المجلة الدولية فى العلوم القانونية والمعلوماتية

The Responsibility of Artificial Intelligence for Cyber Crimes: A Comparative Legal Study

Ali Khadir Abbas Al-Saeedi[1,2,*]

[1] PhD student in Criminal Law and Criminology, Faculty of Law and Political Science, University of Mazandaran - Babolsar, Iran.
[2] Lecturer in the Faculty of Law and Political Science, Department of Law, Islamic University of Diwaniyah Branch.

Received: 10 Aug. 2025, Revised: 10 Sep. 2025, Accepted: 05 Oct. 2025.
Published online: 1 Jan. 2026.

Abstract: The world today is witnessing a rapid digital revolution led by artificial intelligence, which has become an active element in various aspects of life, including the cyber realm. Despite the numerous positives it provides, the use of artificial intelligence in committing cybercrimes has resulted in deep legal issues related to the extent to which this non-human entity can be held criminally liable. This research addresses the legal responsibility for cybercrimes committed using tools or systems reliant on artificial intelligence, focusing on the challenges facing the application of traditional concepts of criminal responsibility, such as moral element, awareness, and will. The research also highlights the positions of several comparative legislations, including European, American, and some Arab legislations, aiming to evaluate the extent to which these laws respond to technological changes and to reveal potential legislative gaps. The research concludes by presenting legislative recommendations aimed at developing a balanced legal framework that achieves justice and ensures the safe and responsible use of artificial intelligence technologies in the digital environment.

Keywords: artificial intelligence, cyber crimes, criminal liability, cyber law, smart algorithms, comparative legislation, deepfake.

*Corresponding author e-mail: alikhudhair9797@gmail.com

© 2026 SCINAT
ISCI Academy Publishing

مسؤولية الذكاء الاصطناعي عن الجرائم الإلكترونية: دراسة قانونية مقارنة

علي خضير عباس السعيدي.

طالب دكتوراه في القانون الجنائي وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة مازندران – بابلسر – إيران.
تدريسي في كلية القانون والعلوم السياسية قسم القانون في الجامعة الإسلامية فرع الديوانية.

الملخص: يشهد العالم اليوم ثورة رقمية متسارعة يقودها الذكاء الاصطناعي، الذي أصبح عنصرًا فاعلًا في مختلف مناحي الحياة ، بما في ذلك المجال السيبراني. وبالرغم من الإيجابيات العديدة التي يوفرها، فإن استخدام الذكاء الاصطناعي في تنفيذ الجرائم الإلكترونية قد أفرز إشكاليات قانونية عميقة تتعلق بمدى إمكانية مساءلة هذا الكيان غير البشري جنائيًا. يتناول هذا البحث دراسة المسؤولية القانونية عن الجرائم الإلكترونية التي يُرتكب بعضها عبر أدوات أو أنظمة تعتمد على الذكاء الاصطناعي، مع التركيز على التحديات التي تواجه تطبيق المفاهيم التقليدية للمسؤولية الجنائية، كالعنصر المعنوي والإدراك والإرادة. كما يُسلط البحث الضوء على مواقف عدد من التشريعات المقارنة، من بينها القانون الأوروبي، الأمريكي، وبعض التشريعات العربية، بهدف تقييم مدى استجابة هذه القوانين للمتغيرات التقنية، والكشف عن الثغرات التشريعية المحتملة، ويختتم البحث بتقديم توصيات تشريعية تهدف إلى تطوير إطار قانوني متوازن يحقق العدالة، ويضمن الاستخدام الآمن والمسؤول لتقنيات الذكاء الاصطناعي في البيئة الرقمية.

الكلمات المفتاحية: الذكاء الاصطناعي، الجرائم الإلكترونية، المسؤولية الجنائية، القانون السيبراني، الخوارزميات الذكية، التشريعات المقارنة، التزييف العميق.

المقدمة:

مع التطور التكنولوجي المتسارع، أصبح الذكاء الاصطناعي واحدًا من أبرز ملامح الثورة الصناعية الرابعة، حيث تغلغل في مختلف مناحي الحياة الإنسانية، من المجالات الطبية والتعليمية" إلى النظم العسكرية" والمالية. ولم تكن البيئة الرقمية بمعزل عن هذا التأثير، إذ لعب الذكاء الاصطناعي دورًا محوريًا في تحسين الخدمات السيبرانية" من جهة، وفي" فتح الباب أمام ظهور نمط جديد من الجرائم الإلكترونية من جهة أخرى، أكثر تعقيدًا وتطورًا وتهديدًا للخصوصية والأمن السيبراني." ففي الوقت الذي "مكّن فيه الذكاء الاصطناعي المستخدمين من تطوير تقنيات الحماية والردع، فقد استُخدم أيضًا كأداة" من قِبل مجرمين إلكترونيين" لتنفيذ هجمات أكثر دقة وفاعلية، مثل التزييف العميق (**Deepfake**)، الاختراقات المؤتمتة، وهجمات التصيد الذكية". وهنا يبرز" تساؤل قانوني جوهري: من المسؤول عن الأفعال الإجرامية الناتجة عن قرارات أو أفعال يقوم بها نظام ذكاء اصطناعي؟ هل يمكن تحميل النظام نفسه المسؤولية؟ أم تقع على مطوّر النظام أو مستخدمه أو مالكه"؟

إن" الطبيعة الذاتية لبعض خوارزميات الذكاء الاصطناعي، والتي تمنح الأنظمة قدرات "تعلم ذاتي" واتخاذ قرارات دون تدخل بشري مباشر"، تخلق" إشكاليات قانونية حقيقية أمام القواعد التقليدية للمسؤولية الجنائية. فهذه القواعد تقوم على وجود إنسان يتمتع بالإرادة والتمييز والوعي الكامل بالفعل الإجرامي"، وهي شروط لا تنطبق" حرفيًا على الأنظمة التقنية، مما يطرح تحديًا على الصعيدين التشريعي والقضائي. ولا يقل الأمر تعقيدًا في مجال المسؤولية غير المباشرة، حيث قد تُثار المسؤولية على المطوّرين"، أو مشغلي الأنظمة"، أو حتى المؤسسات التي تعتمد الذكاء الاصطناعي، وذلك بناءً على درجة الرقابة "التي يملكونها أو نية الاستخدام، أو مدى "توقعهم لنتائج الأفعال الصادرة عن النظام. ولعل ما يزيد من حدة الإشكال أن الكثير" من التشريعات"، سواء في الدول المتقدمة أو النامية، لا تزال تفتقر إلى نصوص صريحة وواضحة تنظم المسؤولية القانونية" في هذا الإطار، "ما يفتح الباب أمام اجتهادات قضائية متباينة، وقد يؤدي إلى نتائج غير متسقة تهدد استقرار العدالة الجنائية. انطلاقًا من ذلك، يسعى هذا البحث إلى دراسة مسؤولية الذكاء" الاصطناعي "عن الجرائم الإلكترونية، من خلال تحليل المفاهيم الأساسية، والاطلاع على التطورات التقنية ذات العلاقة، وتفصيل "الإشكاليات القانونية المرتبطة بمفهوم المسؤولية، سواء الجنائية أو المدنية، في هذا السياق. كما سيجري" مقارنة بين مواقف بعض التشريعات، ولا سيما في الاتحاد الأوروبي"، الولايات المتحدة، وبعض التشريعات العربية"، للوقوف على أوجه الاتفاق والاختلاف، ومحاولة تقديم توصيات تساعد في سد الفراغ التشريعي في هذا المجال".

ومن "خلال هذا الجهد البحثي، سيتم التركيز على الإجابة عن السؤال المحوري التالي: كيف يمكن تنظيم المسؤولية القانونية عن الجرائم الإلكترونية المرتكبة باستخدام "أو بواسطة الذكاء الاصطناعي"؟ وهل يجب إعادة صياغة المفاهيم القانونية التقليدية أم ابتكار أطر تشريعية جديدة تتلائم مع الواقع الرقمي الحديث؟"

أهداف البحث

"يسعى هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، من أبرزها":

1. "بيان المفهوم القانوني للذكاء الاصطناعي، وخصائصه التي تميّزه عن الوسائل التقليدية".
2. "تحليل طبيعة الجرائم الإلكترونية المرتكبة باستخدام الذكاء الاصطناعي، مع تصنيفها".
3. "تحديد الإشكاليات القانونية المتعلقة بالمسؤولية الجنائية في حال ارتكاب الجريمة بواسطة أنظمة الذكاء الاصطناعي".
4. "مقارنة مواقف بعض التشريعات الوطنية والدولية تجاه هذه المسؤولية."
5. "بيان مدى كفاية القواعد القانونية التقليدية لمعالجة هذه الظاهرة الحديثة".
6. "اقتراح حلول وتوصيات تشريعية لسد الفراغ القانوني ومواكبة التطور التكنولوجي".

ثالثا : فرضيات البحث

"ينطلق البحث من فرضيات علمية تسعى الدراسة لاختبارها"، وهي:

© 2026 SCINAT
ISCI Academy Publishing.

1. "الفرضية الأولى: القواعد التقليدية للمسؤولية الجنائية غير كافية للتعامل مع الجرائم الإلكترونية المرتكبة بواسطة الذكاء الاصطناعي."
2. "الفرضية الثانية: هناك تباين واضح في التشريعات الوطنية والدولية بشأن تحديد المسؤول عن أفعال الذكاء الاصطناعي".
3. "الفرضية الثالثة: يمكن وضع إطار قانوني خاص بمساءلة أنظمة الذكاء الاصطناعي، يراعي طبيعتها التقنية ويوازن بين الابتكار والمسؤولية".
4. "الفرضية الرابعة: المسؤولية "القانونية قد تقع على عدة أطراف (المبرمج، المستخدم، المشغل) بحسب طبيعة الجريمة ونمط تدخلهم".

رابعا: أسئلة البحث

1. "ما المقصود بالذكاء الاصطناعي في الإطار القانوني، وما خصائصه التقنية والقانونية"؟
2. "ما هي أبرز أشكال الجرائم الإلكترونية المرتكبة بواسطة الذكاء الاصطناعي"؟
3. "هل تنطبق قواعد المسؤولية الجنائية التقليدية على الذكاء الاصطناعي؟ ولماذا"؟
4. "من هو المسؤول قانونيًا عند ارتكاب جريمة إلكترونية باستخدام الذكاء الاصطناعي"؟
5. "هل يمكن مساءلة النظام الذكي ذاته، أم أن المسؤولية تقع على مطوّره أو مستخدمه أو مالكه"؟
6. "ما موقف التشريعات المقارنة (مثل الأوروبية، الأمريكية، والعربية) من هذه الإشكالية"؟
7. "هل هناك حاجة لتعديل أو سنّ قوانين خاصة بمساءلة الذكاء الاصطناعي؟ وما أبرز التوصيات "المقترحة؟

خامسا: إشكالية البحث

"هل يمكن مساءلة الذكاء الاصطناعي جنائيًا عن الجرائم الإلكترونية"؟ وإذا "تعذر ذلك، فمن هو المسؤول قانونًا؟ وهل تكفي التشريعات الحالية لمواجهة هذا النوع من الجرائم"؟

سادسا: أهمية البحث

-1 "تسليط الضوء على ثغرة قانونية متزايدة الخطورة."
-2 "ربط القانون بالواقع التكنولوجي المتطور."
-3 "المساهمة في تطوير إطار تشريعي يوازن بين الابتكار والمسؤولية".

سابعا: منهجية البحث

"المنهج التحليلي: لتحليل النصوص القانونية والمفاهيم المرتبطة بالذكاء الاصطناعي والجرائم الإلكترونية."

"المنهج المقارن: مقارنة التشريعات (مثل القانون الأمريكي، الأوروبي، العراقي أو المصري)."

"المنهج الاستشرافي: لتقديم مقترحات مستقبلية."

ثامنا: خطة البحث المقترحة

"الفصل الأول: الإطار المفاهيمي للذكاء الاصطناعي والجرائم الإلكترونية"

"المبحث الأول: تعريف الذكاء الاصطناعي وتصنيف أنواعه"

"المبحث الثاني: مفهوم الجريمة الإلكترونية وأشكالها الحديثة"

"المبحث الثالث: العلاقة بين الذكاء الاصطناعي والجرائم الإلكترونية"

"الفصل الثاني: المسؤولية القانونية عن الجرائم المرتكبة عبر الذكاء الاصطناعي"

"المبحث الأول: شروط تحقق المسؤولية الجنائية التقليدية"

"المبحث الثاني: مدى انطباق المسؤولية على الذكاء الاصطناعي (الروبوتات، الخوارزميات)"

"المبحث الثالث: المسؤولية الجنائية للمستخدم أو المبرمج أو المطور"

"الفصل الثالث: موقف التشريعات المقارنة والمقترحات القانونية"

"المبحث الأول: موقف القانون الأمريكي والأوروبي من مسؤولية الذكاء الاصطناعي"

"المبحث الثاني: موقف التشريعات العربية (العراق، مصر، الإمارات كمثال)"

"المبحث الثالث: التوصيات والمقترحات لتحديث الإطار التشريعي"

الفصل الأول

الإطار المفاهيمي للذكاء الاصطناعي والجرائم الإلكترونية

© 2026 SCINAT
ISCI Academy Publishing.

ويتكون هذا الفصل من ثلاث مباحث:

المبحث الأول: مفهوم الذكاء الاصطناعي وخصائصه

أولًا: تعريف الذكاء الاصطناعي

"يُعرّف الذكاء الاصطناعي (**Artificial Intelligence**) بأنه قدرة الأنظمة البرمجية أو الآلات على محاكاة السلوك البشري" الذكي، من خلال" التعلم، التحليل، واتخاذ القرارات، دون تدخل بشري مباشر. وقد تطور هذا المفهوم ليتجاوز" مجرد المعالجة "البرمجية إلى نماذج أكثر تعقيدًا تعتمد على "التعلم الآلي" و"التعلم العميق"، والتي تُمكن الأنظمة من تطوير سلوكها ذاتيًا استنادًا إلى البيانات." ([1])

ومن" منظور قانوني، لا يوجد حتى الآن تعريف موحد للذكاء الاصطناعي في غالبية التشريعات، ما يخلق تحديًا في التعامل" معه كـ"شخص معنوي" أو كـ"وسيلة تقنية". بعض "التعريفات القانونية الأوروبية، مثل مشروع لائحة الاتحاد الأوروبي" لعام 2021، تُعرفه بأنه: "نظام يتلقى مدخلات من البيئة وينتج مخرجات من خلال عمليات تعتمد على القواعد أو البيانات لتحقيق أهداف معينة".

ثانيًا: خصائص الذكاء الاصطناعي

1. "الاستقلالية الذاتية: قدرة النظام على اتخاذ القرار دون تدخل بشري مباشر".
2. "التحليل والتعلم: من خلال خوارزميات تتفاعل مع كميات ضخمة من البيانات."
3. "قابلية التطوير الذاتي: النظام يطوّر نفسه باستمرار بناءً على المدخلات والتجارب السابقة."
4. "عدم التنبؤ الكامل بالسلوك: يخلق صعوبة قانونية في تحميل المسؤولية عند ارتكاب الأفعال الضارة". [(2)]

المبحث الثاني: الجريمة الإلكترونية – المفهوم والتطورات الحديثة

أولًا:" تعريف الجريمة الإلكترونية"

"الجريمة الإلكترونية هي أي فعل غير مشروع يُرتكب باستخدام الوسائل التقنية أو في البيئة الرقمية، ويهدف إلى الإضرار بالأفراد أو المؤسسات "أو الدول، و"تشمل أفعالًا مثل اختراق الأنظمة، سرقة البيانات، الابتزاز الإلكتروني، الاحتيال الإلكتروني، وبث المحتوى الضار"[(3)]

ثانيًا: "أشكال الجرائم الإلكترونية المرتبطة بالذكاء الاصطناعي"

1. "هجمات التزييف العميق (**Deepfake**): إنشاء فيديوهات مزيفة لأشخاص باستخدام تعلم الآلة."
2. "الاحتيال الآلي: تنفيذ عمليات احتيال مصرفي أو استغلال ثغرات أمنية باستخدام أدوات ذكية."
3. "اختراق الأنظمة بواسطة برامج تعلم ذاتي: يمكن للذكاء الاصطناعي التعرف على ثغرات الأنظمة الأمنية واستغلالها بشكل آلي".
4. برمجيات هجومية مستقلة: مثل "بوتات" الاختراق والهجمات الموزعة." [(4)]

المبحث الثالث: العلاقة بين الذكاء الاصطناعي والجرائم الإلكترونية

"تطورت العلاقة بين الذكاء الاصطناعي والجريمة الإلكترونية من كون الذكاء الاصطناعي" مجرد "وسيلة" مساعدة، "إلى كونه فاعلًا مباشرًا في بعض الأفعال الإجرامية الرقمية، مما يخلق إشكالًا قانونيًا خطيرًا".

أولًا: الذكاء الاصطناعي كأداة للجريمة

"يُستخدم من قِبل الجناة لتحسين دقة الهجمات، وزيادة فعاليتها، وصعوبة تعقبها."

أمثلة: "اختراق الحسابات، التنبؤ بسلوك المستخدمين، خداع أنظمة الحماية".

ثانيًا: الذكاء الاصطناعي كفاعل محتمل للجريمة

"في بعض الحالات، يُمكن للأنظمة أن تتخذ قرارات مؤذية دون تدخل بشري مباشر". [(5)]

"يُطرح تساؤل: هل يمكن اعتبار الذكاء الاصطناعي "شخصًا معنويًا" يخضع للمساءلة القانونية"؟

الفصل الثاني

المسؤولية القانونية عن الجرائم المرتكبة باستخدام الذكاء الاصطناعي

ويتكون هذا الفصل من ثلاث مباحث :

المبحث الأول: شروط تحقق المسؤولية الجنائية التقليدية

أولًا: الركن المادي في الجريمة

[1] (ناصر محمد البقمي (2008).مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية,ابوظبي,مركز الإمارات للدراسات والبحوث الاستراتيجية ,ص12.
[2]) موسى مصطفى محمد, ,(2003),أساليب إجرامية للتقنية الرقمية : ماهيتها, مكافحتها ,القاهرة ,دار النهضة العربية ,ص56.

[3] (عبد المطلب ممدوح عبد المجيد , (2001),جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية : الجريمة عبر الانترنت ,مكتبة دار الحقوق ص 226 .
[4] (حنان ريحان مبارك ,الجرائم المعلوماتية دراسة مقارنة , منشورات الحلبي الحقوقية , ط1, 2014,ص56 .
[5]) محمد علي العريان,(2004), الجرائم المعلوماتية ,الإسكندرية , الدار الجامعية الجديدة للنشر ,ص157.

© 2026 SCINAT
ISCI Academy Publishing.

"الركن المادي يمثل الفعل الخارجي المكوّن للجريمة، وهو السلوك الذي يقع من الجاني ويؤدي إلى نتيجة مجرّمة قانونًا." [6]

"عند الحديث عن الذكاء الاصطناعي، يثور التساؤل: هل يُعد السلوك الصادر من نظام ذكي (مثل خوارزمية تتسبب باختراق أو تدمير نظام) فعلًا" ماديًا تقوم" عليه الجريمة؟ الإشكال هنا أن الفعل قد لا يصدر من إنسان، بل من نظام ذاتي العمل، ما يجعل إثبات الركن المادي معقدًا".

ثانيًا: الركن المعنوي (القصد الجنائي)

"القصد الجنائي هو نية ارتكاب الجريمة، ويمثل الركن الأساسي في معظم الجرائم". [7]

فهل" يمكن للذكاء الاصطناعي أن "يقصد" ارتكاب جريمة؟

بما "أن الأنظمة الذكية لا تملك إرادة أو وعيًا، فالقانون لا يمكنه ـ حتى الآن ـ نسب القصد إليها"، ما يعفيها تقنيًا من المسؤولية الجنائية المباشرة وفقًا للمفاهيم التقليدية."

ثالثًا: أهلية المسؤولية الجنائية

"الأهلية الجنائية تقتضي أن يكون الفاعل إنسانًا، عاقلًا، بالغًا، ومدركًا لأفعاله". وهي" شروط لا تنطبق على الأنظمة التقنية، مما يُخرج "الذكاء الاصطناعي "من دائرة الفاعلين التقليديين للجريمة، ويدفع القانون إلى البحث عن "فاعل بديل" يحمل المسؤولية." [8]

المبحث الثاني

مدى انطباق المسؤولية على الذكاء الاصطناعي

أولًا: هل يمكن مسائلة الذكاء الاصطناعي بذاته؟

حتى اللحظة، لا" يُعتبر الذكاء الاصطناعي "شخصًا قانونيًا" يملك ذمة قانونية مستقلة. القانون لا يحمّل الآلة المسؤولية، بل يبحث عن الإنسان الذي يتحكم بها أو أنتجها أو استخدمها."

ثانيًا: الذكاء الاصطناعي بين "الأداة" و"الفاعل"

"بعض الجرائم، يكون الذكاء الاصطناعي مجرد أداة لتنفيذ الفعل الإجرامي (كأن يستخدمه المخترق). في حالات" أخرى، يتصرف" الذكاء الاصطناعي ذاتيًا، ما يجعل منه فاعلًا غير مباشر، لكنه بلا مسؤولية مباشرة قانونيًا".

ثالثًا: مقترح "الشخصية الإلكترونية"

"بعض الفقهاء اقترحوا منح الأنظمة الذكية "شخصية قانونية خاصة"، كما هو الحال مع الشركات، لتحميلها مسؤولية مدنية أو حتى جنائية". هذا" الطرح لا يزال مثار جدل، ويصطدم بمفاهيم الإرادة، الوعي، والعقوبة، خاصة إذا لم يكن للنظام الذكي مالك محدد أو جهة مشغلة". [9]

المبحث الثالث

المسؤولية الجنائية للمبرمج والمستخدم والمشغل

أولًا: المبرمج أو المطور

إذا "ثبت أن المبرمج تعمّد تصميم خوارزمية تؤدي إلى فعل إجرامي (مثل اختراق، أو تخريب)، فإنه يُعد فاعلًا أصليًا أو شريكًا في الجريمة". تقع "عليه المسؤولية الجنائية الكاملة في حال توفر القصد والعلم بنتائج أفعاله". [10]

ثانيًا: المستخدم

المستخدم" الذي يستعمل النظام الذكي لأغراض إجرامية يُعد مسؤولًا جنائيًا، كمن يستخدم برنامج ذكاء اصطناعي للابتزاز" أو التزوير. قد" تثور مسؤولية المستخدم حتى لو لم يكن هو من برمج النظام، ما دام يعلم بنتائج استخدامه". [11]

ثالثًا: الشركة أو المشغّل التقني

في" بعض الحالات، تقع المسؤولية على الكيان الذي يقوم بتشغيل النظام أو يقدّمه كخدمة (مثل شركات التقنية)، خاصة إذا علمت باحتمال وقوع ضرر ولم تتخذ إجراءات للمنع."

الفصل الثالث

موقف التشريعات المقارنة والتوصيات القانونية

هذا "الفصل يُحلل كيف تعاملت بعض التشريعات المقارنة (الأوروبية، الأمريكية، العربية) مع مسؤولية الذكاء الاصطناعي في الجرائم الإلكترونية، ويُختتم بتوصيات عملية لسد الفراغ التشريعي".

المبحث الأول

---

[6] (عبد الله بن عبد العزيز اليوسف ,(1999), الظواهر الإجرامية المستحدثة وسبل مواجهتها ,الرياض ,جامعة نايف العربية للعلوم الأمنية ,ص13.

[7]) موسى مصطفى محمد, ,(2003),أساليب إجرامية للتقنية الرقمية : ماهيتها, مكافحتها ,القاهرة ,دار النهضة العربية ,ص66.

[8] (ناصر محمد البقمي (2008).مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية,ابوظبي,مركز الإمارات للدراسات والبحوث الاستراتيجية ,ص15.

[9]) ناصر محمد البقمي (2008).مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية,ابوظبي,مركز الإمارات للدراسات والبحوث الاستراتيجية ,ص23.

[10] (محمد علي سالم ,حسون عبيد ,الجريمة المعلوماتية, مجلة جامعة بابل للعلوم الإنسانية,مجلد14,عدد2,العراق,2007,ص92.

[11] (د . عبد الإله محمد النوايسة , جرائم تكنولوجيا المعلومات ـ شرح الأحكام الموضوعية في قانون الجرائم الالكترونية ,ط1 ,دار وائل للنشر والتوزيع , عمان, الأردن ,2017م, ص78-79.

© 2026 SCINAT
ISCI Academy Publishing.

موقف التشريع الأوروبي والأمريكي

أولًا: التشريع الأوروبي

"يعمل الاتحاد الأوروبي منذ عام 2021 على صياغة "قانون الذكاء الاصطناعي" (**AI Act**) لتنظيم استخدام أنظمة الذكاء الاصطناعي، وخصوصًا في القطاعات الحساسة". [12]

القانون الأوروبي لا يُحمّل الذكاء الاصطناعي مسؤولية جنائية بذاته، لكنه :

"يُصنف بعض التطبيقات على أنها عالية الخطورة. يُحمل مطوّري الأنظمة والمشغلين المسؤولية في حال الإهمال أو الإخلال بالضوابط. توجد مقترحات" لمنح "الشخصية الإلكترونية" للروبوتات" الذكية، لكنها لم تُعتمد رسميًا". [13]

ثانيًا: التشريع الأمريكي

في "الولايات المتحدة، لا يوجد قانون فيدرالي شامل ينظم الذكاء الاصطناعي حتى الآن. تُطبق قواعد المسؤولية القائمة، مثل قانون "المسؤولية التقصيرية (**Tort Law**) والقانون" الجنائي التقليدي على الجهة التي تستخدم الذكاء الاصطناعي. بعض الولايات" (مثل كاليفورنيا) أقرت" تشريعات جزئية تنظم استخدام الذكاء الاصطناعي في مجالات مثل السيارات ذاتية القيادة، والخصوصية. المسؤولية غالبًا "تُلقى على "المستخدم أو المطوّر" إذا ثبت علمه بإمكانية ارتكاب الجريمة. [14]

المبحث الثاني

موقف التشريعات العربية (العراق، الإمارات، مصر)

أولًا: القانون العراقي

لا "يوجد نص صريح ينظم الذكاء الاصطناعي في القانون العراقي حتى الآن. يتم التعامل مع الجرائم المرتكبة عبر الذكاء الاصطناعي وفق قانون العقوبات" وقانون" الجرائم المعلوماتية رقم 31 لسنة 2023. المسؤولية تقع على المستخدم أو المبرمج أو من يوجه الذكاء الاصطناعي نحو ارتكاب" الفعل. [15]

ثانيًا: القانون الإماراتي

"دولة الإمارات من الدول العربية الرائدة في تشريعات الذكاء الاصطناعي. في عام 2017، أنشأت وزارة للذكاء الاصطناعي، وفي 2021 أصدرت سياسة "الإمارات للذكاء "الاصطناعي. ومع ذلك، لا يوجد بعد قانون جنائي محدد يحمّل النظام الذكي مسؤولية، بل المسؤولية تقع على المستخدم أو "الشركة. [16]

ثالثًا: القانون المصري

"اعتمدت مصر قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، لكنه لا يتناول الذكاء الاصطناعي بشكل مباشر. تُستخدم المبادئ العامة في المسؤولية الجنائية لتحديد الفاعل، دون الاعتراف بالذكاء الاصطناعي ككيان قانوني". [17]

المبحث الثالث

التوصيات والمقترحات التشريعية

1. سن" تشريعات خاصة بالذكاء الاصطناعي في الدول العربية، تتضمن تعريفًا قانونيًا واضحًا، وتصنيفًا للأنظمة حسب درجة" الخطورة.
2. "إنشاء نظام مسؤولية قانونية مشترك، بحيث توزَّع المسؤولية بين المطوّر، المستخدم، والمشغّل بناءً على درجة الإشراف والنية".
3. "إدخال مفاهيم جديدة إلى القانون الجنائي مثل "الفاعل التقني" أو "الفاعل المساعد غير البشري".
4. "تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ذات العلاقة بالذكاء الاصطناعي، عبر الاتفاقيات والمعايير التقنية المشتركة".
5. "التدريب القضائي والنيابي للتعامل مع قضايا الذكاء الاصطناعي والأدلة الرقمية الناشئة عنه".

الخاتمة

مع" تسارع وتيرة التقدم التكنولوجي، أصبحت أنظمة الذكاء الاصطناعي تلعب دورًا محوريًا في تشكيل ملامح الحياة الرقمية، الأمر الذي جعلها شريكًا فعّالًا في البيئة "السيبرانية، سواء" كمساعد تقني أم كفاعل مباشر في بعض الأفعال الرقمية، بما في ذلك الجرائم الإلكترونية. وقد بيّن هذا البحث، من خلال " التحليل والمقارنة، أن هذه" الظاهرة الجديدة تفرض تحديات غير مسبوقة على قواعد المسؤولية القانونية التقليدية، ولا سيما المسؤولية الجنائية. "انطلق البحث من إشكالية أساسية تتعلق بإمكانية مساءلة الذكاء الاصطناعي قانونيًا، لا سيما عند ارتكاب أفعال مجرّمة دون تدخل بشري مباشر، وهو ما أظهر الحاجة إلى إعادة النظر في الأركان المكوّنة " للمسؤولية الجنائية، من فعل مادي وقصد جنائي وأهلية. كما كشف البحث أن غالبية "التشريعات الحالية، سواء في الدول العربية أو الغربية، لا تزال تتعامل مع الذكاء الاصطناعي كأداة تقنية، لا كفاعل قانوني " مستقل، مما " يجعل المسؤولية تقع غالبًا على المستخدم، المطوّر أو المشغّل. وتبيّن من خلال الدراسة المقارنة أن الاتحاد الأوروبي هو الأكثر تقدمًا في محاولة تنظيم هذه المسألة، عبر مشاريع" تشريعية تتعلق بمخاطر" الذكاء الاصطناعي، بينما تتخذ الولايات المتحدة موقفًا مرنًا قائمًا على المسؤولية المدنية والجنائية التقليدية، وتُظهر بعض الدول العربية "بوادر

[12] (سعيدة بعرة, الجريمة الالكترونية في التشريع الجزائري - دراسة مقارنة ,رسالة ماجستير ,كلية الحقوق والعلوم السياسية ,جامعة محمد خيضر بسكرة ,الجزائر,2019م,ص37-38.

[13] (زهراء عادل سلبي ,جريمة الابتزاز الالكتروني (دراسة مقارنة),ط1,دار الأكاديميون للنشر والتوزيع ,عمان - الأردن,2020,ص61.

[14] (رحيمة نمد يلي, خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة , أعمال المؤتمر الدولي الرابع عشر "الجرائم الالكترونية" مركز جيل العلمي ,طرابلس ,24-25مارس 217,ص102.

[15] (أ . د. احمد رضا توحيدي , صور الجرائم المعلوماتية ومواجهتها بالتشريعات القانونية , مجلة اكليل للدراسات الانسانية , كلية الحقوق , جامعة قم ,العدد11, ايلول ,2022 .

[16] (د. نورة عبدالله محمد المطلق , ابتزاز الفتيات احكامه وعقوبته في الفقه الاسلامي , كلية الشريعة , جامعة الامام محمد بن أسعود الاسلامية ,الرياض ,ص9 .

[17] (محمد عبدالمحسن شلهوب , جريمة الابتزاز ,دراسة مقارنة بين الفقه والنظام , رسالة ماجستير , المعهد العالي للقضاء , قسم السياسة الشرعية , جامعة الامام محمد بن سعود الاسلامية , 2011م, ص46 - ص47 .

© 2026 SCINAT
ISCI Academy Publishing.

اهتمام لكنها لا تزال بحاجة "إلى تنظيم قانوني صريح ومباشر. وانتهى البحث إلى أن الحل لا يكمن بالضرورة "في منح "شخصية قانونية" للذكاء "الاصطناعي، بل في بناء نظام قانوني مختلط يُحدد المسؤولية بحسب طبيعة التدخل" البشري، ومدى "القدرة على التنبؤ بنتائج سلوك النظام الذكي، مع وضع تشريعات مرنة تواكب التطورات المستقبلية وتوفّر الحماية القانونية" للمجتمع.

اولا: النتائج

1. الذكاء "الاصطناعي أصبح أداة فعالة في ارتكاب الجرائم الإلكترونية، وأحيانًا فاعلًا غير بشري مباشرًا".
2. "المسؤولية القانونية لا تزال تقع على البشر المرتبطين بالنظام" (مطور، مستخدم، مشغّل).
3. القواعد" الجنائية التقليدية تعجز عن استيعاب هذه الحالات بشكل دقيق".
4. هناك "تفاوت كبير في تنظيم التشريعات لمسؤولية الذكاء الاصطناعي".
5. "الحاجة ماسة لوضع إطار قانوني جديد يأخذ بعين الاعتبار خصوصية هذه التقنية.

ثانيا: التوصيات

1. "ضرورة صياغة تعريف قانوني واضح للذكاء الاصطناعي في التشريعات" العربية.
2. "تعديل قوانين العقوبات لتشمل أفعالًا ترتكب من خلال أنظمة "ذكية.
3. سنّ قوانين" خاصة بالجرائم الإلكترونية المرتبطة بالذكاء الاصطناعي".
4. إنشاء "هيئات رقابية لمتابعة تطورات الذكاء الاصطناعي وتقويم استخدامه".
5. تعزيز" التعاون الدولي في مواجهة الجرائم الذكية العابرة للحدود".

قائمة المصادر والمراجع

أولا: الكتب القانونية

1- عبد الله بن عبد العزيز اليوسف ,(1999), الظواهر الإجرامية المستحدثة وسبل مواجهتها ,الرياض ,جامعة نايف العربية للعلوم الأمنية.

2- موسى مصطفى محمد, ,(2003),أساليب إجرامية للتقنية الرقمية : ماهيتها, مكافحتها ,القاهرة ,دار النهضة العربية.

3- حنان ريحان مبارك ,الجرائم المعلوماتية دراسة مقارنة , منشورات الحلبي الحقوقية , ط1, 2014 .

4- عبد المطلب ممدوح عبد المجيد , (2001),جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية : الجريمة عبر الانترنت ,مكتبة دار الحقوق.

5- محمد علي العريان,(2004), الجرائم المعلوماتية ,الإسكندرية ,الدار الجامعية الجديدة للنشر.

6- ناصر محمد البقمي (2008).مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية ,ابوظبي ,مركز الإمارات للدراسات والبحوث الاستراتيجية.

7- د . عبد الإله محمد النوايسة , جرائم تكنولوجيا المعلومات ـ شرح الأحكام الموضوعية في قانون الجرائم الالكترونية , دار وائل للنشر والتوزيع , عمان, الأردن ,2017, ط1.

8- زهراء عادل سلبي ,جريمة الابتزاز الالكتروني (دراسة مقارنة),ط1,دار الأكاديميون للنشر والتوزيع, عمان ـ الأردن,2020.

9- محمد علي سالم ,حسون عبيد ,الجريمة المعلوماتية, مجلة جامعة بابل للعلوم الإنسانية,مجلد14,عدد2,العراق,2007.

10- سعيدة بعرة, الجريمة الالكترونية في التشريع الجزائري , دراسة مقارنة ,رسالة ماجستير ,كلية الحقوق والعلوم السياسية ,جامعة محمد خيضر بسكرة ,الجزائر,2019م .

11- رحيمة نمد يلي, خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة , أعمال المؤتمر الدولي الرابع عشر "الجرائم الالكترونية" مركز جيل العلمي ,طرابلس ,24-25مارس 2017.

12- أ . د. احمد رضا توحيدي , صور الجرائم المعلوماتية ومواجهتها بالتشريعات القانونية , مجلة اكليل للدراسات الانسانية , كلية الحقوق , جامعة قم ,العدد11, ايلول ,2022 .

13- د. نورة عبدالله محمد المطلق , ابتزاز الفتيات احكامه وعقوبته في الفقه الاسلامي , كلية الشريعة , جامعة الامام محمد بن أسعود الاسلامية ,الرياض .

14- محمد عبدالمحسن شلهوب , جريمة الابتزاز ,دراسة مقارنة بين الفقه والنظام , رسالة ماجستير , المعهد العالي للقضاء , قسم السياسة الشرعية , جامعة الامام محمد بن سعود الاسلامية , 2011م.

ثانياً: قوانين وتشريعات

15- قانون مكافحة الجرائم المعلوماتية العراقي رقم 31 لسنة 2023.

16- سياسة الإمارات للذكاء الاصطناعي 2031.

17- مشروع قانون الاتحاد الأوروبي لتنظيم الذكاء الاصطناعي (**AI Act**)، 2021.

© 2026 SCINAT
ISCI Academy Publishing.