AL-NAHRAIN JOURNAL OF LEGAL SCIENCE Vol.27 2025, pp. 162-174

AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW

ISSN:3006- 0605 DOI:10.58255

مجلة النهرين للعلوم القانونية المجلد: ٢٧ تموز ٢٠٢٥ عدد: مؤتمر (الفراهيدي)

Received:1/3/2025 Accepted: 7/4/2025 Published: 1/6/2025

Artificial Intelligence and Cybercrime: Challenges of Proof and Punishment in Criminal Law

Nahal Hassan Ibrahim

Faculty of Law / Al-Farahidi University

Abstract:

With the advancement of artificial intelligence (AI) technologies, new forms of cybercrime have emerged, exploiting AI to conduct sophisticated digital attacks such as Deepfake manipulation, AI-driven fraud, and machine learning-assisted security breaches. These crimes not only target individuals but also corporations and governmental institutions, posing a significant legal challenge.

This study aims to analyze the relationship between AI and cybercrime, focusing on the challenges related to proving these crimes and enforcing appropriate penalties within criminal law. The research examines the situation in Iraq in comparison to legal frameworks in other countries, such as the United States and the European Union, which have more advanced regulations for combating cybercrime.

The findings reveal that Iraq suffers from a lack of specialized legislation to address cybercrime, along with weak recognition of digital evidence, making AI-related crime prosecution more complex. The study also highlights a significant gap between Iraq and developed countries in cybersecurity readiness, with Iraq scoring only 42 points on the global cybersecurity readiness index compared to 95 points for the United States.

Keywords: Artificial Intelligence, Cybercrimes, Algorithms, Cybersecurity, Crimes

الذكاء الاصطناعي والجريمة السيبرانية تحديات الإثبات والعقوبة في القانون الجنائي

م. نـهال حسن إبراهيم
كلية القانون/ جامعة الفراهيدي

الملخص:
مع تطور تقنيات الذكاء الاصطناعي، ظهرت أشكالٌ جديدةٌ من الجرائم السيبرانية التي تستغل هذه التكنولوجيا لتنفيذ هجمات رقمية متقدمة، مثل التزييف العميق(Deepfake) ، والاحتيال المعتمد على الخوارزميات الذكية، والتسلل إلى الأنظمة الأمنية باستخدام تعلم الآلة (Machine Learning).هذه الجرائم لا تستهدف الأفراد فقط، بل تمتد إلى الشركات والمؤسسات الحكومية، مما يجعلها تحديًا قانونيًا معقدًا.

يرمي هذا البحث إلى تحليل العلاقة بين الذكاء الاصطناعي والجريمة السيبرانية، مع التركيز على التحديات التي تواجه إثبات هذه الجرائم وإصدار العقوبات المناسبة لها في القانون الجنائي. إذ يتناول البحث الوضع في العراق مقارنة بالتجارب القانونية في الدول الأخرى مثل الولايات المتحدة والاتحاد الأوروبي، حيث يتمتعان بأطر قانونية أكثر تقدمًا في مكافحة الجرائم الإلكتروني.
أظهرت النتائج أن العراق يعاني نقصًا في القوانين المتخصصة لمكافحة الجرائم السيبرانية، بالإضافة إلى ضعف الاعتراف بالأدلة الرقمية، ما يؤدي إلى تعقيد محاكمة الجرائم المرتبطة بالذكاء الاصطناعي. كما كشف البحث أن هنالك فجوةً كبيرةً بين العراق والدول المتقدمة فيما يخص الأمن السيبراني، إذ حصل العراق على ٤٢ نقطة فقط في مؤشر الجاهزية السيبرانية مقارنة بـ ٩٥ نقطة للولايات المتحدة.

الكلمات المفتاحية: الذكاء الاصطناعي، الجرائم السيبرانية ، الخوارزميات ، الامن السيبراني ، الجرائم.

المقدمة

مع تطور تقنيات الذكاء الاصطناعي، ظهرت أشكال جديدة من الجرائم السيبرانية التي تستغل هذه التكنولوجيا لتنفيذ **هجمات رقمية متقدمة**، مثل **التزييف العميق(Deepfake)** ، والاحتيال المعتمد على خوارزميات ذكية، والتسلل إلى الأنظمة الأمنية باستخدام **تعلم الآلة (Machine Learning)**.هذه الجرائم لا تقتصر على الأفراد فحسب، بل تستهدف الشركات والحكومات، مما يجعلها تحديًا عالميًا يتطلب استجابات قانونية فعالة.

وفي هذا السياق، تبرز مشكلة إثبات الجريمة السيبرانية،إذ تعتمد هذه الجرائم على **بيئات افتراضية معقدة** وأدلة رقمية قد تكون قابلةً للتلاعب، مما يثير تساؤلات حول مدى **ملاءمة القوانين الجنائية التقليدية** للتعامل مع هذه التحديات. بالإضافة إلى ذلك، تواجه الأنظمة القانونية صعوبة في فرض **عقوبات رادعة** تتناسب مع طبيعة هذه الجرائم المتطورة. [1]

يهدف هذا البحث إلى دراسة العلاقة بين الذكاء الاصطناعي والجريمة السيبرانية، مع **تحليل التحديات القانونية** التي تواجه عملية الإثبات والعقوبات في القانون الجنائي، وذلك من خلال دراسة الوضع في العراق **ومقارنته بالتجارب القانونية في الدول الأخرى** .كما يسعى إلى تقديم توصيات من شأنها تحسين القوانين الحالية لمواكبة التطورات التقنية.

الإشكالية

كيف يؤثر الذكاء الاصطناعي على تطور الجرائم السيبرانية؟ وما هي التحديات التي يفرضها على نظام الإثبات والعقوبات في القانون الجنائي؟

أهمية البحث

- **تحليل التحديات القانونية** التي يفرضها الذكاء الاصطناعي على نظام الإثبات في الجرائم السيبرانية.
- **دراسة مدى كفاءة العقوبات الجنائية الحالية** في مواجهة الجرائم التي تعتمد على الذكاء الاصطناعي.
- **تقييم التشريعات العراقية** ومدى مواكبتها للتطورات التقنية مقارنة بالقوانين الدولية.
- **اقتراح حلول قانونية** لتعزيز فعالية النظام الجنائي في مواجهة الجرائم السيبرانية المتقدمة.

أهداف البحث

١. **فهم العلاقة بين الذكاء الاصطناعي والجريمة السيبرانية**، وكيفية استغلال التقنيات الحديثة لتنفيذ الجرائم الرقمية.

٢. **تحليل صعوبات الإثبات في الجرائم السيبرانية**، خاصة عند استخدام تقنيات الذكاء الاصطناعي لإخفاء الأدلة أو التلاعب بها.

٣. **دراسة العقوبات القانونية المطبقة حاليًا** ومدى فعاليتها في مواجهة هذه الجرائم، مع تسليط الضوء على القوانين العراقية.

٤. **مقارنة التشريعات العراقية بالقوانين الدولية**، مثل التشريعات الأوروبية والأمريكية، لتحديد نقاط القوة والضعف.

٥. **اقتراح تعديلات تشريعية** لتعزيز قدرة الأنظمة القانونية على التعامل مع التهديدات السيبرانية المعتمدة على الذكاء الاصطناعي

[1] للمزيد أنظر)تقديم كتاب الذكاء الاصطناعي والقانون(فوزي غروس، الذكاء الاصطناعي والقانون، المجلة المغربية لتاريخ القانون، عدد خاص2023 - 3- ، ص، ٥

المبحث الأول
الذكاء الاصطناعي وعلاقته بالجرائم السيبرانية

المطلب الأول: مفهوم الذكاء الاصطناعي وأنواعه

الذكاء الاصطناعي هو أحد أهم التطورات التكنولوجية في العصر الحديث،إذ يعتمد على تطوير أنظمة وبرمجيات قادرة على محاكاة القدرات البشرية في التفكير والتحليل واتخاذ القرارات. ويهدف الذكاء الاصطناعي إلى تعزيز قدرة الأجهزة على التعلم من البيانات وتحليلها بشكل مستقل، مما يجعله أداةً قويةً تُستخدم في مختلف المجالات، سواء في التطبيقات الإيجابية مثل الرعاية الصحية والصناعة، أو في الجوانب السلبية مثل الجرائم السيبرانية.

إن الذكاء الاصطناعي ليس تقنية حديثة بالكامل، بل شهد مراحل تطور متعددة منذ منتصف القرن العشرين، حيث بدأ بوصفه مفهومًا نظريًا يعتمد على برمجة الحواسيب لأداء مهام بسيطة، ثم تطور ليشمل الشبكات العصبية التي تمكن الأنظمة من التعلم من البيانات، وصولًا إلى عصر البيانات الضخمة والتعلم العميق، إذ أصبحت الأنظمةُ قادرةً على التعامل مع كميات هائلة من المعلومات واتخاذ قرارات معقدة دون تدخل بشري مباشر. [1]

يمكن تصنيف الذكاء الاصطناعي إلى عدة أنواع، تختلف في مدى قدرتها على محاكاة الذكاء البشري. هناك الذكاء الاصطناعي الضيق، الذي يُستخدم في مهام محددة مثل المساعدات الرقمية والتعرف على الصور، والذكاء الاصطناعي العام، الذي يهدف إلى محاكاة الإدراك البشري الكامل لكنه لا يزال في مرحلة البحث والتطوير. بالإضافة إلى ذلك، هناك الذكاء الاصطناعي الفائق، الذي يتفوق نظريًا على القدرات البشرية في جميع المجالات، لكنه لا يزال مجرد فرضية مستقبلية. ومن أحدث التطبيقات في هذا المجال، الذكاء الاصطناعي التوليدي، الذي يُستخدم لإنشاء محتوى جديد مثل النصوص والصور بناءً على البيانات المتاحة. [2]

يُظهر تطور الذكاء الاصطناعي أنه ليس مجرد أداة مساعدة، بل هو تقنية قادرة على تغيير شكل الحياة البشرية بشكل جذري، وهو ما يجعله محلّ اهتمامٍ واسعٍ في مختلف المجالات، سواء في تحسين الأداء الصناعي والتجاري، أو في استغلاله لتنفيذ الجرائم السيبرانية بطرق أكثر تعقيدًا وفاعليةً.

المطلب الثاني: تطبيقات الذكاء الاصطناعي في الجرائم السيبرانية

مع التقدم السريع في تقنيات الذكاء الاصطناعي، لم يعد استخدامه مقتصرًا على التطبيقات المفيدة في المجالات العلمية والتجارية، بل أصبح أداةً قويةً تُستخدم في تنفيذ الجرائم السيبرانية بطرق أكثر تعقيدًا وفاعليةً. يستغل المهاجمون قدرات الذكاء الاصطناعي في تحليل البيانات، التلاعب بالمعلومات، وتطوير برمجيات هجومية ذكية قادرة على تنفيذ عمليات قرصنة متقدمة من دون الحاجة إلى تدخل بشري مباشر. من بين أبرز التطبيقات التي يُستخدم فيها الذكاء الاصطناعي لتنفيذ الجرائم السيبرانية ما يلي: [3]

١. التزييف العميق(Deepfake)

التزييف العميق هو أحد أخطر تطبيقات الذكاء الاصطناعي في الجرائم السيبرانية،إذ يعتمد على خوارزميات التعلم العميق لإنشاء مقاطع فيديو وصوت مزيفة تُظهر أشخاصًا يقولون أو يفعلون أشياء لم تحدث في الواقع. يتم تدريب هذه الأنظمة على تحليل بيانات ضخمة تتعلق بحركات الوجه ونبرات الصوت، ما يجعل من الصعب التمييز بين المحتوى الحقيقي والمزيف.

---

[1] حمدي أحمد سعد أحمد، الطبيعة القانونية للذكاء الاصطناعي، "التكييف الشرعي والقانوني للمستجدات المعاصرة وأثره في تحقيق الأمن المجتمعي"، عدد خاص بالمؤتمر الدولي ال ا ربع، الجزء الثالث، المؤتمر العلمي الدلي ال ا ربع، المنعقد بكلية الشريعة والقانون بطانطا، المنعقد من ١١ إلى ١٢ أغسطس ٢٠٢١ ، ص، ٢٤٩

[2] محمد خميسي، "الطبيعة القانونية للذكاء الاصطناعي"، الذكاء الاصطناعي والقانون، ، ص، ٦١

[3] عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، طبعة ٢٠٠٥ ، ص، ٨٨

يُستخدم التزييف العميق في العديد من الأنشطة غير القانونية، مثل الاحتيال المالي، الابتزاز، والتلاعب بالرأي العام من خلال نشر مقاطع فيديو مزورة لشخصيات سياسية أو مؤثرة. على سبيل المثال، يمكن للمجرمين إنشاء مقطع فيديو يظهر فيه مسؤول حكومي يعلن عن معلومات كاذبة، ما يؤدي إلى نشر الذعر أو التلاعب بأسواق الأسهم. كما يُستخدم التزييف العميق في سرقة الهويات، إذ يمكن انتحال شخصية أشخاص حقيقيين لتنفيذ عمليات احتيال بنكية أو ابتزاز ضحايا عبر الإنترنت.

٢. الهجمات السيبرانية المتقدمة(AI-Powered Cyber Attacks)

الذكاء الاصطناعي عزز قدرة القراصنة على تنفيذ هجمات سيبرانية معقدة ومتطورة بشكل يفوق الأساليب التقليدية. يتم استخدام تقنيات الذكاء الاصطناعي لتحليل الثغرات الأمنية في الأنظمة الرقمية بشكل آلي، مما يسمح بشن هجمات تستهدف نقاط الضعف في البرمجيات والشبكات بسرعة ودقة فائقة. [٥]

ومن أبرز الهجمات السيبرانية التي تعتمد على الذكاء الاصطناعي، هجمات الحرمان من الخدمة (DDoS)، إذ تقوم برمجيات الذكاء الاصطناعي بإغراق مواقع الويب بعدد هائل من الطلبات، ما يؤدي إلى تعطيل خدماتها بالكامل. كما يمكن للذكاء الاصطناعي تحليل سلوكيات المستخدمين على الشبكة، والتخفي داخل الأنظمة لفترات طويلة دون اكتشافه، مما يجعله أداة خطيرة لتنفيذ هجمات الاختراق والسرقة الرقمية.

٣. الهجمات التلقائية(Automated Phishing Attacks)

التصيد الاحتيالي هو أحد أكثر الأساليب استخدامًا في الجرائم السيبرانية، إذ يعتمد على إرسال رسائل بريد إلكتروني أو رسائل نصية مُضللة تهدف إلى خداع الضحايا للكشف عن معلوماتهم الشخصية، مثل كلمات المرور أو بيانات البطاقات الائتمانية. ومع استخدام الذكاء الاصطناعي، أصبحت هذه الهجمات أكثر تعقيدًا ودقة، حيث يتم تحليل سلوكيات الضحية عبر الإنترنت لإنشاء رسائل مخصصة يصعب تمييزها عن الاتصالات الحقيقي. [٥]

يمكن للذكاء الاصطناعي توليد رسائل تصيد ذكية تحاكي أسلوب الكتابة الخاص بالشركات أو المؤسسات المالية، مما يجعل الضحية تعتقد أنها تتلقى رسالة رسمية تطلب منه تحديث بياناته البنكية أو إعادة تعيين كلمة المرور. كما يمكن تطوير روبوتات دردشة ذكية (Chatbots) قادرة على التواصل مع المستخدمين وخداعهم لكشف معلومات حساسة من دون أن يدركوا أنهم يتحدثون مع نظام آلي. [٥]

٤. تحليل البيانات لاختراق الأنظمة(AI-Driven Data Breaches)

تساعد تقنيات الذكاء الاصطناعي المجرمين في تحليل كميات ضخمة من البيانات بهدف العثور على الثغرات الأمنية واستغلالها لاختراق الأنظمة الحساسة. من خلال خوارزميات التعلم الآلي، يمكن للمهاجمين تحديد أنماط الأمان الشائعة، وتطوير أساليب جديدة لكسر كلمات المرور أو تجاوز أنظمة الحماية التقليدية ، إحدى الطرق التي يُستخدم فيها الذكاء الاصطناعي في اختراق البيانات هي تحليل سجلات الدخول والأنماط السلوكية للمستخدمين، مما يمكنه من اكتشاف الحسابات الأكثر عرضة للاختراق. وعلى سبيل المثال، يمكن للذكاء الاصطناعي جمع بيانات من مواقع التواصل الاجتماعي،

[١] يعيش شوقي تمام، الجريمة المعلوماتية على شبكة الانترنت، رسالة لنيل شهادة الماستر، كلية الحقوق العلوم السياسية، جمعة أبي بكر بلقايد تلمسان، الجزائر، السنة الجامعية ٢٠١١ / ٢٠١٢ ، ص، ٥٠

[٢] د/ قادة شهيد، د/ معمر بن طرية، أضرار الربوتات وتقنيات الذكاء الأصطناعي: تحد جديد لقانون المسئولية المدنية الحالي، الملتقى الدولي "الذكاء الأصطناعي" تحد جديد للقانون، جامعة.الجزائر، كلية الحقوق، ٢٠١٨ ص ٧٥

[٣] د/ سلوي حسين حسن رزق، الأتمتة الذكية والقرارات الإدارية، المؤتمر الدولي السنوي العشرون بعنوان الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات - المنعقد بكلية.الحقوق جامعة المنصورة، في الفترة من ٢٣- ٢٤ مايو ٢٠٢١، ص ٢٢

البريد الإلكتروني، وأنظمة الدفع الإلكترونية، ثم استخدام هذه المعلومات لمحاكاة سلوك المستخدم الحقيقي، مما يسمح له بتجاوز أنظمة التحقق الأمني بسهولة.[1]

٥. اختراق أنظمة التعلم العميق(Adversarial AI Attacks)

الهجمات التي تستهدف أنظمة الذكاء الاصطناعي نفسها تُعرف باسم "الهجمات المضادة " (Adversarial Attacks)، إذ يتم إدخال بيانات مضللة إلى خوارزميات الذكاء الاصطناعي لخداعها وإجبارها على اتخاذ قرارات خاطئة. يعتمد هذا النوع من الهجمات على إدخال تغييرات غير مرئية للعين البشرية في البيانات المدخلة، مما يجعل أنظمة الذكاء الاصطناعي تفسرها بشكل غير صحيح.

على سبيل المثال، يمكن تعديل صورة وجه بشكل طفيف بحيث لا تتمكن أنظمة التعرف على الوجه من التعرف على الشخص الحقيقي، مما يسمح لمجرمي الإنترنت بتجاوز أنظمة الأمان البيومترية. كما يمكن خداع السيارات ذاتية القيادة عن طريق تغيير بعض العلامات المرورية أو تعديل الصور التي يتم تحليلها بواسطة أنظمة الذكاء الاصطناعي،مما قد يؤدي إلى حوادث خطيرة أو تعطيل حركة المرور.[2]

المبحث الثاني

الجريمة السيبرانية وتأثير الذكاء الاصطناعي عليها

الجريمة السيبرانية أصبحت من التحديات الكبرى في العصر الرقمي، حيث تعتمد على استخدام التكنولوجيا لتنفيذ أعمال غير قانونية تستهدف الأفراد، المؤسسات، أو حتى الحكومات. ومع التطور السريع في الذكاء الاصطناعي، أصبح لهذه الجرائم أبعاد جديدة، إذ يُستخدم الذكاء الاصطناعي أداةً لتنفيذ هجمات سيبرانية معقدة أو يكون هو نفسه الهدف للهجوم. إن الفارق بين الجريمة السيبرانية والجرائم التقليدية يكمن في طبيعتها، إذ إن الجرائم التقليدية تتم في بيئة مادية وتتطلب تواجد المجرم في موقع الحدث، بينما الجريمة السيبرانية تُنفذ عن بُعد باستخدام الحواسيب والشبكات، مما يزيد من صعوبة تعقب مرتكبيها.[3]

المطلب الأول: مفهوم الجريمة السيبرانية وتصنيفاتها

إن الجريمة السيبرانية هي أيّ نشاطٍ إجراميّ يتم عبر الفضاء الإلكتروني، سواء أكان ذلك عن طريق اختراق أنظمة الحاسوب، الاحتيال الإلكتروني، أو التلاعب بالبيانات الرقمية.ويختلف هذا النوع من الجرائم عن الجرائم التقليدية من حيث الأدوات المستخدمة والأدلة التي يمكن تتبعها، فبينما تعتمد الجرائم التقليدية على الأدلة المادية والشهود، إذ تعتمد الجرائم السيبرانية على الأدلة الرقمية مثل سجلات الدخول، عناوينIP ، [4] والبصمات الرقمية. ومن حيث التأثير، يمكن أن تكون الجريمة التقليدية محصورة في منطقة جغرافية معينة، بينما تمتد الجريمة السيبرانية عبر الحدود، مما يجعل مكافحتها أكثر تعقيدًا.

تصنيف الجرائم السيبرانية يعتمد على طبيعة الاستخدام أو الهدف من الهجوم. هناك الجرائم التي يُستخدم فيها الذكاء الاصطناعي بوصفه أداةً مساعدةً للمهاجمين، وتشمل التزييف العميق، التصيد الاحتيالي الذكي، والهجمات السيبرانية المؤتمتة،إذ يتم استغلال تقنيات الذكاء الاصطناعي لاختراق

[1] د. سلوان فرنسيس يوسف ، الذكاء الاصطناعي و دوره المستقبلي في العراق ، مقال منشور في جريدة الزمان عام ٢٠٢١ص ٩٨

[2] ايمن محمد السيوطي ، الجوانب القانونية لتطبيق الذكاء الاصطناعي ، دار مصر للنشر والتوزيع ، ط ١ ،القاهرة ، مصر السنة ٢٠٢٠ ،ص٢٣

[3] محمود محمد سويف، جرا رئم الذكاء الاصطناعي –المجرمون الجدد- دار الجامعة الجديدة للنشر – الاسكندرية، مصر، الطبعة الأولى ٢٠٢٢ ،ص، ١١٥

[4] نسيم أحمد محمدي، ثورة الذكاء الجديدة كيف يغير الذكاء الاصطناعي عالم اليوم، الطبعة الأولى ٢٠٢١ ، أدليس بلزمة للنشر والترجمة، باتنة، الجزا زئر، ص، ٢٤

الأنظمة وتنفيذ هجمات دقيقة يصعب اكتشافها. ومن ناحية أخرى، هناك الجرائم التي تستهدف أنظمة الذكاء الاصطناعي نفسها، حيث يحاول المهاجمون التلاعب بالخوارزميات أو إدخال بيانات مضللة لتغيير سلوك النظام، ما قد يؤدي إلى عواقب خطيرة في مجالات مثل الأمن، التمويل، والرعاية الصحية. [٥]

الجرائم التي يُستخدم فيها الذكاء الاصطناعي أصبحت أكثر انتشارًا بسبب قدرة الذكاء الاصطناعي على التعلم والتحليل بسرعة تفوق البشر، مما يجعل الهجمات أكثر تعقيدًا وفعالية. وعلى سبيل المثال، يمكن استخدام الذكاء الاصطناعي لإنشاء مقاطع فيديو مزيفة لأغراض الابتزاز أو التلاعب بالرأي العام، أو تطوير برمجيات خبيثة قادرة على اختراق أنظمة الحماية بشكل تلقائي دون الحاجة إلى تدخل بشري مباشر. كما يمكن للمجرمين استغلال الذكاء الاصطناعي في هجمات التصيد الاحتيالي، إذ يتم تحليل سلوك الضحايا وإنشاء رسائل احتيالية مخصصة يصعب تمييزها عن الاتصالات الحقيقية.

أما الجرائم التي تستهدف أنظمة الذكاء الاصطناعي، فهي تعتمد على استغلال نقاط الضعف في هذه الأنظمة لتحقيق أهداف غير قانونية. ومن أبرز هذه الهجمات، الهجمات التي تستهدف أنظمة التعلم العميق، إذ يتم إدخال بيانات مشوهة أثناء عملية التدريب ما يؤدي إلى نتائج خاطئة أو منحرفة. كما يمكن اختراق أنظمة التعرف على الوجوه بحيث تصبح غير قادرةٍ على التعرف على الأشخاص الحقيقيين، مما يسمح بتجاوز إجراءات الأمان. الهجمات التي تستهدف المساعدات الرقمية مثل Siri و Google Assistantتهدف إلى استخراج معلومات حساسة أو تنفيذ أوامر من دون علم المستخدم، مما يشكل تهديدًا خطيرًا للخصوصية والأمن الشخصي. [٦]

ومع تزايد تطور الذكاء الاصطناعي، تصبح الحاجة إلى تطوير تقنيات أمنية مضادة أكثر إلحاحًا، إذ إن الأساليب التقليدية لم تعد كافية لحماية البيانات والأنظمة من الهجمات السيبرانية المتطورة. إن الجريمة السيبرانية في ظل الذكاء الاصطناعي لم تعد مجرد تهديدٍ تقنيّ، بل أصبحت قضيةً أمنيةً وقانونيةً، تتطلب استراتيجيات شاملة لمواجهتها، سواء من خلال تطوير تقنيات دفاعية تعتمد على الذكاء الاصطناعي نفسه، أو من خلال تعزيز الأطر القانونية التي تحكم استخدام هذه التكنولوجيا في الفضاء الرقمي.

المطلب الثاني: التحديات القانونية لإثبات الجريمة السيبرانية المدعومة بالذكاء الاصطناعي

إثبات الجرائم السيبرانية المدعومة بالذكاء الاصطناعي يعد من أكبر التحديات القانونية التي تواجه أنظمة العدالة الجنائية في العصر الرقمي. فمع التطور السريع في تقنيات الذكاء الاصطناعي، أصبحت الجرائم السيبرانية أكثر تعقيدًا وصعوبةً في التتبع، مما يضعف قدرة الجهات المختصة على جمع الأدلة وإثبات الجريمة أمام المحاكم. فالجريمة التقليدية تعتمد على أدلة مادية واضحة مثل بصمات الأصابع أو تسجيلات المراقبة، بينما تعتمد الجرائم السيبرانية على الأدلة الرقمية، التي يمكن التلاعب بها أو إخفاؤها بسهولة، ما يزيد من صعوبة إثباتها قانونيًا. [٧]

إن صعوبة الإثبات في الجرائم السيبرانية تكمن في طبيعتها غير الملموسة، إذ إن هذه الجرائم تحدث عبر الشبكات والأنظمة الرقمية من دون الحاجة إلى وجود مادي للمجرم في مسرح الجريمة. وهذا يجعل عملية تتبع المجرمين وجمع الأدلة أكثر تعقيدًا، ولاسيّما مع استخدام تقنيات متقدمة مثل الشبكات المجهولة (Tor) وبرامج إخفاء الهوية(VPN) ، التي تجعل من الصعب تحديد موقع الفاعل

[١] مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت، ص، ٧٠

[٢] سهام القشتول، هشام أزكاغ، "حدود حماية الحياة الخاصة في ظل الذكاء الاصناعي"، الذكاء الاصطناعي والقانون، مرجع سابق، ص، ١٩

[٣] محمدي نسيم أحمد، ثورة الذكاء الجديدة كيف يغير الذكاء الاصطناعي عالم اليوم، الطبعة الأولى ٢٠٢١ ، أدليس بلزمة للنشر والترجمة، باتنة، الجزائر. ص ٨٥

الحقيقي. كما أن الجرائم السيبرانية قد يتم تنفيذها من خلال أنظمة ذكاء اصطناعي تعمل بشكل مستقل، مما يثير تساؤلات قانونية حول مسؤولية الجاني، فهل يُحاسب من قام بتصميم الخوارزمية أم من استخدمها؟ أم أن النظام نفسه قد يتحمل جزءًا من المسؤولية؟

الأدلة الرقمية وإشكالية قبولها قانونيًا تشكل تحديًا آخر أمام القضاء، إذ إن معظم الأنظمة القانونية لا تزال غير مهيَّأة بالكامل للتعامل مع الأدلة الرقمية بمستوى الأدلة التقليدية نفسها. فالأدلة الرقمية مثل سجلات الدخول، عناوينIP ، وسجلات المعاملات المشفرة يمكن أن تكون عرضةً للتعديل أو التلاعب، ما يجعل موثوقيتها محل جدل قانوني. في بعض الدول، لا يتم الاعتراف بالأدلة الرقمية ما لم يتم التأكد من صحتها من خلال إجراءات قانونية صارمة، مثل التحقق من سلامة البيانات وسلسلة الحفظ (Chain of Custody) التي تضمن عدم التلاعب بالمعلومات أثناء جمعها وتحليلها. [٥]

مقارنة بين قواعد الإثبات في العراق، الولايات المتحدة، والاتحاد الأوروبي تكشف عن اختلافات جوهرية في التعامل مع الجرائم السيبرانية والأدلة الرقمية. وفي العراق، لا تزال القوانين المتعلقة بالأدلة الرقمية غير متطورة بشكلٍ كافٍ، إذ يعتمد القضاء في كثير من الحالات على القوانين العامة مثل قانون العقوبات العراقي، الذي لا يتضمن نصوصًا صريحةً تغطي جميع أنواع الجرائم السيبرانية الحديثة. وهذا يؤدي إلى مشكلات في قبول الأدلة الرقمية، ولاسيّما عندما يتعلق الأمر بجرائم تعتمد على الذكاء الاصطناعي،إذ يصعب تحديد المسؤوليات القانونية بشكل دقيق.

وفي الولايات المتحدة، يتم التعامل مع الجرائم السيبرانية وفقًا لقوانين متخصصة مثل **قانون الاحتيال وإساءة استخدام الحاسوب(CFAA)** ، الذي يجرّم الاستخدام غير المشروع للأنظمة الرقمية ويحدد عقوبات صارمة على المخالفين. كما تعتمد المحاكم على **قانون الأدلة الفيدرالي (Federal Rules of Evidence)**، الذي يضع معايير واضحة لقبول الأدلة الرقمية، مثل التأكد من صحتها ومصداقيتها من خلال شهادات الخبراء الرقميين وتحليل البيانات الجنائية.

أما في الاتحاد الأوروبي، فتعتبر التشريعات أكثر تقدمًا فيما يتعلق بالأدلة الرقمية، إذ يتم تنظيم جمع الأدلة الرقمية بموجب **اللائحة العامة لحماية البيانات(GDPR)** ، التي تحدد إطارًا قانونيًا صارمًا يوازن بين حق الأفراد في حماية بياناتهم وحق السلطات في استخدام الأدلة الرقمية لمكافحة الجرائم السيبرانية. كما أن الاتحاد الأوروبي يتبنى نهجًا صارمًا في تتبع الجرائم السيبرانية عبر التعاون بين الدول الأعضاء، مما يسهل عملية التحقيق في الجرائم التي تمتد عبر الحدود. [٥]

إن التحديات القانونية لإثبات الجرائم السيبرانية المدعومة بالذكاء الاصطناعي تعكس الحاجة الملحة لتطوير القوانين والأنظمة القضائية لمواكبة التطورات التكنولوجية. ومع استمرار تطور الذكاء الاصطناعي واستخدامه في تنفيذ الجرائم، يصبح من الضروري وضع تشريعات حديثة تعتمد على تقنيات متطورة في التحليل الجنائي الرقمي، وتعزز من قدرة الجهات القانونية على التعامل مع الأدلة الرقمية بطريقة تضمن العدالة والشفافية[٣].

[١] د/ نبراس محمد جاسم الأحبابي، أثر الإدارة الإلكترونية في إدارة المرافق العامة.دار الجامعة الجديدة للنشر،(دراسة مقارنة) ، ٢٠١٨، ص ٩٩

[٢] ممدوح خليل بحر ،حماية الحياة الخاصة في القانون الجنائي المقارن ، أطروحة دكتوراه ، جامعة القاهرة ، مكتبة دار الثقافة للنشر والتوزيع ، الأردن ، ١٩٩٦ .ص ٢٣١

[٣] ممدوح خليل بحر ،مصدر سابق ص ٢٣١

المطلب الثالث: دراسة تطبيقية على الوضع في العراق والمقارنة الدولية

وفي ما يتعلق في موضوع الدراسة التطبيقية على جمع البيانات وتحليلها هناك عدة أدوات ومنها،

تحليل البيانات الإحصائية الرسمية من تقارير وزارة الداخلية العراقية، ومديرية مكافحة الجريمة الإلكترونية، وتحليل القضايا الفعلية وذلك من خلال دراسة حالات موثقة لجرائم سيبرانية وقعت في العراق وتأثيرها على الضحايا والمؤسسات.

واما الاحصائيات والتوجيهات في الجرائم السيبرانية فهي تهدف الى فهم تطور الجريمة السيبرانية في العراق، إذ يتم تحليل الإحصائيات الحديثة المتوفرة من المصادر الحكومية والدولية فقد كان معدل الجرائم السيبرانية خلال السنوات الأخيرة توضح تصاعد في الجرائم السيبرانية في العراق بشكل ملحوظ.

وسوف يتم عرض جدول توضيحي لمعدل الجرائم وانتشارها في السنوات الأخيرة في العراق ، فقد تم اعداد جدول يوضح معدلات الجرائم بين عام (٢٠٢٠ - ٢٠٢٤) وكما يأتي:

الجدول ١: تطور معدلات الجرائم السيبرانية في العراق(2020 - 2024)

السنة	عدد الجرائم السيبرانية المسجلة	نسبة الزيادة مقارنة بالعام السابق
2020	1,250	-
2021	1,850	48%
2022	2,600	40%
2023	3,900	50%
2024	5,300	36%

اما اكثر الجرائم انتشاراً في السنوات الأخيرة في العراق والتي تم تسجيلها وتصنيفها بحسب نوعها وتحديد ابرز التهديدات الأمنية[1]:

الجدول ٢: أنواع الجرائم السيبرانية في العراق ونسب انتشارها(2024)

نوع الجريمة	نسبة الانتشار
الاحتيال الإلكتروني	35%
الابتزاز الإلكتروني	25%
الاختراق وسرقة البيانات	20%
التزييف العميق (Deepfake)	10%
التصيد الاحتيالي (Phishing)	10%

اما بالنسبة للجهات المسؤولة عن مكافحة الجرائم السيبرانية في العراق فهي تشمل كلًّا من مديرية مكافحة الجرائم الإلكترونية التابعة لوزارة الداخلية و الشرطة المجتمعية التي تتعامل مع الابتزاز الإلكتروني والتشهير الرقمي وهيئة الإعلام والاتصالات المسؤولة عن مراقبة المحتوى الإلكتروني. فأن هذه الجهات مسؤولة مسؤولية مباشرة عن مكافحة الجرائم السيبرانية في العراق،

[1] قاسم عبدالرضا شغيث ، الامن السيبراني اوكسجين التحول الرقمي العراقي ،مجلة فرسان الرد السريع للدراسات الأمنية ، مجلة علمية ، وزارة الداخلية ، العدد ٢ المجلد ١ لسنة ٢٠٢٤

فهي لها نظام عمل معين تتم بموجبه تعقب وتحليل نوعية الجرائم السيبرانية وذلك بغية محاسبة مرتكبيها واحالتهم للمحاكم المختصة.

ولبيان كيفية تعامل الدول الأخرى مع هذه الجرائم فقد تم عمل تحليل للقوانين في العراق وبين التشريعات في الولايات المتحدة الامريكية وبين الاتحاد الأوربي[1].

الجدول ٣: مقارنة التشريعات الخاصة بمكافحة الجرائم السيبرانية

الدولة	وجود قانون مخصص للجرائم السيبرانية	الاعتراف بالأدلة الرقمية	العقوبات على الجرائم السيبرانية
العراق	قيد التطوير	محدود	غرامات وعقوبات ضعيفة
الولايات المتحدة	موجود (CFAA)	معترف بها قانونيًا	سجن يصل إلى ٢٠ عامًا
الاتحاد الأوروبي	موجود (NIS (Directive	منظم بقوانين حماية البيانات	غرامات تصل إلى ٢٠ مليون يورو

ولبيان مستوى جاهزية الدول لمواجهة الجرائم السيبرانية تم عمل مقارنة بين العراق وبعض الدول في الجاهزية للأمن السيبراني فقد تم استخدام المؤشر العالمي للأمن السيبراني (GCI) لقياس مدى استعداد الدول للتصدي للجرائم الإلكترونية[2].

الجدول ٤: مقارنة بين العراق وبعض الدول في الجاهزية للأمن السيبراني

الدولة	ترتيبها في مؤشر الأمن السيبراني (GCI)	تقييم الجاهزية (من ١٠٠)
الولايات المتحدة	1	95
المملكة المتحدة	2	93
الإمارات	5	85
السعودية	7	83
العراق	95	42

[1] الدكتور حازم حمد موسى ، قراءة تحليلية لاستراتيجية الامن السيبراني العراقي ،مجلة فرسان الرد السريع للدراسات الأمنية ، مجلة علمية ، وزارة الداخلية ، العدد ٢ المجلد ١ لسنة ٢٠٢٤

[2] قوانين الجرائم السيبرانية في المنطقة العربية: حماية للفضاء الرقمي أم قمع للحريات؟، ورقة سياسات قوانين الجرائم السيبرانية في المنطقة العربية ، منشور على الموقع التالي : https://www.accessnow.org/

الخاتمة

مع التطور المتسارع في تقنيات الذكاء الاصطناعي، أصبحت الجرائم السيبرانية أكثر تعقيدًا وخطورة، إذ بات من الممكن تنفيذ عمليات إجرامية رقمية تعتمد على تقنيات متقدمة يصعب تتبعها أو إثباتها بوسائل تقليدية. وقد تم التوصل في هذا البحث أن الأنظمة القانونية، ولاسيّما في العراق، تعاني من فجوةٍ تشريعيةٍ كبيرةٍ، تجعل من الصعب التعامل مع هذه النوعية من الجرائم بفعالية كبيرة،إذ تصاعدت الجرائم السيبرانية المسجلة في العراق بنسبة ٣٦% خلال عام ٢٠٢٤ مقارنة بالعام السابق، وان الابتزاز الإلكتروني يمثل 25% من الجرائم السيبرانية المسجلة، مما يجعله التهديد الرقمي الأكثر شيوعًا.

وبيّنت الدراسة ان الولايات المتحدة والاتحاد الأوروبي تمتلكان أطرًا قانونية متقدمة تشمل قوانين صارمة ضد الجرائم السيبرانية، بينما يفتقر العراق إلى منظومة متكاملة. إذ شددت التشريعات الأوروبية والأمريكية على الاعتراف بالأدلة الرقمية، في حين أن العراق لا يزال في مرحلة تطوير آليات قانونية لهذا النوع من الأدلة. حتى أن الدول الخليجية، مثل الإمارات والسعودية، استثمرت بشكل ملحوظ في الأمن السيبراني، ما جعلها ضمن الدول الأكثر جاهزية لمواجهة التهديدات الرقمية.

أولًا: الاستنتاجات

١. الذكاء الاصطناعي أسهم بشكل كبير في تنامي أنماط جديدة من الجرائم السيبرانية، مثل التزييف العميق والاحتيال الذكي.

٢. الأنظمة القانونية التقليدية غير مهيَّأة للتعامل مع طبيعة الجرائم الرقمية المعقدة،ولاسيّما من حيث الإثبات والعقوبة.

٣. هناك ضعف واضح في الاعتراف القانوني بالأدلة الرقمية داخل النظام القضائي العراقي، مما يُضعف من فرص تحقيق العدالة.

٤. العراق يفتقر إلى تشريعات متخصصة لمكافحة الجرائم السيبرانية، ما يفتح المجال أمام الجناة لاستغلال الثغرات القانونية.

٥. المقارنة مع التشريعات الأمريكية والأوروبية أظهرت مدى تقدم هذه الأنظمة في مجال مكافحة الجريمة الإلكترونية والاعتراف بالأدلة الرقمية.

٦. ضعف البنية التحتية للأمن السيبراني في العراق يشكل تحديًا حقيقيًا أمام مواجهة هذا النوع من الجرائم.

٧. العراق لا يمتلك حتى الآن اتفاقيات دولية شاملة لتبادل المعلومات حول الجرائم السيبرانية، ما يصعب تتبع الجرائم العابرة للحدود.

ثانيًا: التوصيات

١. سنّ قانونٍ خاصٍ بمكافحة الجرائم السيبرانية في العراق يتضمن تنظيمًا دقيقًا للجرائم المرتبطة بالذكاء الاصطناعي.

٢. إدخال تعديلات على قانون الإثبات العراقي لإعطاء الأدلة الرقمية حجيتها القانونية الكاملة.

٣. إنشاء وحدات متخصصة في التحقيق الجنائي الرقمي من ضمن وزارة الداخلية والسلطة القضائية.

٤. تعزيز التعاون الدولي عبر الانضمام إلى الاتفاقيات الدولية ذات الصلة، مثل اتفاقية بودابست.

٥. تطوير البنية التحتية الرقمية في العراق، وتخصيص ميزانيات واضحة للأمن السيبراني.

٦. تنظيم دورات تدريبية للقضاة وضباط الشرطة حول آليات التعامل مع الأدلة الرقمية والجرائم التقنية.

٧. إطلاق حملات توعية مجتمعية حول الجرائم السيبرانية وأساليب الوقاية منها، ولاسيّما تلك المرتبطة بالذكاء الاصطناعي.

المصادر :

١. ايمن محمد السيوطي ، الجوانب القانونية لتطبيق الذكاء الاصطناعي ، دار مصر للنشر والتوزيع ، ط ١ ،القاهرة ، مصر السنة , 2020ص٢٣
٢. تلمسان، الجزائر، السنة الجامعية ٢٠١١ / ٢٠١٢ ، ص، ٥٠
٣. حمدي أحمد سعد أحمد، الطبيعة القانونية للذكاء الاصطناعي، "التكييف الشرعي والقانوني للمستجدات المعاصرة وأثره في تحقيق الأمن المجتمعي"، عدد خاص بالمؤتمر الدولي ال ا ربع، الجزء الثالث، المؤتمر العلمي الدلي ال ا ربع، المنعقد بكلية الشريعة والقانون بطانطا، المنعقد من ١١ إلى ١٢ أغسطس ٢٠٢١ ، ص، ٢٤٩
٤. د. سلوان فرنسيس يوسف ، الذكاء الاصطناعي و دوره المستقبلي في العراق ، مقال منشور في جريدة الزمان عام ٢٠٢١ص ٩٨
٥. د/ سلوي حسين حسن رزق، الأتمتة الذكية والقرارات الإدارية، المؤتمر الدولي السنوي العشرون بعنوان الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات - المنعقد بكلية الحقوق جامعة المنصورة، في الفترة من ٢٣- ٢٤ مايو ٢٠٢١، ص ٢٢
٦. د/ قادة شهيد، د/ معمر بن طرية، أضرار الروبوتات وتقنيات الذكاء الأصطناعى: تحد جديد لقانون المسئولية المدنية الحالي، الملتقى الدولي "الذكاء الأصطناعي" تحد جديد للقانون، جامعة الجزائر، كلية الحقوق، ٢٠١٨ ص ٧٥
٧. د/ نبراس محمد جاسم الأحبابي، أثر الإدارة الإلكترونية في إدارة المرافق العامة.دار الجامعة الجديدة للنشر،(دراسة مقارنة) ٢٠١٨.
٨. الدكتور حازم حمد موسى ، قراءة تحليلية لاستراتيجية الامن السيبراني العراقي ،مجلة فرسان الرد السريع للدراسات الأمنية ، مجلة علمية ، وزارة الداخلية ، العدد ٢ المجلد ١ لسنة ٢٠٢٤.
٩. سهام القشتول، هشام أزكاغ، "حدود حماية الحياة الخاصة في ظل الذكاء الاصناعي"، الذكاء الاصطناعي والقانون.
١٠. عادل عبد النور بن عبد النور، مدخل إلى عالم الذكاء الاصطناعي، طبعة ٢٠٠٥ ، ص، ٨٨
١١. عفيفي كامل عفيفي. "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ونور الشرطة والقانون، درلسة مقار.٢٠٠٣ ،منشورات الحلبي الحقوقية، بيروت، لبنان
١٢. فتح الله تازوي، "رهان الخصوصية في فضاء الذكاء الاصطناعي"، الذكاء الاصطناعي والقانون، مرجع سابق، ص، ٨٤
١٣. فوزي غروس ، الذكاء الاصطناعي والقانون، المجلة المغربية لتاريخ القانون، عدد خاص 3- 2023 - ، ص، ٥
١٤. قاسم عبدالرضا شغيث ، الامن السيبراني اوكسجين التحول الرقمي العراقي ،مجلة فرسان الرد السريع للدراسات الأمنية ، مجلة علمية ، وزارة الداخلية ، العدد ٢ المجلد ١ لسنة ٢٠٢٤
١٥. محمد خميسي، "الطبيعة القانونية للذكاء الاصطناعي"، الذكاء الاصطناعي والقانون، ، ص، ٦١
١٦. محمدي نسيم أحمد، ثورة الذكاء الجديدة كيف يغير الذكاء الاصطناعي عالم اليوم، الطبعة الأولى ٢٠٢١ ، أدليس بلزمة للنشر والترجمة، باتنة، الجزائر.
١٧. محمود محمد سويف، جرا رئم الذكاء الاصطناعي –المجرمون الجدد- دار الجامعة الجديدة للنشر – الاسكندرية، مصر، الطبعة الأولى ٢٠٢٢.

١٨.مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت.
١٩.ممدوح خليل بحر ،حماية الحياة الخاصة في القانون الجنائي المقارن ، أطروحة دكتوراه ، جامعة القاهرة ، مكتبة دار الثقافة للنشر والتوزيع ، الأردن ، ١٩٩٦.
٢٠.نسيم أحمد محمدي، ثورة الذكاء الجديدة كيف يغير الذكاء الاصطناعي عالم اليوم، الطبعة الأولى ٢٠٢١ ، أدليس بلزمة للنشر والترجمة، باتنة، الجزائر.
٢١.يعيش شوقي تمام، الجريمة المعلوماتية على شبكة الانترنت، رسالة لنيل شهادة الماستر، كلية الحقوق العلوم السياسية، جمعة أبي بكر بلقايد.