الذكاء الاصطناعي والجرائم الرقمية والإطار القانوني للمساءلة الجنائية في العراق

م.م. بتول لفته عبد الزهرة

مركز دراسات البصرة والخليج العربي/ قسم الدراسات السياسية والاستراتيجية

جامعة البصرة

Email : batoollaftah@gmail.com

الملخص

يشهد العالم في العصر الحديث تطورًا متسارعًا في تقنيات الذكاء الاصطناعي، مما أدى إلى ظهور أنماط جديدة من الجرائم الرقمية التي تتسم بالتعقيد والتنوع، وتطرح تحديات قانونية غير مسبوقة أمام الأنظمة الجنائية التقليدية. ويهدف هذا البحث إلى دراسة العلاقة بين الذكاء الاصطناعي والجرائم الرقمية، وتحليل الإطار القانوني للمساءلة الجنائية عنها في التشريع العراقي، مع بيان مدى كفاية النصوص القانونية القائمة في مواجهة هذه الجرائم المستحدثة.

وقد اعتمد البحث على المنهج التحليلي المقارن، من خلال استعراض المفاهيم الأساسية للذكاء الاصطناعي والجرائم الرقمية، وبيان صور الجرائم المرتبطة باستخدام تقنيات الذكاء الاصطناعي، مثل الاختراقات السيبرانية، والتزوير الرقمي، وانتهاك الخصوصية، إضافة إلى تحليل موقف المشرّع العراقي من هذه الجرائم، سواء في قانون العقوبات أو التشريعات ذات الصلة.

وتوصل البحث إلى أن الإطار القانوني العراقي لا يزال قاصرًا في تنظيم المسؤولية الجنائية الناشئة عن استخدام الذكاء الاصطناعي، خاصة فيما يتعلق بتحديد المسؤولية بين المستخدم والمبرمج والنظام الذكي نفسه، مما يستدعي تدخلًا تشريعيًا حديثًا يواكب التطورات التكنولوجية. كما أوصى البحث بضرورة تبني تشريعات خاصة بالجرائم الإلكترونية والذكاء الاصطناعي، وتعزيز التعاون الدولي في هذا المجال و لا تزال الطبيعة القانونية للذكاء الاصطناعي محل جدل فقهي وتشريعي واسع، إذ لم يستقر الفقه القانوني المقارن على توصيف قانوني نهائي لهذه الأنظمة، نظرًا لتعدد مستويات استقلاليتها وتنوع وظائفها التقنية. فبعض الاتجاهات الفقهية تتعامل مع الذكاء الاصطناعي بوصفه مجرد أداة تقنية تخضع لمسؤولية المستخدم أو المبرمج، في حين يرى اتجاه آخر ضرورة تطوير إطار قانوني خاص يتلاءم مع خصوصية الأنظمة الذكية ذاتية التعلم. ومن ثم، فإن الدراسة لا تتبنى موقفًا حاسمًا بشأن الشخصية القانونية أو الطبيعة المستقلة للذكاء الاصطناعي، بل تنطلق من ضرورة تحليل الإشكالية ضمن حدود التشريعات العراقية النافذة، مع التركيز على مدى كفاية القواعد الجنائية التقليدية في استيعاب الجرائم المرتكبة بواسطة هذه التقنيات.

الكلمات المفتاحية : الذكاء الاصطناعي، الجرائم الرقمية، الجرائم الإلكترونية، المسؤولية الجنائية.

Artificial Intelligence, Digital Crimes, and the Legal Framework for Criminal Liability in Iraq

Assist. Lect. Batool Lafta Abdulzahra
Center for Basra and Arab Gulf Studies/ Department of Political and Strategic Studies / University of Basrah
Email : batoollaftah@gmail.com

Abstract

The Rapid advancement of artificial intelligence (AI) technologies has led to the emergence of new forms of digital crimes characterized by complexity and diversity, thereby posing unprecedented challenges to traditional criminal justice systems. This study aims to examine the relationship between artificial intelligence and digital crimes and to analyze the legal framework governing criminal liability in Iraq, with a focus on assessing the adequacy of existing legal provisions in addressing such emerging offenses.

The research adopts a comparative analytical approach by exploring the fundamental concepts of artificial intelligence and digital crimes, and by identifying various forms of crimes associated with AI technologies, such as cyberattacks, digital forgery, and violations of privacy. It also analyzes the position of the Iraqi legislator under the Penal Code and related legislation.

The study concludes that the Iraqi legal framework remains insufficient in regulating criminal liability arising from the use of artificial intelligence, particularly with regard to determining responsibility among users, developers, and intelligent systems themselves. Accordingly, it recommends the enactment of modern legislation that keeps pace with rapid technological developments, as well as the strengthening of international cooperation in combating AI-related cybercrimes.

Moreover, the legal nature of artificial intelligence remains a subject of extensive doctrinal and legislative debate, as comparative legal scholarship has not yet reached a settled characterization of such systems due to their varying levels of autonomy and functional complexity. Some legal approaches treat AI merely as a technical tool subject to the responsibility of the user or developer, while others argue for the development of a specific legal framework tailored to the unique nature of self-learning intelligent systems. This study does not adopt a definitive position regarding the legal personality or independent legal status of artificial intelligence; rather, it focuses on analyzing the issue within the framework of existing Iraqi legislation, emphasizing the adequacy of traditional criminal rules in addressing crimes committed through such technologies.

Keywords: Artificial Intelligence , Digital Crimes , Cybercrime, Criminal Liability.

المقدمة

أولاً: خلفية الدراسة

شهد العالم خلال العقود الأخيرة تطورًا متسارعًا في مجال تكنولوجيا المعلومات والاتصالات، تزامن معه ظهور الذكاء الاصطناعي بوصفه أحد أبرز مخرجات الثورة الصناعية الرابعة، حيث لم يعد هذا الذكاء مجرد أداة تقنية مساعدة، بل أصبح عنصرًا فاعلًا في مختلف مجالات الحياة، بما في ذلك الاقتصاد، والصحة، والتعليم، والإدارة، والأمن. وقد أسهمت تطبيقات الذكاء الاصطناعي، مثل التعلم الآلي ومعالجة البيانات الضخمة والأنظمة الذكية، في تحسين كفاءة الأداء وتسريع اتخاذ القرار، إلا أن هذا التطور لم يخلُ من آثار سلبية، تمثلت في استغلال هذه التقنيات في ارتكاب أنماط جديدة من الجرائم الرقمية التي تتجاوز الحدود التقليدية للجريمة. وتتميز هذه الجرائم بكونها عابرة للحدود، سريعة التنفيذ، وصعبة الاكتشاف، كما أنها قد تُرتكب بواسطة أنظمة ذكية قادرة على التعلم الذاتي واتخاذ القرار دون تدخل بشري مباشر. الأمر الذي يطرح إشكاليات قانونية عميقة تتعلق بتكييف هذه الأفعال إجراميًا، وتحديد المسؤولية الجنائية عنها، خاصة في ظل قصور العديد من التشريعات التقليدية عن مواكبة هذا التحول الرقمي المتسارع.

ثانياً: مشكلة الدراسة

تتمثل مشكلة الدراسة في وجود فجوة تشريعية واضحة في القانون العراقي فيما يتعلق بتنظيم الجرائم الرقمية المرتبطة بالذكاء الاصطناعي، حيث لا تزال النصوص القانونية القائمة، وعلى رأسها قانون العقوبات، غير كافية لمواجهة التعقيدات التي تفرضها هذه الجرائم الحديثة. إذ تثير الجرائم المرتكبة باستخدام الذكاء الاصطناعي إشكاليات جوهرية تتعلق بطبيعة الفعل الإجرامي، ومدى إمكانية إسناده إلى شخص طبيعي أو معنوي، خاصة في الحالات التي يعمل فيها النظام الذكي بشكل مستقل أو شبه مستقل. كما تبرز إشكالية تحديد المسؤولية بين الأطراف المختلفة، مثل المبرمج، والمستخدم، والجهة المالكة للنظام، فضلًا عن التساؤل حول مدى إمكانية مساءلة "الآلة" ذاتها من الناحية القانونية. ويزداد تعقيد هذه المشكلة في ظل غياب تشريع عراقي خاص ينظم الذكاء الاصطناعي أو الجرائم المرتبطة به بشكل مباشر، مما يؤدي إلى صعوبات عملية في تطبيق النصوص القانونية الحالية، ويحدّ من فاعلية العدالة الجنائية في التصدي لهذه الجرائم.

ثالثاً: أهمية الدراسة

تنبع أهمية هذه الدراسة من كونها تتناول موضوعًا حديثًا ومتجددًا يمسّ صميم الأمن القانوني والمجتمعي في ظل التحول الرقمي المتسارع، حيث أصبحت الجرائم الرقمية المرتبطة بالذكاء الاصطناعي تمثل تهديدًا حقيقيًا للدول والأفراد على حد سواء. وتكتسب الدراسة أهميتها من الناحية

العلمية من خلال إسهامها في إثراء المكتبة القانونية العربية ببحث متخصص في مجال لا يزال في طور التشكّل، كما تسهم في تسليط الضوء على أوجه القصور في التشريع العراقي، وتقديم تحليل قانوني معمق للمفاهيم المرتبطة بالذكاء الاصطناعي والمسؤولية الجنائية. أما من الناحية العملية، فإن هذه الدراسة تساعد صُنّاع القرار والمشرّعين على إدراك حجم التحديات التي تفرضها هذه الجرائم، وتوفر أساسًا علميًا يمكن الاعتماد عليه في تطوير تشريعات حديثة تتلاءم مع التطور التكنولوجي. كما تعزز الوعي القانوني لدى المختصين والباحثين حول طبيعة الجرائم الرقمية وآليات مكافحتها، بما يسهم في تحقيق التوازن بين الاستفادة من التقنيات الحديثة وحماية المجتمع من مخاطرها.

رابعاً: هدف الدراسة

يهدف هذا البحث إلى تحليل العلاقة بين الذكاء الاصطناعي والجرائم الرقمية، وبيان الإطار القانوني للمساءلة الجنائية عنها في العراق، من خلال دراسة مدى كفاية التشريعات الجنائية القائمة في مواجهة هذه الجرائم المستحدثة. كما يسعى البحث إلى توضيح الطبيعة القانونية للجرائم المرتبطة باستخدام تقنيات الذكاء الاصطناعي، وتحديد أركانها، وبيان الخصائص التي تميزها عن الجرائم التقليدية. ويهدف كذلك إلى تحليل الإشكاليات المتعلقة بإسناد المسؤولية الجنائية في حالات استخدام الأنظمة الذكية، سواء تعلق الأمر بالمستخدم أو المبرمج أو الجهة المشغّلة، فضلًا عن استكشاف مدى إمكانية تطوير مفهوم المسؤولية الجنائية ليتلاءم مع طبيعة الذكاء الاصطناعي. كما يسعى البحث إلى تقديم رؤية قانونية نقدية تساهم في اقتراح حلول تشريعية مناسبة لمعالجة أوجه القصور القائمة.

خامساً: أهداف الدراسة

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف التفصيلية التي تنبثق عن الهدف العام، ومن أبرزها:

بيان مفهوم الذكاء الاصطناعي وخصائصه التقنية والقانونية، ومدى تأثيره في البيئة الرقمية.

تحديد مفهوم الجرائم الرقمية وتمييزها عن الجرائم التقليدية، مع بيان أبرز صور الجرائم المرتبطة بالذكاء الاصطناعي.

تحليل أركان الجريمة الرقمية المرتكبة باستخدام تقنيات الذكاء الاصطناعي، وبيان خصوصيتها القانونية.

دراسة الإطار التشريعي العراقي المنظم للجرائم الإلكترونية، وتقييم مدى كفايته في مواجهة الجرائم المرتبطة بالذكاء الاصطناعي.

بحث إشكالية المسؤولية الجنائية في ظل استخدام الأنظمة الذكية، وتحديد الجهات التي يمكن مساءلتها قانونًا.

تقديم مقترحات وتوصيات تشريعية تسهم في تطوير النظام القانوني العراقي بما يتلاءم مع التحديات الرقمية الحديثة.

المبحث الأول: ماهية الذكاء الاصطناعي والجرائم الرقمية

يشهد العالم في الوقت الراهن تحولًا نوعيًا في بنية الجريمة نتيجة التطور المتسارع في تقنيات الذكاء الاصطناعي، حيث لم يعد هذا الأخير مجرد أداة تقنية مساعدة، بل أصبح عنصرًا فاعلًا في تشكيل أنماط جديدة من السلوك الإجرامي. فقد أدت التطورات في مجالات التعلم الآلي ومعالجة البيانات الضخمة إلى تمكين الأنظمة الذكية من أداء مهام معقدة قد تتجاوز في بعض الأحيان القدرة البشرية، الأمر الذي انعكس بصورة مباشرة على طبيعة الجرائم الرقمية، وجعلها أكثر تعقيدًا وخطورة، خاصة في ظل القدرة على إنتاج محتوى مزيف يصعب تمييزه، مثل تقنيات التزييف العميق (Deepfake) التي باتت تُستخدم في الابتزاز والتشهير[١].

كما أن الجرائم الرقمية المرتبطة بالذكاء الاصطناعي تتميز بخصائص تجعلها مختلفة جذريًا عن الجرائم التقليدية، إذ تتسم بالسرعة، والانتشار العابر للحدود، وصعوبة التتبع، فضلًا عن إمكانية ارتكابها دون تدخل بشري مباشر في بعض الحالات. وقد أدى ذلك إلى ظهور إشكاليات قانونية تتعلق بتكييف هذه الجرائم ضمن الأطر التقليدية للقانون الجنائي، خاصة وأن هذه الأطر تقوم أساسًا على فكرة السلوك الإنساني والإرادة الجنائية، وهو ما لا ينطبق دائمًا على الأنظمة الذكية التي قد تعمل بشكل مستقل أو شبه مستقل[٢] .

وفي السياق العراقي، تزداد أهمية دراسة هذه الظاهرة في ظل غياب تشريع خاص ينظم الجرائم المرتبطة بالذكاء الاصطناعي، حيث يعتمد القضاء على النصوص التقليدية في قانون العقوبات لمعالجة هذه الجرائم، كما في حالات الابتزاز الإلكتروني باستخدام تقنيات الذكاء الاصطناعي، التي تم تكييفها وفق نصوص التهديد أو الاحتيال[٣] إلا أن هذا التطبيق يثير العديد من الإشكاليات العملية، نظرًا لعدم ملاءمة النصوص الحالية لمواكبة التطور التكنولوجي المتسارع، الأمر الذي قد يؤدي إلى توسيع سلطة القاضي في التفسير، وقد يهدد مبدأ الشرعية الجنائية[٤].

وعلى المستوى النظري، تطرح الجرائم المرتبطة بالذكاء الاصطناعي تساؤلات عميقة حول طبيعة المسؤولية الجنائية، خاصة فيما يتعلق بإمكانية إسناد الفعل الإجرامي إلى النظام الذكي ذاته، أو إلى الأطراف المرتبطة به، مثل المبرمج أو المستخدم. وقد ذهب بعض الفقهاء إلى أن القواعد التقليدية

للمسؤولية الجنائية لم تعد كافية لمواجهة هذه التحديات، نظرًا لخصوصية الأنظمة الذكية وقدرتها على اتخاذ قرارات مستقلة، مما يستدعي إعادة النظر في المفاهيم التقليدية للجريمة والمسؤولية[٥].

وعليه، فإن دراسة ماهية الذكاء الاصطناعي والجرائم الرقمية المرتبطة به تمثل خطوة أساسية لفهم الإطار القانوني لهذه الظاهرة، وتحديد أبعادها المختلفة، تمهيدًا لتحليل مدى كفاية التشريعات الجنائية القائمة، واقتراح الحلول المناسبة لمواجهة التحديات التي تفرضها هذه الجرائم في العصر الرقمي.

المطلب الأول: مفهوم الذكاء الاصطناعي وخصائصه القانونية

أدى التطور التكنولوجي المتسارع إلى بروز الذكاء الاصطناعي بوصفه أحد أهم التحولات التي أعادت تشكيل العديد من المفاهيم القانونية التقليدية، ولا سيما في مجال المسؤولية الجنائية. فلم يعد الذكاء الاصطناعي مجرد أداة تقنية مساعدة، بل أصبح نظامًا قادرًا على محاكاة القدرات الذهنية البشرية، واتخاذ قرارات قد تترتب عليها آثار قانونية خطيرة. وقد انعكس هذا التطور بشكل مباشر على بنية الجرائم الرقمية، حيث أصبحت بعض الأفعال الإجرامية تُرتكب باستخدام أنظمة ذكية قادرة على التعلم والتكيف دون تدخل بشري مباشر، مما يثير تساؤلات جوهرية حول مدى إمكانية إخضاع هذه الأنظمة للقواعد التقليدية للقانون الجنائي[٦].

وفي هذا السياق، تبرز أهمية تحديد مفهوم الذكاء الاصطناعي، وبيان خصائص الأنظمة الذكية، وتحليل طبيعتها القانونية، باعتبار ذلك أساسًا ضروريًا لفهم الإشكاليات المرتبطة بالمسؤولية الجنائية الناشئة عن استخدام هذه التقنيات. إذ إن غموض المفهوم وعدم وضوح الإطار القانوني يؤديان إلى صعوبات في التكييف القانوني، ويؤثران على فعالية التشريعات في مواجهة الجرائم المستحدثة المرتبطة بالذكاء الاصطناعي[٧].

الفرع الأول: تعريف الذكاء الاصطناعي

يُعد الذكاء الاصطناعي من المفاهيم متعددة الأبعاد التي يصعب حصرها في تعريف واحد جامع، نظرًا لتطوره المستمر وتعدد تطبيقاته. فقد عرّفه الباحثان Russell و Norvig بأنه "فرع من علوم الحاسوب يُعنى بتصميم أنظمة قادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا، مثل التعلم، والاستدلال، واتخاذ القرار"[٨] كما عرّفته المفوضية الأوروبية بأنه "نظام يعتمد على الآلة يمكنه، لدرجة معينة من الاستقلالية، تحليل البيئة المحيطة به واتخاذ إجراءات لتحقيق أهداف محددة"[٩].

وفي الفقه العربي، يُنظر إلى الذكاء الاصطناعي بوصفه مجموعة من التقنيات التي تمكن الآلة من محاكاة السلوك الإنساني الذكي، بما يشمل القدرة على التعلم والتكيف واتخاذ القرار، وهو ما يجعله مختلفًا عن البرامج التقليدية التي تعمل وفق تعليمات ثابتة[١٠]. ويُلاحظ أن هذه التعريفات تتفق على عنصرين أساسيين، هما: القدرة على المحاكاة الذهنية، والاستقلال النسبي في اتخاذ القرار.

وتكمن أهمية تحديد مفهوم الذكاء الاصطناعي من الناحية القانونية في كونه يمثل نقطة الانطلاق لفهم طبيعة الأفعال التي قد تصدر عن هذه الأنظمة، ومدى إمكانية إخضاعها للقواعد القانونية التقليدية، خاصة في المجال الجنائي، حيث يشكل عنصر الإرادة أحد الأركان الأساسية للجريمة. وبالتالي، فإن تطور مفهوم الذكاء الاصطناعي يفرض على الفقه القانوني إعادة النظر في المفاهيم التقليدية للجريمة والمسؤولية(١١).

الفرع الثاني: خصائص الأنظمة الذكية

تتميز الأنظمة الذكية بمجموعة من الخصائص التي تجعلها تختلف جوهريًا عن الأنظمة البرمجية التقليدية، ومن أبرز هذه الخصائص الاستقلالية، والتعلم الذاتي، والقدرة على اتخاذ القرار. فالاستقلالية تعني قدرة النظام على العمل دون تدخل بشري مباشر، وهو ما يثير إشكالية قانونية تتعلق بإسناد الفعل الإجرامي، خاصة إذا تصرف النظام بشكل غير متوقع(١٢).

أما خاصية التعلم الذاتي، فهي تمكّن الأنظمة الذكية من تحسين أدائها بناءً على البيانات والخبرات السابقة، مما يجعل سلوكها متغيرًا وغير ثابت، وهو ما يزيد من صعوبة التنبؤ بنتائج أفعالها. وتظهر خطورة هذه الخاصية في الحالات التي تتعلم فيها الأنظمة من بيانات غير موثوقة أو منحازة، مما قد يؤدي إلى اتخاذ قرارات ضارة أو غير قانونية .

وتتمثل الخاصية الثالثة في القدرة على اتخاذ القرار، حيث تستطيع الأنظمة الذكية تحليل البيانات واتخاذ قرارات قد يكون لها أثر قانوني مباشر، مثل أنظمة القيادة الذاتية أو أنظمة التوصية أو الأنظمة الأمنية. وتكمن الإشكالية هنا في أن هذه القرارات قد تُتخذ دون إشراف بشري مباشر، مما يثير التساؤل حول من يتحمل المسؤولية القانونية عنها(١٣).

وعليه، فإن هذه الخصائص مجتمعة تجعل من الذكاء الاصطناعي ظاهرة قانونية معقدة، تتطلب إعادة تقييم القواعد التقليدية للمسؤولية، خاصة في المجال الجنائي، حيث تقوم المسؤولية على أساس الإدراك والإرادة، وهما عنصران يصعب تطبيقهما على الأنظمة الذكية .

الفرع الثالث: الطبيعة القانونية للذكاء الاصطناعي

تُعد مسألة تحديد الطبيعة القانونية للذكاء الاصطناعي من أكثر الإشكاليات إثارة للجدل في الفقه القانوني المعاصر، حيث انقسمت الآراء حول ما إذا كان ينبغي اعتباره مجرد أداة، أم كيانًا قانونيًا مستقلاً. فالاتجاه التقليدي يرى أن الذكاء الاصطناعي لا يعدو كونه أداة في يد الإنسان، وبالتالي فإن المسؤولية الجنائية تقع على عاتق المستخدم أو المبرمج، باعتبارهما أصحاب الإرادة الحقيقية(١٤).

في المقابل، ذهب اتجاه حديث إلى ضرورة الاعتراف بنوع من "الشخصية القانونية الإلكترونية" للأنظمة الذكية، خاصة تلك التي تتمتع بدرجة عالية من الاستقلالية، وذلك بهدف سد الفراغ التشريعي في حالات يصعب فيها تحديد المسؤول البشري. وقد ناقش البرلمان الأوروبي هذا الاتجاه في إطار مقترحاته المتعلقة بتنظيم الذكاء الاصطناعي(١٥) .

إلا أن هذا الاتجاه يواجه انتقادات عديدة، أبرزها تعارضه مع المبادئ الأساسية للقانون الجنائي، التي تقوم على فكرة المسؤولية الشخصية القائمة على الإدراك والإرادة. كما أن منح الذكاء الاصطناعي شخصية قانونية قد يؤدي إلى إضعاف مساءلة الإنسان الحقيقي، وهو ما يتعارض مع أهداف العدالة الجنائية .

وبناءً على ذلك، يمكن القول إن الطبيعة القانونية للذكاء الاصطناعي لا تزال محل جدل فقهي وتشريعي، وإن الاتجاه الغالب يميل إلى اعتباره أداة تقنية متطورة، مع ضرورة تطوير قواعد المسؤولية القانونية بما يتلاءم مع خصوصيته، دون الإخلال بالمبادئ الأساسية للقانون الجنائي.

المطلب الثاني: مفهوم الجرائم الرقمية المرتبطة بالذكاء الاصطناعي

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إحداث تحولات جوهرية في طبيعة الجرائم الرقمية، حيث لم تعد هذه الجرائم تقتصر على الأفعال التقليدية المرتبطة باستخدام الحاسوب أو الشبكات، بل أصبحت أكثر تعقيدًا نتيجة توظيف الأنظمة الذكية في تنفيذها. فقد أسهم الذكاء الاصطناعي في تطوير أدوات متقدمة قادرة على تحليل البيانات، وإنشاء محتوى مزيف، واختراق الأنظمة، مما أتاح للجناة وسائل جديدة لارتكاب الجرائم بطرق يصعب اكتشافها أو تتبعها .

كما أن الجرائم الرقمية المرتبطة بالذكاء الاصطناعي تتميز بكونها عابرة للحدود، وسريعة التنفيذ، وقادرة على إحداث أضرار واسعة النطاق في وقت قصير، وهو ما يطرح تحديات قانونية كبيرة أمام الأنظمة الجنائية، خاصة في ظل عدم كفاية التشريعات التقليدية لمواكبة هذه التطورات. ومن ثم، تبرز أهمية دراسة مفهوم الجرائم الرقمية، وخصائصها، وأهم صورها المرتبطة بالذكاء الاصطناعي، باعتبار ذلك أساسًا لفهم طبيعة هذه الجرائم وآليات مواجهتها قانونيًا .

الفرع الأول: تعريف الجرائم الرقمية

تُعرف الجرائم الرقمية (أو الجرائم الإلكترونية) بأنها الأفعال غير المشروعة التي تُرتكب باستخدام الحاسوب أو الشبكات الإلكترونية، سواء كان الحاسوب وسيلة لارتكاب الجريمة أو هدفًا لها. وقد عرّفتها منظمة الأمم المتحدة بأنها "أي نشاط إجرامي يتم تنفيذه عبر أنظمة الحاسوب أو الشبكات الرقمية، ويستهدف البيانات أو الأنظمة أو المستخدمين" .

كما يرى الفقه القانوني أن الجرائم الرقمية تشمل مجموعة واسعة من الأفعال، مثل الاختراق، وسرقة البيانات، والتزوير الإلكتروني، والاحتيال عبر الإنترنت، والابتزاز الإلكتروني، وهي جرائم تتسم بكونها غير مادية في طبيعتها، وتعتمد على الفضاء الرقمي كبيئة لارتكابها . وفي السياق العربي، عُرّفت الجرائم الإلكترونية بأنها "كل فعل غير مشروع يتم باستخدام وسائل تقنية المعلومات ويستهدف الإضرار بالأفراد أو المؤسسات أو الدولة"(١٦).

وتزداد أهمية هذا التعريف في ظل ارتباط الجرائم الرقمية بالذكاء الاصطناعي، حيث أصبحت بعض هذه الجرائم تُرتكب باستخدام أنظمة قادرة على التعلم والتكيف، مما يجعلها أكثر تعقيدًا وخطورة. وبالتالي، فإن تحديد مفهوم الجرائم الرقمية يمثل خطوة أساسية لفهم نطاق هذه الجرائم، وتحديد الأفعال التي تستوجب التجريم والعقاب في التشريعات الحديثة.

الفرع الثاني: خصائص الجرائم الإلكترونية

تتميز الجرائم الإلكترونية بمجموعة من الخصائص التي تجعلها مختلفة عن الجرائم التقليدية، ومن أبرز هذه الخصائص الطابع العابر للحدود، حيث يمكن ارتكاب الجريمة من دولة واستهداف ضحية في دولة أخرى، مما يثير إشكاليات تتعلق بالاختصاص القضائي والتعاون الدولي(١٧).

كما تتسم هذه الجرائم بالسرعة والانتشار الواسع، إذ يمكن تنفيذها في وقت قصير جدًا وإحداث أضرار كبيرة، خاصة في ظل استخدام الذكاء الاصطناعي الذي يمكّن الجناة من أتمتت العمليات الإجرامية وزيادة كفاءتها. بالإضافة إلى ذلك، تتميز الجرائم الإلكترونية بصعوبة الاكتشاف والتتبع، نتيجة استخدام تقنيات متقدمة مثل التشفير وإخفاء الهوية، مما يعقّد عملية التحقيق الجنائي(١٨).

ومن الخصائص المهمة أيضًا الطبيعة غير المادية لهذه الجرائم، حيث لا تتطلب وجودًا ماديًا للجاني في مكان الجريمة، بل يمكن ارتكابها عن بُعد، وهو ما يختلف عن الجرائم التقليدية. كما أن الأدلة في هذه الجرائم تكون رقمية، مما يتطلب خبرات فنية متخصصة للتعامل معها .

وعليه، فإن هذه الخصائص تجعل من الجرائم الإلكترونية تحديًا حقيقيًا للأنظمة القانونية، وتستدعي تطوير آليات قانونية وتقنية لمواجهتها، خاصة في ظل تزايد دور الذكاء الاصطناعي في تسهيل ارتكابها.

الفرع الثالث: صور الجرائم المرتبطة بالذكاء الاصطناعي

تتعدد صور الجرائم المرتبطة بالذكاء الاصطناعي، ومن أبرزها جرائم التزييف العميق (Deepfake)، التي تعتمد على تقنيات الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صوت مزيف يبدو واقعيًا للغاية، ويُستخدم في التشهير أو الابتزاز أو التضليل الإعلامي(١٩) (وتكمن خطورة هذه التقنية في صعوبة التمييز بين المحتوى الحقيقي والمزيف، مما يهدد الثقة في المعلومات الرقمية.

كما يُعد الابتزاز الإلكتروني من أبرز الجرائم المرتبطة بالذكاء الاصطناعي، حيث يتم استخدام تقنيات تحليل البيانات أو التزييف العميق للحصول على معلومات حساسة أو إنشاء محتوى مزيف بهدف تهديد الضحية وإجبارها على دفع مبالغ مالية أو تنفيذ مطالب معينة.

أما الاحتيال الرقمي، فقد شهد تطورًا كبيرًا بفضل الذكاء الاصطناعي، حيث أصبح بإمكان الجناة استخدام تقنيات مثل الروبوتات الذكية (Bots) أو الرسائل المزيفة المدعومة بالذكاء الاصطناعي لخداع الضحايا وسرقة أموالهم أو بياناتهم الشخصية. وقد حذرت وكالة الشرطة الأوروبية (Europol) من تزايد هذا النوع من الجرائم نتيجة استخدام الذكاء الاصطناعي في إنشاء هجمات أكثر إقناعًا وفعالية[٢٠]. وبناءً على ذلك، فإن هذه الجرائم تمثل نموذجًا واضحًا للتحديات التي يفرضها الذكاء الاصطناعي على الأنظمة القانونية، حيث تتطلب تطوير أدوات تشريعية وتقنية قادرة على مواكبة هذا التطور المتسارع.

المبحث الثاني: الإطار القانوني للمساءلة الجنائية في العراق

يُعدّ تحديد الإطار القانوني للمساءلة الجنائية عن الجرائم الرقمية المرتبطة بالذكاء الاصطناعي من أهم التحديات التي تواجه الأنظمة القانونية المعاصرة، ولا سيما في الدول التي لم تُطوّر بعد تشريعات متخصصة لمواكبة التحول الرقمي. ففي العراق، ما تزال المنظومة الجنائية تعتمد بصورة رئيسة على النصوص التقليدية الواردة في قانون العقوبات، والتي وُضعت في سياق مختلف تمامًا عن البيئة الرقمية الحالية، الأمر الذي يثير تساؤلات جدية حول مدى كفايتها في التعامل مع الجرائم المستحدثة[٢١] .

وقد أدى هذا الواقع إلى بروز فجوة تشريعية واضحة، خاصة مع تزايد استخدام الذكاء الاصطناعي في ارتكاب الجرائم، مثل التزييف العميق والاحتيال الإلكتروني والاختراقات السيبرانية. كما أن الطبيعة المعقدة لهذه الجرائم، وارتباطها بتقنيات متطورة، تجعل من الصعب تطبيق القواعد التقليدية للمسؤولية الجنائية عليها دون إعادة تفسير أو تطوير تشريعي .

وعليه، فإن دراسة الإطار القانوني للمساءلة الجنائية في العراق تتطلب تحليل النصوص القائمة، ومناقشة مشاريع القوانين ذات الصلة، وبيان موقف القضاء من هذه الجرائم، تمهيدًا لتقييم مدى كفاية هذا الإطار في مواجهة التحديات الرقمية الحديثة.

المطلب الأول: التنظيم القانوني للجرائم الرقمية في التشريع العراقي

يشكل التنظيم القانوني للجرائم الرقمية في العراق أحد الموضوعات التي تثير جدلًا واسعًا في الفقه القانوني، نظرًا لحداثة هذه الجرائم وتعقيدها، وعدم وجود تشريع خاص ينظمها بشكل شامل حتى الآن. إذ يعتمد القضاء العراقي في مواجهة الجرائم الإلكترونية على النصوص العامة في قانون

العقوبات، إلى جانب بعض القوانين ذات الصلة، وهو ما يؤدي إلى إشكاليات في التكييف القانوني، خاصة في ظل ظهور جرائم تعتمد على الذكاء الاصطناعي[٢٢].

كما أن محاولات المشرّع العراقي لإصدار قانون خاص بالجرائم المعلوماتية لا تزال في طور المشروع، ولم يتم إقراره بصورة نهائية، مما يترك فراغًا تشريعيًا في هذا المجال. ويزداد هذا التحدي مع تطور التقنيات الحديثة، التي تتطلب نصوصًا قانونية مرنة وقادرة على مواكبة التغيرات السريعة في طبيعة الجرائم الرقمية[٢٣].

الفرع الأول: قانون العقوبات العراقي وتطبيقه على الجرائم الرقمية

يعتمد النظام القانوني العراقي في مواجهة الجرائم الرقمية بشكل أساسي على قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، حيث يتم تطبيق نصوصه العامة على الجرائم المرتكبة عبر الوسائل الإلكترونية، مثل جرائم الاحتيال، والتهديد، وانتهاك الخصوصية. فعلى سبيل المثال، يتم تكييف جرائم الابتزاز الإلكتروني ضمن جرائم التهديد، في حين تُكيف بعض جرائم الاحتيال الرقمي وفق النصوص المتعلقة بالاحتيال التقليدي .

إلا أن هذا التطبيق يواجه عدة إشكاليات، أبرزها عدم ملاءمة النصوص التقليدية لطبيعة الجرائم الرقمية، التي تتسم بكونها غير مادية، وعابرة للحدود، وتعتمد على تقنيات متقدمة مثل الذكاء الاصطناعي. كما أن قانون العقوبات يقوم على أساس السلوك الإنساني المباشر، في حين أن بعض الجرائم الرقمية قد تُرتكب بواسطة أنظمة ذكية تعمل بشكل مستقل، مما يثير إشكالية في تحديد المسؤولية الجنائية ..يعتمد النظام القانوني العراقي في مواجهة الجرائم الرقمية، ومنها الجرائم المرتكبة باستخدام تطبيقات الذكاء الاصطناعي، على نصوص قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، إذ يتم تكييف كثير من الأفعال الرقمية ضمن النصوص التقليدية الخاصة بالتهديد أو الاحتيال أو القذف والتشهير أو انتهاك الخصوصية. ويظهر ذلك بوضوح في جرائم الابتزاز الإلكتروني، حيث غالبًا ما تُكيف وفق المادة (١/٤٣٠) من قانون العقوبات، متى كان التهديد مصحوبًا بطلب أو ابتزاز أو حمل المجني عليه على القيام بفعل أو الامتناع عنه .

وقد أكد القضاء العراقي هذا الاتجاه في أكثر من تطبيق قضائي، إذ أصدرت محكمة جنايات الرصافة حكمًا بالسجن لمدة ست سنوات بحق مدان قام بابتزاز فتاة من خلال تهديدها بنشر صور مفبركة لها باستخدام تطبيقات الذكاء الاصطناعي، وقد صدر الحكم استنادًا إلى أحكام المادة (١/٤٣٠) من قانون العقوبات، وبدلالة مواد الاشتراك (٤٧ و٤٨ و٤٩)، وهو ما يكشف عن اتجاه القضاء العراقي إلى التعامل مع التزييف بالذكاء الاصطناعي باعتباره صورة من صور التهديد والابتزاز متى اقترن بطلب مالي أو ضغط على المجني عليه .

كما أصدرت محكمة التمييز الاتحادية/هيئة الأحداث قرارها المرقم (١٨٥١/هيئة الأحداث/٢٠٢٤) في ٢٠ تشرين الأول/أكتوبر ٢٠٢٤، وبيّنت فيه أن تطبيق المادة (١/٤٣٠) من قانون العقوبات يقتضي التحقق من وجود تهديد واضح، وأن يكون التهديد مقرونًا بطلب أو تكليف أو أمر أو امتناع عن فعل، مؤكدة أن المحكمة لا يجوز لها حسم الدعوى دون تحديد صورة التهديد وماهية الطلب الصادر من المتهم. ويمثل هذا القرار أهمية خاصة في الجرائم الرقمية، لأنه يفرض على المحكمة تحديد عناصر الفعل الرقمي بدقة قبل إسناد المسؤولية الجنائية[٢٤].

وفي قرار آخر، هو القرار المرقم (١٨٤١/هيئة الأحداث/٢٠٢٤) الصادر في ١٥ تشرين الأول/أكتوبر ٢٠٢٤، أكدت محكمة التمييز الاتحادية أن التهديد المصحوب بطلب وفق المادة (١/٤٣٠) يُعد من جرائم الجنايات، وأن الصلح لا يقبل فيه بذات الطريقة التي تقبل في جرائم الجنح، الأمر الذي يعكس خطورة التهديد الرقمي والابتزاز الإلكتروني عندما يكون مصحوبًا بطلب أو منفعة غير مشروعة[٢٥].

وعلى الرغم من أهمية هذه التطبيقات القضائية، فإن الاعتماد على قانون العقوبات وحده لا يكفي لمواجهة الجرائم الرقمية الحديثة، ولا سيما تلك التي تعتمد على الذكاء الاصطناعي أو التزييف العميق أو الاختراق المؤتمت. فالنصوص التقليدية لم توضع ابتداءً لمعالجة جرائم غير مادية وعابرة للحدود وتعتمد على أدوات تقنية متطورة، مما يفرض ضرورة تدخل تشريعي خاص يجرّم صراحة استخدام الذكاء الاصطناعي في التهديد والاحتيال والتشهير والاختراق الرقمي، مع وضع قواعد واضحة للإثبات والمسؤولية الجنائية[٢٦]. وعليه، فإن الاعتماد على قانون العقوبات وحده لا يكفي لمواجهة الجرائم الرقمية الحديثة، بل يتطلب الأمر تطوير نصوص قانونية خاصة تأخذ بعين الاعتبار خصوصية هذه الجرائم، وتوفر أدوات قانونية أكثر فاعلية لمكافحتها.

الفرع الثاني: مشروع قانون الجرائم المعلوماتية

سعى المشرّع العراقي إلى معالجة الفراغ التشريعي في مجال الجرائم الرقمية من خلال إعداد مشروع قانون الجرائم المعلوماتية، الذي يهدف إلى تنظيم الأفعال المرتكبة باستخدام وسائل تقنية المعلومات، وتحديد العقوبات المناسبة لها. وقد تضمن المشروع نصوصًا تجرّم مجموعة واسعة من الأفعال، مثل الاختراق، وسرقة البيانات، ونشر المحتوى غير المشروع[٢٧].

إلا أن هذا المشروع واجه انتقادات واسعة، سواء من قبل الفقهاء أو منظمات المجتمع المدني، حيث اعتُبر أنه يتضمن نصوصًا فضفاضة قد تُستخدم لتقييد حرية التعبير، كما أنه لا يعالج بشكل كافٍ الجرائم المرتبطة بالذكاء الاصطناعي، التي تتطلب تنظيمًا أكثر تخصصًا ودقة .

كما أن عدم إقرار هذا المشروع حتى الآن أدى إلى استمرار الفراغ التشريعي، مما يجعل النظام القانوني العراقي غير قادر على مواكبة التطور التكنولوجي المتسارع، ويضعف من قدرته على مواجهة الجرائم الرقمية بفعالية.

الفرع الثالث: موقف القضاء العراقي من الجرائم المرتبطة بالذكاء الاصطناعي

يلعب القضاء العراقي دورًا مهمًا في مواجهة الجرائم الرقمية، من خلال تفسير النصوص القانونية القائمة وتطبيقها على الوقائع المستحدثة. وقد أظهر القضاء مرونة نسبية في التعامل مع الجرائم الإلكترونية، حيث تم تكييف العديد من الأفعال المرتبطة بالتكنولوجيا ضمن الجرائم التقليدية، مثل التهديد والاحتيال[٢٨].

إلا أن هذا الدور يظل محدودًا في ظل غياب تشريع واضح ينظم الجرائم المرتبطة بالذكاء الاصطناعي، حيث يواجه القضاة صعوبات في تحديد المسؤولية الجنائية، خاصة في الحالات التي يكون فيها النظام الذكي طرفًا في ارتكاب الجريمة. كما أن الاعتماد على الاجتهاد القضائي قد يؤدي إلى تفاوت الأحكام وعدم استقرارها، مما يهدد مبدأ الأمن القانوني.

وعليه، فإن تعزيز دور القضاء في هذا المجال يتطلب دعمًا تشريعيًا واضحًا، وتوفير تدريب متخصص للقضاة في مجال الجرائم الرقمية، بما يمكنهم من التعامل مع هذه الجرائم بكفاءة وفعالية.

المطلب الثاني: إشكالية المسؤولية الجنائية عن جرائم الذكاء الاصطناعي

تُعد مسألة تحديد المسؤولية الجنائية عن الجرائم المرتبطة بالذكاء الاصطناعي من أكثر الإشكاليات القانونية تعقيدًا في العصر الرقمي، وذلك بسبب الطبيعة الخاصة لهذه الأنظمة التي تتميز بالاستقلالية والقدرة على التعلم واتخاذ القرار دون تدخل بشري مباشر. وقد أدى هذا التطور إلى إرباك المفاهيم التقليدية للمسؤولية الجنائية، التي تقوم أساسًا على توافر الإرادة والإدراك لدى الفاعل، وهو ما يطرح تساؤلات حول إمكانية تطبيق هذه المفاهيم على الأنظمة الذكية .

كما أن تعدد الأطراف المتدخلة في تشغيل أنظمة الذكاء الاصطناعي، مثل المبرمج والمستخدم والشركة المنتجة، يزيد من تعقيد مسألة تحديد المسؤول الحقيقي عن الفعل الجرمي. ويزداد الأمر تعقيدًا في الحالات التي تتصرف فيها الأنظمة الذكية بشكل غير متوقع نتيجة التعلم الذاتي، مما يجعل إسناد الفعل إلى شخص معين أمرًا محل جدل فقهي وقانوني .

وعليه، فإن دراسة هذه الإشكالية تتطلب تحليل الجهات المحتملة للمسؤولية، وبيان أوجه القصور في التشريع الحالي، ثم تقديم حلول تشريعية قادرة على مواكبة التطور التكنولوجي.

الفرع الأول: تحديد المسؤول (المبرمج – المستخدم – النظام الذكي)

تثير الجرائم المرتبطة بالذكاء الاصطناعي إشكالية أساسية تتمثل في تحديد الشخص المسؤول جنائيًا، حيث تتعدد الأطراف التي يمكن أن تُنسب إليها الجريمة، وفي مقدمتها المبرمج، والمستخدم، والنظام الذكي نفسه.

فبالنسبة للمبرمج، يُمكن تحميله المسؤولية إذا ثبت أنه صمم النظام بطريقة تسمح بارتكاب الجريمة أو أهمل في وضع الضوابط اللازمة لمنع الاستخدام غير المشروع، وهو ما يُعرف بمسؤولية "الفاعل غير المباشر" أو المسؤولية عن الفعل الناتج عن أدواته. أما المستخدم، فيُعد مسؤولًا إذا استخدم النظام الذكي بشكل متعمد لارتكاب الجريمة، كأن يستعمل تقنيات التزييف العميق في الابتزاز أو الاحتيال.

وفي المقابل، يثور جدل حول إمكانية مساءلة النظام الذكي ذاته، خاصة في ظل تمتعه بدرجة من الاستقلالية، إلا أن الاتجاه الغالب في الفقه والقانون يرى أن المسؤولية الجنائية لا يمكن أن تُنسب إلا للشخص الطبيعي، لارتباطها بعنصر الإرادة والوعي، وهو ما تفتقر إليه الأنظمة الذكية.

وبالتالي، فإن المسؤولية الجنائية في جرائم الذكاء الاصطناعي غالبًا ما تُسند إلى الإنسان، سواء كان المبرمج أو المستخدم، مع إمكانية توزيع المسؤولية بين عدة أطراف وفقًا لدرجة تدخل كل منهم في الفعل الجرمي.

الفرع الثاني: قصور التشريع الحالي

تعاني التشريعات الجنائية الحالية من قصور واضح في التعامل مع الجرائم المرتبطة بالذكاء الاصطناعي، حيث تم وضع معظم هذه التشريعات في ظل بيئة تقليدية لا تأخذ بعين الاعتبار وجود أنظمة ذكية قادرة على اتخاذ قرارات مستقلة.

ومن أبرز أوجه هذا القصور عدم وضوح القواعد المتعلقة بإسناد المسؤولية، حيث لا توجد نصوص صريحة تحدد المسؤول عن الأفعال التي ترتكبها الأنظمة الذكية، مما يؤدي إلى صعوبة في التكييف القانوني لهذه الجرائم. كما أن القواعد التقليدية للمسؤولية الجنائية، التي تقوم على الخطأ الشخصي، لا تتلاءم مع حالات التعلم الذاتي التي قد تؤدي إلى نتائج غير متوقعة .

إضافة إلى ذلك، تعاني التشريعات من بطئ في مواكبة التطور التكنولوجي، وهو ما يُعرف بمشكلة "الفجوة الزمنية التشريعية"، حيث تتطور التقنيات بشكل أسرع من قدرة المشرّع على تنظيمها .

كما أن الطبيعة العابرة للحدود لهذه الجرائم تجعل من الصعب تطبيق القوانين الوطنية عليها بشكل فعال، خاصة في ظل غياب تعاون دولي كافٍ، مما يزيد من تعقيد مسألة الملاحقة الجنائية.

الفرع الثالث: الحلول التشريعية المقترحة

في مواجهة التحديات التي تطرحها جرائم الذكاء الاصطناعي، برزت عدة اتجاهات فقهية وتشريعية تهدف إلى تطوير الإطار القانوني للمسؤولية الجنائية بما يتلاءم مع هذه التطورات.

ومن أهم هذه الحلول اعتماد مبدأ المسؤولية المشتركة، بحيث يتم توزيع المسؤولية بين جميع الأطراف المتدخلة في تصميم وتشغيل النظام الذكي، وفقًا لدرجة مساهمتهم في وقوع الجريمة. كما يُقترح تبني نظام المسؤولية الصارمة في بعض الحالات، خاصة عندما يتعلق الأمر بأنظمة عالية الخطورة، بحيث يتم تحميل المسؤولية دون الحاجة لإثبات الخطأ .

كما يدعو بعض الفقهاء إلى ضرورة وضع تشريعات خاصة بالذكاء الاصطناعي، تتضمن قواعد واضحة لتحديد المسؤولية، وتفرض التزامات على الشركات المطورة، مثل ضمان سلامة الأنظمة، وإجراء تقييمات للمخاطر قبل استخدامها .

ومن الاتجاهات الحديثة أيضًا اقتراح منح الذكاء الاصطناعي "شخصية قانونية محدودة"، تسمح بإسناد بعض المسؤوليات إليه بشكل رمزي، مع إبقاء المسؤولية الفعلية على عاتق الإنسان، وهو ما يمثل محاولة للتوفيق بين التطور التكنولوجي والمفاهيم القانونية التقليدية .

وعليه، فإن تطوير التشريعات الجنائية لمواجهة جرائم الذكاء الاصطناعي يتطلب مقاربة شاملة تجمع بين تحديث القوانين الوطنية وتعزيز التعاون الدولي، بما يضمن تحقيق العدالة وحماية المجتمع من مخاطر هذه التقنيات.

الخاتمة

في ضوء ما تقدم، يتبين أن التطور المتسارع في تقنيات الذكاء الاصطناعي لم يؤدِ فقط إلى تطور وسائل ارتكاب الجرائم الرقمية، بل أسهم في ظهور أنماط إجرامية جديدة تتسم بدرجة عالية من التعقيد التقني والتنظيمي، الأمر الذي فرض تحديات غير مسبوقة على المنظومة الجنائية التقليدية. فقد أصبحت الجرائم المرتبطة بالذكاء الاصطناعي، مثل التزييف العميق، والاختراق المؤتمت، والاحتيال الرقمي الذكي، تشكل تهديدًا مباشرًا للأمن القانوني والاجتماعي، في ظل قصور العديد من التشريعات الوطنية عن مواكبة هذه التحولات.

وقد أظهر البحث أن قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل، رغم إمكانية تطبيق بعض نصوصه العامة، مثل المواد (٤٣٠) الخاصة بالتهديد، و(٤٣٣) المتعلقة بالقذف والتشهير، و(٤٥٦) الخاصة بالاحتيال، على بعض صور الجرائم الرقمية، إلا أن هذه النصوص وُضعت أصلًا لمعالجة أفعال تقليدية، ولا توفر معالجة دقيقة أو كافية للجرائم المرتبطة بالذكاء الاصطناعي. كما أن غياب قانون عراقي متخصص ينظم الجرائم الرقمية الحديثة أدى إلى بقاء فراغ تشريعي واضح، يضعف من كفاءة المواجهة القانونية ويجعل القضاء مضطرًا إلى الاعتماد على التفسير الموسع للنصوص القائمة.

كذلك، كشفت الدراسة أن الإشكالية الأكثر تعقيدًا تتمثل في تحديد المسؤولية الجنائية في ظل تعدد الأطراف المتدخلة، كالمبرمج، والمستخدم، والجهة المشغلة، خصوصًا في الحالات التي تعمل فيها الأنظمة الذكية بدرجة من الاستقلالية. وعلى الرغم من أن الاتجاه القانوني الغالب لا يمنح الذكاء الاصطناعي شخصية قانونية مستقلة، إلا أن تصاعد قدراته التقنية يفرض إعادة النظر في آليات الإسناد الجنائي التقليدي.

وعليه، فإن مواجهة الجرائم المرتبطة بالذكاء الاصطناعي في العراق لا يمكن أن تقتصر على الحلول العامة أو التوصيات النظرية، بل تتطلب إصلاحًا تشريعيًا وقضائيًا مباشرًا، يشمل تحديث البنية القانونية الوطنية، وتطوير آليات الإثبات الرقمي، وإنشاء أدوات مؤسسية متخصصة، بما يضمن حماية المجتمع دون تعطيل التطور التكنولوجي المشروع.

النتائج

أسهم الذكاء الاصطناعي في ظهور صور مستحدثة من الجرائم الرقمية، تتسم بارتفاع مستوى التنظيم والاحترافية وصعوبة الكشف.

تعتمد المنظومة الجنائية العراقية حاليًا على النصوص التقليدية في قانون العقوبات، مثل المواد (٤٣٠، ٤٣٣، ٤٥٦)، لمعالجة الجرائم الرقمية، رغم محدودية ملاءمتها لهذه الجرائم.

يفتقر العراق إلى قانون متخصص ينظم الجرائم المرتبطة بالذكاء الاصطناعي والتزييف العميق والاختراق الذكي.

يمثل غياب النصوص الخاصة تحديًا مباشرًا أمام القضاء العراقي في التكييف القانوني الدقيق لهذه الجرائم.

تعد مسألة تحديد المسؤولية الجنائية من أكثر الإشكالات القانونية تعقيدًا، نتيجة تعدد الفاعلين التقنيين والبشريين.

لا يزال الاتجاه القانوني السائد يحمل المسؤولية للعنصر البشري، دون الاعتراف بالذكاء الاصطناعي كفاعل قانوني مستقل.

يتطلب التعامل الفعال مع الجرائم الرقمية الحديثة تطويرًا تشريعيًا وإجرائيًا خاصًا بالأدلة الرقمية والجرائم المؤتمتة.

التوصيات

إصدار قانون عراقي خاص بالجرائم الرقمية والذكاء الاصطناعي يتضمن:

تعريفًا قانونيًا واضحًا للتزييف العميق.

تجريمًا صريحًا لانتحال الشخصية الرقمية.

تنظيمًا دقيقًا للمسؤولية الجنائية في الجرائم المرتكبة بواسطة الأنظمة الذكية.

تعديل قانون العقوبات العراقي بإضافة نصوص خاصة تعالج:

الاحتيال الرقمي الذكي.

الاختراقات المؤتمتة.

الابتزاز باستخدام الذكاء الاصطناعي.

الجرائم القائمة على المحتوى الاصطناعي المزيف.

إنشاء محاكم أو دوائر قضائية متخصصة في الجرائم الرقمية داخل السلطة القضائية العراقية، مدعومة بخبراء تقنيين في الأدلة الإلكترونية.

اعتماد دليل قضائي عراقي للأدلة الرقمية يحدد آليات جمع وفحص وتوثيق الأدلة المرتبطة بالذكاء الاصطناعي.

إلزام شركات الاتصالات ومنصات التواصل الاجتماعي العاملة في العراق بتوفير استجابة قانونية وتقنية عاجلة لطلبات القضاء في الجرائم الرقمية.

تضمين برامج المعهد القضائي العراقي ودورات الادعاء العام تدريبًا متخصصًا في الجرائم السيبرانية والذكاء الاصطناعي.

تفعيل مشروع قانون الجرائم المعلوماتية العراقي بعد مراجعته بما يحقق التوازن بين الأمن الرقمي وضمان الحقوق والحريات.

الهوامش

(١) النجار، سحر فؤاد مجيد. (٢٠٢٤). الاستجابة الجنائية للجرائم الناجمة عن استخدام تقنية التزييف العميق.

(٢) دياب، محمد فتحي شحاتة. (٢٠٢٤). المسؤولية الجنائية عن الذكاء الاصطناعي والأنظمة المستقلة. القاهرة: دار النهضة العربية.

(٣) مجلس القضاء الأعلى العراقي. (٢٠٢٥). الموقع الرسمي لمجلس القضاء الأعلى العراقي. تم الاسترجاع من: https://www.hjc.iq

(٤) بايوي، سعاد شاكر. (٢٠٢٢). الجرائم الإلكترونية في القانون العراقي. بغداد: دار الكتب القانونية.

(٥) أحمد فتحي سرور. (١٩٨٩). الوسيط في قانون العقوبات – القسم العام. دار النهضة العربية، القاهرة.

(6)Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson

(٧) دياب، محمد فتحي شحاتة. (٢٠٢٤). المسؤولية الجنائية عن الذكاء الاصطناعي والأنظمة المستقلة. القاهرة: دار النهضة العربية.

(8)Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson

(٩) المفوضية الأوروبية. (٢٠٢١). مقترح قانون الذكاء الاصطناعي الأوروبي.

(١٠) النجار، سحر فؤاد مجيد. (٢٠٢٤). الاستجابة الجنائية للجرائم الناجمة عن استخدام تقنية التزييف العميق.

(١١) حسين علي، حيدر، وآخرون. (٢٠٢٥). المسؤولية الجنائية الناجمة عن الجرائم التي ترتكبها الروبوتات.

(١٢) المفوضية الأوروبية. (٢٠٢١). مقترح قانون الذكاء الاصطناعي الأوروبي.

(١٣) دياب، محمد فتحي شحاتة. (٢٠٢٤). المسؤولية الجنائية عن الذكاء الاصطناعي والأنظمة المستقلة. القاهرة: دار النهضة العربية.

(١٤) النجار، سحر فؤاد مجيد. (٢٠٢٤). الاستجابة الجنائية للجرائم الناجمة عن استخدام تقنية التزييف العميق.

(١٥) المفوضية الأوروبية. (٢٠٢١). مقترح قانون الذكاء الاصطناعي الأوروبي

(١٦) بايوي، سعاد شاكر. (٢٠٢٢). الجرائم الإلكترونية في القانون العراقي. بغداد: دار الكتب القانونية.

(١٧) الإنتربول. (٢٠٢٣). الجريمة الإلكترونية.

(١٨) الإنتربول. (٢٠٢٣). الجريمة الإلكترونية

(19)Kietzmann, J., et al. (2020). Deepfakes: Trick or treat

(٢٠) يوروبول. (٢٠٢٣). تقييم تهديدات الجريمة المنظمة عبر الإنترنت.

(٢١) بايوي، سعاد شاكر. (٢٠٢٢). الجرائم الإلكترونية في القانون العراقي. بغداد: دار الكتب القانونية.

(٢٢) النجار، سحر فؤاد مجيد. (٢٠٢٤). الاستجابة الجنائية للجرائم الناجمة عن استخدام تقنية التزييف العميق.

(٢٣) الإنتربول. (٢٠٢٣). الجريمة الإلكترونية

(٢٤) محكمة التمييز الاتحادية – هيئة الأحداث. (٢٠٢٤). القرار المرقم (١٨٥١/هيئة الأحداث/٢٠٢٤) الصادر بتاريخ ٢٠ تشرين الأول/أكتوبر ٢٠٢٤، بغداد، العراق.

(٢٥) محكمة التمييز الاتحادية، هيئة الأحداث. (٢٠٢٤، ١٥ تشرين الأول). القرار رقم (١٨٤١/هيئة الأحداث/٢٠٢٤). بغداد، العراق.

(٢٦) دياب، محمد فتحي شحاتة. (٢٠٢٤). المسؤولية الجنائية عن الذكاء الاصطناعي والأنظمة المستقلة. القاهرة: دار النهضة العربية.

(٢٧) بايوي، سعاد شاكر. (٢٠٢٢). الجرائم الإلكترونية في القانون العراقي. بغداد: دار الكتب القانونية.

(٢٨) مجلس القضاء الأعلى العراقي. (٢٠٢٣). إحصائية الدعاوى المحسومة المتعلقة بالجرائم الاقتصادية والابتزاز الإلكتروني والعنف الأسري في المحاكم العراقية خلال عام ٢٠٢٣. بغداد، العراق.

المصادر

المصادر العربية

١. أحمد فتحي سرور. (١٩٨٩). الوسيط في قانون العقوبات – القسم العام. القاهرة: دار النهضة العربية.

٢. بايوي، سعاد شاكر. (٢٠٢٢). الجرائم الإلكترونية في القانون العراقي. بغداد: دار الكتب القانونية.

٣. حسين علي، حيدر، وآخرون. (٢٠٢٥). المسؤولية الجنائية الناجمة عن الجرائم التي ترتكبها الروبوتات.

٤. دياب، محمد فتحي شحاتة. (٢٠٢٤). المسؤولية الجنائية عن الذكاء الاصطناعي والأنظمة المستقلة. القاهرة: دار النهضة العربية.

٥. النجار، سحر فؤاد مجيد. (٢٠٢٤). الاستجابة الجنائية للجرائم الناجمة عن استخدام تقنية التزييف العميق.

٦. مجلس القضاء الأعلى العراقي. (٢٠٢٣). إحصائية الدعاوى المحسومة المتعلقة بالجرائم الاقتصادية والابتزاز الإلكتروني والعنف الأسري في المحاكم العراقية خلال عام ٢٠٢٣. بغداد، العراق.

٧. مجلس القضاء الأعلى العراقي. (٢٠٢٥). الموقع الرسمي لمجلس القضاء الأعلى العراقي. تم الاسترجاع من: مجلس القضاء الأعلى العراقي

٨. محكمة التمييز الاتحادية – هيئة الأحداث. (٢٠٢٤، ١٥ تشرين الأول). القرار رقم (١٨٤١/هيئة الأحداث/٢٠٢٤). بغداد، العراق.

٩. محكمة التمييز الاتحادية – هيئة الأحداث. (٢٠٢٤، ٢٠ تشرين الأول). القرار رقم (١٨٥١/هيئة الأحداث/٢٠٢٤). بغداد، العراق.

١٠. المفوضية الأوروبية. (٢٠٢١). مقترح قانون الذكاء الاصطناعي الأوروبي.

١١. الإنتربول. (٢٠٢٣). الجريمة الإلكترونية.

١٢. يوروبول. (٢٠٢٣). تقييم تهديدات الجريمة المنظمة عبر الإنترنت.

المصادر الأجنبية

13-Kietzmann, J., McCarthy, I. P., Kietzmann, T. C., & others. (2020). Deepfakes: Trick or Treat? Business Horizons, 63(2), 135–146 .

14-Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

References

1-Sorour, A. F. (1989). ***Al-Wasit fi Qanun Al-Uqubat: Al-Qism Al-'Am (The Mediator in Criminal Law: General Part).*** **Cairo: Dar Al-Nahda Al-Arabiya.**

2-Bayawi, S. S. (2022). ***Cybercrimes in Iraqi Law.*** **Baghdad: Dar Al-Kutub Al-Qanuniyya.**

3-Ali, H., et al. (2025). ***Criminal Liability Arising from Crimes Committed by Robots.***

4-Diab, M. F. S. (2024). ***Criminal Liability for Artificial Intelligence and Autonomous Systems.*** **Cairo: Dar Al-Nahda Al-Arabiya.**

5-Al-Najjar, S. F. M. (2024). ***The Criminal Response to Crimes Resulting from the Use of Deepfake Technology.***

6-Iraqi Supreme Judicial Council. (2023). ***Statistics of Resolved Cases Related to Economic Crimes, Electronic Blackmail, and Domestic Violence in Iraqi Courts During 2023.*** **Baghdad, Iraq.**

7-Iraqi Supreme Judicial Council. (2025). ***Official Website of the Iraqi Supreme Judicial Council.***

8-Federal Court of Cassation – Juvenile Authority. (2024, October 15). ***Decision No. 1841/Juvenile Authority/2024.*** **Baghdad, Iraq.**

9-Federal Court of Cassation – Juvenile Authority. (2024, October 20). ***Decision No. 1851/Juvenile Authority/2024.*** **Baghdad, Iraq.**

10-European Commission. (2021). ***Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).***

11-INTERPOL. (2023). ***Cybercrime.***

12-Europol. (2023). ***Internet Organised Crime Threat Assessment (IOCTA).***

13-Kietzmann, J., McCarthy, I. P., Kietzmann, T. C., et al. (2020). Deepfakes: Trick or Treat? ***Business Horizons, 63*****(2), 135–146.**

14-Russell, S., & Norvig, P. (2021). ***Artificial Intelligence: A Modern Approach*** **(4th ed.). Pearson.**