإلكتروني : كل من صمم بريدًا إلكتروني أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعي أو اعتباري فهو يعد من أهداف الجرائم الإلكترونية(3،ص24).

7-أهداف الجر ائم الإلكترونية:

يمكن توضيح اهداف الجر ائم الالكترونية بالاتي (14،ص533):

1- التمكن من الوصول الى المعلومات بشكل غير شرعي كسرقة المعلومات او الاطلاع عليها او حذفها او تعديلها بما يحقق هدف المجرم.

2- الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها

3- محاولة المجرمون الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها .

4- الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الائتمان وسرقة الحسابات المصرفية الخ

8-أسباب الجريمة على المستوي المجتمعي:

هناك عدة اسباب للجريمة على المستوى المجتمعي(3،ص45) وهي ما يأتي:

1- التمدن (Urbanization)

يعد التمدن او التحضر احد الاسباب الرئيسية للجرائم الإلكترونية في كثير من دول العالم ومنها العراق. أذ ان الهجرة السكانية المتفاقمة من الريف الى المدن الكبيرة والمراكز الحضرية الاخرى لعبت دورا كبيرا في تفاقم الجرائم الالكترونية ، وفي كثير من الاحيان يهاجر الشباب الذين لا يستطيعون تلبية متطلبات الحياه الحضرية ولا يستطيعون مواجهتها نتيجة تكاليفها الباهظة ، الامر الذي يفرض عليهم العيش في مناطق ذات سكن عشوائي او ما يعرف بالعشوائيات او الأحياء الطرفية والهامشية ونتيجة لذلك يجد الاشخاص انفسهم غير قادرين على تلبية متطلبات الحياه وكنتيجة لهذه الظروف المتراكمة يلجؤون الى ما يعرف بالجريمة الإلكترونية.

2- البطالة(Unemployment)

تعد البطالة من الاسباب الرئيسية الاخرى المسببة للجريمة الإلكترونية، أذ ان ارتفاع معدلات البطالة قد تؤدي إلى يأس الشخص وتدهور حالته المادية أضافة الى عدم وجود وسائل بديلة للدعم، أذ ان البطالة أحد العوامل التي تزيد من احتمالية ارتكاب الجرائم، فصعوبة الحصول على العمل من قبل الاشخاص وعدم تأمين احتياجاتهم الأساسية يمكن أن يلجؤوا إلى الجريمة كوسيلة لكسب المال.

3-الضغوط العامة(Strains)

بعض الضغوط التي يتعرض لها الافراد و منها ضعف الايمان الديني، او تفكك الاسرة ، الفقر وعدم الوعي بالأخلاق، تنامي ظاهرة الجهل والأمية، ، البطالة، عدم المساواة، ضعف السيطرة على الدوافع، ونماذج السلوك الإجرامي السيئة، كلها عوامل تؤدي الى ارتكاب الجرائم الالكترونية .

4-البحث عن الثروة(Quest for Wealth) ان بعض الناس تلجأ إلى الجرائم الإلكترونية ، من اجل البحث عن الثراء والشهرة ،أذ ان المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

5- التوظيف: ان عدم الحصول على وظيفة مناسبة ومستقرة يعد

عاملاً مهماً في الجريمة او الحد منها ،أذ ان الحصول الوظيفة المناسبة قد يحد من ارتكاب الجرائم، حيث يمكن أن يوفر العمل القانوني أوسع فرص الدخل والاستقرار الاجتماعي.

6-ضعف إنفاذ القانون وتطبيقه في الجريمة الإلكترونية (lack of law enforcement and implementation)، يعد ضعف نفاذ القانون وعدم تطبيقه بشكل صارم ، من الاسباب الرئيسية التي تؤدي تفاقم الجرائم الالكترونية ، أذ ان هناك بعض الدول لم تطور قوانينها وأجهزة العدالة فيها لكي تتمكن من مواكبة التقدم والتطور في الجرائم الإلكترونية وأساليبها المتعددة.

9-خصائص الجرائم الإلكترونية:

تتميز الجرائم الإلكترونية بعدة خصائص منها:

1- القدرة على الإختراق والاختراق الذاتي.

2- السرية والتعتيم والتمويه.

3- تمكن المجرمين من الوصول الى معلومات حساسة وسرية.

4- التلاعب والتحكم بالمعلومات والبيانات.

5- القدرة على الإضرار بالأفراد والمؤسسات والدول.

6-الصعوبة في تعقب وتحديد المتسببين فيها.

7- الإمكانات الكبيرة للجني السريع للأموال.

8- الانتشار الواسع للجرائم الإلكترونية وزيادتها المستمرة.

10-مخاطر الجرائم الالكترونية وأضرارها :

ان الجرائم الالكترونية عبارة عن مرض ووباء يفتك بأمان وسلامة المجتمع ، ويسبب له بعض المخاطر والأضرار منها مايأتي (18،ص22) :

1-هدم بناء الأسرة وتفككها نتيجة ارتكاب بعض الجرائم بحق احد افراد الاسرة ، و الاضرار بسمعة الأفراد من خلال اظهارهم بصورة غير لائقة أمام المجتمع .

2- خسائر كبيرة للأفراد والشركات في راس المال،

3- تعرض الجرائم الإلكترونية معلومات الأفراد الشخصية للخطر أي فقدان الخصوصية، مثل سرقة البيانات، وكذلك تسبب خسائر كبيرة للأفراد والشركات في راس المال منها سرقة الأموال، الاحتيال في المعاملات.

4- تؤدي إلى اختراق الأجهزة والنظم، مثل برامج الفدية التي تمنع وصول المستخدمين إلى ملفاتهم، وهجمات الفيروسات التي تضر بالأنظمة.

5-تمثل الجرائم الإلكترونية تهديدًا للأمن القومي للدول، مثل الهجمات على البنية التحتية الحساسة، وجمع المعلومات الاستخباراتية.

6-تسبب الجرائم الإلكترونية تأثيراً على صحة الأفراد، مثل التعرض لمحتوى ضار، أو الحصول على معلومات طبية غير صحيحة.

7- تعمل الجرائم الإلكترونية على تقويض الثقة في الأنظمة الرقمية، الامر الذي يجعل الناس أكثر تحفظًا في استخدام الإنترنت.

8-التأثير على الثقة بالنظام الرقمي: تؤدي الجرائم الإلكترونية إلى تقويض الثقة في الأنظمة الرقمية، مما يجعل الناس أكثر تحفظًا في استخدام الإنترنت.

11-مواجهة الجرائم الإلكترونية:

يمكن استخدام الذكاء الاصطناعي في مجال المكافحة ضد الجرائم الإلكترونية عن طريق(11،ص27):

1-**تحليل البيانات** :يمكن للذكاء الاصطناعي تحليل الكميات الضخمة من البيانات المتاحة عبر الإنترنت لاستخدامها في تحديد أنماط الجريمة الإلكترونية وتطوير استراتيجيات مكافحتها.

2- **عمليات التعرف على الجريمة** :يمكن استخدام الذكاء الاصطناعي لتدريب نماذج التعرف على الجرائم الإلكترونية والتنبؤ بمخاطرها.

3- **التحليل الجنائي** : يمكن استخدام تقنيات الذكاء الاصطناعي المتقدمة لتشخيص جرائم القرصنة الإلكترونية وتحليل الأدلة الرقمية في سرعة فائقة.

4- **الكشف المبكر** :من خلال تطوير نماذج اصطناعية من خلال تحليل كمية البيانات والأنماط الزمنية ، يمكن الكشف عن الجريمة الإلكترونية في مراحل مبكرة واتخاذ إجراءات المكافحة والوقاية منها.

5- **الكشف عن الاحتيال والتزوير**: يمكن استخدام الذكاء الاصطناعي لتحليل نماذج السلوك الغريب التي تشير إلى الاحتيال والتزوير في المعاملات المالية الإلكترونية.

12- استخدام الذكاء الاصطناعي في مكافحة الجريمة:

يمكن استخدام الذكاء الاصطناعي في مكافحة الجرائم الالكترونية بعدة طرق منها ما يأتي:

1- تحليل البيانات: يمكن استخدام تحليل البيانات والتعلم الآلي للكشف عن أنماط مشتركة في الجرائم وتوقع نمط الجريمة المحتملة وتحديد مناطق الخطر، مما يساعد الشرطة في التركيز على المناطق والمجموعات التي تشير البيانات إلى احتمالية ارتكاب جرائم

بها.

2- التعرف على الصور: يمكن استخدام تكنولوجيا التعرف على الصور لتحديد هوية لصوص ومجرمين، مما يساعد الشرطة في تحديد هوية الأشخاص الذين قاموا بارتكاب جرائم، وتسهل عملية القبض عليهم.

3- التنبؤ بالجرائم: يمكن استخدام التعلم الآلي لتحليل البيانات وتحديد الأنماط الجغرافية للجرائم ، مما يساعد في التنبؤ بالجرائم المحتملة واتخاذ التدابير اللازمة للحد منها.

4- مراقبة الكاميرات: يمكن استخدام تكنولوجيا التعرف على الصور ومراقبة الكاميرات لتحديد الأشخاص الذين يقومون بسلوك غير قانوني، مثل السطو على المتاجر، وتسهل عملية اعتقالهم.

5- الرصد الذكي: يمكن استخدام تكنولوجيا الرصد الذكي للكشف عن أنشطة مشبوهة، مثل الصوت العالي، وتلك الإجراءات تساعد في توجيه عمليات الشرطة إلى الأماكن التي تحتاج إلى تواجد الشرطة بشكل ضروري، (1،ص66).

13-طرق مكافحة الجرائم الإلكترونية والحد من انتشارها:

لقد توسعت الانشطة الاجرامية في الآونة الاخيرة الى حد بعيد وذلك من خلال اعتمادها على التكنلوجية الحديثة والذكاء الاصطناعي ويمكن للأجهزة الامنية ان تطور من قدراتها من خلال استخدامها لتقنية الذكاء الاصطناعي وفق الاتي (11،ص2824) :

1-الشرطة الاستباقية، وتعني ردع العمل الاجرامي من خلال العمل الاستباقي، الشرطي المدفوع بتحليلات البيانات والادلة المادية، ومن اهم الاجراءات التي تساعد على ذلك تبني الاجهزة الامنية لأنظمة التخزين الحسابي الذي يكون عاملاً رئيسياً في الحد من الجرائم الالكترونية.

2-تطوير اجهزة الشرطة لتصبح أكثر اعتماداً على التقنيات الحديثة في كل ما يقوم به رجال الشرطة بهدف الاستفادة من الوفرة في الادلة الرقمية (الشرطة الرقمية)، والتي يمكن الحصول عليها من سجلات الهاتف، ورسائل البريد الالكتروني .

3-استخدام برامج مكافحة الفيروسات وإبقائها محدثة فهذه أيضًا تعتبر طريقة ذكية لحماية النظام من أي هجمات. إذ تتيح برامج مكافحة الفيروسات فحص التهديدات واكتشافها وإزالتها.

4-الاعتماد على شبكة الانترنيت في رفع الملفات الرقمية للقضايا التي تحتوي على ادلة جنائية لإتاحة استخدامها من قبل العديد من المسؤولين في ذاته، ولا يمكن ذلك برفع ملفات الجرائم فقط وانما لابد من تحول الحكومة بأكملها الى حكومة رقمية لتواكب الاتجاه الكبير في رقمنه كل شيء(19،ص2825).

5-عدم فتح المرفقات التي تتواجد ضمن رسائل البريد الإلكتروني العشوائية

6-وضع خطط استجابة لحوادث الأمن السيبراني.

7-عدم فتح المرفقات التي تتواجد ضمن رسائل البريد الإلكتروني العشوائية.

8-تحديث البرامج وأنظمة التشغيل بشكل مستمر.

9-وضع رقم سري قوي يجعل عملية القرصنة أكثر صعوبة إذ يجب أن يحوي أكثر من ثمانية أحرف. وأن تتكون من رموز وأحرف ولغات مختلفة إلخ.

10-الابتعاد قدر الإمكان عن الاتصال بالشبكات العامة، وإن كنت مضطرّاً لذلك، تجنّب إجراء معاملات سريّة.

11-فحص عناوين الـ URL قبل فتح الروابط، والتأكّد من أمانها ومصداقيتها.

12-تجاهل الرسائل غير المرغوب بها في رسائل البريد الإلكتروني.

14-قوانين مكافحة الجرائم الالكترونية في العراق:

1-قانون مكافحة الجرائم الإلكترونية في العراق لسنة 2019:

يهدف هذا القانون الى(22،2019):

1-حماية الافراد والمجتمع من الجرائم الالكترونية.

2-مكافحة الجريمة الالكترونية والتي تشكل تهديداً لامن الدولة وسلامتها.

3-زيادة الوعي العام بمخاطر الجريمة الالكترونية.

4-تطوير قدرات العاملين على انفاذ هذا القانون وتقديم الدعم التقني للسلطة القضائية لمواكبة اخر التطورات الحاصلة بمجال الجرائم الالكترونية.

تسري احكام هذا القانون على اي من الجرائم المنصوص عليها فيه سواء ارتكبت جزءاً او كلاً داخل او خارج العراق او امتد اثرها داخل العراق وسواء كان الفاعل أصلياً او شريكاً او محرضاً على ان تكون الجرائم معاقب عليها خارج العراق مع مراعاة الاتفاقيات الدولية بهذا الشأن.

ومن اهم البنود التي نص عليها هذا القانون والتي يحاسب عليها مرتكبيها هي ما يأتي:

1- جرائم التعدي على سرية وسلامة البيانات والمعلومات الالكترونية ونظم المعلومات.

2-جرائم التهديد والابتزاز.

3-الجرائم الواقعة على البطاقات الالكترونية.
4-جرائم التحريض والاتفاق والاشتراك والشروع في الجرائم الالكترونية.
5-جرائم النظام العام والآداب.
6-تسري احكام هذا القانون على اي من الجرائم المنصوص عليها فيه سواء ارتكبت جزءاً او كلاً داخل او خارج العراق او امتد اثرها داخل العراق وسواء كان الفاعل أصلياً او شريكاً او محرضاً على ان تكون الجرائم معاقب عليها خارج العراق مع مراعاة الاتفاقيات الدولية بهذا الشأن.

بهدف توفير الحماية القانونية وإيجاد نظام عقابي لمرتكبي جرائم الحاسوب وشبكة المعلومات ومكافحة الجرائم الالكترونية التي رافقت نشوء ونمو وتطور نظم الحاسوب والشبكات وثورة تقنية المعلومات ولما تنطوي عليه من مخاطر عدة تلحق بالمؤسسات والافراد خسائر كبيرة باعتبارها تستهدف الاعتداء على البيانات والمعلومات وتمس بالحياة الخاصة للأفراد وتهدد الأمن الوطني والسيادة الوطنية وتضعف الثقة بالتقنيات الحديثة وتهدد ابداع العقل البشري ومن اجل توفير الحماية القانونية لنظم الحاسوب التي تعمل الدولة على تشجيع الاعتماد عليها في الانشطة كافة فقد شرع هذا القانون(2019،22). ونص قانون سنة 2012 المقترح ، (قانون جرائم المعلوماتية العراقي)

أذ يقول القانون المقترح في المادة 2 أنه يهدف إلى "توفير الحماية القانونية للاستخدام المشروع للحاسوب وشبكة المعلومات، ومعاقبة مرتكبي الأفعال التي تشكل اعتداءً على حقوق مستخدميها." على وجه التحديد يوفر القانون عقوبات على استخدام أجهزة الحاسوب فيما له علاقة بالعديد من الأنشطة الممنوعة، مثل الاحتيال المالي والاختلاس (المادة 7) وغسيل الأموال (المادة 10) وتعطيل الشبكات (المادة 14) والمراقبة غير المشروعة (المادة 15 (أولاً) (ب) والمادة 16) والاعتداءات على الملكية الفكرية (المادة 21). ومع ذلك فإن هذا القانون لا يقتصر في استهدافه على نطاق محدود، بالأحرى ستجري أحكامه استخدام الحاسوب فيما يتصل بنطاق واسع من الأنشطة التي يتم تعريفها بشكل فضفاض – والكثير منها غير خاضع للقواعد حاليا – دون الرجوع إلى أي معايير محددة. وبالسماح للسلطات العراقية بمعاقبة الأفراد بهذه الطريقة، تبدو أحكام القانون متعارضة مع القانون الدولي والدستور العراقي، وإذا تم تطبيقها فسوف تشكل تقليصًا خطيرًا لحق العراقيين في حرية التعبير وتكوين الجمعيات (23 ، 2012).

وبالرجوع الى قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل لم يكن مواكبا لهذه الجرائم مع انه نص في المادة 182 علي معاقبة من ينشر أو يذيع اخبار بأية صورة وعلي أي وجه وبأية وسيلة معلومات أو صور أو وثائق أو مكاتبات أو غير ذلك، خاصة بدوائر الدولة والمصالح الحكومية وكانت محظور نشرها أو اذاعتها، كما ورد في بعض مواده تعريف الاصطناع في المادة 291 عقوبات (انشاء محرر لم يكن له وجود من قبل ونسبته إلى غير محرره دون ما ضرورة لتعمد تقليد محرر بالذات وخط انسان معين)، وعاقب في المادة 361 من عطل عمدا وسيلة من وسائل الاتصال السلكية أو اللاسلكية المخصصة للمنفعة العامة، وفي المادة 403 عاقب صانع أو مستورد أو حائز المطبوعات والكتب والرسوم المخلة بالحياء والآداب العامة، وفي المادة 404 عاقب كل من جهر باغان أو اقوال فاحشة أو مخلة بالحياء بنفسه أو بواسطة جهاز آلي وفي محل عام، وفي المادة 432 عاقب كل من هدد بالقول أو الفعل أو الإشارة كتابة أو شفاها، واعتبر في المادة 434 أفعال رمي الغير بما يخدش الشرف أو الاعتبار أو جرح المشاعر وان لم يتضمن اسناد واقعة معينة من الظروف المشددة اذا وقع بطريق النشر بالصحف أو المطبوعات أو طرق الاعلام الأخرى(7،ص2).

15-بعض النقاط الرئيسية التي ينبغي مراعاتها لضمان تقنين الجرائم الإلكترونية دون المساس بحرية التعبير(2023،6):

1-تعريف دقيق وواضح للجرائم الالكترونية ، اذ ينبغي ان تكون التعاريف القانونية للجرائم مثل(الابتزاز،الاختراق،الاحتيال الالكتروني) وغيرها، محددة وواضحة ، لتجنب التفسيرات الواسعة التي قد تستخدم لقمع الرأي.

2-ضرورة التمييز بين الجريمة الالكترونية والتعبير عن الرأي، اذ يجب ان لا تصنف الآراء النقدية أو السخرية السياسية او الاجتماعية كجرائم، ويجب حماية حرية الصحافة والمدونات والتعبير .

3-ضمان الحق في الدفاع والمحاكمة العادلة ، اذ يجب ان يحصل المتهم في الجرائم الالكترونية على محاكمة عادلة، وحق الدفاع ، مع احترام الاجراءات القانونية، وكذلك يجب ان تخضع ممارسات المراقبة والحجب وحذف المحتوى الالكتروني الى اذن قضائي، وذلك لمنع التعسف في استخدام السلطة.

4-حماية البيانات الشخصية وخصوصية الافرار، اذ يجب ان تتضمن القوانين احكاماً تحمي خصوصية المعلومات وعدم استخدامها دون موافقة او مبرر قانوني.

5-الشفافية في تنفيذ القانون ، من حيث الاعلان عن الحالات التي يفرض فيها حجب او الملاحقة القضائية، واتاحة امكانية الطعن على قرارات الحجب او الادانة

6-الموازنة بين الامن وحقوق الانسان ، اذ ان مكافحة الارهاب والتطرف او الجرائم لا يجب ان تكون ذريعة لانتهاك خصوصية الافراد او تقييد تعبيرهم .

ولما كان قانون مكافحة الجرائم الالكترونية يهدف إلى مكافحة هذه الجرائم التي تشكل تهديدا لأمن المجتمع وامن الدولة والاستقرار، بالإضافة إلى أن التطور السريع في مجال تقنية المعلومات تستوجب توفير الحماية القانونية ومعاقبة كل من يرتكب فعلا يخالف القانون واقتران تلك العقوبات بالظروف المشددة عند فرض العقوبة، خصوصا بعد ظهور حالات الابتزاز والانتحال والاحتيال والتعدي على الشرف والأخلاق وقيم المجتمع، وظهور صور جديدة تتمادى في أفعالها تتحدى القانون والمجتمع وتتطوع العقل العلمي والفني إلى عقل إجرامي مقترن بخلل نفسي، ليكون ضرره كبيرا، وتمس بالحياة الخاصة للأفراد وتهدد الأمن الوطني والسيادة الوطنية وتضعف الثقة بالتقنيات الحديثة وتهدد ابداع العقل البشري، ومن أجل توفير الحماية القانونية لنظم الحاسوب التي تعمل الدولة على تشجيع الاعتماد عليها في الأنشطة كافة، خصوصا أن العراق يضع أقدامه حديثا، سالكا طريق التطور التقني والمعلوماتي، الذي يسهم بشكل مؤكد في ترصين خطوات بناء دولة القانون التي ينشدها الجميع(2023،7)كل ذلك يحتاج الى توفير الحماية ومعاقبة مرتكبها.

الاستنتاجات:

1- هناك عدة مميزات للذكاء الصناعي كان لها دور كبير في عدة مجالات، منها في جرائم نقل البيانات والاستيلاء عليها ، **وجرائم الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وجرائم البنوك**. وغيرها من الاستخدامات.

2-كان للتقدم التكنولوجي والتحول الرقمي، دور كبير في ظهور انواع من الجرائم ، لها تسميات عديدة منها الجرائم السيبرانية أو الجرائم المعلوماتية، أو الجرائم التكنولوجية.

3- لقد أدى التطور السريع والمتلاحق لتقنية المعلومات إلى مضاعفة المخاطر والاعتداءات على الحريات الشخصية، وحرمة الحياة الخاصة، ومؤسساتها وامنها القومي، وكيانها.

4- ان التطور في مجال تقنيات الذكاء الاصطناعي يبسط عمل المجرمين لابتزاز ضحاياهم.

5-استنتجت الدراسة ان هناك عدة طرق لمواجهة الجريمة الالكترونية منها، لو تبعت لكان لها دور كبير في الحد من هذه الجرائم او التقليل منها.

6- العراق احد الدول التي تعاني من الجرائم الالكترونية ، وهناك قوانين عالجت هذه الجرائم، الغرض منها هو تأمين الحماية القانونية للافراد وتقنين الجرائم الالكترونية .

7- **تعد جريمة الاعتداء على الانظمة المعلوماتية الخاصة بالدولة احد صور الاعتداء على سلامة شبكات وانظمة وتقنيات المعلومات.**

8- أضافت برامج الذكاء الاصطناعي الكثير في مواجهة الجريمة الالكترونية والسيبرانية ومكان الجريمة، وذلك من خلال اعتمادها في مكافحة الجريمة والقبض على مرتكبها.

التوصيات:

1- تنمية الاشخاص العاملين في مجالات مكافحة الجرائم الالكترونية.

2- العمل على توعية المجتمع وتنبيهه بمخاطر الجرائم الالكترونية، واعتماد برامج واعلانات في القنوات الفضائية توضح مخاطر الجرائم الالكترونية.

3-اعتماد قوانين رادعة للحد من ارتكاب الجرائم الالكترونية .

4- العمل على تطوير العلاقات الدولية وتحقيق الأمن الداخلي والخارجي.

5-ضرورة احترام .حرية التعبير وخصوصية الافراد في مواقع التواصل الاجتماعي.

6-تحقيق التوازن بين الأمان الإلكتروني وحرية التعبير بعيداً عن الحجب والملاحقة والرقابة،جانب مهم في تقنين الجرائم الإلكترونية بشكل فعال وعادل.

7-توعية الأشخاص بكل مكان عن أسباب حدوث الجرائم المعلوماتية وكيفية تنفيذها، فالإعلام له دور هام في توعية المواطنين عن مدى خطورة الجرائم الإلكترونية، كما يجب الإشارة أيضاً إلى كيفية التعامل معها والحماية منها.

المصادر:

1- يوسف، أمير فرج - الجرائم المعلوماتية على شبكة الإنترنت دار المطبوعات الجامعية الإسكندرية 2008.

2- الحياري، أيمان ، أنواع الجرائم الإلكترونية،موضوع،2022.

3- مرعي، اسراء جبريل رشاد ،الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها،**المركز الديمقراطي**

العربي،2016.

4- شحاته، اميرة ، جرائم الذكاء الاصطناعي قتل وإيذاء بدنى ونصب وتحريض على الانتحار، اليوم السابع،2023.

5- نجيب، أشرف محمد ، جرائم الاعتداء على سلامة شبكات وانظمة وتقنيات المعلومات ، مجلة روح القوانين ، العدد الخامس والتسعون ، 2021.

6- محمود، خالد وليد ، الجرائم الإلكترونية كظاهرة عالمية، الجزيرة نت ،2023.

7- عبود، زهير كاظم ، الجرائم الالكترونية في القانون العراق، مقالات، وكالة الانباء العراقية،2023.

8- ابراهيم، علي احمد ، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية ، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)،2020.

9- علاوي، عمار ، المجيد، ومحمد عبد ، استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها، مجلة جامعة الشارقة للعلوم القانونية، العدد(4)،المجلد (20)،2023.

10- رضوان، علاء ، دور الذكاء الاصطناعي في النيابة العامة وكشف الجريمة، اليوم السابع،2021.

11- ابراهيم، علي احمد ، تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الالكترونية ، المجلة القانونية، المجلد 9، العدد 8، 2021.

12- ال قاسم، فهد ، الذكاء الاصطناعي، المملكة العربية السعودية ، 2017.

13- الرشيدي، محمد ، إجراءات التصدي للجريمة الإلكترونية وعقوبة مرتكبيها ،بوابة الاهرام ، مصر،2022.

14- قطر، محامي ، انواع الجرائم الالكترونية قطر وطرق الوقاية منها،2024.

15- ،شركة الحلول الادارية المتقدمة المحدودة، المملكة العربية السعودية،2024.14Empower-مركز ذكاء، الجرائم الالكترونية

16- رمضان، نسيم ، كيف يمكن للذكاء الاصطناعي أن يؤجج الجرائم الإلكترونية، الشرق الاوسط،2024.

17- الاخنش، نور امينة ، العيداني، محمد ،الذكاء الاصطناعي كالية لمجابهة الجريمة الالكترونية، مجلة القانون والعلوم البيئية،العدد(02)،2023.

18- النجار، يوسف وليد ، الجرائم الالكترونية وعلاقة القانون بها، منصة سنا، 2023.

19- ابراهيم، هند ، مدى فاعلية أحكام القانون الجنائي العراقي حول التصدي للجرائم الإلكترونية،2024.

20- عثمان، وليد ، أنواع الجرائم الالكترونية وعقوبتها،مصر،2022.

21-المجموعة السعودية لأمن المعلومات، وزارة التعليم السعودي، **ماهي الجرائم الالكترونية، أنواعها ، كيفية تنفيذها وطرق مواجهتها، 2024.**

22- قانون مكافحة الجرائم الإلكترونية في العراق لسنة 2019، 2020.

23- هيومن رايتس ووتش | يوليو/ تموز 11 2012.