التحديات القانونية أمام إثبات الضرر السيبراني
في ظل تطور تقنيات الذكاء الاصطناعي

د. محمد عبد المنعم الزهيري

دكتوراه القانون المدني – كلية الحقوق – جامعه المنصورة

(ISSN: 2537- 0758)

التحديات القانونية أمام إثبات الضرر السيبراني في ظل تطور تقنيات الذكاء الاصطناعي

د. محمد عبد المنعم الزهيري

ملخص البحث باللغة العربية:

يُعتبر إثبات الضرر من الدعائم الأساسية للمسؤولية القانونية في فرعي القانون المدني والجنائي، حيث لا يُتصور قيام المسؤولية بدون تحقق ضرر فعلي يمكن نسبه إلى فاعل محدد. غير أن التطور السريع في تقنيات المعلومات والاتصالات، لاسيما في مجال الذكاء الاصطناعي، قد أوجد تحديات جديدة أمام الفقه والقضاء، أبرزها تعقيد عملية إثبات الضرر الناجم عن الأنشطة السيبرانية ففي البيئة الرقمية المعاصرة، صار من الصعوبة بمكان تحديد الجهة المسؤولة عن الأضرار الناتجة عن استخدام أو سوء استعمال الأنظمة الذكية، خاصة في الحالات التي تتسم بالتعقيد التقني واللامركزية في التنفيذ. ويتفاقم هذا الإشكال مع قدرة الأنظمة المعتمدة على الذكاء الاصطناعي على التعلم الذاتي واتخاذ قرارات مستقلة دون تدخل بشري مباشر، وهو ما يضعف الركن المعنوي التقليدي في المسؤولية، ويثير تساؤلات حول مدى انطباق مفاهيم الخطأ أو الإهمال على هذه الأنظمة.

يتناول هذا البحث مجموعة من الإشكالات القانونية المتعلقة بإبراز الضرر السيبراني، ومنها صعوبة تتبع مصدر الضرر وتحديد العلاقة السببية بين الفعل الضار والنتيجة، وكذلك غياب الوضوح بشأن من تقع عليه المسؤولية، أهو المبرمج، المشغّل، مالك النظام، أم النظام ذاته؟ كما يلاحظ البحث أوجه النقص في التشريعات التقليدية التي لم تصمم للتعامل مع خصائص الضرر الرقمي، خاصة في الحالات التي يكون فيها الضرر غير مادي، كاختراق الخصوصية أو تسريب البيانات أو الاعتداء على السمعة الرقمية ومن الإشكاليات البارزة أيضًا ما يتعلق بالاختصاص القضائي، نظرًا للطبيعة العابرة للحدود للجرائم السيبرانية، مما يجعل تحديد المحكمة المختصة والقانون الواجب التطبيق مسألة معقدة تتطلب تنسيقًا دوليًا وتشريعات متقدمة تراعي هذه الخصوصية.

الكلمات المفتاحية: الضرر السيبراني، الذكاء الاصطناعي، الإثبات الإلكتروني، تحديات الإثبات، البيئة الرقمية

Abstract in English:

The proof of harm is considered one of the fundamental pillars of legal liability in both civil and criminal law, as liability cannot be established without actual harm that can be attributed to a specific actor. However, the rapid development of information and communication technologies, particularly in the field of artificial intelligence, has introduced new challenges for scholars and the judiciary. One of the most prominent of these challenges is the complexity of proving harm resulting from cyber activities. In the contemporary digital environment, it has become increasingly difficult to identify the party responsible for damages caused by the use or misuse of smart systems, especially in cases characterized by technical complexity and decentralized execution. This issue is further exacerbated by the ability of AI-based systems to self-learn and make independent decisions without direct human intervention, which weakens the traditional mental element of liability and raises questions about the applicability of the concepts of fault or negligence to these systems.

This research addresses a range of legal issues related to demonstrating cyber harm, including the difficulty of tracing the source of harm and determining the causal relationship between the harmful act and its result, as well as the lack of clarity regarding who is responsible—whether it is the programmer, the operator, the system owner, or the system itself. The research also highlights the deficiencies in traditional legislation, which were not designed to address the characteristics of digital harm, particularly in cases where the harm is intangible, such as privacy violations, data breaches, or attacks on digital reputation. Another significant issue concerns jurisdiction, given the cross-border nature of cybercrimes, which makes determining the competent court and applicable law a complex matter that requires international coordination and advanced legislation that takes these unique circumstances into account.

Keywords : Cyber damage, artificial intelligence, cyber change, real-world challenges, digital environment.

(ISSN: 2537- 0758)

المقدمة:

مع تزايد الاعتماد على تقنيات الذكاء الاصطناعي في مختلف المجالات، برزت إشكاليات قانونية عميقة تتعلق بكيفية التعامل مع الأضرار التي تنشأ في الفضاء السيبراني نتيجة تدخل هذه التقنيات أو استعمالها. إذ أصبحت الأنظمة الذكية لا تقتصر على تنفيذ التعليمات البشرية، بل تطوّرت إلى حد اتخاذ قرارات مستقلة، وهو ما أفرز إشكاليات قانونية جوهرية على مستوى المسؤولية، خاصة فيما يتعلق بإثبات الضرر وتحديد العلاقة السببية بين التصرف الآلي والنتيجة الضارة. وفي إطار القانون، يُعد إثبات الضرر عنصراً جوهرياً لا غنى عنه لترتيب المسؤولية المدنية، سواء في صورة الخطأ التقني، أو العيب البرمجي، أو الإخفاق في حماية البيانات. غير أن الأضرار السيبرانية الناتجة عن الذكاء الاصطناعي تتسم بتعقيد بالغ، ليس فقط لطبيعتها التقنية الخفية، وإنما أيضاً لتعدد أطرافها وتشعب مراحل تطويرها وتشغيلها. وهذا ما يجعل من مهمة الإثبات تحدياً حقيقياً، يتطلب أدوات قانونية وتقنية تتجاوز القوالب التقليدية المألوفة.

كما أن إثبات الضرر السيبراني يصطدم بجملة من الإشكاليات، من أبرزها: صعوبة تتبع الأثر الرقمي، غياب السجلات الكافية أو الشفافة للعمليات التي تؤدي إلى الضرر، واحتمالية تدخل خوارزميات غير قابلة للفهم الكامل حتى من قِبل مطوريها أنفسهم. ويزداد الأمر تعقيداً في ظل غياب تشريعات واضحة ومتكاملة تنظم آليات المسؤولية عن تصرفات أنظمة الذكاء الاصطناعي، وتحدد الجهة التي ينبغي أن تتحمل عِبء الإثبات. ومن ثم، فإن تناول التحديات القانونية المرتبطة بإثبات الضرر السيبراني في ظل تطور الذكاء الاصطناعي لا يُعد فقط مسألة فنية أو إجرائية، بل هو ضرورة تشريعية تستوجب إعادة صياغة المفاهيم القانونية التقليدية لتتلاءم مع واقع قانوني جديد، تتداخل فيه التكنولوجيا بالقانون، ويتطلب حلولاً مبتكرة لضمان العدالة وحماية الحقوق في عصر رقمي متسارع.

أولًا- اشكالية الدراسة:

تدور إشكالية الدراسة حول توضيح تساؤل رئيسي تتشكل عليه الدراسة، ألا وهو: ما هي التحديات القانونية التي تواجه إثبات الضرر السيبراني في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي، وكيف يمكن مواجهتها تشريعياً وقضائياً؟

وفيما يلي لأبرز التساؤلات الفرعية:

١. ما المراد بالضرر الإلكتروني، وما سماته التي تميزه عن الأضرار الاعتيادية؟
٢. كيف أثرّ تقدم تقنيات الذكاء الاصطناعي على طبيعة الهجمات السيبرانية وصعوبة إثباتها؟
٣. إلى أي حدّ كفاية القرائن الرقمية المستخدمة حالياً في إثبات الضرر الإلكتروني أمام المحكمة؟
٤. كيف يتم تحديد المسؤولية القانونية في حال كان الفعل الضار صادراً عن نظام ذكاء اصطناعي؟
٥. ما هي أبرز الثغرات التشريعية في التشريعات الراهنة بخصوص الأضرار الإلكترونية؟
٦. ما هي الاقتراحات التشريعية الممكنة لتقوية آليات الإثبات في هذا الميدان؟

ثانياً- أهمية الدراسة:

تكمن أهمية هذه البحث في دعم تطوير إطار قانوني ناجع لمواكبة تطور تقنيات الذكاء الاصطناعي، عبر معالجة صعوبات إثبات الأذى السيبراني، مما يساهم في حماية الحقوق الرقمية، تعزيز الإنصاف، دعم الأمن السيبراني، وتحفيز تحديث التشريعات الوطنية والدولية.

ثالثاً- أهداف الدراسة:

١. تحليل التحديات القانونية المتعلقة بإثبات الأذى السيبراني في ظل استخدام تقنيات الذكاء الاصطناعي.
٢. تحديد أوجه النقص في التشريعات الحالية بشأن الأضرار الناتجة عن الأنظمة الذكية.
٣. اقتراح حلول قانونية ناجعة لمعالجة صعوبات الإثبات وتحقيق العدالة الرقمية.
٤. تسليط الضوء على مسؤولية الجهات المعنية في حال وقوع ضرر سيبراني ناتج عن الذكاء الاصطناعي.
٥. دعم تطوير تشريعات وطنية ودولية تواكب التطورات التقنية وتحفظ الحقوق الرقمية.
٦. تعزيز التعاون بين الخبراء القانونيين والتقنيين لضمان استجابة شاملة للتحديات السيبرانية.

(ISSN: 2537- 0758)

رابعاً- منهجية الدراسة:

اعتمد الباحث على الأسلوب الوصفي التحليلي لبحث المعوقات القانونية المتصلة بإثبات الأضرار السيبرانية الناجمة عن تقنيات الذكاء الاصطناعي. يتجلى الأسلوب الوصفي في رصد الظواهر القانونية الراهنة، وتحليل تشريعات الأمن السيبراني وأطر المسؤولية القانونية المتعلقة بالضرر السيبراني. بينما الأسلوب التحليلي يستهدف تحليل وتفسير الجوانب القانونية لهذه الأضرار عبر فحص النصوص القانونية والقضائية ذات الصلة، وتقييم مدى فعاليتها في التعامل مع التطورات التكنولوجية المستحدثة. من خلال هذا النهج، تهدف الدراسة إلى تقديم حلول قانونية فعاله واقتراحات للتطوير التشريعي بغية تعزيز القدرة على إثبات الأضرار وحماية الحقوق الرقمية في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي.

خامساً- خطة الدراسة:

يتناول البحث ثلاثة فصول رئيسيه كما يلي:

الفصل الأول: الإطار المفاهيمي للضرر السيبراني والذكاء الاصطناعي؟

المبحث الأول: مفهوم الضرر السيبراني وانواعه

المبحث الثاني: تطور تقنيات الذكاء الاصطناعي ودورها في الفضاء السيبراني

الفصل الثاني: التحديات القانونية في إثبات الضرر السيبراني الناتج عن الذكاء الاصطناعي؟

المبحث الأول: صعوبة تحديد المسؤولية في الجرائم السيبرانية المدعومة بالذكاء الاصطناعي

المبحث الثاني: إشكالية الإثبات في ظل طبيعة الهجمات السيبرانية

الفصل الثالث: سبل تطوير الإطار القانوني لمعالجة الضرر السيبراني الناتج عن الذكاء الاصطناعي؟

المبحث الأول: تعزيز البنية القانونية والتشريعية

المبحث الثاني: تفعيل أدوات الإثبات الإلكتروني والرقمي

المبحث الثالث: التعاون الدولي وتوحيد الجهود القانونية

الفصل الأول
الإطار المفاهيمي للضرر السيبراني والذكاء الاصطناعي

تمهيد وتقسيم:

يشهد العالم تبدلاً رقمياً متسارعاً أوجد مفاهيم حديثة مثل الأذى السيبراني والذكاء الاصطناعي، والتي أصبحت تُشكّل صعوبات قانونية وأمنية متزايدة. فرغم منافع الذكاء الاصطناعي، قد ينتج عنه أضرار خطيرة عند سوء استعماله، بينما يمثل الأذى السيبراني تهديداً رقمياً غير تقليدي يضر الأفراد والمنظمات وهذا ما سوف يتم عرضه خلال البحث.

المبحث الأول
مفهوم الضرر السيبراني وانواعه؟

تمهيد:

. **مفهوم الضرر**: من الناحية اللغوية، هو "الأذى أو الشر" الذي يلحق بالإنسان أو ممتلكاته أو مصالحه. اما في "لسان العرب" يعني ضدّ النفع، وهو ما يصيب الإنسان من سوء في جسده أو ماله أو سمعته أو غير ذلك.

. **مفهوم كلمه** السيبراني: هو مصطلح حديث مشتق من لفظة Cyber الإنجليزية، ويُستعمل لوصف كل ما يخص العالم الإلكتروني، أي المحيط الرقمي الذي يشتمل على الإنترنت، الشبكات، الأجهزة الذكية، والمنظومات المعلوماتية.

. **الأصل اللغوي** والاصطلاحي: الكلمة Cyber مأخوذة من "Cybernetics"، وهي كلمة تعود إلى اللغة اليونانية (cabernets_κυβερνήτης) وتعني: "الحاكم" أو "الموجه"، وقد استُخدمت لوصف علم التحكم في الأنظمة المعقدة. ثم تطورت لتُستعمل في العصر الرقمي للإشارة إلى كل ما هو إلكتروني أو رقمي ومتصل بالحوسبة والاتصالات.

المعنى الحديث لكلمة "**سيبراني**": يعني كل ما يتعلق باستعمال أو حماية أو إدارة الأنظمة الإلكترونية، المعلومات الرقمية، الشبكات، والبيانات ويُستخدم المصطلح في مجالات متعددة مثل: الأمن السيبراني (Cybersecurity): حماية الأنظمة الرقمية من الاختراقات والمخاطر.

(ISSN: 2537- 0758)

الحرب السيبرانية (Cyberwarfare): استعمال الهجمات الرقمية كجزء من الصراعات بين الدول.

الجرائم السيبرانية (Cybercrime): الجرائم التي تُرتكب باستعمال الإنترنت أو التقنية.

الفضاء السيبراني (Cyberspace): البيئة الافتراضية التي تنشأ من التفاعل بين الإنترنت والأجهزة[١]

استخدام المصطلح في اللغة العربية: "سيبراني" هو نعت يُضاف إلى مفردات أخرى ليدل على صلتها بالعالم الرقمي، مثل: الأمن السيبراني، الهجمات السيبرانية والبنية التحتية السيبرانية ويُعتبر من المصطلحات المعتمدة حديثًا في المعاجم التقنية والمؤسسات الرسمية.

ماهية الضرر السيبراني:

الضرر السيبراني هو الأذى أو الفقدان الذي يقع نتيجةً للتهديدات أو الهجمات في الفضاء السيبراني (البيئة الرقمية). هذه البيئة تشمل الإنترنت، الشبكات، والأنظمة الحاسوبية [٢] ويمكن أن يحدث الضرر السيبراني نتيجةً لطائفة متنوعة من الهجمات الرقمية مثل:

الاختراقات: حيث يقوم المهاجمون بالوصول غير المصرّح به إلى الأنظمة أو البيانات.

البرمجيات الخبيثة: مثل الفيروسات، الديدان، وأحصنة طروادة التي تُستخدم لإلحاق الضرر في الأجهزة أو سرقة البيانات.

---

[١] يُعرف المعجم العسكري لوزارة الدفاع الأمريكية الفضاء السيبراني على النحو التالي: "المنطقة العالمية داخل بيئة المعلومات التي تتكون من شبكات مترابطة من البنية التحتية للبيانات وتكنولوجيا المعلومات مثل الإنترنت وشبكات الاتصالات والحوسبة والمعالجة والتحكم، وتخدم شبكات المعلومات حوسبة عالم الفضاء السيبراني ، والمعلومات الشبكة هي حجم رقمي المعلومات التي لا تعتمد كليا على البيئة التي تم إنشاؤها فيها، ولكن مفرداتها تغطي مجموعة واسعة من المعالجات بالإضافة إلى سرعات نقل البيانات والوصول إلى الشبكة وما إلى ذلك، وبيئة الفضاء الإلكتروني تتعامل مع البيانات أثناء تدفقها .

[٢] الجرائم السيبراني وتأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها مجلة معالم للدراسات القانونية والسياسية المركز الجامعي تندوف المجلد ٠٤ العدد ٠٢ ٢٠٢٠، ص ٦٠ ص٦١.

الاحتيال الإلكتروني: بما في ذلك التصيد الاحتيالي (Phishing) للحصول على معلومات حساسة.

الضرر السيبراني يمكن أن يكون ملموسًا (مثل الخسائر المالية) أو معنويًا (مثل التأثير على السمعة الشخصية أو المؤسساتية).

اذا فالتهديدات السيبرانية تعني استغلال الحواسيب وتقنية المعلومات لإفساد البنية الأساسية الاستخباراتية للخصم وتدميرها، وأيضًا تعطيل شبكات الدفاع الجوي وفقًا لخطط مُعدّة بعناية واستخدام البريد الإلكتروني ومكاتب المراقبة التابعة لرئيس الدولة، كما تعني إتلاف أنظمة المعلومات وغيرها من الأعمال وبالتالي، فإن التهديد السيبراني أو الهجوم السيبراني يمثل خطر على الأمن الاجتماعي والأمن الاقتصادي والأمن القومي، وقد حُدّد هذا الهدف لأن التهديدات السيبرانية ليس لها عواقب أخلاقية أو جسدية [٣].

كما يمكن القول ان الضرر السيبراني هو أي نشاط غير قانوني أو ضار يُنفّذ عبر الإنترنت أو شبكات الحاسوب وتشمل مجموعة متنوعة من الأنشطة الضارة مثل الاقتحامات السيبرانية والبرامج الضارة والاحتيال السيبراني وسرقة الهوية والتجسس السيبراني والهجمات المنسقة على البنية التحتية الشبكية، كما يمكن أن تكون للأضرار السيبرانية تأثيرات خطيرة على الأفراد والشركات والحكومات، كما نجد أنها تتنوع باستمرار، حيث يستخدم المهاجمون تقنيات متقدمة ومتطورة للوصول إلى الأنظمة والشبكات. وعليه، تتطلب الحماية من الاضرار السيبرانية اتخاذ إجراءات أمنية قوية.

أنواع الضرر السيبراني:

- **الضرر المالي (الاقتصادي):**

تتمثل الأضرار المالية في الخسائر المباشرة أو غير المباشرة التي تلحق بالأفراد أو المؤسسات نتيجة للهجمات الإلكترونية، مثل سرقة الأموال من الحسابات البنكية، أو الاحتيال باستخدام بطاقات الائتمان، أو دفع الفدية في هجمات الفدية (Ransomware)، إضافة إلى تعطيل الأنظمة عن العمل وما يترتب عليه من خسائر تشغيلية كبيرة.

[٣] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري مجلة مصداقية، جامعة العربي تبسي تبسة، المجلد ٠١، العدد ٠١، ٢٠١٩، ص ١٠٨

(ISSN: 2537- 0758)

- **الضرر المعنوي (النفسي/الاجتماعي):**

ينشأ الضرر المعنوي عندما يتعرض الأفراد أو الجهات لأذى نفسي أو اجتماعي نتيجة لتسريب معلومات خاصة أو التشهير بهم، مثل تسريب الصور أو المحادثات الشخصية، أو تشويه السمعة على وسائل التواصل الاجتماعي، أو نشر معلومات حساسة دون إذن مسبق [٤].

- **الضرر التقني (التشغيلي):**

يظهر الضرر التقني في صورة تعطل أو تلف يصيب الأنظمة التقنية كأنظمة التشغيل أو قواعد البيانات أو الشبكات، مما يؤدي إلى إعاقة عمل المؤسسات أو الأفراد، وذلك من خلال هجمات مثل حجب الخدمة (DDoS)، أو إدخال فيروسات تؤدي إلى فقدان البيانات، أو اختراق أنظمة البنية التحتية الحيوية مثل الكهرباء والمستشفيات.

- **الضرر القانوني:**

تحدث الأضرار القانونية عندما تُواجه الأفراد أو المؤسسات تبعات قانونية نتيجة لفشلهم في حماية البيانات، كأن تتعرض الشركات للغرامات بسبب تسريب بيانات المستخدمين، أو ملاحقة المسؤولين عن الخروقات الأمنية قضائيًا، أو عند مخالفة الأنظمة والقوانين مثل اللائحة العامة لحماية البيانات (GDPR).

- **الضرر الأمني (الاستراتيجي):**

يُعد الضرر الأمني من أخطر الأضرار، حيث يستهدف أمن الدولة أو مؤسساتها الحيوية من خلال هجمات إلكترونية تخترق الأنظمة الحكومية أو العسكرية، أو تسرب وثائق سرية، أو تنفذها جهات معادية بشكل منظم بهدف زعزعة الاستقرار الوطني [٥].

- **الضرر الأخلاقي:**

ينتج الضرر الأخلاقي عن السلوكيات غير المشروعة التي تُمارَس عبر الإنترنت، مثل الابتزاز الإلكتروني، أو استغلال القُصّر ونشر المحتويات الضارة، أو ممارسة التنمر الإلكتروني، وهو ما يؤدي إلى تفشي ظواهر اجتماعية خطيرة وانحرافات سلوكية [٦].

---

[4] UNESCO – Cyber Violence Against Women and Girls
https://en.unesco.org/news/cyber-violence-against-women

[5] (WEF) World Economic Forum – Global Cybersecurity Outlook
https://www.weforum.org/reports/global-cybersecurity-outlook

[6] UNODC – Cybercrime and Online Exploitation,
https://www.unodc.org/unodc/en/cybercrime

المبحث الثاني
تطور تقنيات الذكاء الاصطناعي ودورها في الفضاء السيبراني؟

تمهيد:

يُعتبر الذكاء الاصطناعي من أبرز التقنيات الحديثة التي شهدت تقدمًا متسارعًا في العقود الأخيرة، حيث أصبح جزءًا لا يتجزأ من أنظمة العمل والإدارة والبحث العلمي في شتى المجالات. يعتمد الذكاء الاصطناعي على خوارزميات متطورة تحاكي الذكاء البشري في التحليل واتخاذ القرار، مما جعله أداة فعالة لدعم العمليات الرقمية وتحسين الأداء بشكل كبير. وفي ظل هذا التطور، أصبح الفضاء السيبراني يمثل البيئة الرقمية التي تتجمع فيها البيانات، وتُدار من خلالها الاتصالات والمعاملات الإلكترونية، سواء على المستوى الفردي أو المؤسسي أو الحكومي. ومع تزايد أهمية هذا الفضاء في الحياة اليومية، ظهرت تحديات أمنية كبيرة، نتيجة للهجمات السيبرانية المعقدة التي تهدف إلى اختراق الأنظمة وسرقة المعلومات أو تعطيل الخدمات.

من هذا المنطلق، برزت الحاجة إلى توظيف تقنيات الذكاء الاصطناعي في حماية الفضاء السيبراني، من خلال أدوات قادرة على التنبؤ بالهجمات، وتحليل السلوكيات المشبوهة، والاستجابة الفورية للمخاطر. فقد ساهم الدمج بين الذكاء الاصطناعي والأمن السيبراني في تطوير أنظمة دفاعية أكثر ذكاء وفعالية، مما يفتح آفاقًا جديدة لتعزيز الأمن الرقمي في المستقبل. وتتناول هذه الدراسة بالتحليل تطور تقنيات الذكاء الاصطناعي، ودورها المتزايد في تعزيز أمن الفضاء السيبراني، مع التركيز على التطبيقات العملية والتحديات المرافقة لهذا التداخل التقني.

. ماهية الذكاء الاصطناعي:

الذكاء الاصطناعي هو ميدان يعتني بتطوير أنظمة الحاسوب القادرة على إنجاز المهام التي تتطلب تفكيرًا وتحليلاً بشريًا ذكيًا، وهو تطور هائل في حقل التكنولوجيا يسمح للأنظمة الذكية بالتعلم والتكيف والتفاعل مع البيئة المحيطة. وتكشف مراجعة الأدبيات حول موضوع الذكاء الاصطناعي أن العديد من التعريفات لمفاهيم تكنولوجيا الذكاء الاصطناعي قد نُشرت ليس فقط من قبل المنظمات والخبراء في هذا الميدان، لكن أيضًا من قبل الأشخاص المهتمين بمجال التكنولوجيا، وفيما يلي بعض تعريفات الذكاء الاصطناعي. يصف سيمون الذكاء الاصطناعي بأنه متصل بعلم النفس والعلوم

(ISSN: 2537- 0758)

المعرفية وغيرها من العلوم التي تمكن أجهزة الكمبيوتر من أداء المهام بكفاءة، وتقليد القدرات البشرية، وجعل أجهزة الكمبيوتر تفكر بذكاء. ويعرف ريتش وكينج الذكاء الاصطناعي بأنه دراسة كيفية إنجاز أجهزة الكمبيوتر للمهام على نحو أفضل من البشر.

ويعرف مجلس صناعة المعلومات (IT) الذكاء الاصطناعي بأنه مجموعة من التقنيات القادرة على التعلم واستخدام المنطق والتكيف وإنجاز المهام بطرق مستوحاة من العقل البشري.

الذكاء الاصطناعي يشتمل على العلم والمعرفة التي يتم دمجها منطقيًا في أنظمة الحاسوب ويتم تجميعها وفقًا لخوارزميات محددة تعالج المشكلات التي تتطلب ذكاءً غير عادي[٧]. ويشير الذكاء الاصطناعي إلى قدرة الآلات مثل أجهزة الحاسوب على اكتساب الذكاء والتفكير المنطقي (الصوت) على غرار قدرة الإنسان على التفكير أو تفسير كميات كبيرة من البيانات (مثل البيانات المكتوبة أو المنطوقة)[٨] وهذه التعريفات ليست حصرية، هناك عدد لا يحصى من تعريفات الذكاء الاصطناعي، كل منها محدد من زوايا مختلفة اعتمادًا على مجال خبرة الفرد واهتماماته، وتجدر الإشارة أيضًا إلى أن العلماء لا يتفقون على تعريف واحد وعلى الرغم من اختلاف العديد من الباحثين حول إمكانات الذكاء الاصطناعي للوصول إلى مستوى العقل البشري بسبب الاختلافات الجوهرية، أصبح الذكاء الاصطناعي واقعًا ملموسًا وأصبح جزءًا من حياتنا العملية، ويتم استخدامه بشكل يومي.

---

[٧] حسن بن محمد حسن العمري، الذكاء الاصطناعي ودوره في العلاقات الدولية، المجلة العربية للنشر العلمي، العدد ٢٩، ٢ مارس ٢٠٢١م على الرابط
https://www.ajsp.net/research/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A%١D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A_%D9%88%D8%AF%D9%88%D8%B1%D9%87_%D9%81%D9%8A_%D8%A7%D9%84%D8%B9%D9%84%D8%A7%D9%82%D8%A7%D8%AA %D8%A7%D9%%٨٤D8%AF%D9%88%D9%84%D9%8A%D8%A9.pdf

[٨] نرمين مجدي، الذكاء الاصطناعي وتعلم الآلة، سلسلة كتيبات تعريفية العدد ٠٣، صندوق النقد العربي أبو ظبي، ص ٠٥، الإمارات العربية المتحدة ٢٠٢٠، على الرابط
https://www.amf.org.ae/sites/default/files/publications/2021-12/artificial-intelligence-machine-learning.pdf

- **دور الذكاء الاصطناعي في الفضاء السيبراني:**

يلعب الذكاء الاصطناعي (AI) دورًا متزايد الأهمية في الفضاء السيبراني، حيث يُستخدم لتعزيز الأمن، تقييم التهديدات، والرد على الهجمات السيبرانية. إليك أبرز مهامه:

١. **كشف المخاطر السيبرانية:** الذكاء الاصطناعي يمكنه تحليل كميات ضخمة من البيانات بسرعة فائقة لاكتشاف الأنماط غير المعتادة أو المشبوهة التي قد تشير إلى نشاط سيبراني ضار (مثل البرمجيات الخبيثة أو هجمات التصيد)[٩].

٢. **الاستجابة الآلية للهجمات:** يُستخدم AI لتفعيل أنظمة دفاع تلقائية قادرة على عزل الأجهزة أو إغلاق المنافذ عند رصد تهديد، مما يقلل الوقت اللازم للاستجابة ويحدّ من الضرر.

٣. **تحليل السلوك الشبكي:** يمكن للذكاء الاصطناعي مراقبة سلوك المستخدمين داخل الشبكة وتحديد التصرفات غير المألوفة، مثل الدخول من موقع جغرافي غير مألوف أو تحميل بيانات ضخمة بشكل مفاجئ.

٤. **التنبؤ بالهجمات القادمة:** من خلال تعلم الأنماط السابقة للهجمات السيبرانية، يمكن للذكاء الاصطناعي التنبؤ بمحاولات الاختراق المستقبلية والاستعداد لها.

٥. **التصدي للهجمات المعقدة والمتقدمة (APT):** الذكاء الاصطناعي يساعد في الكشف المبكر عن الهجمات المتقدمة التي تستغرق وقتًا طويلًا في التخطيط والتنفيذ، والتي غالبًا ما يصعب رصدها بالوسائل التقليدية. [١٠]

٦. **تحسين أمان كلمات المرور والمصادقة:** تُستخدم تقنيات AI لتحسين آليات التحقق من الهوية، مثل التعرف على الوجه أو تحليل نمط الكتابة أو الصوت.

٧. **الهجمات المُعززة بالذكاء الاصطناعي:** على الجانب الآخر، يمكن للجهات المهاجمة استخدام الذكاء الاصطناعي لتنفيذ هجمات أكثر تعقيدًا، مثل إنشاء رسائل تصيد دقيقة جدًا أو تجاوز أنظمة الدفاع الذكية.

---

[٩] السالمي، علاء عبد الرزاق(2022) ، **المدخل إلى الذكاء الاصطناعي السيبراني**، المنظمة العربية للتنمية الإدارية، ص٢٢٣.

[١٠] الإيادي، حمد عبد الله (٢٠٢٢)، "الدليل السيبراني المستمد من الذكاء الاصطناعي"، **مجلة الفكر القانوني والسياسي**، العدد ٣٢، ص١٢٤٥-١٢٦٦.

(ISSN: 2537- 0758)

الفصل الثاني
التحديات القانونية في إثبات الضرر السيبراني الناتج عن الذكاء الاصطناعي

تمهيد وتقسيم:

التوسع السريع في استعمال تقنيات الذكاء الاصطناعي في مختلف المجالات، من الرعاية الصحية إلى الأنظمة المالية والأمن السيبراني، أصبحت هذه التقنيات تؤدي دوراً محورياً في الحياة اليومية للأفراد والمؤسسات. وعلى الرغم مما تقدمه من فوائد هائلة في الكفاءة والدقة، إلا أن استعمالها يصحبه عدد من المخاطر، لعل أبرزها الأضرار السيبرانية التي قد تنشأ عن قرارات أو أفعال صادرة عن أنظمة ذكاء اصطناعي ذاتية التشغيل أو مدعومة بخوارزميات معقدة.

وهنا تظهر إشكالية قانونية معقدة تخص كيفية إثبات الضرر السيبراني الناتج عن الذكاء الاصطناعي، خصوصاً في ظل الطبيعة التقنية الغامضة لهذه الأنظمة، وغياب إطار قانوني محدد يواكب التطورات المتسارعة في هذا المجال. يستلزم هذا النوع من القضايا تخطي التحديات المرتبطة بإثبات العلاقة السببية، وتحديد المسؤولية القانونية، وإثبات القصد أو الخطأ في سياق تتسم فيه العمليات بالاستقلالية والاعتماد الكبير على البيانات والخوارزميات. في هذا الإطار، تتناول هذه الدراسة أبرز التحديات القانونية التي تواجه إثبات الضرر السيبراني الناجم عن الذكاء الاصطناعي، وتدرس أبعادها الفنية والقانونية ضمن بيئة رقمية متغيرة ومعقدة.

المبحث الأول: صعوبة تحديد المسؤولية في الجرائم السيبرانية المدعومة بالذكاء الاصطناعي

أولا: اشكاليه نسبه الفعل الي فاعل محدد:

مقدمه:

التطورات السريعة في تقنيات الذكاء الاصطناعي (AI)، أصبحت هذه الأدوات جزءاً جوهرياً من البنية التكنولوجية التي يعتمد عليها الأفراد والمؤسسات والدول. إلا أن استعمال الذكاء الاصطناعي في المجال السيبراني – سواء كان استعمالاً مباشراً أو غير مباشر – أفرز نوعاً جديداً من الجرائم المعقدة يُطلق عليها "الجرائم السيبرانية المدعومة بالذكاء الاصطناعي". وتكمن أبرز الإشكاليات القانونية في هذه الجرائم في مسألة نسبة الفعل إلى فاعل محدد، أي تحديد الشخص المسؤول عن الفعل الإجرامي في ظل وجود أنظمة ذكية تتصرف باستقلالية نسبية عن العنصر البشري.

- **الطبيعة المستقلة للذكاء الاصطناعي وصعوبة ربط الفعل بالفاعل:**

تُستخدم أنظمة الذكاء الاصطناعي في تنفيذ عمليات خبيثة مثل: اختراق الشبكات، انتحال الهوية، هجمات حجب الخدمة (DoS)، والهندسة الاجتماعية المؤتمتة، وغيرها من الأفعال التي تندرج تحت بند الجرائم السيبرانية. وفي كثير من الحالات، لا يكون هنالك تدخل مباشر من الإنسان عند تنفيذ الجريمة، بل يتم تنفيذها بواسطة برمجيات ذكية تتخذ قراراتها بناءً على معطيات وتعلم ذاتي. هذا الطابع "شبه المستقل" يجعل من الصعب قانوناً إسناد الجريمة إلى شخص معين، لا سيما عند عدم وضوح العلاقة بين فعل الذكاء الاصطناعي ونية الفاعل البشري، مما يُعقّد الركن المعنوي للجريمة [١١].

- **غياب القصد الجنائي المباشر وتفكك العلاقة السببية:**

تعتمد المسؤولية الجنائية في القواعد العامة على توافر "القصد الجنائي" إلى جانب "الركن المادي". لكن في حالات الجرائم المدعومة بالذكاء الاصطناعي، قد لا يكون هنالك قصد إجرامي واضح، لا من جانب المبرمج، ولا من جانب المشغّل. فمثلًا، إذا تم تدريب نظام ذكاء اصطناعي على تحليل سلوك المستخدمين، ثم استغل ثغرة أمنية تلقائياً دون أمر مباشر من المستخدم أو المبرمج، فمن يتحمل المسؤولية؟ هل المبرمج الذي صمّم النظام؟ أم المستخدم الذي فعّله؟ أم أن النظام نفسه يجب أن يخضع لتقنين جديد؟ إضافة إلى ذلك، فإن العلاقة السببية بين الفعل والفاعل تصبح غير واضحة، حيث تكون خوارزميات الذكاء الاصطناعي قد اتخذت قرارًا استنادًا إلى تحليلها الذاتي دون تدخل بشري مباشر، مما يخلق "فراغاً تشريعياً" فيما يتعلق بتحديد الجهة المسؤولة.

- **التحديات العملية في تتبع الفاعل السيبراني:**

الجرائم السيبرانية بطبيعتها تُنفذ في بيئة افتراضية معقدة، وتتسم بما يلي:

١. إخفاء الهوية الرقمية عبر تقنيات مثل ال .VPN أو الشبكات المظلمة (Dark Web).

٢. تشغيل الأدوات من عدة دول مختلفة مما يخلق صعوبة في تطبيق مبدأ الاختصاص القضائي.

عدم قابلية بعض النظم الذكية للتفسير (Black Box AI)، أي أنها تقدم نتائج دون أن يمكن تحليل طريقة اتخاذها للقرار. كل هذه العوامل تجعل من الصعب جمع

[١١] الخطيب، نزار. الجريمة السيبرانية والذكاء الاصطناعي: دراسة قانونية مقارنة. بيروت: منشورات الحلبي الحقوقية، ٢٠٢٢، ص. ٨٩.

(ISSN: 2537- 0758)

أدلة رقمية تُثبت مسؤولية شخص معين، أو حتى تحديد ما إذا كانت الأوامر صادرة عن إنسان أو نظام مستقل.

٣. الحاجة إلى تطوير تشريعي خاص بالذكاء الاصطناعي:

لمواكبة هذه التحديات، ينبغي أن تقوم التشريعات الحديثة بما يلي:

. الاعتراف بمسؤولية مشتركة: بين المطور، المشغّل، والمستخدم، بحيث تُوزع المسؤولية بحسب درجة تدخل كل طرف.

. فرض التزامات قانونية على مطوري الذكاء الاصطناعي مثل ضمان خضوع الأنظمة للرقابة ومنع استعمالها في أعمال ضارة.

. إلزام الأنظمة الذكية بالشفافية من خلال تبني الذكاء الاصطناعي القابل للتفسير (Explainable AI)، مما يُسهم في تتبع أسباب اتخاذ القرارات [١٢].

. دراسة إمكانية إضفاء شخصية قانونية محدودة على بعض الكيانات الذكية التي تعمل باستقلال شبه تام، بحيث تتحمل مسؤولية مدنية أو جنائية في حالات معينة.

ثانيا: مسؤوليه الانظمة الذاتية والبرمجيات:

التقدم التكنولوجي الهائل في مجال الذكاء الاصطناعي، ادي الي ان الأنظمة الذاتية (Autonomous Systems) اصبحت أكثر حضورًا في حياتنا اليومية، بدءًا من الأجهزة الذكية وصولاً إلى الأنظمة المتقدمة التي تدير الأعمال التجارية والصناعية. ومع ذلك، فإن هذه الأنظمة، التي تتمتع بقدرة على اتخاذ قرارات مستقلة، تثير العديد من القضايا القانونية المعقدة، خاصة عندما يتم استخدامها في الجرائم السيبرانية. يبرز تحدي رئيسي يتمثل في صعوبة تحديد المسؤولية القانونية في حالة وقوع الأضرار الناجمة عن هذه الأنظمة الذكية.

صعوبة تحديد المسؤولية حيث تتعدد الأسباب التي تجعل تحديد المسؤولية في الجرائم السيبرانية المدعومة بالذكاء الاصطناعي أمرًا بالغ الصعوبة بسبب:

. **غياب تدخل الإنسان المباشر:** الأنظمة الذاتية تعمل بشكل مستقل عن التدخل البشري المباشر، مما يجعل تحديد الطرف المسؤول عن الأفعال التي تقوم بها هذه الأنظمة معقدًا للغاية. فالمطور قد لا يتوقع السلوكيات غير المشروعة التي قد يتخذها النظام بعد إطلاقه [١٣].

---

[١٢] الموسوي، حسين. التشريعات الحديثة لمواجهة تحديات الذكاء الاصطناعي. بغداد: دار الأكاديميون، ٢٠٢٣، ص. ١٣٤.

[١٣] الجابري، محمد سالم، "الجرائم الإلكترونية: نظرة قانونية في التشريعات العربية"، دار الفكر العربي، ٢٠١٩، ص ١١٢.

. **التعلم الآلي:** تعتمد بعض الأنظمة على تقنيات التعلم الآلي (Machine Learning) التي تسمح لها بتطوير سلوكيات وتعديلات تتغير بمرور الوقت بناءً على البيانات المدخلة. هذه الأنظمة قد تُظهر سلوكيات غير متوقعة، مما يصعب تحديد المسؤولية عن أي فعل غير قانوني.

. **القدرة على اتخاذ قرارات مستقلة:** قد يتخذ النظام الذكي قرارًا يتسبب في ضرر دون أي تدخل بشري. وعليه، يبرز السؤال حول من يتحمل المسؤولية: هل هو المبرمج الذي قام بتصميم الخوارزمية؟ أم الجهة المالكة للنظام؟ أم ربما النظام نفسه؟

وفي ظل هذا الامر، يمكن تحديد عدة أطراف قد تتحمل المسؤولية القانونية، بحسب ظروف الجريمة:

١.**المطورون:** قد يتحمل المطورون المسؤولية إذا كانت الأنظمة التي صمموها تحتوي على أخطاء تصميمية أو ثغرات أمنية تجعلها عرضة لاستخدامها في الجرائم. لكن، في الكثير من الحالات، قد يكون من الصعب إثبات أن المطور كان على علم بأن النظام سيُستخدم لأغراض غير قانونية [١٤].

٢.**المستخدمون:** في بعض الحالات، قد يتحمل المستخدمون المسؤولية إذا تم استخدام الأنظمة الذكية بشكل غير قانوني، أو إذا كانوا قد قاموا بتعديل هذه الأنظمة لاستخدامات ضارة. ومع ذلك، يبقى الأمر معقدًا لأن الأنظمة قد تتخذ قرارات بدون تدخل بشري مباشر.

٣.**الشركات المالكة:** يمكن تحميل الشركات المالكة للمعدات أو الأنظمة الذكية المسؤولية إذا كانت هناك ثغرات في أمان النظام أو إذا لم يتم اتخاذ التدابير الوقائية المناسبة لمنع استخدام الأنظمة في الجرائم السيبرانية [١٥].

---

[١٤] عبد الرحمن، سامي، "المسؤولية القانونية في الجرائم الإلكترونية: التحديات الحديثة"، دار التنوير للنشر، ٢٠٢٢، ص ٢٤٣.

[١٥] العتيبي، فهد بن عبد الله، "المسؤولية القانونية للأنظمة الذاتية في الجرائم الإلكترونية"، مكتبة الحقوق الدولية، ٢٠٢٠، ص ١٥٧.

(ISSN: 2537- 0758)

المبحث الثاني
إشكالية الإثبات في ظل طبيعة الهجمات السيبرانية

أولا: صعوبة جمع الأدلة الرقمية وحمايتها:

١. **تسارع التكنولوجيا وتطور أساليب المعتدين:** التطور المستمر للهجمات: مع استمرار تقدم تكنولوجيا الذكاء الاصطناعي وتقنيات الهجوم الرقمي، يعتمد المهاجمون على أساليب متطورة للغاية، بما في ذلك الخوارزميات الذكية التي يمكنها التكيف مع الهجمات أو حتى إخفاء أدلة الهجوم بشكل ديناميكي. فمثلًا، الهجمات المدعومة بالذكاء الاصطناعي قد تستخدم تقنيات مثل "التعلم الآلي" لتعديل البيانات أو جعلها غير قابلة للكشف عن طريق جعل الأنظمة تتعامل مع الهجوم بشكل مختلف في كل مرة.

٢. **الهجمات التي تعتمد على إخفاء الأدلة:** الهجمات السيبرانية قد تُنفذ باستخدام تقنيات متطورة لطمس أو تغيير البيانات بحيث تصبح الأدلة غير قابلة للاكتشاف أو التتبع. على سبيل المثال، قد تُستخدم أدوات لتعديل سجلات الخوادم أو استبدال الملفات الهامة بحيث تَصعب معرفة ما تم تعديله أو حذفه.

٣. **التشفير والأنظمة المجهولة:**

التشفير المتقدم: المهاجمون يمكنهم استعمال

تقنيات التشفير المتقدمة، مثل تشفير الاتصال عبر بروتوكولات (VPN) أو (Tor)، بحيث يصعب تحديد هوية المهاجمين أو تتبع مساراتهم. هذه التقنيات تمنع الجهات الأمنية من جمع البيانات الحيوية مثل عناوين الـ IP أو سجلات الحركة في الشبكة[١٦].

- **الدرك ويب:** يستخدم العديد من المهاجمين الـ "دارك ويب" (Dark Web) وهو مساحة عبر الإنترنت غير مفهرسة وغير مرئية لمعظم محركات البحث، مما يتيح لهم العمل بشكل مجهول تمامًا. هذه البيئة تجعل من الصعب جدًا تحديد الجهة المسؤولة عن الهجوم، بالإضافة إلى أن الأدلة التي قد يتم العثور عليها تكون عادة غير قابلة للاستخدام في المحاكم.

[16] De Capitani, G., & Sciarrone, G. (2019). Cryptography and Network Security: Principles and Practice. Prentice Hall, pp. 200-215.

- إخفاء الهوية عبر شبكات افتراضية خاصة: استخدام شبكات VPN وأدوات مشابهة يمكّن المهاجمين من إخفاء موقعهم الجغرافي الحقيقي، مما يجعل من الصعب تتبعهم.

٤. **الحاجة إلى تقنيات متخصصة في جمع الأدلة الرقمية:**

- **التحليل الجنائي الرقمي المتقدم:** جمع الأدلة الرقمية يتطلب أدوات وتقنيات متقدمة لتحليل البيانات والمعلومات. هذه الأدوات تساعد في استعادة البيانات المحذوفة، تحليل الحركات في الشبكة، وتحديد وجود البرمجيات الخبيثة على الأنظمة المتأثرة. ولكن، هذه الأدوات تحتاج إلى مستويات عالية من الخبرة والمعرفة، وبالتالي يصبح الوصول إلى الأدلة الرقمية بشكل صحيح تحديًا كبيرًا [١٧].
- **تحديد المواقع في الأنظمة المعقدة:** في حالة الهجمات السيبرانية المعقدة، قد يتم إخفاء الأدلة في أماكن متعددة، مثل الخوادم البعيدة أو في أجهزة الضحايا، ويجب على المحققين تحديد المواقع الدقيقة لهذه الأدلة عبر الشبكات المتشعبة.
- **الحماية أثناء جمع الأدلة:** عند جمع الأدلة الرقمية، من الضروري أن يتم ذلك بطريقة تحمي الأدلة من التلاعب أو الفقدان. وهذا يشمل التحقق من سلاسل الأدلة الرقمية وتوثيق كل خطوة من خطوات جمع الأدلة. أي خطأ في عملية جمع الأدلة قد يؤدي إلى فقدان قيمتها القانونية أو قد يؤدي إلى التشكيك في مصداقيتها.

٥. **التحديات المرتبطة بالتخزين والتعامل مع الأدلة الرقمية:**

- **إمكانية التلاعب بالأدلة بعد جمعها:** حتى بعد جمع الأدلة الرقمية، من الممكن أن يتم التلاعب بها إذا لم يتم تخزينها بشكل آمن. مثلاً، إذا كانت الأدلة في شكل بيانات مخزنة على جهاز أو خادم، قد يتعرض هذا الجهاز للتهديدات من هجمات سيبرانية أخرى قبل أن يتم حفظها بشكل آمن. هذا يجعل من الصعب الحفاظ على صحة الأدلة من اللحظة التي يتم جمعها حتى استخدامها في المحكمة.
- **التخزين الآمن للأدلة الرقمية:** من المهم أن يتم تخزين الأدلة الرقمية في بيئة محكمة ومؤمنة ضد أي محاولات للتلاعب بها أو التلاشي. التخزين في بيئة آمنة يُعتبر أحد العوامل الأساسية لضمان صحة الأدلة وتجنب فقدانها.

[17] Case, T., & Ward, A. (2018). Digital Forensics and Incident Response. CRC Press, pp. 120-145

(ISSN: 2537- 0758)

٦. التحديات القانونية المتعلقة بجمع الأدلة:

القوانين الدولية والأخلاقيات: جمع الأدلة الرقمية يخضع للقوانين المتعلقة بالخصوصية وحماية البيانات، خاصة في الحالات التي تشمل شركات أو أشخاصًا من دول مختلفة. من هنا يأتي التحدي في ضمان جمع الأدلة بطريقة قانونية وبالتوافق مع التشريعات المحلية والدولية. بعض الدول قد تكون لديها سياسات صارمة حول كيفية جمع الأدلة من أنظمة أو شبكات تابعة لجهات أخرى، ما يزيد من صعوبة جمع الأدلة عبر الحدود [١٨]

ثانيًا: إثبات العلاقة السببية بين الهجوم والضرر:

- **الأساس القانوني للعلاقة السببية:** تُعرَف العلاقة السببية بأنها الصلة التي تربط بين الخطأ (أو الفعل المؤذي) والنتيجة الناجمة عنه[١٩]، بحيث لا يمكن تصور حدوث الضرر لولا وقوع الفعل. وقد وردت معظم التشريعات المدنية على لزوم توافر هذه العلاقة لقيام المسؤولية، كما جاء في المادة (١٦٣) من القانون المدني المصري: "كل خطأ سبب ضررًا للغير يلتزم من ارتكبه بالتعويض." وتشترط هذه المادة أن يكون الخطأ هو السبب المباشر أو الفعلي في إحداث الضرر، وأن يكون الضرر متوقعًا ومباشرًا.
- **المعضلات العملية لإثبات العلاقة السببية في الهجمات السيبرانية:**

١. **إخفاء هوية الجاني:** يستخدم منفذو الهجمات أدوات مثل VPN، التشفير، والشبكات المظلمة لإخفاء آثارهم، مما يُصعّب وصل الضرر بفاعل محدد[٢٠]. وقد يُدار الهجوم من دولة أخرى، مما يزيد صعوبة التتبع والتقاضي.

٢. **تعدد المساهمين في الضرر:** قد تتسبب أخطاء من جهات متعددة (مثل ضعف النظام الأمني الداخلي أو ثغرات برمجية) في تفاقم الضرر، ما يجعل العلاقة السببية معقدة وغير واضحة.

٣. **استقلالية أدوات الذكاء الاصطناعي:** قد تُستخدم أنظمة ذكية في تنفيذ الهجمات أو إدارتها بشكل تلقائي، مما يثير إشكالية تحديد "الإرادة الفاعلة" و"المسؤولية البشرية" عن تصرفات هذه الأنظمة[٢١].

---

[18] Binns, R. (2021). Legal Aspects of Cybersecurity. Cambridge University Press, pp. 70-90

[١٩] محكمة النقض المصرية، الطعن رقم ١٠٣٦ لسنة ٥٨ قضائية، جلسة ١٩٩٤/١٢/٢٠.

[٢٠] أحمد طارق النجار، الجرائم الإلكترونية: دراسة مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠٢١، ص. ١٣٤.

الفصل الثالث
سبل تطوير الإطار القانوني لمعالجة الضرر السيبراني الناتج عن الذكاء الاصطناعي

المقدمة:

بفضل الثورة الرقمية المتسارعة، صار الذكاء الاصطناعي أحد أبرز التحولات التكنولوجية التي تؤثر بشكل جوهري في جميع جوانب الحياة، بما في ذلك المجالات القانونية والاقتصادية والاجتماعية. فقد أدت تطبيقات الذكاء الاصطناعي، لا سيما المعتمدة على الخوارزميات الذاتية التعلم، إلى تغييرات عميقة في طريقة عمل الأنظمة الرقمية، وأسهمت في زيادة فعالية الخدمات، لكنها في الوقت عينه أفرزت تحديات قانونية غير مسبوقة، وعلى رأسها تلك المتصلة بالضرر السيبراني.

الضرر السيبراني الناجم عن الذكاء الاصطناعي يطرح إشكاليات قانونية معقدة تتعلق بصعوبة تحديد المسؤولية، وغياب الأطر القانونية الواضحة التي تنظم العلاقة بين الإنسان والآلة، إضافة إلى هشاشة البنية القانونية التقليدية في مواجهة أنظمة قادرة على اتخاذ قرارات شبه مستقلة. وتزداد هذه التحديات حدة مع تنامي قدرة الذكاء الاصطناعي على التفاعل داخل الفضاء السيبراني، ما قد يؤدي إلى وقوع أضرار تتراوح بين انتهاك الخصوصية وهجمات إلكترونية مدمرة. الا ان الإطار القانوني الحالي، في العديد من الدول، لا يزال يعتمد على مفاهيم المسؤولية التقليدية، ولا يواكب الطبيعة الديناميكية والمعقدة للذكاء الاصطناعي. وعليه، فإن تطوير هذا الإطار أصبح ضرورة قانونية ملحة، سواء من خلال استحداث تشريعات جديدة، أو تعديل القوانين القائمة، بما يضمن التوازن بين حماية الحقوق والحريات من ناحية، وتشجيع الابتكار التكنولوجي من ناحية أخرى. من هذا المنطلق، يسعى هذا البحث إلى دراسة وتحليل أبرز الثغرات القانونية في معالجة الضرر السيبراني الناجم عن الذكاء الاصطناعي، واقتراح سبل تطوير الإطار القانوني لضمان فعالية الحماية القانونية، وتفعيل أدوات الاثبات الالكتروني والرقمي، وأيضا التعاون الدولي وتوحيد الجهود القانونية.

---

[٢١] حسن إبراهيم منصور، **المسؤولية القانونية عن تصرفات الذكاء الاصطناعي**، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢، ص. ١٠٣.

(ISSN: 2537- 0758)

المبحث الاول

تعزيز البنية القانونية والتشريعية؟

أولا: مقترحات لتعديل التشريعات الوطنية:

١. تعديل نظام جرائم الإنترنت:

- إدخال نص قانوني يجرم استعمال الذكاء الاصطناعي في:
- تنفيذ هجمات إلكترونية (مثل برامج الذكاء الاصطناعي التي تتعلم لاختراق الأنظمة).
- توليد محتوى مزيف (مثل التزييف العميق – Deepfake – أو المحتوى المضلل).
- تصنيف الجرائم التي تتم باستخدام الذكاء الاصطناعي كـ "جرائم مشددة العقوبة" نظرًا لتعقيد كشفها وخطورتها[٢٢].
- إضافة مادة عن "المسؤولية القانونية لمشغلي الأنظمة الذكية"، في حال عدم اتخاذ الإجراءات التقنية للحد من إساءة الاستعمال.

٢. تعديل قانون حماية البيانات الشخصية:

- النص على الحق في التفسير: أي إلزام الجهات التي تستخدم أنظمة ذكاء اصطناعي باتخاذ قرارات مؤتمتة بتوضيح كيفية اتخاذ القرار.
- توسيع مفهوم "البيانات الحساسة" ليشمل البيانات التي يمكن للذكاء الاصطناعي استخلاصها، مثل الحالة النفسية أو التوجهات السياسية من خلال تحليل السلوك.
- إلزام الشركات والمطورين بالحصول على موافقة صريحة ومستنيرة عند استخدام الذكاء الاصطناعي في تحليل البيانات.

٣. تعديل القانون المدني (المسؤولية المدنية):

- استحداث مادة تنص على المسؤولية عن الأضرار الناتجة عن الأنظمة المؤتمتة، حتى بدون وجود خطأ بشري مباشر.
- اعتماد مبدأ "المسؤولية التضامنية" بين المطور، والمشغّل، والمستخدم النهائي، وفقًا لنسبة مساهمته في الضرر[٢٣].

---

[٢٢] إسلام مصطفى جمعة مصطفى، "ضرورة التدخل التشريعي لمواجهة مخاطر تطور الذكاء الاصطناعي ومعالجة تطوره لحماية القيم الإنسانية في المجتمع المصري"، مجلة القانون، جامعة القاهرة، ٢٠٢٤، ص. ١-٣٠.

[٢٣] أ.د/ أيمن عبد الله فكرى، "المسؤولية الجنائية عن أعمال الذكاء الاصطناعي"، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، ٢٠٢٤، ص. ٤٥١-٤٧٤

- إنشاء صندوق تعويض خاص للحوادث الناتجة عن تقنيات الذكاء الاصطناعي غير المتوقعة.

٤. **تعديل قانون التجارة الإلكترونية والعقود:**

- إدخال مفهوم "الوكلاء الأذكياء" في نظام العقود، والاعتراف بشرعية العقود التي يبرمها نظام ذكاء اصطناعي بالنيابة عن شخص طبيعي أو اعتباري.
- اشتراط الشفافية في التعامل مع أنظمة الذكاء الاصطناعي عند التعاقد، وإبلاغ المستهلك إذا كان يتعامل مع نظام مؤتمت.

٥. **إدخال تشريعات جديدة بالكامل عند غيابها**

مثال: قانون خاص بالذكاء الاصطناعي يشمل قواعد للمساءلة، التسجيل الإلزامي لبعض الأنظمة عالية الخطورة، التزامات مطوري الذكاء الاصطناعي، وآليات الرقابة والتفتيش [٢٤].

٦. **تعديل قانون العمل:**

- النص على حق الموظف في معرفة ما إذا كان يخضع لتقييم مؤتمت.
- وضع قيود على قرارات الفصل أو الترقية التي تعتمد كليًا على أنظمة ذكاء اصطناعي.
- وضع برامج إعادة تأهيل وتدريب للموظفين المهددين بالإحلال نتيجة الأتمتة.

ثانيا: اهميه وجود قانون خاص بالذكاء الاصطناعي والامن السيبراني:

أصبح سنّ تشريع خاص بتنظيم الذكاء الاصطناعي والأمن السيبراني ضرورة تشريعية ماسّة في ظل التطور المتسارع الذي تشهده تقنيات الذكاء الاصطناعي وارتباطها الوثيق بأنظمة البنية التحتية الرقمية. فالأنظمة الذكية الحديثة لا تقتصر على كونها أدوات تقنية، بل أضحت فاعلاً جديداً في الحياة القانونية والاجتماعية، قادرة على اتخاذ قرارات مؤتمتة تؤثر في الحقوق والحريات الأساسية للأفراد، بما في ذلك الخصوصية، والمساواة، والحصول على الخدمات.

[٢٤] د/ شوقي محمد صلاح، "المسؤولية المدنية الناشئة عن استخدام الذكاء الاصطناعي"، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، ٢٠٢٤، ص. ٣١-٦٢.

(ISSN: 2537- 0758)

تنبع أهمية وجود قانون مستقل من عدة أوجه جوهرية:

- سدّ الفراغ التشريعي القائم حيال المسؤولية القانونية عن الأفعال الصادرة عن أنظمة الذكاء الاصطناعي، لا سيما في الحالات التي يتعذّر فيها تحديد الفاعل البشري المسؤول عن الضرر الناتج عن قرارات أو أخطاء خوارزمية [٢٥].
- تعزيز الأمن السيبراني الوطني من خلال تنظيم آليات تطوير وتدريب ونشر أنظمة الذكاء الاصطناعي، والتصدي لاستخدامها في أنشطة عدائية كالهجمات المؤتمتة، التزييف العميق (Deepfake)، والتجسس الرقمي المدعوم بالخوارزميات.
- تأسيس إطار قانوني للمساءلة يوازن بين حماية الابتكار التقني وبين صون الحقوق الأساسية، مع فرض واجبات محددة على مطوّري ومشغّلي أنظمة الذكاء الاصطناعي، واشتراط معايير للأمان، والشفافية، والتفسير، والموافقة المسبقة على استخدام البيانات.
- تحقيق الأمن القانوني للمجتمع الرقمي من خلال منح الجهات القضائية والتنفيذية الأدوات القانونية اللازمة لتنظيم وحوكمة الذكاء الاصطناعي، ووضع ضوابط قانونية واضحة لاستخدامه في القطاعات الحساسة كالصحة، والتعليم، والأمن.
- مواءمة التشريع الوطني مع المعايير الدولية، لا سيما مع توجهات الاتحاد الأوروبي (قانون الذكاء الاصطناعي ٢٠٢٤) ومنظمة التعاون الاقتصادي والتنمية (OECD) فيما يتعلق بالمبادئ الأخلاقية والقانونية الحاكمة لاستخدام الذكاء الاصطناعي.

إن إصدار قانون وطني خاص بالذكاء الاصطناعي والأمن السيبراني من شأنه أن يوفّر إطاراً متكاملاً ومرناً، يُمكّن الدولة من مواكبة التحولات التكنولوجية المعاصرة ويُحصّن المجتمع قانونياً في مواجهة المخاطر السيبرانية الناشئة عن سوء استخدام أو انحراف هذه التقنية.

[٢٥] إسلام مصطفى جمعة" .ضرورة التدخل التشريعي لمواجهة مخاطر تطور الذكاء الاصطناعي ومعالجة تطوره لحماية القيم الإنسانية في المجتمع المصري." مجلة القانون، جامعة القاهرة، العدد ٢، ٢٠٢٤، ص. ١–٣٠.

المبحث الثاني
تفعيل أدوات الإثبات الإلكتروني والرقمي.

ثانيا: تطوير أليات الاثبات القضائي الرقمي:

١.إقرار التوقيع الإلكتروني والتوثيق الرقمي كأدلة قضائية:

- ينبغي الاعتراف بالتوقيع الإلكتروني، والوثائق الرقمية، والرسائل الإلكترونية كأدلة قانونية مُعترَف بها أمام المحاكم. يتيح ذلك تسريع الإجراءات القانونية ويقلل من الحاجة إلى الأوراق التقليدية، ما يسهل التحليل والتدقيق في الأدلة الرقمية.
- يمكن الاعتماد على تقنيات مثل التوقيع الرقمي والمصادقة الثنائية لضمان عدم العبث بالأدلة.

٢.استخدام تقنيات البلوك تشين لتوثيق الأدلة الرقمية:

- يمكن استعمال تقنية البلوك تشين لضمان نزاهة الأدلة الرقمية، حيث تسمح بتوثيق البيانات بطريقة تمنع التعديل أو التلاعب بها بعد تسجيلها. هذا النظام يضمن للمحاكم أن الأدلة التي تم تقديمها لم تتعرض لأي تغيير أو تزوير، ما يعزز من مصداقية الإجراءات القانونية.

٣.وضع معايير لتوثيق الأدلة الرقمية وحفظها:

- تطوير معايير قانونية واضحة تحدد كيفية توثيق الأدلة الرقمية وحفظها لضمان سلامتها وصحتها. يجب تحديد أدوات وبرمجيات معترف بها من قبل النظام القضائي لضمان أمان الأدلة الرقمية. يتضمن ذلك معايير لحفظ الصور، مقاطع الفيديو، والملفات الصوتية في شكل رقمي يمكن الرجوع إليه بسهولة.

٤.تطوير آليات للتحقق من صحة الأدلة الرقمية:

- يجب وضع تقنيات وآليات تمكن المحاكم من التحقق من صحة الأدلة الرقمية، مثل التحقق من هويات الأطراف المرسلة والتأكد من أن البيانات الواردة لم يتم التلاعب بها أو تعديلها.
- يمكن استعمال أدوات مثل الخوارزميات لتحليل البيانات وتحديد أي تغيير في محتوى الأدلة.

(ISSN: 2537- 0758)

٥.استخدام الذكاء الاصطناعي في تحليل الأدلة:

- تقنيات الذكاء الاصطناعي يمكن أن تُستخدم في فحص الأدلة الرقمية بشكل أسرع وأكثر دقة. على سبيل المثال، يمكن استعمال الذكاء الاصطناعي لتحليل سجلات البيانات الكبيرة لاكتشاف الأنماط، التعرف على العبث في الصور والفيديوهات (Deepfake) أو التحقق من صحة الوثائق.
- يمكن أيضًا أن يساعد في تحديد وجود أي هجوم سيبراني أو تلاعب في المعلومات الرقمية المقدمة للمحكمة [٢٦].

٦.تحديد قواعد قبول الأدلة الرقمية عبر الحدود:

- في الحالات التي تشمل أطرافًا دولية، يجب أن يكون هنالك تشريع يحدد كيفية قبول الأدلة الرقمية عبر الحدود، خاصة إذا كانت الأدلة تُرسل عبر الإنترنت أو تم تخزينها في خوادم خارج الدولة.
- يتطلب الأمر معايير قانونية واضحة حول كيفية التعامل مع الأدلة الرقمية الدولية لتجنب القضايا المتعلقة بالاختصاصات القضائية المتعددة.

٧.إدخال التدريب على الأدلة الرقمية ضمن برامج القضاة والمحامين:

- يجب على النظام القضائي توفير تدريب متخصص للقضاة والمحامين حول كيفية التعامل مع الأدلة الرقمية. ويشمل ذلك فهم كيفية قبول الأدلة الرقمية، كيفية فحصها، والكيفية القانونية لاستعمالها في المحكمة.
- تدريب الكوادر القانونية على استخدام التكنولوجيا الحديثة مثل الذكاء الاصطناعي وتحليل البيانات سيساعد في تحسين سرعة وكفاءة التعامل مع القضايا الرقمية.

٨.إجراءات قانونية للتعامل مع الأدلة الرقمية في محاكمات الخصوصية والأمن السيبراني:

- ينبغي أن يتم تطوير معايير قانونية خاصة للتعامل مع الأدلة الرقمية في قضايا الخصوصية والأمن السيبراني، لضمان حماية المعلومات الشخصية ولتفادي تدهور الحقوق الأساسية للأفراد نتيجة لاستعمال الأدلة الرقمية في قضايا معقدة.

---

[٢٦] الخضيري، ناصر محمد. "دور الذكاء الاصطناعي في دعم نظام العدالة وتحليل الأدلة الرقمية." المجلة السعودية للدراسات القانونية، جامعة الإمام محمد بن سعود، ٢٠٢٣، ص. ١٤٣–١٦٦.

- تحليل الأدلة المتعلقة بالهجمات السيبرانية يتطلب تطوير أدوات قانونية وتقنية قادرة على فحص الأدلة الرقمية بشكل دقيق [٢٧].

أولا: دور الخبراء التقنيين في دعم المحاكم:

١. تدقيق القرائن الرقمية:

- يقوم الخبراء بتدقيق محتوى الأجهزة الإلكترونية (مثل الحواسيب والهواتف) واستعادة المعطيات المحذوفة أو المخفية.
- تشمل القرائن الرقمية: الرسائل النصية، رسائل البريد الإلكتروني، سجلات التصفح، كاميرات المراقبة، أنظمة GPS، وغيرها.

٢. تأكيد سلامة البراهين الإلكترونية:

- يتولى الخبير التأكد من أن المعطيات لم تُحرَّف أو تُعدَّل.
- يستخدم تقنيات مثل "سلاسل التحقق" (Hashing) و"البصمات الرقمية" لضمان مصداقية البراهين.

٣. الشرح الفني للمحكمة:

- يُبسّط المفاهيم التقنية للقضاة وأطراف الدعوى.
- يشرح كيفية عمل النظم التقنية، مثل التوقيع الرقمي، أو كيفية وقوع اختراق إلكتروني.

٤. إعداد التقارير الفنية:

- يُعد الخبير تقارير مفصلة ومحايدة تُرفق بملف القضية.
- هذه التقارير قد تكون حاسمة في توجيه المحكمة نحو الإدانة أو البراءة [٢٨].

٥. المشاركة في جلسات الاستماع:

- يُدعى الخبير أحيانًا للإدلاء بشهادته أمام المحكمة.
- يجيب على أسئلة القاضي أو المحامين بخصوص الجوانب التقنية.

٦. تطوير البنية القضائية الرقمية:

- يشارك الخبراء في تصميم منصات التقاضي الإلكتروني.

---

[27] European Commission. "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act)." Brussels, 2021.
[28] Council of Europe – Cybercrime and Electronic Evidence https://www.coe.int/en/web/cybercrime

(ISSN: 2537- 0758)

- يساعدون في اعتماد أدوات مثل التوقيع الرقمي، وتوثيق المستندات، والتحقق من الهوية الرقمية.

٧. دعم التحقيقات في الجرائم السيبرانية:

- يقدمون العون في تتبع مصدر الهجمات الإلكترونية.
- يستخدمون أدوات متقدمة لتحديد الجناة وتحليل أساليب الاختراق.

المبحث الثالث

التعاون الدولي وتوحيد الجهود القانونية

أولا: دور الاتفاقيات الدولية في ملاحقه الجريمة السيبرانية:

١.التأثير العالمي للذكاء الاصطناعي:

- بالنظر إلى أن تقنيات الذكاء الاصطناعي تُستعمل في العديد من الدول ولديها تأثير عالمي، فإن التعاون بين الدول يصبح أمرًا بالغ الأهمية. فوجود قوانين موازية ومتوافقة يساهم في تقليل التناقضات القانونية التي قد تعيق مكافحة الأضرار الناجمة عن هذه التقنيات.

٢.مكافحة الجرائم السيبرانية العابرة للحدود:

- الهجمات السيبرانية المتعلقة بالذكاء الاصطناعي قد تكون معقدة وتحدث عبر عدة دول في آن واحد. لذا، التعاون الدولي بين أجهزة إنفاذ القانون، مثل الشرطة الدولية (الإنتربول) ووكالات الأمن السيبراني، ضروري للتحري ومكافحة هذه الجرائم.

٣.الاستجابة السريعة للأزمات السيبرانية:

- في حال وقوع أزمة سيبرانية ناشئة عن الذكاء الاصطناعي (مثل اختراق أنظمة تستخدم الذكاء الاصطناعي)، يكون التعاون بين الدول أمرًا حاسمًا للتمكن من معالجة الأضرار وتقديم الدعم الفني والتقني لمكافحة هذه الهجمات.
- **سبل توحيد الجهود القانونية الدولية:**

١. إعداد معاهدات دولية: من الضروري العمل على صياغة معاهدات دولية مُلزمة بشأن الذكاء الاصطناعي والجرائم السيبرانية. مثل هذه المعاهدات يمكن أن تتناول مسائل عدة مثل حقوق الأفراد في الفضاء الرقمي، وكيفية التعامل مع الجرائم التي تشمل

تقنيات الذكاء الاصطناعي، وكذلك تحديد المسؤولية القانونية للأطراف المختلفة (مطورون، شركات، أو حتى حكومات).

٢. **توحيد المعايير القانونية:** يمكن للدول أن تعمل معًا لتطوير معايير قانونية مشتركة في مجالات مثل حماية البيانات، مسؤولية الشركات التي تطور تقنيات الذكاء الاصطناعي، معايير الأمن السيبراني، والمساءلة القانونية عن الأضرار الناجمة عن الذكاء الاصطناعي. هذه المعايير توفر أرضية مشتركة للعديد من القوانين الوطنية والدولية.

٣. **تعزيز تبادل المعلومات بين الدول:** التعاون بين الدول يجب أن يتضمن تبادل المعلومات بخصوص الهجمات السيبرانية والتهديدات للذكاء الاصطناعي. من خلال منصات مشتركة بين الدول، يمكن تيسير هذا التبادل وبالتالي تقليل الوقت اللازم في اكتشاف الحوادث والتعامل معها.

٤. **تأسيس هيئات رقابية دولية:** يمكن إنشاء هيئات رقابية دولية تشرف على تطوير واستعمال الذكاء الاصطناعي، مثل وضع معايير أخلاقية وقانونية لضمان الاستخدام الآمن. هذه الهيئات قد تكون مشابهة لمنظمات دولية مثل منظمة الصحة العالمية، لكن تركيزها سيكون على تطوير وتنظيم الذكاء الاصطناعي.

٥. **دعم حقوق الإنسان وحمايتها:** القوانين الدولية يجب أن تركز على صون حقوق الإنسان في العالم الرقمي. عند تطوير قوانين عالمية بشأن الذكاء الاصطناعي، يجب التأكد من حماية الخصوصية، الحريات المدنية، ومنع التمييز الذي قد ينتج عن استعمال تقنيات الذكاء الاصطناعي.

ثانيا: انشاء هيئات تحقيق دوليه متخصصة:

إنشاء هيئات تحقيق عالمية متخصصة في مجال الذكاء الاصطناعي والضرر السيبراني هو خطوة مهمة لضمان معالجة الحوادث التي تتعلق باستعمال هذه التقنيات بشكل فعّال وعادل. إليك بعض النقاط التي تبرز أهمية هذه الهيئات وتفاصيل عن كيفية تأسيسها:

١. **دور الهيئات العالمية المتخصصة:**

- **تحقيق الحوادث السيبرانية:** تتولى هذه الهيئات التحقيق في الحوادث السيبرانية المتعلقة بالذكاء الاصطناعي، مثل الاختراقات الأمنية أو الاستخدام المؤذي للذكاء الاصطناعي في الهجمات السيبرانية

(ISSN: 2537- 0758)

- **تحليل الآثار القانونية:** تقوم الهيئات بتحديد المسؤولية القانونية، بما في ذلك تحديد الأطراف المتورطة وتقسيم المسؤولية بين الدول، الشركات، والمطورين.
- **تنسيق الجهود بين الدول:** هذه الهيئات توفر منصة للتعاون بين الدول المختلفة للتعامل مع الحوادث التي تتخطى الحدود الوطنية.

٢. المهام الأساسية:

- **إجراء التحقيقات:** على غرار التحقيقات التي تقوم بها المنظمات الدولية في الجرائم العابرة للحدود، يجب أن تكون هذه الهيئات قادرة على جمع الأدلة وتحليلها من جميع الدول المعنية.
- **تقديم التقارير والنتائج:** رفع تقارير عن النتائج إلى المجتمع الدولي ودعوة الحكومات والمؤسسات الأخرى إلى اتخاذ الإجراءات اللازمة.
- اقتراح حلول للتنظيم القانوني: هذه الهيئات يمكنها أيضًا اقتراح تعديلات على التشريعات والسياسات الوطنية والدولية لمعالجة القضايا الناشئة بشكل أفضل.

٣. كيفية إنشاء هذه الهيئات:

- **التعاون الدولي:** يجب أن يتم تأسيس هذه الهيئات عبر اتفاقيات دولية بين الدول الأعضاء في منظمات مثل الأمم المتحدة أو الاتحاد الأوروبي. تتطلب العملية توافقًا عالميًا لضمان أن الهيئات تتمتع بالشرعية والقدرة على إجراء التحقيقات عبر الحدود.
- **البنية القانونية:** يجب إنشاء إطار قانوني واضح ينظم عمل الهيئات ويحدد نطاق صلاحياتها، وتوفير آليات لتنفيذ القرارات الدولية الصادرة عنها.
- التعاون مع المؤسسات الأمنية: الهيئات المتخصصة ستحتاج إلى التعاون الوثيق مع وكالات الأمن السيبراني الدولية، مثل الإنتربول ومنظمة الأمن السيبراني الأوروبية.

٤. أمثلة على الهيئات العالمية التي قد تؤدي دورًا مشابهًا:

- **الإنتربول:** يمكن للإنتربول، الذي يعنى بتنسيق الجهود بين أجهزة الشرطة الدولية، أن يكون له دور مكمل في التحقيقات المتعلقة بالذكاء الاصطناعي والهجمات السيبرانية.
- **اللجنة الدولية للصليب الأحمر:** في سياق النزاعات المسلحة واستعمال الذكاء الاصطناعي في الحروب، يمكن أن تلعب المنظمات الإنسانية دورًا في التحقيق في الهجمات التي تؤثر على المدنيين.

الخاتمة:

ما جرى تقديمه من تحديات قضائية أمام إثبات الضرر الإلكتروني في ظل تطور تقنيات الذكاء الاصطناعي، يتبين أن النظام الحقوقي في العديد من البلدان يواجه عسرًا في مواكبة هذا التطور السريع. فوجود ثغرات في التشريعات الحالية يعيق مقدرة المتضررين على الحصول على تعويض عادل، ويؤدي إلى صعوبة تحديد المسؤولية القضائية بدقة في الحوادث المتعلقة بالأمن السيبراني. لذا، فإنه من اللازم على المشرعين والجهات القانونية تطوير تشريعات مرنة وفعالة، تواكب تطور تقنيات الذكاء الاصطناعي وتضمن صون الحقوق القانونية للأفراد والمؤسسات. يجب أن تشمل هذه التشريعات تحديدًا دقيقًا للضرر السيبراني، وآليات واضحة للتحقيق وتوثيق البراهين الرقمية، إضافة إلى وضع قواعد صريحة لتوزيع المسؤولية بين الأطراف المعنية، سواء كانت الشركات التقنية أو الأفراد المستعملين. ختامًا، إن ضمان حماية الأفراد من الأضرار السيبرانية يتطلب تعاونًا دوليًا مستمرًا، وتحديثًا دائمًا للأنظمة القانونية بما يكفل تحقيق العدالة وحفظ الحقوق في ظل التكنولوجيا الحديثة.

أولاً- النتائج:

أسفر البحث في موضوع التحديات القانونية امام اثبات الضرر السيبراني في ظل تطور تقنيات الذكاء الاصطناعي عن جملة من النتائج القانونية، يمكن تلخيصها على النحو الآتي:

١. **تعقيد إثبات الضرر السيبراني:** تشير الاستنتاجات القانونية إلى أن إثبات الضرر السيبراني في ظل استخدام تقنيات الذكاء الاصطناعي يعد أمرًا بالغ الصعوبة بسبب الطبيعة المعقدة لهذه الأنظمة. حيث يصعب تحديد العلاقة السببية بين الأضرار الحاصلة والتقنيات المستخدمة، مما يؤدي إلى إبهام في تحديد المسؤولية القانونية.
٢. **تحديات في تحديد المسؤولية القانونية:** على الرغم من تطور تقنيات الذكاء الاصطناعي، تظل مشكلة تحديد المسؤولية القانونية قائمة. غالبًا ما يصعب تحديد من يتحمل المسؤولية عن الأضرار الناتجة عن الخوارزميات أو الأنظمة المدعومة بالذكاء الاصطناعي، سواء كان ذلك المطورون، الشركات المالكة للتقنيات، أو المستخدمون النهائيون.
٣. **الفجوة التشريعية:** الاستنتاجات تشير إلى وجود فجوات كبيرة في التشريعات الحالية التي تعالج القضايا المتعلقة بالضرر السيبراني. معظم القوانين الحالية لا تغطي بشكل كافٍ التحديات التي يفرضها الذكاء الاصطناعي، مما يستدعي ضرورة

(ISSN: 2537- 0758)

تحديث هذه التشريعات لتشمل القضايا المستجدة المتعلقة بالأمن السيبراني والتكنولوجيا الحديثة.

٤. **صعوبة حماية البيانات الشخصية والخصوصية:** مع تطور تقنيات الذكاء الاصطناعي، أصبح من الصعب ضمان حماية البيانات الشخصية والخصوصية، مما يعزز من تعقيد إثبات الأضرار المتعلقة بانتهاك هذه الحقوق. وقد يؤدي ذلك إلى تصاعد النزاعات القانونية المتعلقة بكيفية جمع، معالجة، واستخدام البيانات الشخصية في الأنظمة المدعومة بالذكاء الاصطناعي.

٥. **التهديدات العابرة للحدود الوطنية:** الاستنتاجات القانونية تشير أيضًا إلى التحديات المرتبطة بالقضايا السيبرانية العابرة للحدود. حيث أن الأضرار الناتجة عن الهجمات السيبرانية أو الانتهاكات القانونية في هذا السياق قد تتجاوز حدود الدول، مما يعقد من عملية اتخاذ الإجراءات القانونية المناسبة في محاكم دولية أو إقليمية.

٦. **صعوبة جمع الأدلة الإلكترونية:** من أهم الاستنتاجات القانونية التي تم التوصل إليها هي صعوبة جمع الأدلة الإلكترونية في حالة حدوث ضرر سيبراني. قد يكون من الصعب في بعض الحالات تتبع الأفعال المسببة للضرر بسبب التشفير أو تقنيات التلاعب الحديثة التي يمكن أن تتيح إخفاء الأدلة أو تعديلها.

٧. **ضرورة وضع أطر قانونية مرنة:** بناءً على الاستنتاجات المستخلصة، يتضح أن هناك حاجة ماسة إلى تطوير أطر قانونية مرنة وقابلة للتكيف مع التغيرات السريعة في مجال تقنيات الذكاء الاصطناعي. هذا يتطلب التشريع المتكامل الذي يوازن بين حماية الحقوق القانونية للأفراد واستمرار الابتكار التكنولوجي.

٨. **أهمية التعاون الدولي:** الاستنتاجات أظهرت أن التحديات القانونية المتعلقة بالضرر السيبراني لا يمكن معالجتها بشكل فردي من قبل الدول، بل تستدعي التعاون الدولي لتنظيم القوانين بشكل موحد يعالج القضايا العابرة للحدود ويوفر حماية فعالة من الأضرار السيبرانية.

بناءً على هذه الاستنتاجات، يصبح من الواضح أن النظام القانوني يحتاج إلى تطوير تشريعات جديدة وشاملة لمعالجة الأضرار السيبرانية في عصر الذكاء الاصطناعي، وضمان حقوق الأفراد في ظل التقنيات الحديثة.

ثانيا التوصيات:

استنادًا إلى ما تم التوصل إليه من نتائج، وبالنظر إلى التحديات القانونية المعاصرة التي تفرضها تطبيقات الذكاء الاصطناعي خاصه ف المجال السيبراني، فإن هذا البحث يوصي بما يلي:

- **تطوير تشريعات قانونية شاملة:** يُوصى بإنشاء تشريعات قانونية شاملة وواضحة تتناول كافة جوانب الضرر السيبراني الناجم عن تقنيات الذكاء الاصطناعي. يجب أن تشمل هذه التشريعات تعريفات دقيقة للضرر السيبراني، وأطر قانونية لمعالجة قضايا الأضرار المتعلقة بالأمن السيبراني، وحقوق الأفراد في ظل تقنيات الذكاء الاصطناعي.
- **تحديد المسؤولية القانونية بوضوح:** من الضروري تحديد المسؤولية القانونية بوضوح فيما يخص الأضرار السيبرانية الناتجة عن استخدام الذكاء الاصطناعي. يجب أن تشمل هذه التوصية تحديد المسؤولية بين مختلف الأطراف: مطوري التكنولوجيا، الشركات المالكة للأنظمة، والأفراد المستخدمين. كما يجب تحديد مدى المسؤولية في حال كانت الأخطاء ناتجة عن خلل في الخوارزميات أو الانحياز في البيانات.
- **تحقيق التوازن بين حماية الخصوصية والتطور التكنولوجي:** يجب وضع تشريعات تحمي حقوق الخصوصية وحماية البيانات الشخصية، مع مراعاة ضرورة التطور التكنولوجي. يُوصى بوضع قواعد واضحة لمعالجة البيانات الشخصية باستخدام تقنيات الذكاء الاصطناعي، مع ضمان الشفافية في كيفية جمع واستخدام هذه البيانات.
- **تعزيز التعاون الدولي في مكافحة الأضرار السيبرانية:** نظرًا لأن الأضرار السيبرانية قد تتجاوز الحدود الوطنية، فإن التعاون الدولي بين الدول أمر بالغ الأهمية. يجب تطوير اتفاقيات دولية موحدة بشأن الأمن السيبراني وحماية الحقوق القانونية عبر الحدود، وتنسيق الجهود لمواجهة التهديدات السيبرانية العابرة للحدود.
- **تطوير آليات فعالة لجمع الأدلة الرقمية:** يُوصى بإنشاء آليات فعالة لجمع الأدلة الرقمية في القضايا المتعلقة بالضرر السيبراني. يجب تدريب المحققين والمتخصصين في الأمن السيبراني على كيفية جمع الأدلة بشكل فعال وآمن، مع ضمان عدم تعديل أو إخفاء هذه الأدلة.

(ISSN: 2537- 0758)

- **إصلاح قوانين المسؤولية الجنائية المرتبطة بالتكنولوجيا:** ينبغي تحديث القوانين الجنائية لتشمل أفعالًا قد تنشأ نتيجة لاستخدام تقنيات الذكاء الاصطناعي، مثل الهجمات السيبرانية أو التلاعب بالأنظمة. يجب أن تشمل هذه القوانين عقوبات صارمة ضد الأفراد أو الكيانات التي تستغل تقنيات الذكاء الاصطناعي لإلحاق الضرر بالآخرين.
- **تشجيع تطوير تقنيات الذكاء الاصطناعي الآمنة والمسؤولة:** يُوصى بتشجيع الشركات والمطورين على تبني مبادئ الذكاء الاصطناعي الآمن والمسؤول. يجب وضع معايير قانونية وأخلاقية لتصميم وتطوير تقنيات الذكاء الاصطناعي، مع التأكيد على ضرورة مراجعة أنظمة الذكاء الاصطناعي بشكل دوري للكشف عن الثغرات أو الأخطاء التي قد تؤدي إلى أضرار.
- **تعزيز الوعي القانوني والتدريب المهني:** من الضروري توفير التدريب والوعي القانوني للمحامين والمحققين في القضايا المتعلقة بالضرر السيبراني. يجب أن يتلقى المحامون والمتخصصون في القانون تدريبًا متخصصًا لفهم التحديات الفنية المتعلقة بالذكاء الاصطناعي وكيفية التعامل مع الأدلة الرقمية في المحاكم.
- **إصدار تشريعات متخصصة في الذكاء الاصطناعي:** يُوصى بإصدار تشريعات خاصة بالذكاء الاصطناعي لضمان معالجته كجزء من النظام القانوني المعاصر. هذه التشريعات يجب أن تشمل تحديد المسؤوليات، المعايير الأخلاقية، وأطر عمل واضحة لتقييم الأضرار الناجمة عن تقنيات الذكاء الاصطناعي.
- **الاستفادة من الذكاء الاصطناعي لتحسين النظام القانوني:** من المهم استخدام تقنيات الذكاء الاصطناعي نفسها لتحسين فعالية النظام القانوني في التعامل مع الأضرار السيبرانية. يمكن توظيف الذكاء الاصطناعي في تحليل البيانات القانونية، تحسين الإجراءات القضائية، وتقديم المشورة القانونية في القضايا المعقدة المتعلقة بالأمن السيبراني.

باتباع هذه التوصيات، يمكن للأنظمة القانونية أن تكون أكثر استعدادًا لمواكبة التحديات القانونية التي تطرأ بسبب تطور تقنيات الذكاء الاصطناعي، وضمان حماية الحقوق وحل النزاعات بشكل عادل وفعّال في عالم تزداد فيه التحديات السيبرانية.

قائمة المراجع

أولًا– المواد القانونية والأحكام القضائية:

- المادة ١٦٣ من القانون المدني المصري – تنص على أن كل خطأ سبب ضررًا للغير يُلزم من ارتكبه بالتعويض.
- القانون المصري رقم ١٧٥ لسنة ٢٠١٨ – ينظم مكافحة جرائم تقنية المعلومات ويحدد مسؤوليات المتسببين في الأضرار الإلكترونية.
- نظام مكافحة الجرائم المعلوماتية السعودي (٢٠٠٧) – يجرّم الاعتداءات السيبرانية ويحدد العقوبات المتعلقة بالأمن المعلوماتي.
- قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ – يُعالج الحقوق الرقمية للمستخدمين والضرر الناتج عن إساءة استخدام البيانات.
- اللائحة العامة لحماية البيانات (GDPR) الأوروبية – تنظم جمع ومعالجة البيانات الشخصية وتفرض مسؤولية قانونية على منتهكيها.
- قضية Loomis v. Wisconsin (٢٠١٦) – تناولت شرعية استخدام الذكاء الاصطناعي في إصدار الأحكام القضائية ومدى قابلية تفسير نتائجه.
- قضية Schrems II – محكمة العدل الأوروبية (٢٠٢٠) – أكدت على ضرورة حماية البيانات المنقولة خارج الاتحاد الأوروبي من المعالجة الآلية غير الآمنة.
- أحكام المحاكم الإماراتية في قضايا الابتزاز السيبراني (٢٠٢١–٢٠٢٣) – طبقت قوانين الجرائم الإلكترونية ضد استخدام الذكاء الاصطناعي في ارتكاب جرائم إلكترونية.
- محمد أبو زيد، المسؤولية المدنية عن الأضرار الناتجة عن الذكاء الاصطناعي، دار النهضة العربية، ٢٠٢٢ – دراسة تحليلية موسعة حول مسؤولية التقنيات الذكية.

ثانيًا– الكتب والمؤلفات:

- د. محمد أبو زيد، المسؤولية المدنية عن الأضرار الناتجة عن الذكاء الاصطناعي، دار النهضة العربية، القاهرة، ٢٠٢٢.
- د. سامي جمال الدين، الجرائم الإلكترونية والمسؤولية الجنائية عنها، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٠.
- د. عبد الفتاح بيومي حجازي، الجرائم الإلكترونية في ضوء التشريعات العربية والمقارنة، دار الفكر الجامعي، ٢٠٢١.
- د. أحمد فتحي سرور، الوسيط في قانون العقوبات – القسم العام، دار النهضة العربية، الطبعة الحديثة.
- د. سليمان المطاوي، نظرية الإثبات في القانون، دار الفكر العربي، القاهرة، ٢٠١٨.

(ISSN: 2537- 0758)

- د. محمد القاسم، حجية الأدلة الرقمية في الإثبات المدني والجنائي، دار النهضة العربية، ٢٠١٩.
- در شريف درويش اللبان: تكنولوجيا النشر الصحفي، الاتجاهات الحديثة، الدار المصرية اللبنانية، القاهرة، ٢٠٠١.
- عبد الله محمد الهويمل: الذكاء الاصطناعي والمسؤولية القانونية المدنية والجنائية، الرياض: مكتبة القانون الجامعية، ٢٠٢١.
- عبد الله محمد الهويمل، الذكاء الاصطناعي والمسؤولية القانونية المدنية والجنائية، الرياض: مكتبة القانون الجامعية، ٢٠٢١.
- ياسين الجبوري: الوجيز في شرح القانون المدني الأردني "مصادر الحقوق الشخصية مصادر الواجب: دراسة مقارنة" دار الثقافة للنشر والتوزيع عمان، ٢٠١١.

ثالثًا– الأبحاث والرسائل العلمية:

- حسام الدين عبد الله، التحديات القانونية في مواجهة الذكاء الاصطناعي: دراسة تحليلية في المسؤولية المدنية، رسالة ماجستير، جامعة القاهرة، كلية الحقوق، ٢٠٢٢.
- نورا العتيبي، المسؤولية القانونية عن الأضرار الناتجة عن استخدام الذكاء الاصطناعي في القانون السعودي، رسالة ماجستير، جامعة الملك سعود، ٢٠٢٣.
- سارة إبراهيم، إثبات الجرائم المعلوماتية في القانون المصري، بحث منشور في مجلة الدراسات القانونية المعاصرة، العدد ١٨، ٢٠٢٢.
- عبد الرحمن آل الشيخ، الأدلة الرقمية في قضايا الجرائم السيبرانية، بحث منشور في المجلة السعودية للدراسات القانونية، ٢٠٢٣.
- إيهاب محمد، التكييف القانوني للأفعال الضارة الناتجة عن نظم الذكاء الاصطناعي، مجلة الحقوق المعاصرة، جامعة عين شمس، ٢٠٢٣.
- هدى سالم، الحماية القانونية للبيانات الشخصية في ظل استخدام الذكاء الاصطناعي، رسالة دكتوراه، جامعة تونس المنار، كلية الحقوق، ٢٠٢٣.

رابعًا– المجلات والدوريات المُحكّمة:

- مجلة القانون والتقنية – جامعة الأمير نايف للعلوم الأمنية، العدد ١٢، ٢٠٢٣، "التكييف القانوني لأضرار الذكاء الاصطناعي في نطاق الجريمة السيبرانية."
- المجلة المصرية للقانون والاقتصاد – كلية الحقوق، جامعة القاهرة، العدد ٤٥، ٢٠٢٢، "أثر الذكاء الاصطناعي على قواعد الإثبات المدني في الجرائم الإلكترونية."
- مجلة البحوث القانونية والاقتصادية – جامعة المنصورة، العدد ٧٦، ٢٠٢٣، "حجية الأدلة الرقمية في الإثبات القانوني للأضرار السيبرانية."
- مجلة الشريعة والقانون – جامعة الإمارات، العدد ٨٥، ٢٠٢٢، "المسؤولية المدنية الناشئة عن استخدام أنظمة الذكاء الاصطناعي في بيئة إلكترونية.

- حمد فوزي عبد الرحيم: "الذكاء الاصطناعي والتزييف العميق: تهديدات رقمية للحق في الخصوصية والأمن القومي"، مجلة القانون والتكنولوجيا الحديثة، العدد٢، ٢٠٢٣.
- حنان محمد عبد العال: التزييف العميق كأحد تطبيقات الذكاء الاصطناعي: التحديات القانونية والواقع التشريعي العربي، مجلة القانون والتكنولوجيا، جامعة الإسكندرية، العدد ٧، ٢٠٢٣.
- هشام فتحي عبد المقصود: "المسؤولية الجنائية عن جرائم التزييف العميق في القانون المصري"، مجلة البحوث القانونية والاقتصادية – كلية الحقوق، جامعة المنصورة، العدد (٩٠)، سنة ٢٠٢٣.
- وليد عبد الحميد الشافعي: المسؤولية القانونية عن استخدام الذكاء الاصطناعي في إنتاج المحتوى الرقمي: دراسة تحليلية في ضوء القانون المقارن، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد ٨١، ٢٠٢٢.
- أحمد اسماعيل: ايدلوجيا الإعلام الجديد والوعي الزائف، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، برلين، العدد ٨، أغسطس / ٢٠١٨.
- مصطفى صبري عبد الجواد: "التنظيم القانوني لاستخدام تقنيات الذكاء الاصطناعي في المجال الإعلامي: دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، جامعة المنوفية، العدد ٧٧، ٢٠٢٣.
- عبير عبد الله إبراهيم: "الذكاء الاصطناعي والجرائم الإلكترونية: دراسة قانونية"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد ٨٣، ٢٠٢٣.
- عمرو عبد الرحمن أبو العطا: "تنظيم المحتوى الرقمي في ظل الذكاء الاصطناعي: نحو إطار قانوني متوازن"، المجلة المصرية للدراسات القانونية والتقنية، العدد١٢، ٢٠٢٣.
- فؤاد عبد المنعم رياض: "الحق في الخصوصية وحمايته في ضوء الدستور والقانون المصري"، مجلة الحقوق – جامعة الكويت، العدد ٤، السنة ٣٦، ٢٠١٢.
- محمد عبد الفتاح عبد الله أبو زيد: "المسؤولية المدنية عن إساءة استخدام تقنيات الذكاء الاصطناعي" مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، العدد ٨٤، ٢٠٢٣.

خامسًا– المواقع الالكترونية:

- أبو العلا، أ. س. (٢٠٢٣). المسئولية الجنائية عن مخاطر تقنيات الذكاء الاصطناعي. مجلة القانون والتكنولوجيا.
https://las.journals.ekb.eg/article_343874.html

(ISSN: 2537- 0758)

- البيومي، ر. إ. ع. (٢٠٢٣). الحماية القانونية من مخاطر الذكاء الاصطناعي: دراسة تحليلية مقارنة. مجلة القانون. https://jlaw.journals.ekb.eg/article_325097.html
- الديب، أ.، & أمين، د. إ. (٢٠٢٤). انعكاسات الذكاء الاصطناعي على قواعد الإثبات. المجلة المصرية للعلوم القانونية. https://mjle.journals.ekb.eg/article_386604.html
- الأسيوطي، أ. م. س. (٢٠٢٠). حماية التصرفات القانونية وإثباتها عبر تطبيق الذكاء الاصطناعي. الباحث العربي. https://journal.carjj.org/index.php/AR/article/view/16
- الإيادي، ح. ع. ع. م. (٢٠٢٢). الدليل السيبراني المستمد من الذكاء الاصطناعي. مجلة القانون. https://jlaw.journals.ekb.eg/article_269910.html

سادسًا– مراجع باللغة الأجنبية:

1. Kingston, J. (2018). *Artificial Intelligence and Legal Liability.* arXiv. https://arxiv.org/abs/1802.07782

2. Musser, M., et al. (2023). *Adversarial Machine Learning and Cybersecurity: Risks, Challenges, and Legal Implications.* arXiv. https://arxiv.org/abs/2305.14553

3. Fernández Llorca, D., et al. (2022). *Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof.* arXiv. https://arxiv.org/abs/2211.01817

4. Oseni, A., et al. (2021). *Security and Privacy for Artificial Intelligence: Opportunities and Challenges.* arXiv. https://arxiv.org/abs/2102.04661

5. Marta, P., et al. (2023). *AI and Cybersecurity: Possible New Risks and Legal Implications.* New York Law Journal. https://www.law.com/newyorklawjournal/2023/05/08/ai-and-cybersecurity-possible-new-risks-and-legal-implications/

6. Alvarez & Marsal. (2023). *AI Raises Stakes Across Cybersecurity and Disputes Landscape.* https://www.alvarezandmarsal.com/insights/ai-raises-stakes-across-cybersecurity-and-disputes-landscape

7. IoTSI. (2023). *Legal Challenges in AI-Driven Cybersecurity: Attribution, Accountability, and Regulatory Solutions.* https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/152-legal-challenges-in-ai-driven-cybersecurity-attribution-accountability-and-regulatory-solutions

8. Law Society. (2023). *Legal Frameworks for AI and Cybercrime: Navigating Current Challenges.* https://lawsociety.blog/legal-frameworks-for-ai-and-cybercrime/

9. Legal Service India. (2023). *AI and Cybersecurity Law: Protecting Against AI-Powered Cyber Threats.* https://www.legalserviceindia.com/legal/article-13307-ai-and-cybersecurity-law-protecting-against-ai-powered-cyber-threats.html

10. IntechOpen. (2023). *Cybersecurity Global Clashes in the Era of AI.* https://www.intechopen.com/online-first/89430