

" المسؤولية الجنائية الناشئة عن استخدامات الذكاء الاصطناعي في الجرائم الإلكترونية "

إعداد الطالب/

نايف محمد فهد القحطاني

العام الدراسي:

٢٠٢٥

مقدمة:

إن الحمد لله، نحمده ونستعينه ونستغفره، ونعوذ بالله من شرور أنفسنا ومن سيئات أعمالنا، من يهده الله فهو المهتد، ومن يضلل فلا هادي له، وأشهد أن لا إله إلا الله وحده لا شريك له، وأشهد أن محمدًا عبده ورسوله، وبعد: شهد العالم منذ منتصف القرن العشرين تطورًا متسارعًا في مجال التكنولوجيا، حيث بدأت ملامح الثورة الرقمية بالظهور تدريجيًا، وصولًا إلى مرحلة الذكاء الاصطناعي التي تعد واحدة من أبرز الابتكارات التقنية في العصر الحديث. لقد أحدث الذكاء الاصطناعي تغييرًا جذريًا في طريقة تفكيرنا وتعاملنا مع مختلف الأنشطة اليومية. فقد أصبحت هذه التقنية المحرك الأساسي للكثير من العمليات المعقدة، حيث تُستخدم في تحليل البيانات الضخمة، التنبؤ بالسلوكيات، وأداء مهام كانت في الماضي تتطلب التدخل البشري الكامل.

هذا التقدم الكبير في مجال الذكاء الاصطناعي لم يأت دون تحديات، بل فتح الباب أمام إشكاليات جديدة وغير مسبوقة، خصوصًا في المجال القانوني. من أبرز هذه التحديات ما يتعلق بالمسؤولية الجنائية، حيث ظهرت تساؤلات عديدة بشأن كيفية التعامل مع الجرائم التي يكون الذكاء الاصطناعي طرفًا فيها، سواء كأداة أو كعنصر مستقل يقوم بأداء أفعال يمكن أن تُصنّف كجرائم.

الجرائم الإلكترونية تُعد مثالًا بارزًا على التحديات التي أفرزها الذكاء الاصطناعي. فهي جرائم معقدة تعتمد على التكنولوجيا الحديثة، وتشمل عمليات مثل اختراق الأنظمة الإلكترونية، التلاعب بالبيانات، الهجمات السيبرانية، والتزييف العميق. هذه الجرائم أصبحت أكثر تقدمًا بفضل قدرات الذكاء الاصطناعي، الذي يمكنه تعلم الأنماط واستخدامها بطرق تفوق القدرات البشرية التقليدية.

على سبيل المثال، تبرز تقنية "التزييف العميق" كإحدى التطبيقات المثيرة للجدل للذكاء الاصطناعي، حيث يمكن استخدامها لإنشاء مقاطع فيديو مزيفة لكنها واقعية تمامًا، مما يثير مشكلات قانونية تتعلق بتشويه السمعة، التزوير، وحتى التحريض على جرائم. كما أن استخدام البرمجيات الخبيثة المزودة بالذكاء الاصطناعي يُعقد جهود الجهات الأمنية في تتبع مصدر الهجمات السيبرانية، نظرًا لقدرتها على التكيف والاختفاء.

هذه الجرائم تطرح إشكاليات قانونية معقدة تتعلق بتحديد المسؤولية الجنائية. فالقوانين التقليدية غالبًا ما تُبنى على فرضية أن الجريمة تُرتكب من قبل إنسان ذي إرادة ووعي. لكن عندما يكون الفاعل نظام ذكاء اصطناعي، تبرز

تساؤلات حول من يجب أن يتحمل المسؤولية. هل هي الشركة المطورة للنظام؟ أم المبرمج الذي صمم الخوارزمية؟ أم المستخدم الذي استغل النظام لأغراض غير مشروعة؟

على الجانب الآخر، يبرز تساؤل آخر أكثر عمقاً: هل يمكن تحميل الذكاء الاصطناعي نفسه مسؤولية جنائية؟ وهل يمكن اعتباره "شخصاً معنوياً" له إرادة مستقلة عن صانعه أو مستخدمه؟ هذه التساؤلات ليست مجرد فرضيات فلسفية، بل تمثل تحدياً حقيقياً للأنظمة القانونية حول العالم.

إضافة إلى ذلك، تعكس هذه القضية أبعاداً اجتماعية وأخلاقية عميقة. فالجرائم الإلكترونية المدعومة بالذكاء الاصطناعي لا تقتصر على الأضرار الفردية، بل تمتد إلى تهديد الأمن القومي، خصوصاً عندما تستهدف البنى التحتية الحيوية مثل شبكات الطاقة، المؤسسات المالية، أو أنظمة الصحة. كما أن الاعتماد المتزايد على الذكاء الاصطناعي في القطاعات المختلفة يجعل من الصعب الفصل بين الجاني والضحية في كثير من الأحيان، حيث يمكن أن يتحول المستخدم إلى ضحية لعيوب النظام نفسه.

ومع ازدياد هذه التحديات، أصبح من الضروري إعادة التفكير في الإطار القانوني الحالي، الذي صُمم في زمن لم يكن يتصور فيه أحد أن الآلة قد تصبح شريكاً مباشراً في ارتكاب الجريمة.

ومن هنا تبرز الحاجة إلى دراسة المسؤولية الجنائية في الجرائم الإلكترونية التي تعتمد على الذكاء الاصطناعي، لفهم التحديات القانونية المستجدة واقتراح حلول تشريعية فعالة.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في التحديات التي تواجه القانون الجنائي في تحديد المسؤولية الجنائية في الجرائم الإلكترونية التي يكون الذكاء الاصطناعي جزءاً منها. وتواجه القوانين الجنائية تحدياً في مواكبة التطورات التقنية المرتبطة بالذكاء الاصطناعي، وذلك لضمان تحقيق العدالة وحماية المجتمع من الجرائم المستحدثة.

أهمية الدراسة:

أولاً: الأهمية العلمية:

تتمثل الأهمية العلمية لهذه الدراسة في إثراء المعرفة القانونية حول الذكاء الاصطناعي من خلال تحليل الإشكاليات المتعلقة بمسؤوليته الجنائية. تُساهم الدراسة في سد الفجوات المعرفية الموجودة في الأبحاث السابقة عبر

تقديم رؤية شاملة حول استخدامات الذكاء الاصطناعي في الجرائم الإلكترونية، مما يدعم تطوير نظريات قانونية جديدة تتماشى مع التطورات التقنية.

ثانياً: الأهمية العملية:

تنعكس الأهمية العملية للدراسة في توفير إطار قانوني متكامل يمكن الاستفادة منه في تطوير التشريعات الوطنية والدولية لمكافحة الجرائم الإلكترونية الناتجة عن الذكاء الاصطناعي. كما تقدم الدراسة أدوات عملية للمشرعين وصناع القرار لتعزيز الحماية القانونية والاجتماعية، مما يساهم في الوقاية من الجرائم وضمان أمن المعلومات.

تساؤلات الدراسة

- ١- هل يمكن تحميل الذكاء الاصطناعي مسؤولية جنائية مباشرة؟
- ٢- ما هو الدور الذي يلعبه الذكاء الاصطناعي في الجرائم الإلكترونية؟
- ٣- ما الجهة التي يجب أن تتحمل المسؤولية الجنائية في حال ارتكب الذكاء الاصطناعي جريمة إلكترونية؟
- ٤- ما التعديلات القانونية للتعامل مع المسؤولية الجنائية للذكاء الاصطناعي؟
- ٥- ما مدى إمكانية مساءلة الذكاء الاصطناعي نفسه؟

أهداف الدراسة:

- ١- تحليل الأطر القانونية القائمة لتحديد المسؤولية الجنائية في الجرائم الإلكترونية.
- ٢- دراسة مفهوم الذكاء الاصطناعي ودوره في الجرائم الإلكترونية.
- ٣- استكشاف الفجوات القانونية المتعلقة بمسؤولية الذكاء الاصطناعي.
- ٤- تقديم مقترحات لتطوير القوانين الجنائية بما يتناسب مع تطورات الذكاء الاصطناعي.

فروض الدراسة:

- ١- الذكاء الاصطناعي لا يتمتع بكيان قانوني مستقل، وبالتالي لا يمكن مساءلته جنائياً بذاته وفقاً للقوانين التقليدية.

٢- الجرائم الإلكترونية التي يعتمد فيها الجاني على الذكاء الاصطناعي أكثر تعقيداً من الجرائم التقليدية، مما يتطلب أدوات قانونية وتقنية متطورة لمواجهتها.

٣- يمكن تحميل المسؤولية الجنائية عن الجرائم المرتكبة باستخدام الذكاء الاصطناعي لأكثر من طرف، مثل المطور، المبرمج، أو المستخدم، وفقاً لدوره في تنفيذ الجريمة.

٤- التزييف العميق وتقنيات الذكاء الاصطناعي الأخرى تمثل تهديداً قانونياً واجتماعياً متزايداً، وقد تؤثر على مصداقية الأدلة القانونية في المحاكم.

٥- القوانين الجنائية الحالية غير كافية لمواجهة تحديات الذكاء الاصطناعي في الجرائم الإلكترونية، مما يستدعي استحداث تشريعات متخصصة.

٦- استخدام الذكاء الاصطناعي في الجرائم السيبرانية يجعل من الصعب تتبع الجناة، مما يستوجب تطوير آليات تحقيق رقمية متقدمة.

٧- الذكاء الاصطناعي قد يُستخدم لأغراض مشروعة وغير مشروعة على حد سواء، مما يعقد عملية تصنيف الأفعال الجنائية المرتبطة به.

٨- هناك حاجة ملحة لوضع إطار قانوني يحدد متى تكون الشركة المطورة مسؤولة عن الأفعال غير المشروعة التي يقوم بها نظام الذكاء الاصطناعي الخاص بها.

٩- يجب إعادة النظر في مفهوم الإرادة والنية الإجرامية عند التعامل مع الذكاء الاصطناعي في الجرائم الإلكترونية، حيث يمكن أن يكون الفعل الجرمي ناتجاً عن خلل في الخوارزمية وليس عن قصد إجرامي بشري.

١٠- الأمن القومي قد يتعرض للخطر نتيجة الاستخدام غير القانوني للذكاء الاصطناعي، مما يستوجب تعاوناً دولياً لتنظيم هذه التقنية قانونياً.

١١- يمكن أن تساهم تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية بقدر ما يمكن استخدامها لارتكابها، مما يستوجب تفعيل استخدامها في التحقيقات الجنائية.

١٢- هناك حاجة لوضع معايير قانونية جديدة لتقييم مدى مسؤولية الذكاء الاصطناعي عن الأضرار الناتجة عن قراراته المستقلة.

الدراسات السابقة:

الدراسة الأولى: خالد، صقر (٢٠٢١). المسؤولية الجنائية عن أفعال الذكاء الاصطناعي - دراسة تحليلية استشرافية. مجلة روح القوانين، ٣٣(٩٦)، ١-١٥٦.

النتائج:

- ١- عدم وضوح الوضع القانوني للذكاء الاصطناعي كشخصية اعتبارية أو كأداة.
- ٢- صعوبة تحديد المسؤولية عند استخدام الذكاء الاصطناعي كأداة لارتكاب الجرائم الإلكترونية.
- ٣- الحاجة إلى تحديث التشريعات القانونية لمواكبة التقدم التكنولوجي.

التوصيات:

- ١- تبني تعريف قانوني واضح للذكاء الاصطناعي.
- ٢- تطوير إطار تشريعي يحدد المسؤولية الجنائية لمستخدمي الذكاء الاصطناعي.
- ٣- تعزيز التعاون الدولي لتقنين الجرائم الإلكترونية المتعلقة بالذكاء الاصطناعي.

أوجه التشابه مع دراستي:

- كلا الدراستين تناقشان مسؤولية استخدام الذكاء الاصطناعي في الجرائم الإلكترونية.
- تركّز دراستي أيضًا على معالجة الغموض التشريعي.

أوجه الاختلاف:

- دراستي أكثر تخصيصًا في ربط المسؤولية الجنائية بتطبيقات الذكاء الاصطناعي في الجرائم الإلكترونية، بينما هذه الدراسة تركّز على الذكاء الاصطناعي بشكل عام.

الدراسة الثانية: إبراهيم، علي أحمد. (٢٠٢٣). الجرائم الإلكترونية واستخدام الذكاء الاصطناعي - دراسة تحليلية. المجلة القانونية، ١٥ (٤٢)، ١٢٣-١٥٠.

النتائج:

١- الجرائم الإلكترونية باستخدام الذكاء الاصطناعي أصبحت أكثر تعقيداً بسبب القدرة على التعلم الذاتي.

٢- تحديات إثبات النية الجنائية عند استخدام تقنيات الذكاء الاصطناعي.

٣- ضعف الأنظمة القانونية في رصد ومقاضاة الجرائم المعتمدة على الذكاء الاصطناعي.

التوصيات:

١- إنشاء هيئة متخصصة للتحقيق في الجرائم الإلكترونية المتعلقة بالذكاء الاصطناعي.

٢- تدريب القضاة والمحامين على فهم تقنيات الذكاء الاصطناعي.

٣- وضع بروتوكولات لتحديد المسؤوليات بين المطورين والمستخدمين.

أوجه التشابه مع دراستي:

- كلاهما يبحث في التحديات التي يفرضها الذكاء الاصطناعي على النظام القانوني.

- التركيز على ضرورة تطوير التشريعات.

أوجه الاختلاف:

دراستي أكثر شمولاً من حيث تناول المسؤولية الجنائية بكافة جوانبها، بينما هذه الدراسة ركزت على الجانب العملي (التحديات والأنظمة).

الدراسة الثالثة: باسل محمد. (٢٠١٦). أثر الذكاء الاصطناعي في تطور الجرائم الإلكترونية. المجلة القانونية. ٣٣ (٧٤).

النتائج:

١- الذكاء الاصطناعي يساهم في تحسين أساليب التشفير وإخفاء الهوية، مما يزيد صعوبة التتبع.

٢- غياب التشريعات المحددة يؤدي إلى إفلات العديد من المجرمين من العقاب.

٣- معظم القوانين الحالية تُلقي المسؤولية فقط على المستخدم النهائي، وليس المطورين.

التوصيات:

١- تطوير تشريعات جديدة تشمل كل الفاعلين في الجرائم الإلكترونية.

٢- وضع معايير أخلاقية ملزمة للمطورين.

٣- توحيد الجهود الدولية لرصد الجرائم الإلكترونية التي تعتمد على الذكاء الاصطناعي.

أوجه التشابه مع دراستي:

- تناول نفس المجال، مع التركيز على الذكاء الاصطناعي كعنصر جديد في الجرائم الإلكترونية.

- أهمية التعاون الدولي والتشريعات الحديثة موجودة في كلا الدراستين.

أوجه الاختلاف:

- دراستي تُركز على المسؤولية الجنائية، بينما هذه الدراسة تناولت الأثر العام للذكاء الاصطناعي في الجرائم الإلكترونية.

المنطلقات النظرية للدراسة:

مع التطور السريع للذكاء الاصطناعي، أصبح لهذا المجال تأثير متزايد على مختلف جوانب الحياة، بما في ذلك الجريمة ومكافحتها. فبينما يسهم الذكاء الاصطناعي في تعزيز الأمن السيبراني وكشف الجرائم، فإنه في الوقت ذاته يتيح فرصاً جديدة لارتكاب الجرائم الإلكترونية بأساليب أكثر تعقيداً يصعب تتبعها. هذه التحولات تطرح إشكاليات قانونية جوهرية، تتعلق بتحديد المسؤول عن الأفعال الإجرامية التي تنفذها الأنظمة الذكية، ومدى إمكانية مساءلة الذكاء الاصطناعي جنائياً.

ولفهم هذه التحديات، من الضروري الانطلاق من مجموعة من الأسس النظرية التي تشكل الإطار العلمي والقانوني للدراسة. تشمل هذه المنطلقات الأبعاد القانونية التي تحدد نطاق المسؤولية الجنائية، والاعتبارات الفلسفية والأخلاقية المتعلقة بمساءلة الكيانات غير البشرية، بالإضافة إلى الجوانب التقنية التي توضح كيفية عمل الذكاء الاصطناعي في تنفيذ الجرائم الإلكترونية. كما تمتد هذه المنطلقات إلى البعد الاجتماعي الذي يناقش تأثير هذه الظاهرة على المجتمع، والمنظور الاقتصادي الذي يتناول آثار الجرائم الإلكترونية على الاقتصاد العالمي.

انطلاقاً من هذه الرؤية، تستند الدراسة إلى مجموعة من المنطلقات النظرية التي تساهم في تحليل وتفسير العلاقة بين الذكاء الاصطناعي والجريمة، وصولاً إلى مقترحات قانونية تهدف إلى تحقيق التوازن بين التطور التكنولوجي وحماية المجتمع من المخاطر الناجمة عنه.

١- المنطلق القانوني

يعتمد هذا المنطلق على تحليل الأطر القانونية الوطنية والدولية المتعلقة بمساءلة الذكاء الاصطناعي، ويشمل:

النظرية التقليدية للمسؤولية الجنائية: التي تشترط توافر الركنين المادي والمعنوي لتحميل الشخص المسؤولية.

القانون الجنائي المعلوماتي: الذي يتناول الجرائم الإلكترونية ويوضح مدى انطباقه على الجرائم المرتكبة بواسطة الذكاء الاصطناعي.

الاتفاقيات والمعاهدات الدولية: مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية ومدى كفايتها لتنظيم استخدام الذكاء الاصطناعي.

مبدأ الشرعية الجنائية: وكيفية التعامل مع الجرائم الناشئة عن الذكاء الاصطناعي في ظل غياب نصوص صريحة تجرم بعض الأفعال.

٢- المنطلق الفلسفي والأخلاقي

يركز هذا المنطلق على القضايا الأخلاقية والفلسفية المتعلقة بمساءلة الجنائية للذكاء الاصطناعي، ويشمل:

إشكالية المسؤولية الأخلاقية: هل يمكن اعتبار الذكاء الاصطناعي "فاعلًا" مسؤولًا أخلاقيًا أم أنه مجرد أداة في يد الإنسان؟

العدالة الجنائية: مدى تحقيق العدالة عند مساءلة الأفراد عن أفعال ارتكبها الذكاء الاصطناعي نتيجة تعلمه العميق أو قراراته المستقلة.

التوازن بين الابتكار وحماية المجتمع: ضرورة إيجاد توازن بين تطوير الذكاء الاصطناعي وتعزيز الضوابط القانونية لمنع استغلاله إجراميًا.

٣- المنطلق التقني

يرتبط هذا المنطلق بفهم طبيعة الذكاء الاصطناعي وآلية عمله وتأثيره على الجريمة، ويشمل:

آليات تعلم الآلة والتعلم العميق: كيف يتخذ الذكاء الاصطناعي قراراته وما مدى استقلاليته في تنفيذ الأوامر.

الأمن السيبراني: دور الذكاء الاصطناعي في تطوير أساليب جديدة لارتكاب الجرائم الإلكترونية وصعوبة تتبعها.

إشكالية القابلية للتلاعب: إمكانية اختراق أو تعديل أنظمة الذكاء الاصطناعي لجعلها أدوات لارتكاب الجرائم دون معرفة المالك الفعلي لها.

٤- المنطلق الاجتماعي

يركز هذا المنطلق على تأثير الذكاء الاصطناعي على المجتمع وارتباطه بالسلوك الإجرامي، ويشمل:

التغيرات الاجتماعية الناجمة عن الذكاء الاصطناعي: هل يمكن أن يؤدي استخدامه إلى زيادة الجريمة أو تقليلها؟

الثقة في الذكاء الاصطناعي: مدى تقبل المجتمع لمخرجات أنظمة الذكاء الاصطناعي وقراراتها، خاصة في المجالات الجنائية والقضائية.

دور الذكاء الاصطناعي في منع الجريمة: إمكانية استخدامه في التنبؤ بالجرائم واتخاذ تدابير وقائية.

٥- المنطلق الاقتصادي

يرتبط هذا المنطلق بتأثير الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي على الاقتصاد العالمي، ويشمل:

الخسائر الاقتصادية: الناجمة عن الجرائم الإلكترونية مثل الاحتيال المالي والتزيف العميق.

مسؤولية الشركات التقنية: مدى التزام الشركات بتطوير ذكاء اصطناعي آمن لا يمكن استغلاله إجراميًا.

تكلفة مكافحة الجرائم الإلكترونية: الحاجة إلى استثمارات ضخمة في الأمن السيبراني لمواجهة التهديدات الناجمة عن الذكاء الاصطناعي.

المنهجية وطرق البحث:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي والاستقرائي لتحليل القواعد العامة واللوائح التنظيمية والأدبيات القانونية السابقة ذات الصلة بالمسؤولية الجنائية الناشئة عن استخدامات الذكاء الاصطناعي في الجرائم الإلكترونية.

أدوات الدراسة:

تعتمد هذه الدراسة على مجموعة من الأدوات التي تساعد في جمع المعلومات وتحليلها للوصول إلى نتائج دقيقة حول المسؤولية الجنائية الناشئة عن استخدامات الذكاء الاصطناعي في الجرائم الإلكترونية. ومن أبرز الأدوات المستخدمة في الدراسة ما يلي:

١- تحليل الوثائق والمصادر القانونية

يتم الاعتماد على القوانين والتشريعات الوطنية والدولية ذات الصلة بالجرائم الإلكترونية والذكاء الاصطناعي.

دراسة السوابق القضائية والأحكام المتعلقة بالمسؤولية الجنائية في السياق التكنولوجي.

مراجعة الاتفاقيات والمعاهدات الدولية المتعلقة بالجريمة السيبرانية.

٢- التحليل القانوني والاستقرائي

فحص المبادئ القانونية المرتبطة بالمسؤولية الجنائية ومحاولة استقراء مدى قابليتها للتطبيق على الذكاء الاصطناعي.

تحليل الفجوات القانونية والفراغ التشريعي المتعلق بهذه المسألة.

٣- تحليل البيانات والتقارير الأمنية

مراجعة تقارير المؤسسات الأمنية والمعلوماتية حول الجرائم الإلكترونية الحديثة.

دراسة آليات الهجوم السيبراني المدعوم بالذكاء الاصطناعي وتأثيره على الأمن القانوني.

وتساعد هذه الأدوات في توفير رؤية شاملة لموضوع الدراسة، مما يساهم في تقديم توصيات دقيقة يمكن أن تساعد

في تطوير التشريعات الخاصة بالذكاء الاصطناعي والجرائم الإلكترونية.

حدود الدراسة:

١- الحدود الموضوعية:

تتناول الدراسة المسؤولية الجنائية الناشئة عن استخدامات الذكاء الاصطناعي في الجرائم الإلكترونية، مع التركيز

على التحديات القانونية المتعلقة بتحديد المسؤول عن الأفعال الإجرامية التي يكون الذكاء الاصطناعي طرفاً فيها،

سواء كمجرد أداة أو ككيان مستقل يتخذ قرارات ذات تأثير جنائي.

٢- الحدود الزمنية:

تغطي الدراسة التطورات القانونية والتشريعية المتعلقة بالذكاء الاصطناعي والجرائم الإلكترونية حتى عام ٢٠٢٥، مع

الاستناد إلى السوابق القانونية والأبحاث العلمية الحديثة ذات الصلة.

٣- الحدود المكانية:

تركز الدراسة على الإطار القانوني للمسؤولية الجنائية للذكاء الاصطناعي وفقاً للتشريعات الدولية، مع استعراض

بعض التجارب القانونية في الدول الرائدة في هذا المجال، مثل الاتحاد الأوروبي والولايات المتحدة، إضافة إلى بعض

الأنظمة القانونية العربية عند توفر البيانات.

٤- الحدود المنهجية:

تعتمد الدراسة على المنهج الوصفي التحليلي والاستقرائي، حيث يتم وصف وتحليل القوانين واللوائح التنظيمية

والأحكام القضائية السابقة، إلى جانب استقراء النصوص القانونية والآراء الفقهية ذات الصلة لاستخلاص أهم

التحديات والمقترحات التشريعية.

مفاهيم الدراسة ومصطلحاتها:

الذكاء الاصطناعي: ان مصطلح الذكاء الاصطناعي في اللغة مكون من كلمتين وهي:

الأولى: ذكاء تعني القدرة التي تدل على الحفظ والتأقلم مع المتغيرات الحديثة.

الثانية: اصطناعي تعني بناء على معاجم اللغة العربية، هو اسم ينسب إلى اصطناع، ويطلق على كل ما ينشأ

نتيجة أي فعل تم عن طريق صناعة، ويطلق أيضاً على كل ما هو موجود نتيجة فعل تدخلات غير بشرية.

ويقصد به "أنظمة تعتمد على تقنيات قادرة على جمع البيانات واستخدامها للتنبؤ أو تقديم التوصيات أو

اتخاذ القرارات، مع مستويات مختلفة من التحكم الذاتي، وذلك لاختيار أفضل إجراء لتحقيق أهداف محددة"^(١).

الجريمة الإلكترونية: "أي تصرف يُرتكب من خلال استخدام الحاسب الآلي أو الشبكة الإلكترونية، بما يخالف أحكام

هذا النظام"^(٢).

المسؤولية الجنائية في اللغة: تُعرّف المسؤولية الجنائية في اللغة على أنها اشتقاق من الفعل "سأل"، ويعني

التكليف أو المساءلة عن فعل أو تصرف معين. والمسؤولية تأتي من "المساءلة"، حيث يُطلب من الشخص تقديم تفسير

أو إجابة عن أمر ما قام به. وفي إطار اللغة العربية، يشير المصطلح إلى أن الفرد يُسأل ويُحاسَب على فعل ارتكبه ويجب

أن يتحمل تبعاته.

المطورين: هم الأفراد أو الجهات التي تقوم بتصميم وتطوير أنظمة الذكاء الاصطناعي والبرمجيات المتعلقة بها.

المستخدمون: هم الأفراد أو الجهات التي تقوم باستخدام أنظمة الذكاء الاصطناعي لتحقيق أغراض معينة، والتي قد

تشمل استخدامات غير قانونية مثل الجرائم الإلكترونية.

١- انظر: الموقع الإلكتروني للهيئة السعودية للبيانات والذكاء الاصطناعي، تم الزيارة بتاريخ ١١/٠٩/٢٠٢٤ م، وتم الاطلاع الساعة ١٢:٧ ص، من خلال الرابط التالي:

<https://sdaia.gov.sa/ar/SDAIA/about/Pages/AboutAI.aspx>.

٢- انظر: المادة رقم (١) من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨ هـ قرار مجلس الوزراء رقم ٧٩ بتاريخ ٢٠٢٨/٣/٧.

١٤٢٨ هـ.

تقسيم الدراسة

المبحث الأول: ماهية الذكاء الاصطناعي ودوره في الجرائم الإلكترونية

المطلب الأول: تطور مفهوم الذكاء الاصطناعي.

المطلب الثاني: دور الذكاء الاصطناعي في تطور الجريمة الإلكترونية.

المبحث الثاني: تحديات المسؤولية الجنائية للذكاء الاصطناعي في الجرائم الإلكترونية

المطلب الأول: مفهوم المسؤولية الجنائية وتطبيقاتها في الجرائم الإلكترونية

المطلب الثاني: التحديات القانونية للمسؤولية الجنائية للذكاء الاصطناعي

الخاتمة وفيها أهم النتائج والتوصيات

المصادر والمراجع:

أولاً: قائمة المصادر:

المعاجم اللغوية:

- الفيومي، أحمد بن محمد بن علي ثم الحموي. (١٣٣٣ هـ). المصباح المنير في غريب الشرح الكبير (ط. ٢، ص.

٢٩٧). القاهرة: دار المعارف.

- ابن منظور، محمد. (١٤١٤ هـ). لسان العرب (ط. ١). بيروت: دار صادر.

ثانياً: قائمة المراجع:

الكتب القانونية العامة:

- رشد، علي أحمد. (١٩٧٠ م). مبادئ القانون الجنائي (ط. ١). مكتبة سيد عبد الله وهبة.
- القهوجي، علي عبد القادر. (١٩٩٨ م). شرح قانون العقوبات القسم العام: المسؤولية الجنائية والجزاء الجنائي.
- حسني، محمود نجيب. (١٩٧٥ م). شرح قانون العقوبات اللبناني: القسم العام (ط. ٢). دار النقري.
- حسني، محمود نجيب. (١٩٩٠ م). القانون الجنائي: النظرية العامة للجريمة. دار النهضة العربية.

- سرور، أحمد فتحي. (٢٠٠٣ م). شرح قانون العقوبات: القسم العام. دار الشروق.

الكتب القانونية المتخصصة:

- خوالد أبو بكر (٢٠١٩ م). تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال. المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية (ط.١). برلين: ألمانيا.
- الدهان علي (٢٠١٠ م). معجم المصطلحات العلمية (الذكاء الاصطناعي). دمشق: دار الفكر.
- المهندس الحسيني، أسامة (٢٠٢١ م). الذكاء الاصطناعي والمداخل إلى لغة LISP. بيروت: دار الراتب الجامعية.
- بوبعاية نصيرة، د. الوافي شهرزاد، أ. بوتغان حمزة. (٢٠٢١ م). دور البيانات الضخمة والذكاء الاصطناعي في مواجهة وباء فيروس كورونا. مجلة الدراسات الإسلامية، ١٧(١)، ١٣١-١٥٠.
- كريستيان، يوسف. (٢٠٢٢ م). المسؤولية المدنية عن فعل الذكاء الاصطناعي (ط.١). بيروت: منشورات الحلبي الحقوقية.

المقالات الأكاديمية:

- السبيعي، ناصر. (٢٠٢١ م). مسؤولية المطورين في الجرائم الإلكترونية المتعلقة بالذكاء الاصطناعي. مجلة تكنولوجيا المعلومات والقانون، ١٤(٢)، ٨٨-١٠٥.
- السرحان، منصور. (٢٠٢٢ م). صعوبات إثبات المسؤولية في استخدام الذكاء الاصطناعي. المجلة العربية للقانون، ١٤(٣)، ٦٧-٨٢.
- العتيبي، راشد. (٢٠٢١ م). أهمية التوعية القانونية في استخدام الذكاء الاصطناعي. المجلة القانونية، ١٩(٢)، ٣٣-٤٨.
- العبيدي، كسار. (٢٠٢٣ م). التحديات القانونية للمسؤولية الجنائية للمستخدمين. المجلة العربية للحقوق، ١١(٤)، ٥٥-٧٢.

- يوسف، محمود. (٢٠٢١ م). أهمية مراقبة استخدام الذكاء الاصطناعي. *مجلة الدراسات القانونية*، ١٢ (٢)، ١١٢-١٣٠.
- الرفاعي، عامر. (٢٠٢٠ م). دور المستخدمين في توجيه أنظمة الذكاء الاصطناعي. *مجلة تكنولوجيا المعلومات*، ٩ (١)، ٧٨-٩٠.
- علي، فارس. (٢٠٢٢ م). الأخلاقيات في تطوير أنظمة الذكاء الاصطناعي. *مجلة الأخلاق وتكنولوجيا المعلومات*، ٢٤ (١)، ١٥-٢٩.
- الكندري، محمد. (٢٠٢٣ م). تشريع المسؤولية القانونية للذكاء الاصطناعي. *مجلة الدراسات السياسية*، ١٠ (١)، ٤٥-٦٧.
- الموسوي، رشيد. (٢٠٢٠ م). التحديات القانونية في تحقيقات الذكاء الاصطناعي. *مجلة القانون الدولي*، ٨ (٣)، ٧٨-٩٢.
- عبد الله، سعيد. (٢٠٢١ م). المسؤولية القانونية في عصر الذكاء الاصطناعي. *مجلة القانون والتكنولوجيا*، ١٥ (٢)، ٣٤-٥٦.
- العسيري، محمد. (٢٠٢٣ م). التحديات المرتبطة بالتعلم الذاتي في الذكاء الاصطناعي. *مجلة الذكاء الاصطناعي*، ٨ (١)، ٤٥-٦٠.
- المشاري، زياد. (٢٠٢٢ م). غياب الشخصية القانونية للذكاء الاصطناعي: تحديات قانونية. *المجلة القانونية*، ١٩ (٣)، ٦٠-٧٥.
- القحطاني، عايش. (٢٠٢٣ م). الخوارزميات ومسؤولية الذكاء الاصطناعي: دراسة قانونية. *المجلة العربية للأمن السيبراني*، ١٣ (٢)، ٣٢-٤٧.
- الحامد، سعد. (٢٠٢٢ م). استقلالية الأنظمة الذكية وتأثيرها على المسؤولية القانونية. *مجلة التكنولوجيا والقانون*، ١٥ (٤)، ٧٨-٩٢.

- الحارثي، منير. (٢٠٢١ م). استخدام الذكاء الاصطناعي في الأنظمة المالية والأمنية: المسؤوليات القانونية. *مجلة الدراسات القانونية*، ١٤ (٤)، ٥٥-٧٢.
- الفيصل، ناصر. (٢٠٢٣ م). الذكاء الاصطناعي والجرائم الإلكترونية: البحث عن المسؤولية الجنائية. *مجلة الأمن السيبراني*، ١٥ (١)، ١٠-٢٨.
- المسعودي، جابر. (٢٠٢٢ م). التحديات القانونية للذكاء الاصطناعي: المسؤولية الجنائية في عصر التقنية. *المجلة القانونية*، ٢١ (٢)، ٣٥-٥٠.
- العطار، صقر محمد، وعبد الإله محمد النوايسة. (٢٠٢٤ م). المسؤولية الجنائية الناجمة عن استخدام كيانات الذكاء الاصطناعي. *مجلة جامعة الشارقة للعلوم القانونية*، ٢١ (٢)، ٥٦١-٥٩٤.
- ضبيشه، محمد نجيب حامد عطية. (٢٠٢٤ م). المسؤولية الجنائية الناشئة عن جرائم الذكاء الاصطناعي: دراسة مقارنة. *مجلة روح القوانين، كلية الحقوق جامعة طنط، العدد الخاص بالمؤتمر العلمي الثامن*.

القوانين:

- نظام مكافحة الجرائم المعلوماتية، الصادر بالمرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨ هـ، وقرار مجلس الوزراء رقم (٧٩) بتاريخ ١٤٢٨/٣/٧ هـ.
- نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/١٩) بتاريخ ١٤٤٣/٢/٩ هـ، وقرار مجلس الوزراء رقم (٩٨) بتاريخ ١٤٤٣/٢/٧ هـ.

الوثائق الرسمية:

- الحكومة الروسية. (٢٠١٩). وثيقة رسمية مرسوم رقم ٤٩٠ بشأن إنشاء الاستراتيجية الوطنية للذكاء الاصطناعي الممتدة حتى عام ٢٠٣٠ م. تمت الزيارة بتاريخ ١٣/١٠/٢٠٢٤ م. عبر الرابط-<https://ai.gov.ru/en/national-strategy>.

[strategy](https://ai.gov.ru/en/national-strategy).

المواقع الإلكترونية:

- الهيئة السعودية للبيانات والذكاء الاصطناعي. (٢٠٢٤م). تم الاطلاع عليه بتاريخ ١١ سبتمبر ٢٠٢٤، من خلال

الرابط التالي:

<https://sdaia.gov.sa/ar/SDAIA/about/Pages/AboutAI.aspx>.

- الموقع الرسمي للجريدة الفرنسية. (٢٠٢٤م). تم الاطلاع عليه بتاريخ ١٩ سبتمبر ٢٠٢٤، من خلال الرابط التالي:

<https://www.legifrance.gouv.fr>.

المراجع الأجنبية:

المقالات الأكاديمية الأجنبية:

- Bada, M., & Sasse, M. A. (٢٠١٥). **Cybercrime and cybersecurity: A multidisciplinary approach**.
- Barfield, W., & Pagallo, U. (٢٠١٨). **Research Handbook on the Law of Artificial Intelligence**. Edward Elgar Publishing, pp. ١٢٠-١٤٥.
- Green, T. (٢٠٢١). **User Responsibility in AI Applications: Legal Challenges and Implications**. *Journal of AI and Law*, ١٤(٢), ١٢٣-١٣٧.
- Kesan, J. P., & Hayes, C. M. (٢٠١٢). **Mitigative counterstriking: Self-defense and deterrence in cyberspace**. *Harvard Journal of Law & Technology*.

- Matthias, A. (٢٠٠٤). **The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata.** *Ethics and Information Technology*, ٦(٣), ١٧٥-١٨٣.
- Nissenbaum, H. (٢٠١٠). **Privacy as contextual integrity.** *Washington Law Review*.
- Spiekermann, S., & Pallas, F. (٢٠٠٦). **Technology paternalism – wider implications of ubiquitous computing.** *Poiesis & Praxis*.
- Surden, H. (٢٠١٤). **Machine Learning and Law.** *Washington Law Review*, ٨٩, ٨٧-١١٥.

مراجع المواقع الإلكترونية الأجنبية:

- BankInfoSecurity. (٢٠٢٠, May ٢٧). **Separate phishing attacks target Wells Fargo, BOA customers.**

Retrieved from <https://www.bankinfosecurity.com/separate-phishing-attacks-target-wells-fargo-bo-a-customers-a-١٤٤٧٨>.

- Crucible Law. (٢٠٢٣, June ١٩). **Deepfake Evidence in Criminal Trials: The Emerging Dangers of Believing What You See and Hear.**

Retrieved from <https://crucible.law/insights/deepfake-evidence-in-criminal-trials-the-emerging-dangers-of-believing-what-you-see-and-hear>.

- Europol. (٢٠٢١). **Internet Organised Crime Threat Assessment (IOCTA) ٢٠٢١.**

Retrieved from <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-٢٠٢١>.

- FreeCodeCamp. (n.d.). **The History of AI.**

Retrieved from <https://www.freecodecamp.org/news/the-history-of-ai/>.

- IBM. (n.d.). **History of Artificial Intelligence.**

Retrieved from <https://www.ibm.com/think/topics/history-of-artificial-intelligence>.

- McKinsey & Company. (n.d.). **What is Artificial General Intelligence (AGI)?**

Retrieved from <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-artificial-general-intelligence-agi>.

- Talos Intelligence. (٢٠٢٣, April ١٣). **The Rise of AI-Powered Criminals.**

Retrieved from <https://blog.talosintelligence.com/the-rise-of-ai-powered-criminals>.

- Unite.AI. (٢٠٢٣). **Generative AI: The Idea Behind ChatGPT, DALL-E, Midjourney, and More.**

Retrieved from <https://www.unite.ai/generative-ai-the-idea-behind-chatgpt-dall-e-midjourney-and-more>.

مراجع القوانين الأجنبية:

- **Code Pénal** (French Penal Code).
- Council of Europe. (٢٠٠١). **Convention on Cybercrime (Budapest Convention).**

مراجع تقارير رسمية الأجنبية:

- ENISA. (٢٠٢٠). **Malware ebook: ETL ٢٠٢٠.**

Retrieved from <https://www.enisa.europa.eu/publications/report-files/ETL-translations/it/etl٢٠٢٠-malware-ebook-en-it.pdf/view>.