

الجرائم المستحدثة بواسطة الذكاء الاصطناعي
دراسة تحليلية في ضوء نظام مكافحة الجرائم المعلوماتية السعودي والفقه الإسلامي

Emerging Crimes Committed via Artificial Intelligence: An Analytical Study in Light of the Saudi Anti-Cybercrime Law and Islamic Jurisprudence

[10.35781/1637-000-135-005](#)

الباحث/ عبدالله بن إبراهيم بن سليمان القوييلي*

*طالب دكتوراه في قسم الأنظمة
كلية الأنظمة والاقتصاد
بالجامعة الإسلامية بالمدينة المنورة

الملخص

وقد توصل البحث إلى نتائج جوهرية، أبرزها أن نصوص نظام مكافحة الجرائم المعلوماتية السعودي قادرة بمرونتها على استيعاب الأنماط الإجرامية المستحدثة. ورغم ذلك، فإن التحدي الأكبر يكمن في "إشكالية إسناد المسؤولية الجنائية" نظراً لتعدد الأطراف. وقد خلص البحث إلى أن الفقه الإسلامي يقدم إطاراً تحليلياً لمعالجة هذه الإشكالية عبر قواعده الراسخة في التفريق بين "المباشرة والتسبب"، مما يفتح الباب أمام نموذج فقهي ونظامي لتوزيع المسؤولية بين أطراف المنظومة الذكية.

الكلمات المفتاحية: الذكاء الاصطناعي، الجرائم السيبرانية، نظام مكافحة الجرائم المعلوماتية، الفقه الإسلامي، المسؤولية الجنائية، مقاصد الشريعة، التزييف العميق (Deepfake)، الأمن السيبراني.

يهدف البحث إلى تحليل الأنماط الإجرامية المستحدثة التي ظهرت مع التطورات الأخيرة في الذكاء الاصطناعي التوليدي، وذلك من خلال دراسة مزروجة تقارن بين نظام مكافحة الجرائم المعلوماتية السعودي والمبادئ الحاكمة في الفقه الإسلامي.

وباستخدام المنهج التحليلي المقارن، يستعرض البحث أبرز صور الاستغلال الإجرامي للذكاء الاصطناعي، ويحلل الإشكاليات المتعلقة بالتكييف القانوني والفقهي، وإسناد المسؤولية الجنائية. وقد خلص البحث إلى أن النصوص النظامية الحالية قادرة على استيعاب بعض الأفعال، إلا أنها تواجه تحدياً في معالجة إشكالية المسؤولية الجنائية، وهي إشكالية يقدم الفقه الإسلامي من خلال قواعده العامة أصولاً يمكن الاسترشاد بها لوضع حلول تنظيمية وتشريعية متكاملة.

Emerging Crimes Committed via Artificial Intelligence: An Analytical Study in Light of the Saudi Anti-Cybercrime Law and Islamic Jurisprudence

ABDULLAH IBRAHIM S ALQUWAYFILI*

*PhD Candidate, Department of Law
College of Law and Economics
Islamic University of Madinah

Abstract

This research aims to analyze the emerging criminal patterns associated with recent advancements in generative artificial intelligence, with a focus on assessing the adequacy of the Saudi Anti-Cybercrime Law in addressing them. Using an analytical methodology, the research examines the most prominent forms of criminal exploitation of AI, analyzes the legal complexities related to criminal characterization and the attribution of criminal liability, and links them to the urgent need for legislative development to counter these new threats. The research concludes that while the current law can accommodate some of these acts, it faces a fundamental challenge in addressing the issue of criminal liability and proving crimes committed using these technologies, necessitating legislative intervention to provide clear solutions. Furthermore, the research reached essential findings, most notably

that the provisions of the Saudi Anti-Cybercrime Law, with their inherent flexibility, are capable of accommodating emerging criminal patterns. Nevertheless, the greatest challenge lies in the “problem of attributing criminal liability,” given the multiplicity of actors involved. The research concludes that Islamic jurisprudence offers a robust analytical framework to address this issue through its well-established distinction between *direct action* and *causation*, thereby opening the door to a jurisprudential and legal model for distributing liability among the actors within intelligent systems.

Keywords Artificial Intelligence (AI), Cybercrime, Anti-Cybercrime Law, Criminal Liability, Deepfake, Social Engineering, Cybersecurity, Generative AI.

مقدمة

الحمد لله الذي علم بالقلم، علم الإنسان ما لم يعلم، والصلاة والسلام على نبينا محمد، المبعوث رحمة للعالمين، وعلى آله وصحبه أجمعين، أما بعد :فإن التقدم العلمي والتقني الذي يشهده عصرنا الحالي يفرض على الباحثين في حقل القانون مسؤولية متجددة، تتمثل في استشراف التحديات التي تفرزها هذه التطورات، وتقديم رؤى وحلول تساهم في تحقيق أمن المجتمع واستقراره.

ومن ثم نستعين بالله ونقول:

إن الطفرة الهائلة في تقنيات الذكاء الاصطناعي التوليدي (Generative AI) لم تعد مجرد تطور تقني، بل أصبحت قوة مؤثرة تعيد تشكيل واقعنا بطرق لم تكن متصورة.

فبقدر ما فتحت هذه التقنيات آفاقاً واسعة في شتى المجالات، بقدر ما أفرزت معها أنماطاً إجرامية مستحدثة وأكثر تعقيداً، حيث أصبح بإمكان أي شخص استخدامها في إنشاء محتوى مزيف بواقعية شديدة، أو شن هجمات احتيال متقنة، أو نشر معلومات مضللة على نطاق واسع. وأمام هذا الواقع، تبرز أهمية دراسة مدى جاهزية منظومتنا التشريعية، وفي مقدمتها نظام مكافحة الجرائم المعلوماتية، لمواجهة هذه التحديات الجديدة وضمان حماية المجتمع في الفضاء الرقمي.

وأمام هذا الواقع، تبرز أهمية دراسة مدى جاهزية منظومتنا التشريعية بجناحيها، النظامي المستمد من سلطة ولي الأمر، والشرعي المستمد من أصول الفقه الإسلامي، لمواجهة هذه التحديات الجديدة وضمان حماية المجتمع في الفضاء الرقمي بما يتوافق مع مقاصد الشريعة في حفظ الضروريات الخمس.

أولاً: أهمية البحث ومبررات اختياره

تكمن أهمية هذا البحث في حداثة موضوعه وارتباطه المباشر بأمن المجتمع وقيمه، فهو يتناول ظاهرة تقنية متسارعة من منظور قانوني وشرعي مزدوج، ويسلط الضوء على ضرورة التكامل بين التشريع الوضعي والفقه الإسلامي لمواكبة هذه التطورات، كما تبرز أهميته في ندرة الدراسات التي قامت بهذا الربط التأصيلي، مما يجعل هذا البحث محاولة ضرورية لتقديم رؤية متكاملة.

ثانياً: أهداف البحث

يهدف هذا البحث إلى:

- تحليل أبرز صور الاستغلال الإجرامي لتقنيات الذكاء الاصطناعي التوليدي.
- تقييم مدى كفاية نصوص التجريم الواردة في نظام مكافحة الجرائم المعلوماتية السعودي لمواجهة هذه الجرائم.

- بحث التكييف الفقهي لهذه الجرائم، وتأصيل إشكالية إسناد المسؤولية الجنائية في ضوء قواعد الفقه الإسلامي.
- اقتراح توصيات للمنظم السعودي تجمع بين الحلول النظامية والمبادئ الشرعية.

ثالثاً: مشكلة البحث

أشارت أحدث التقارير الأمنية الدولية إلى أن التطور الهائل في الذكاء الاصطناعي قد أضاف "طبقة جديدة من التعقيد" للمشاهد الأمني، وأن المجرمين يستغلون هذه التقنيات لزيادة حجم وكفاءة عملياتهم الإجرامية بطرق غير مسبوقة.⁽¹⁾

وهنا تبرز الفجوة البحثية التي يسعى هذا البحث لمعالجتها؛ ففي حين أن الخطر التقني معترف به عالمياً، إلا أنه توجد ندرة في الدراسات التي حللت مدى قدرة المنظومة التشريعية السعودية بجناحيها -النظامي والفقهي- على مواكبة هذه التحديات.

وعليه، تتمحور مشكلة البحث في أن هذه الفجوة بين سرعة التطور التقني وبين النصوص النظامية والقواعد الفقهية التقليدية، قد تؤدي إلى صعوبات في التكييف القانوني للفعل، وإسناد المسؤولية الجنائية، وإثبات الجرائم المستحدثة بواسطة الذكاء الاصطناعي.

رابعاً: أسئلة البحث

يسعى هذا البحث إلى الإجابة عن الأسئلة الآتية:

- س1/ ما أبرز صور الاستغلال الإجرامي لتقنيات الذكاء الاصطناعي التوليدي؟
- س2/ إلى أي مدى يمكن تكييف هذه الجرائم ضمن نصوص نظام مكافحة الجرائم المعلوماتية؟
- س3/ ما التكييف الفقهي لهذه الجرائم، وكيف يمكن إسناد المسؤولية الجنائية (الجنائية) في ضوء قواعد الفقه الإسلامي؟
- س4/ ما أبرز التحديات التي تواجه إثبات هذا النوع من الجرائم أمام القضاء؟

(¹) أنظر: يوروبول (Europol)، "اسرق، تعامل، وكرر - كيف يتاجر مجرمو الإنترنت ببياناتك ويستغلونها"، وهو التقرير الاستراتيجي السنوي المعروف بتقييم تهديدات الجريمة المنظمة عبر الإنترنت "IOCTA"، الصادر عن وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون -يوروبول-، وهي الجهة الأمنية الرسمية للاتحاد الأوروبي، ويُعد هذا التقرير من أقوى المصادر المعتمدة عالمياً في تحليل الاتجاهات الحديثة للجريمة الإلكترونية، لوكسمبورغ، مكتب منشورات الاتحاد الأوروبي، 2025م، ص6، متاح على الرابط:

<https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data>.

خامساً: حدود البحث

يتحدد نطاق هذا البحث ضمن حدود متكاملة تضمن تركيز الدراسة ودقتها؛ فمن الناحية الموضوعية، تتركز الدراسة على تحليل الجرائم المستحدثة التي يتم ارتكابها بواسطة تقنيات الذكاء الاصطناعي التوليدي، كالاختيال المالي المتقدم والتزيف العميق لأغراض التشهير والابتزاز. ويتم تحليل هذه الأفعال من منظور مزدوج يجمع بين الجانب النظامي، المتمثل في نصوص نظام مكافحة الجرائم المعلوماتية السعودي، والجانب الفقهي، بالتركيز على قواعد الفقه الجنائي الإسلامي. أما من الناحية المكانية، فيقتصر نطاق الدراسة على الأنظمة المطبقة في المملكة العربية السعودية. ومن الناحية الزمانية، تغطي الدراسة الفترة الممتدة من بداية الانتشار الواسع لهذه التقنيات عام 2022م وحتى تاريخ إعداد هذا البحث (سبتمبر 2025م).

وعليه، يخرج عن النطاق الموضوعي لهذه الدراسة الجوانب التقنية البحتة لبرمجة الذكاء الاصطناعي، وكذلك المسؤولية المدنية (التعويض عن الضرر)، كما لا تتوسع الدراسة في تحليل التشريعات المقارنة إلا بالقدر الذي يخدم المقارنة والتحليل.

سادساً: تقسيم البحث

يتكون هذا البحث من مقدمة، وثلاثة مباحث، وخاتمة، وذلك على النحو التالي:

- **المبحث الأول: الطبيعة المستحدثة للجرائم المرتكبة بواسطة الذكاء الاصطناعي وتكييفها الفقهي.**
 - **المطلب الأول:** ماهية الذكاء الاصطناعي التوليدي كأداة إجرامية.
 - **المطلب الثاني:** صور الاستغلال الإجرامي للذكاء الاصطناعي (الاختيال، التزيف العميق، التحريض).
 - **المطلب الثالث:** التكييف الفقهي للجرائم المستحدثة في ضوء مقاصد الشريعة.
- **المبحث الثاني: المواجهة التشريعية للجرائم المستحدثة بين النظام السعودي والفقه الإسلامي.**
 - **المطلب الأول:** مدى انطباق نصوص التجريم في نظام مكافحة الجرائم المعلوماتية على الجرائم المستحدثة.
 - **المطلب الثاني:** إشكالية إسناد المسؤولية الجنائية في النظام السعودي.
 - **المطلب الثالث:** تأصيل المسؤولية الجنائية في الفقه الإسلامي وتطبيقاتها المعاصرة.

• المبحث الثالث: تحديات الإثبات والمواجهة المستقبلية.

○ **المطلب الأول:** صعوبات إثبات الجرائم المرتكبة بواسطة الذكاء الاصطناعي.

○ **المطلب الثاني:** الآفاق المستقبلية للمواجهة التشريعية والفقهية.

• **النتائج والتوصيات.**

• **الخاتمة.**

المبحث الأول

الطبيعة المستحدثة للجرائم المرتكبة بواسطة الذكاء الاصطناعي وتكييفها الفقهي

تمهيد وتقسيم:

لم يعد الذكاء الاصطناعي مجرد أداة تقنية مساعدة، بل أصبح قوة فاعلة قادرة على محاكاة الإبداع البشري، مما أفرز أنماطاً إجرامية مستحدثة لم تكن معهودة من قبل، وهذه الطبيعة الجديدة تتحدى المفاهيم المعروفة للجريمة التقليدية، وهو الأمر الذي يفرض بدوره على الفقه الإسلامي والنظام القانوني ضرورة البحث عن تكييف دقيق لهذه الأفعال لتحديد مدى خطورتها وأبعادها.

وعليه، فإن فهم هذه الظاهرة يقتضي أولاً تفكيك الأداة نفسها لفهم قدراتها الإجرامية، ثم استعراض أبرز صور استغلالها عملياً، وأخيراً تأصيلها فقهيّاً لبيان حكم الشريعة فيها.

ولتحقيق هذا الهدف، سيتم تقسيم هذا المبحث إلى ثلاثة مطالب متكاملة:

المطلب الأول: ماهية الذكاء الاصطناعي التوليدي كأداة إجرامية.

المطلب الثاني: صور الاستغلال الإجرامي للذكاء الاصطناعي (الاحتيال، التزييف العميق، التحريض).

المطلب الثالث: التكييف الفقهي للجرائم المستحدثة في ضوء مقاصد الشريعة.

المطلب الأول

ماهية الذكاء الاصطناعي التوليدي كأداة إجرامية

يهدف علم الذكاء الاصطناعي، كما عرفه رائد هذا المجال جون مكارثي، إلى "علم وهندسة صنع الآلات الذكية"، ورغم تعدد التعريفات، فإنها تجتمع حول هدف بناء أنظمة ذكية قادرة على محاكاة القدرات البشرية أو التفوق عليها.⁽²⁾

وفيما يخص بحثنا هذا، فإن النوع الأكثر أهمية وخطورة هو "الذكاء الاصطناعي التوليدي" (Generative AI)، وخلافاً للذكاء الاصطناعي التقليدي الذي يحلل البيانات الموجودة، فإن هذا النوع يُنشئ محتوى جديداً وأصيلاً لم يكن موجوداً من قبل، كالنصوص والصور والأصوات. وهذه القدرة على "الخلق والإبداع" هي التي حولته من مجرد أداة تحليل إلى سلاح قوي يمكن استغلاله في ارتكاب جرائم متقدمة، وهو ما سيتم تفصيله في هذا المطلب.⁽³⁾

وتتجلى خطورة هذه الأداة في أنها خفضت من حاجز المهارات المطلوبة لارتكاب الجريمة، وأتاحت للمجرمين قليلي الخبرة تنفيذ هجمات متطورة كانت في السابق حكراً على المحترفين دون غيرهم، ويؤكد تقرير يوروبول لعام 2025 أن الذكاء الاصطناعي يزيد من حجم وكفاءة العمليات الإجرامية، ويحسن من فعالية تقنيات الهندسة الاجتماعية عبر تخصيص التواصل مع الضحايا وأتمتة العمليات الإجرامية ويتم ذلك من خلال عدة قدرات جوهرية يستغلها المجرمون، أبرزها:

أولاً: تعزيز فعالية الهندسة الاجتماعية

حيث تستخدم النماذج اللغوية الكبيرة (LLMs) في إنشاء رسائل تصيد احتيالي (Phishing) تتميز بقدرتها العالية على الإقناع والتخصيص، وقد أثبتت التقارير الحديثة فعاليتها المتزايدة؛ حيث أوضح تقرير من المجلس الأطلسي (Atlantic Council) قدرة الذكاء الاصطناعي على إنتاج رسائل أكثر إقناعاً من الرسائل التقليدية⁽⁴⁾، بينما أكد تقرير الدفاع الرقمي من مايكروسوفت (Microsoft) أن الرسائل المولدة عبر هذه النماذج حققت معدل استجابة أعلى بكثير من الرسائل

(2) سعيد، وليد سعد الدين محمد، "المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي"، مجلة العلوم القانونية والاقتصادية، مجلد 64، عدد 2، 2022م، ص 491.

(3) أنظر: يوروبول (Europol)، "اسرق، تعامل، وكرر - كيف يتاجر مجرمو الإنترنت ببياناتك ويستغلونها"، مرجع سابق، ص 14.

(4) أنظر: Atlantic Council، القرصنة باستخدام الذكاء الاصطناعي: استخدام الذكاء الاصطناعي التوليدي في الأنشطة السيبرانية الخبيثة، الملخص التنفيذي، ص4، متاح على الرابط:

التقليدية، مما يجعلها تهديداً متزايداً على المؤسسات. (5)

ثانياً: إنشاء المحتوى المزيف (Deepfake)

يستغل المجرمون الذكاء الاصطناعي التوليدي لإنشاء صور ومقاطع فيديو وتسجيلات صوتية مزيفة بواقعية شديدة (voice deepfakes)، والتي تُستخدم في التشهير والابتزاز والاحتيال المالي وانتحال الشخصية.

ثالثاً: الأتمتة والنشر على نطاق واسع

يتيح الذكاء الاصطناعي للمجرمين أتمتة عملياتهم، واستهداف عدد كبير من الضحايا بلغات متعددة وفي وقت واحد، مما يجعل جهودهم الإجرامية أكثر كفاءة وانتشاراً. (6)

المطلب الثاني

صور الاستغلال الإجرامي للذكاء الاصطناعي في ضوء النظام السعودي

بعد أن استعرضنا القدرات الجوهرية للذكاء الاصطناعي التوليدي كأداة إجرامية، نتناول في هذا المطلب بالتحليل أبرز صور الاستغلال العملي لهذه القدرات، مع ربط كل صورة منها بنصوص التجريم الواردة في نظام مكافحة الجرائم المعلوماتية السعودي.

الفرع الأول: جرائم الاحتيال المالي والابتزاز المتقدمة

يعالج نظام مكافحة الجرائم المعلوماتية⁽⁷⁾ بشكل مباشر وصريح جريمة الاحتيال المالي المرتكبة عبر الوسائل التقنية، ويتجلى ذلك في المادة الرابعة منه، التي نصت على تجريم فعل "الاستيلاء لنفسه أو لغيره على مال منقول أو على سند... وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة"

وهذا النص النظامي يتصدى مباشرة لجوهر جريمة الاحتيال المالي، والتي تُعد ظاهرة عالمية واسعة الانتشار تهدف إلى تغليب المصلحة الفردية على المصالح العامة بطرق غير مشروعة، وقد عرف دليل مكافحة الاحتيال المالي الصادر من البنك المركزي السعودي الاحتيال المالي بأنه "أي عمل يهدف

(5) أنظر: Microsoft، تقرير الدفاع الرقمي لمايكروسوفت 2024، ص 90، متاح على الرابط:

<https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>

(6) أنظر: يوروبول (Europol)، "اسرق، تعامل، وكرر - كيف يتاجر مجرمو الإنترنت ببياناتك ويستغلونها"، مرجع سابق، ص 6، 14، 22.

(7) المملكة العربية السعودية، نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8هـ.

للحصول على فائدة غير مشروعة عن طريق استغلال وسائل تقنية أو مستندية أو علاقات أو سبل اجتماعية⁽⁸⁾

وقد انتقل هذا المفهوم التقليدي للخداع إلى أبعاد أكثر تعقيداً بفضل الذكاء الاصطناعي، الذي حول الاحتيال من الرسائل العامة والعشوائية إلى هجمات شديدة التخصيص والإقناع. وتتمثل أبرز صور ذلك في رسائل التصيد الاحتيالي الموجهة (Spear Phishing)، حيث تُستخدم النماذج اللغوية الكبيرة (LLMs) لإنشاء رسائل بريد إلكتروني مقنعة وموجهة بدقة، تبدو وكأنها من مصدر موثوق. كما برز الاحتيال الصوتي (Vishing) كأداة خطيرة، حيث يمكن للمجرمين استخدام تقنية تزييف الصوت (Voice Deepfakes) لانتحال شخصية مدير تنفيذي في مكاملة هاتفية لإعطاء أمر بتحويل مبالغ مالية، وهو ما يشكل صورة متقدمة من الاحتيال. وإذا اقترن هذا الفعل بالتهديد، فإنه يدخل في نطاق المادة الثالثة من النظام، التي تجرم "الدخول غير المشروع لتهديد شخص أو ابتزازه."⁽⁹⁾

الفرع الثاني: جرائم التشهير والمساس بالحياة الخاصة عبر التزييف العميق

تُعد تقنية التزييف العميق (Deepfake) من أخطر إفرازات الذكاء الاصطناعي، وقد عرفتها الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) بأنها: "وسائط اصطناعية شديدة الواقعية تم إنشاؤها باستخدام تقنيات التعلم العميق التي تتلاعب بالصوت أو الفيديو أو أي محتوى رقمي آخر لتغيير شكل الأشخاص أو الأشياء أو الأحداث أو أفعالهم أو مظهرهم بشكل مقنع، مما يجعل من الصعب التمييز بين المحتوى الحقيقي والمزيف."⁽¹⁰⁾

ويشكل استخدام هذه التقنية لإنشاء محتوى يسيء لسمعة الأفراد اعتداءً مباشراً يقع تحت طائلة المادة الثالثة من نظام مكافحة الجرائم المعلوماتية التي تجرم صراحةً "التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة"،

كما أن استخدام هذه التقنية في إنشاء مقاطع خادشة للحياء أو تمس بخصوصية الأفراد، يمثل انتهاكاً يمكن تكييفه ضمن جريمة "المساس بالحياة الخاصة" الواردة في ذات المادة. ويمكن أيضاً أن يرقى هذا الفعل إلى مستوى التجريم الوارد في المادة السادسة من النظام، التي تعاقب على "إنتاج ما

(8) المملكة العربية السعودية، البنك المركزي السعودي، دليل مكافحة الاحتيال المالي في البنوك والمصارف العاملة بالمملكة، رقم الإصدار 2، أغسطس 2020، ص. 4-10.

(9) أنظر: يوروبول (Europol)، "اسرق، تعامل، وكرر - كيف يتاجر مجرمو الإنترنت ببياناتك ويستغلونها"، مرجع سابق، ص. 14.

(10) الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، مبادئ التزييف العميق، النسخة 1، بدون تاريخ نشر، ص. 23، متاح على الرابط التالي:

من شأنه المساس... بالآداب العامة، أو حرمة الحياة الخاصة.⁽¹¹⁾

الفرع الثالث: جرائم التحريض ونشر المعلومات المضللة الآلية

يأتي التحريض في الفضاء الرقمي غالباً بشكل عام أو غير مباشر، حيث لا يستهدف المحرض شخصاً محدداً بعينه، بل يهدف إلى بث ثقافة إجرامية رقمية تفتح الباب أمام عدد غير محدود من المتلقين لارتكاب الجريمة، وقد تطور هذا النمط بشكل خطير مع التقنيات الحديثة، لدرجة أصبح معها المحرض قادراً على الاستعانة بتقنيات الذكاء الاصطناعي التوليدي لإنتاج مضامين جذابة وموجهة، كما يمكنه استغلال الحسابات الآلية (Bots) لإعادة إنتاج الخطاب التحريضي بشكل متكرر، مما يخلق وهماً عاماً وجود قبول اجتماعي واسع له.⁽¹²⁾

وهذا النوع من الحملات المنظمة التي تهدف إلى إثارة الفتنة أو زعزعة الاستقرار يجد مواجته النظامية في نصين متكاملين ضمن نظام مكافحة الجرائم المعلوماتية⁽¹³⁾:

أولاً: من حيث المحتوى - بحسب المادة السادسة

تعالج هذه المادة محتوى الرسالة التحريضية نفسها، حيث تجرم بشكل مباشر "إنتاج ما من شأنه المساس بالنظام العام... أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية". وبذلك، فإن أي حملة آلية تستخدم البوتات لنشر معلومات مضللة أو خطاب كراهية يهدف إلى الإخلال بالنظام العام، تقع تحت طائلة هذه المادة، بغض النظر عما إذا كانت تحرض على جريمة أخرى أم لا.

ثانياً: من حيث السلوك - بحسب المادة التاسعة

أما هذه المادة، فهي تعالج فعل التحريض ذاته، فإذا كانت الحملات الآلية التي تستخدم الذكاء الاصطناعي لا تكتفي بالمساس بالنظام العام، بل تحرض على ارتكاب جريمة أخرى منصوص عليها في النظام (مثل التحريض على اختراق موقع إلكتروني، وهي جريمة معاقب عليها في المادة الثالثة)، فإنها تخضع أيضاً لأحكام المادة التاسعة التي تجرم التحريض بشكل خاص.

(11) نظام مكافحة جرائم المعلوماتية، مرجع سابق، المادة 6 و3.

(12) أنظر: بوكراع، محمد ياسين، "التحريض على الجريمة في التشريع الجزائري"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2021م، ص 11-12؛ صالح، ليلى، "جريمة التحريض عبر مواقع التواصل الاجتماعي"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2021م، ص 14-17؛ الشريف، محمود سلامه، "الجرائم المرتكبة عبر الشات بوت Chatbot - والمسؤولية الجنائية عنها"، بحث مقدم في المؤتمر العلمي الثامن: التحديات القانونية في العصر الرقمي، كلية الحقوق، جامعة السلطان قابوس، 2024م، ص 235.

(13) نظام مكافحة جرائم المعلوماتية، مرجع سابق، المادة 6 و9.

المطلب الثالث

التكييف الفقهي للجرائم المستحدثة في ضوء مقاصد الشريعة

تتميز الشريعة الإسلامية بمرونتها وقدرتها على استيعاب النوازل والمستجدات، وذلك من خلال قواعدها الكلية ومقاصدها العليا التي تهدف إلى تحقيق مصالح العباد ودرء المفسد عنهم. والجرائم المستحدثة بواسطة الذكاء الاصطناعي، رغم حداثة أساليبها، إلا أن آثارها وأضرارها تقع ضمن الدائرة التي عالجها الفقه الإسلامي، ولبيان الحكم الشرعي في هذه الأفعال، لا بد من تكييفها فقهيًا من خلال ربطها بمقاصد الشريعة، ثم تحديد نوع العقوبة المناسبة لها.

الفرع الأول: مفهوم التكيف الفقهي

يُعرَّف التكيف في اللغة بأنه مصدر من الفعل "كَيَّفَ" المأخوذ من مادة (كيف)، وهذه الكلمة موضوعة في أصلها للاستفهام عن حال الشيء وصفته، ومن ثم فإن الكيفية هي الحال والهيئة التي يكون عليها الشيء.

أما في الاصطلاح الفقهي فهو مصطلح مؤلّد لم يرد استعماله عند العرب في الجاهلية، وإنما جرى توظيفه عند الفقهاء والأصوليين للدلالة على إلحاق النازلة أو الواقعة المستجدة بأصل فقهي أو قاعدة شرعية معلومة، حتى يتحدد حكمها تبعاً لذلك الأصل، وبناء على هذا فإن التكيف الفقهي يمثل عملية اجتهادية غايتها بيان الصلة بين الحوادث المستحدثة وبين ما تقرر في الشريعة من أحكام كلية أو جزئية، كما في تنزيل صور المعاملات الحديثة أو الجرائم الإلكترونية على أبواب الغرر أو التدليس أو القذف أو أكل المال بالباطل بحسب طبيعتها وما يترتب عليها من آثار.⁽¹⁴⁾

الفرع الثاني: مقاصد الشريعة والضروريات الخمس

يقصد بالضروريات الخمس تلك المقاصد الكلية التي جاءت الشريعة الإسلامية لحفظها، وهي الدين والنفس والعرض والعقل والمال، ويختلف ترتيبها حسب أهميتها ومقام كل منها في تحقيق مصالح الإنسان والدنيا والآخرة.

فقد بين العلماء أن حفظ الدين يُقدم على سائر الضروريات عند المعارضة، لأنه المقصد الأعظم للشرع، كما جاء في قوله تعالى: ﴿وَمَا خَلَقْتُ الْجِنَّ وَالْإِنْسَ إِلَّا لِيَعْبُدُونِ﴾ (الذاريات: 56)، فهو المقصود من أجله وثمرته أكمل الثمرات، إذ يحقق نيل السعادة الأبدية في جوار الله عز وجل.

يلي حفظ الدين في الأهمية حفظ النفس، لأنه أصل حصول العبادات والمصالح الدينية، إذ لا

(14) أنظر: الشمري، إبراهيم بن ممدوح، "التكييف الفقهي وأثر تغيره: دراسة تأصيلية، وتطبيقية على منتجات مالية إسلامية"، مجلة العلوم الشرعية، جامعة الإمام محمد بن سعود الإسلامية، مج. 5، ع. 67، 1444هـ، ص 414.

يمكن للإنسان القيام بواجباته الدينية إلا ببقاء النفس.

ثم يأتي حفظ العرض، لأنه لبقاء نسل الإنسان، إذ بتعظيم تحريم الزنا وحماية النسب يحصل صون تربية الفرد وحفظ حياته.

بعد ذلك يُقدم حفظ العقل على حفظ المال، لأن ضياع العقل يؤدي إلى فساد النفس وسقوط التكليف الشرعي، إذ الإنسان بفقدانه يلتحق بالحيوانات، ولا يقوى على أداء عباداته وأحكامه الشرعية، بينما المال يُحفظ أخيراً، لأن فقدانه لا يفوت الضرورات الكبرى إلا إذا أدى إلى فقدان النفس أو العقل، ويعتبر صيانتها ضرورياً لضمان حياة الإنسان وحقوقه المادية.⁽¹⁵⁾

الفرع الثالث: التكليف الفقهي للجرائم المستحدثة في ضوء مقاصد الشريعة

بناءً على ما سبق من تعريف للتكليف الفقهي وبيان لمقاصد الشريعة، يمكننا الآن تنزيل الجرائم المستحدثة بواسطة الذكاء الاصطناعي على هذه الأصول لتحديد حكمها الشرعي إذ يتضح أن هذه الجرائم، رغم حداثة وسائلها، إلا أنها تمثل اعتداءً مباشراً على الضروريات الخمس التي جاءت الشريعة بحفظها، وذلك على النحو التالي: ما يمس الدين أو العقيدة يُعتبر اعتداءً على الدين، ويشمل ذلك نشر الإلحاد أو التحريض على الفتن الدينية والطائفية.

وما يهدد النفس أو سلامة الإنسان يُعد اعتداءً على النفس، ويشمل التهديد بالعنف أو الإيذاء الجسدي.

أما ما يسيء إلى شرف الفرد أو عرضه، مثل التشهير أو الابتزاز الرقمي، أو التحرش الإلكتروني فيُصنف ضمن الاعتداء على العرض، إذ تمثل هذه الأفعال انتهاكاً لكرامة الإنسان وحقوقه التي حفظتها الشريعة الإسلامية.

وما يضلّل العقل أو يمنع القدرة على التمييز، مثل نشر المعلومات المضللة أو حملات التحريض الإلكتروني، يُعد اعتداءً على العقل لأنه يعطل القدرة على اتخاذ القرار الصحيح ويعيق الاستفادة من المعرفة.

وأخيراً، ما يرتكب من سرقة أو تزوير أو احتيال مالي باستخدام الذكاء الاصطناعي، مثل الاحتيال المصرفي أو التزييف الصوتي للاستيلاء على الأموال، يُصنف ضمن الاعتداء على المال.

وبتيج هذا التكليف الفقهي للفقهاء تحديد العقوبة المناسبة لكل جريمة مستحدثة، بحيث يكون الحكم متوافقاً مع نصوص الشريعة ومقاصدها، ويحقق الموازنة بين صون المصالح العليا ودرء

(15) أنظر: محمود، عباس إبراهيم أحمد، "الضروريات الخمس وأثرها في تحقيق الأمن الاجتماعي"، مجلة كلية الشريعة والقانون - جامعة أم درمان الإسلامية، مج. 3، ع. 3، 2018م، ص 231.

المفاسد المحتملة، مع مراعاة حداثة الوسائل وخصوصية الظروف الرقمية والتكنولوجية المعاصرة، بما يحفظ كرامة الإنسان ويصون المجتمع من الفوضى والانحراف.

وعليه، وبما أن هذه الجرائم مستحدثة في وسائلها ولم يرد فيها حد مقدر أو قصاص، فإنها تدخل بالكامل تحت سلطة ولي الأمر في العقوبة، وهو ما يُعرف في الفقه الإسلامي بباب "التعزير".⁽¹⁶⁾ وهذا يمنح المنظم سلطة تقديرية واسعة لتقدير العقوبة الرادعة التي تحقق المصلحة وتدفع المفسدة، وهو ما يتوافق تماماً مع فلسفة نظام مكافحة الجرائم المعلوماتية السعودي.

المبحث الثاني

المواجهة التشريعية للجرائم المستحدثة بين النظام السعودي والفقه الإسلامي

تمهيد وتقسيم:

بعد أن تم استعراض الطبيعة المستحدثة للجرائم المرتكبة بواسطة الذكاء الاصطناعي وتكييفها الفقهي الأولي، يبرز التساؤل الجوهرى حول مدى جاهزية المنظومة التشريعية لمواجهة هذه التحديات. فهذه الجرائم لا تختبر فقط قدرة النصوص النظامية على استيعابها، بل تثير أيضاً إشكاليات عميقة حول إسناد المسؤولية الجنائية، وهي إشكالية تتطلب تأصيلاً فقهياً وقانونياً دقيقاً.

وعليه، يهدف هذا المبحث إلى تحليل المواجهة التشريعية لهذه الجرائم من خلال منظور مزدوج يجمع بين النظام السعودي والفقه الإسلامي. ولتحقيق هذا الهدف، سيتم تقسيم هذا المبحث إلى ثلاثة مطالب متكاملة:

المطلب الأول: مدى انطباق نصوص التجريم في نظام مكافحة الجرائم المعلوماتية على الجرائم المستحدثة.

المطلب الثاني: إشكالية إسناد المسؤولية الجنائية في النظام السعودي.

المطلب الثالث: تأصيل المسؤولية الجنائية في الفقه الإسلامي وتطبيقاتها المعاصرة.

⁽¹⁶⁾ أنظر: عودة، عبد القادر، "التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي"، ج1، بيروت، دار الكاتب العربي، 1977م، ص 80.

المطلب الأول

مدى انطباق نصوص التجريم في نظام مكافحة الجرائم المعلوماتية على الجرائم المستحدثة

رغم أن نظام مكافحة جرائم المعلوماتية السعودي⁽¹⁷⁾ قد صدر قبل الطفرة الأخيرة في الذكاء الاصطناعي التوليدي، إلا أن نصوصه جاءت بصياغة مرنة تتسم بالعمومية، مما يمنحها القدرة على استيعاب العديد من الأنماط الإجرامية المستحدثة، ويتضح ذلك من خلال تحليل انطباق أبرز موادها على الجرائم التي سبق تفصيلها:

أولاً: مواجهة جرائم الاحتيال المالي والابتزاز المتقدمة

يعالج النظام هذه الجرائم بشكل مباشر؛ فجريمة الاحتيال المالي المرتكبة عبر رسائل التصيد الاحتيالي الموجهة (Spear Phishing) التي يصنعها الذكاء الاصطناعي، تندرج بوضوح تحت طائلة المادة الرابعة من النظام، التي تجرم "الاستيلاء على مال... عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة".

أما استخدام تقنية تزييف الصوت (Voice Deepfakes) في الابتزاز، فيجد تجريمه في المادة الثالثة التي تعاقب على "الدخول غير المشروع لتهديد شخص أو ابتزازه".

ثانياً: مواجهة جرائم التشهير والمساس بالحياة الخاصة

تجد جرائم التزييف العميق (Deepfake) التي تهدف إلى الإساءة للسمعة مواجهتها الصريحة في المادة الثالثة من النظام، التي تجرم "التشهير بالآخرين، وإلحاق الضرر بهم". كما أن استخدام هذه التقنية في إنشاء محتوى يمس بخصوصية الأفراد أو يخل بالآداب، يمكن تكييفه ضمن جريمة "المساس بالحياة الخاصة" الواردة في ذات المادة، أو جريمة "إنتاج ما من شأنه المساس بالآداب العامة أو حرمة الحياة الخاصة" المعاقب عليها في المادة السادسة.

ثالثاً: مواجهة جرائم التحريض ونشر المعلومات المضللة

إن استخدام "البوتات" الذكية في حملات منظمة تهدف إلى إثارة الفتنة أو زعزعة الاستقرار يمثل اعتداءً مباشراً على "النظام العام"، وهو ما تجرمه المادة السادسة من النظام. وإذا كانت هذه الحملات تحرض على ارتكاب جريمة أخرى منصوص عليها في النظام، فإنها تخضع أيضاً لأحكام المادة التاسعة المتعلقة بالتحريض.

(17) نظام مكافحة الجرائم المعلوماتية، مرجع سابق.

ورغم هذه القدرة على الاستيعاب، تبقى هناك تحديات تتعلق بمدى كفاية هذه النصوص في مواجهة تعقيدات إثبات القصد الجنائي وإسناد المسؤولية، وهو ما سيتم بحثه لاحقاً.

المطلب الثاني

إشكالية إسناد المسؤولية الجنائية في النظام السعودي

تعد إشكالية تحديد المسؤول الجنائي هي التحدي الأكبر الذي تفرزه جرائم الذكاء الاصطناعي، وهي إشكالية لم تعالجها النصوص النظامية الحالية بشكل مباشر، فمن المسلم به في الفكر القانوني أن المسؤولية الجنائية لا تقوم إلا على سلوك إنساني صادر عن إدراك وحرية اختيار⁽¹⁸⁾، وهما عنصران لا يتوفران في أنظمة الذكاء الاصطناعي بوضعها الحالي. فهي وإن بلغت درجة عالية من التطور، إلا أنها تفتقر إلى الوعي والإرادة الحرة التي هي مناط التكليف.

وعليه، فإن البحث عن المسؤول الجنائي لا يتجه إلى الآلة نفسها، بل إلى الأشخاص الطبيعيين أو الاعتباريين الذين يقفون خلفها. وفي ضوء النظام السعودي، يمكن تحليل هذه الإشكالية من خلال بحث مسؤولية كل طرف على حدة:

أولاً: مسؤولية المستخدم (User)

وهو الشخص الذي يستخدم الذكاء الاصطناعي كأداة لتحقيق نتيجة إجرامية. في هذه الحالة، تكون المسؤولية واضحة، حيث يُعتبر المستخدم فاعلاً أصلياً للجريمة. فهو لم يرتكب الجريمة بيده، بل استخدم الآلة كوسيط، تماماً كمن يستخدم سلاحاً أو يستعين بحيوان في ارتكاب جريمته. وهنا، يجب على جهات التحقيق إثبات الركنتين المادي والمعنوي، أي إثبات أن المستخدم هو من أعطى الأمر للذكاء الاصطناعي، وأن نيته قد اتجهت لتحقيق النتيجة الإجرامية.⁽¹⁹⁾

ثانياً: مسؤولية المبرمج أو المصنع (Developer/Manufacturer)

تثور مسؤولية المبرمج أو المصنع إذا كانت الجريمة ناتجة عن خطأ في تصميم أو برمجة النظام الذكي. ويمكن تصور مسؤوليتهما في حالتين:

- **حالة العمد:** إذا قام المبرمج عمداً بوضع شيفرة برمجية خبيثة في النظام لتحقيق نتيجة إجرامية معينة، أو صممه لغرض إجرامي محدد.

(18) أنظر: عودة، عبد القادر، "التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي"، مرجع سابق، ص 391.

(19) أنظر: سعيد، وليد سعد الدين محمد، "المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي"، مرجع سابق، ص 517.

- حالة الإهمال: إذا وقعت الجريمة نتيجة إهمال جسيم من المبرمج أو المصنع في وضع ضوابط الأمان اللازمة، أو عدم مراعاته لقواعد الحيطة والحذر لمنع استغلال النظام بشكل إجرامي. وفي هذه الحالة، يمكن مساءلته عن جريمة غير عمدية إذا توافرت أركانها.⁽²⁰⁾

ثالثاً: مسؤولية الغير (Third Party)

وهي الحالة التي يقوم فيها طرف ثالث (كمخترق أو قرصان) باختراق نظام الذكاء الاصطناعي، واستغلاله كأداة لتنفيذ جريمته دون علم المستخدم أو المبرمج. في هذه الحالة، يُعتبر هذا الطرف الثالث هو الفاعل الأصلي للجريمة، لأنه سخر الآلة لتحقيق أهدافه الإجرامية، بينما ينتفي القصد الجنائي لدى المستخدم والشركة المصنعة. وتُعد هذه من أعقد الحالات من حيث الإثبات، حيث تتطلب خبرة تقنية عالية لتتبع المخترق وإثبات علاقته بالجريمة.⁽²¹⁾

رابعاً: مسؤولية الشخص الاعتباري (الشركة المصنعة)

إلى جانب مسؤولية الأفراد، أقر المنظم السعودي صراحةً بالمسؤولية الجنائية للشخص الاعتباري (كالشركة المصنعة أو المالكة للذكاء الاصطناعي). ويتضح هذا بشكل جلي من خلال المادة الأولى من نظام مكافحة الجرائم المعلوماتية، التي عرّفت "الشخص" تعريفاً شاملاً بأنه: "أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة."⁽²²⁾

وبناءً على هذا التعريف، فإن نصوص التجريم في النظام التي تبدأ بعبارة "كل شخص يرتكب..." تنطبق مباشرة على الشركات والمؤسسات إذا ارتكبت الجريمة بواسطة أحد ممثليها أو لحسابها. وفي هذه الحالة، يمكن فرض عقوبات تتناسب مع طبيعة الشخص الاعتباري، كالعقوبات المالية، أو إيقاف الترخيص، أو حتى حل الشخص الاعتباري بناءً على المادة الثالثة عشرة من ذات النظام.⁽²³⁾

(20) أنظر: المرجع السابق، ص 515.

(21) أنظر: المرجع السابق، ص 522.

(22) نظام مكافحة جرائم المعلوماتية، مرجع سابق.

(23) أنظر: المرجع السابق، ص 520.

المطلب الثالث

تأصيل المسؤولية الجنائية في الفقه الإسلامي وتطبيقاتها المعاصرة

يقدم الفقه الجنائي الإسلامي، بقواعده المرنة وأصوله الراسخة، إطاراً تحليلياً عميقاً يمكن الاسترشاد به في معالجة إشكالية المسؤولية الجنائية في جرائم الذكاء الاصطناعي. فبينما تقف النظم القانونية الوضعية أمام تحدي إسناد المسؤولية لفاعل غير بشري، نجد أن الفقه الإسلامي قد أسس لنظريات متكاملة في المسؤولية تقوم على مناط التكليف، وهو العقل والإرادة.

الفرع الأول: أساس المسؤولية الجنائية في الفكر الإسلامي

من المبادئ الثابتة في الشريعة الإسلامية أن الإنسان وحده من بين الخلائق يمكن مساءلته جنائياً، لأن الأحكام المتعلقة بالجنايات، بأوامرها ونواهيها، لا يستوعبها ويحيط بمعانيها ونتائجها إلا الإنسان المختص بميزة العقل والإدراك والإرادة.⁽²⁴⁾

وتقوم المسؤولية الجنائية في الفقه الإسلامي على أساس "أهلية الأداء"، والتي مناطها العقل والتمييز، وتنقسم إلى أهلية كاملة وناقصة بحسب المراحل التي يمر بها الإنسان.⁽²⁵⁾

وهذه الأهلية هي التي تجعل الشخص صالحاً لتحمل نتائج أفعاله المحرمة التي يأتيها وهو مختار ومدرك لمعانيها ونتائجها. وعليه، فإن أساس المسؤولية يقوم على ركنين جوهريين لا تتعقد بدونهما : الإدراك (فهم ماهية الفعل وقيمه الاجتماعية) وحرية الاختيار (القدرة على توجيه الإرادة نحو الفعل أو الترك).⁽²⁶⁾

الفرع الثاني: قواعد إسناد المسؤولية الجنائية في الفقه الإسلامي

لتحديد المسؤول عن الجريمة عند تعدد المساهمين فيها، وضع الفقهاء قواعد دقيقة لتوزيع المسؤولية، أبرزها قاعدة التفريق بين المباشر والمتسبب:

- **الشريك المباشر:** هو من يباشر تنفيذ الركن المادي للجريمة بنفسه أو يساهم فيه مادياً.
- **الشريك المتسبب:** هو من لا يباشر التنفيذ المادي، ولكنه يتسبب في وقوع الجريمة من خلال التحريض أو الاتفاق أو المساعدة.

(24) عودة، عبد القادر، "التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي"، مرجع سابق، ص116.

(25) وزارة الأوقاف والشؤون الإسلامية بالكويت، الموسوعة الفقهية الكويتية، 1404-1427هـ، ج7، ص153.

(26) عودة، عبد القادر، "التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي"، مرجع سابق، ص382.

والقاعدة العامة في الشريعة هي أن العقوبات المقدرة (الحدود والقصاص) تقع على من باشر الجريمة دون المتسبب، أما الشريك المتسبب فجريمته تدخل في باب التعزير. إلا أن الفقهاء استثنوا من ذلك جرائم الاعتداء على النفس وما دونها، نظراً لطبيعتها التي قد تقع بالتسبب بقوة المباشرة.

وتصبح العلاقة أكثر تعقيداً عند اجتماع المباشر والمتسبب في فعل واحد، وهنا وضع الفقهاء ضوابط لترجيح المسؤولية؛ فالأصل أن يُضاف الحكم إلى المباشر، ولكن قد يُقدّم المتسبب على المباشر إذا كان تسببه أقوى من المباشرة، كما في حالة الإكراه، أو استخدام شخص غير أهل للمسؤولية (كصغير أو مجنون) كأداة في الجريمة، أو التفرير بشخص من خلال شهادة الزور.⁽²⁷⁾

الفرع الثالث: تطبيقات القواعد الفقهية على جرائم الذكاء الاصطناعي

بتنزيل هذه القواعد الفقهية على واقع جرائم الذكاء الاصطناعي، يمكننا الخروج بتأصيل واضح لمسؤولية كل طرف:

- **مسؤولية المستخدم (User):** بتطبيق قاعدة "المباشرة والتسبب"، يمكن تكييف المستخدم الذي يعطي الأمر للذكاء الاصطناعي على أنه "فاعل مباشر" أو في حكم المباشر. فهو قد استخدم الآلة كأداة لتحقيق قصده الإجرامي، تماماً كمن يستخدم سلاحاً أو يطلق حيواناً مفترساً على غيره. فالآلة هنا مسخرة بالكامل لإرادته، وتكون المسؤولية الجنائية كاملة عليه.
- **مسؤولية المبرمج أو الشركة المالكة:** يمكن مساءلة المبرمج أو الشركة المالكة من خلال منظورين:

1. من باب "التسبب": إذا ثبت أن الجريمة وقعت بسبب خلل في التصميم أو إهمال جسيم في وضع ضوابط الأمان، فإن المبرمج أو الشركة يُعتبران "متسبباً" في وقوع الجريمة. ورغم أن المستخدم هو المباشر، إلا أن قوة تسبب الشركة في الضرر قد تجعلها شريكة في المسؤولية، ويُقدّر القاضي ذلك تعزيراً.
2. من باب "الإعانة على الإثم والعدوان": إذا أتاحت الشركة المطورة نموذجاً ذكياً للعامة وهي تعلم يقيناً أو يغلب على ظنها أنه سيُستغل في جرائم واضحة كالتزييف العميق، ولم تضع أي ضوابط فنية أو أخلاقية للحد من هذا الاستغلال، فإن فعلها هذا يمكن تكييفه على أنه من باب "الإعانة على الإثم والعدوان"، مما يوجب عليها مسؤولية تعزيرية.

(27) أنظر: المرجع سابق، ص 47، 357

المبحث الثالث

تحديات الإثبات والمواجهة المستقبلية

تمهيد وتقسيم:

بعد أن تم تحليل المواجهة التشريعية والفقهية للجرائم المستحدثة، يتناول هذا المبحث التحديات العملية التي تواجه إثبات هذه الجرائم أمام القضاء، ثم يقدم رؤية مستقبلية لتطوير المنظومة التشريعية بما يتناسب مع خطورة هذه الظاهرة المتجددة.

فالتبيعة الفريدة للجرائم المرتكبة بواسطة الذكاء الاصطناعي لا تثير إشكاليات نظرية في التكيف وإسناد المسؤولية فحسب، بل تفرض تحديات إجرائية غير مسبقة على منظومة الإثبات الجنائي التقليدية.

وعليه، سيتم تقسيم هذا المبحث إلى مطلبين متكاملين؛ يتناول أولهما الصعوبات العملية التي تواجه إثبات هذه الجرائم، ويستشرف ثانيهما الآفاق المستقبلية للمواجهة التشريعية والفقهية.

المطلب الأول

صعوبات إثبات الجرائم المرتكبة بواسطة الذكاء الاصطناعي

إن الطبيعة الفريدة للجرائم المرتكبة بواسطة الذكاء الاصطناعي تفرض تحديات غير مسبقة على منظومة الإثبات الجنائي، تتجاوز مجرد التعامل مع الدليل الرقمي التقليدي. وتتمثل أبرز هذه الصعوبات في الآتي:

أولاً: صعوبة إثبات الفعل ونسبته إلى فاعل محدد

تكمن الصعوبة الجوهرية الأولى في أن الدليل في هذه الجرائم رقمي وغير مادي، يتجسد في بيانات يمكن محوها أو تعديلها بضغط زر، ولكن التحدي يتضاعف مع الذكاء الاصطناعي، حيث يصبح إسناد الفعل نفسه إلى فاعل بشري محدد أمراً معقداً. فخلافاً للتغريدة التي يكتبها شخص، فإن المحتوى الذي يولده الذكاء الاصطناعي قد يكون نتاج تفاعل معقد بين أمر المستخدم وقدرات النموذج الذاتي، مما يجعل من الصعب تتبع آلية اتخاذ القرار داخل النظام وإسناد النتيجة الإجرامية لشخص بعينه بشكل قاطع.⁽²⁸⁾

(28) أنظر: حسن، شريهان ممدوح، الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)، العدد 21، يناير 2020، ص24.

ثانياً: صعوبة إثبات الركن المعنوي (القصد الجنائي)

يمثل إثبات القصد الجنائي التحدي التحليلي الأكبر، فالمستخدم قد يدفع بأن النتيجة الإجرامية (كنص احتيالي أو صورة مزيفة) لم تكن مقصودة بالكامل، وأن النموذج الذكي هو الذي "أساء فهم" الأمر أو "هلوس" وأنتج محتوى خارج نطاق التوقع. وهذا يتطلب من جهات التحقيق ليس فقط خبرة تقنية، بل خبرة تحليلية وقانونية عميقة لفهم سياق الأمر المدخل، وتحليل لغة المخرجات، وتفسير النية الإجرامية، وهو تحدٍ يزداد صعوبة مع تطور قدرات الذكاء الاصطناعي على التصرف بشكل شبه مستقل.⁽²⁹⁾

ثالثاً: تحدي تشتت المسؤولية بين أطراف متعددة

إن الطبيعة المعقدة لمنظومة الذكاء الاصطناعي تؤدي إلى تشتت المسؤولية بين عدة أطراف، مما يجعل مهمة الإثبات أكثر صعوبة. فالمسؤولية قد تقع على:

المستخدم (User): الذي أعطى الأمر، ولكن قد يكون من الصعب إثبات قصده الكامل.

المبرمج أو المصنع (Developer/Manufacturer): الذي صمم النظام، ولكن قد يكون من الصعب إثبات وجود إهمال جسيم أو نية إجرامية في التصميم.

الغير (Third Party): وهو المخترق الذي قد يستغل ثغرة في النظام، مما يتطلب خبرة تقنية عالية لتتبعه.⁽³⁰⁾

هذا التشتت يجعل من الصعب على الادعاء العام تركيز الاتهام على طرف واحد بشكل قاطع، مما قد يؤدي إلى إفلات الجناة من العقاب، وهو ما يمثل تحدياً كبيراً يتطلب تطويراً في قواعد الإثبات التقليدية.

⁽²⁹⁾ أنظر: إمبابي، بسمه سعد الله، "القصد الجنائي الاحتمالي في ضوء الفقه والقضاء المصري والفرنسي"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، المجلد 13، العدد 84، يونيو 2023م، ص 1 وما بعدها.

⁽³⁰⁾ أنظر: سعيد، وليد سعد الدين محمد، "المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي"، مرجع سابق، ص 515، و 517، و 522.

المطلب الثاني

الآفاق المستقبلية للمواجهة التشريعية والفقهية

إن مواجهة هذه التحديات تتطلب رؤية استشرافية لا تكتفي بتطبيق النصوص الحالية، بل تعمل على تطوير المنظومة التشريعية والفقهية لتكون قادرة على استيعاب هذه التطورات. وبناءً على ما سبق، فإن أي مواجهة مستقبلية فعالة تتطلب توفر عدة متطلبات أساسية:

أولاً: على المستوى التشريعي

1. الحاجة إلى نصوص تجريم خاصة:

يتطلب النجاح المستقبلي في المواجهة أن يتدخل المنظم السعودي بإضافة مواد جديدة إلى نظام مكافحة الجرائم المعلوماتية تجرم بشكل صريح ومباشر الاستخدام الخبيث لتقنيات الذكاء الاصطناعي، مثل إنشاء "التزييف العميق" لأغراض الابتزاز والتشهير.

2. الحاجة إلى قواعد واضحة للمسؤولية الجنائية :

من الضروري وضع إطار نظامي يعالج إشكالية إسناد المسؤولية، ويمكن الاسترشاد في ذلك بالقواعد الفقهية المرنة، لوضع نموذج يقوم على "توزيع المسؤولية" بين المستخدم والمبرمج والشركة المالكة، كلٌ بحسب درجة مساهمته في وقوع الجريمة.

ثانياً: على المستوى القضائي والتنفيذي :

3. ضرورة تطوير آليات الإثبات:

يتطلب الأمر تطوير القدرات الفنية لجهات التحقيق من خلال إنشاء وحدات متخصصة في الأدلة الجنائية الرقمية المتعلقة بالذكاء الاصطناعي، ووضع قواعد إجرائية واضحة للتعامل مع هذا النوع من الأدلة.

4. أهمية تعزيز التعاون الدولي:

نظراً للطبيعة العابرة للحدود لهذه الجرائم، فمن الضروري أن تلعب المملكة دوراً رائداً في صياغة اتفاقيات دولية تهدف إلى توحيد الأطر القانونية وتسهيل التعاون في التحقيق وملاحقة مرتكبي هذه الجرائم.

النتائج والتوصيات

أولاً: النتائج

بناءً على ما تم استعراضه وتحليله في هذا البحث، يمكن إيجاز أبرز النتائج التي تم التوصل

إليها في النقاط التالية:

1. أظهر البحث أن تقنيات الذكاء الاصطناعي التوليدي قد أفرزت أنماطاً إجرامية مستحدثة تتميز بالتعقيد وصعوبة الكشف، أبرزها الاحتيال المالي المتقدم، وجرائم التشهير والابتزاز عبر التزييف العميق، وحملات التحريض ونشر المعلومات المضللة الآلية.
2. خلص البحث إلى أن نصوص نظام مكافحة الجرائم المعلوماتية السعودي، بمرونتها، قادرة على تجريم صور الأفعال المستحدثة، حيث يمكن تكييفها ضمن جرائم الاحتيال والتشهير والمساس بالنظام العام.
3. كشف البحث عن أن التكييف الفقهي لهذه الجرائم يندرج تحت باب "التعزير"، وأنها تمثل اعتداءً مباشراً على الضروريات الخمس التي جاءت الشريعة بحفظها.
4. تبين أن التحدي الأكبر الذي يواجه المنظومة التشريعية الحالية هو "إشكالية إسناد المسؤولية الجنائية"، نظراً لتعدد الأطراف المتداخلة (المستخدم، المبرمج، الشركة المالكة).
5. أوضح البحث أن الفقه الإسلامي، من خلال قواعد "المباشرة والتسبب" و"الإعانة على الإثم والعدوان"، يقدم إطاراً تحليلياً مرناً يمكن الاسترشاد به لوضع نموذج يقوم على "توزيع المسؤولية بين الأطراف المختلفة".
6. خلص البحث إلى أن إثبات هذه الجرائم يواجه صعوبات عملية كبيرة، تتمثل في صعوبة إثبات القصد الجنائي، وتشتت المسؤولية بين العديد من الأطراف.

ثانياً: التوصيات

بناءً على النتائج التي تم التوصل إليها، يقترح الباحث حزمة من التوصيات العملية التي تهدف إلى تعزيز المواجهة التشريعية والفقهية لهذه الجرائم:

1. على المستوى التشريعي:

- إضافة نصوص تجريم خاصة: يوصي الباحث بأن يتدخل المنظم السعودي بإضافة مواد جديدة إلى نظام مكافحة الجرائم المعلوماتية تجرم بشكل صريح ومباشر الاستخدام الخبيث لتقنيات الذكاء الاصطناعي، مثل إنشاء "التزييف العميق" لأغراض الابتزاز والتشهير.
- وضع قواعد واضحة للمسؤولية الجنائية: يوصي الباحث بضرورة وضع إطار نظامي يعالج إشكالية إسناد المسؤولية، ويمكن الاسترشاد في ذلك بالقواعد الفقهية المرنة، لوضع نموذج يقوم على "توزيع المسؤولية" بين المستخدم والمبرمج والشركة المالكة، كلٌ بحسب درجة مساهمته في وقوع الجريمة.

2. على المستوى القضائي والتنفيذي:

- تطوير آليات الإثبات: يوصي الباحث بضرورة تطوير القدرات الفنية لجهات التحقيق من خلال إنشاء وحدات متخصصة في الأدلة الجنائية الرقمية المتعلقة بالذكاء الاصطناعي، ووضع قواعد إجرائية واضحة للتعامل مع هذا النوع من الأدلة.
- تعزيز التعاون الدولي: نظراً للطبيعة العابرة للحدود لهذه الجرائم، يوصي الباحث بضرورة أن تلعب المملكة دوراً رائداً في صياغة اتفاقيات دولية تهدف إلى توحيد الأطر القانونية وتسهيل التعاون في التحقيق وملاحقة مرتكبي هذه الجرائم.

الخاتمة

وفي ختام هذا البحث، الذي سعى إلى تحليل الإطار التشريعي والفقه للجرائم المستحدثة بواسطة الذكاء الاصطناعي، يتضح أننا أمام نقلة نوعية في عالم الجريمة تتحدى المفاهيم القانونية التقليدية.

وقد أظهر البحث أن المنظومة التشريعية في المملكة العربية السعودية، ممثلة في نظام مكافحة الجرائم المعلوماتية، تمتلك من المرونة ما يمكنها من استيعاب صور هذه الجرائم، إلا أن التحدي الأكبر يكمن في إثباتها وإسناد المسؤولية الجنائية لفاعلها في ظل الطبيعة المعقدة والمشاركة لهذه التقنيات.

وقد كشف البحث عن ثراء الفقه الإسلامي وقدرته على تقديم حلول تأصيلية مرنة لهذه الإشكالية، من خلال قواعده الراسخة في التفريق بين المباشرة والتسبب، ومبدأ توزيع المسؤوليات. وهذا يؤكد على أن أي مواجهة مستقبلية فعالة يجب أن تقوم على رؤية متكاملة تجمع بين التحديث التشريعي المستمر، والاسترشاد بالأصول الفقهية العميقة، وتطوير القدرات التقنية والقضائية.

ويأمل الباحث أن يكون هذا العمل قد أسهم في تقديم رؤية واضحة حول هذا الموضوع الحيوي، وأن تكون نتائجه وتوصياته لبنة في صرح الجهود الوطنية الرامية إلى تحقيق فضاء سيبراني آمن وموثوق، يتوافق مع قيمنا الشرعية ويحقق مقاصد رؤيتنا الوطنية الطموحة.

وآخر دعوانا أن الحمد لله رب العالمين.

قائمة المراجع

أولاً: الأنظمة واللوائح والتنظيمات:

1. المملكة العربية السعودية، البنك المركزي السعودي، دليل مكافحة الاحتيال المالي في البنوك والمصارف العاملة بالمملكة، رقم الإصدار 2، أغسطس 2020م.
2. المملكة العربية السعودية، نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم (م/17)، بتاريخ 1428/03/08هـ.

ثانياً: الكتب:

3. عودة، عبد القادر، التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، بيروت، دار الكاتب العربي، 1977م.
4. وزارة الأوقاف والشؤون الإسلامية بالكويت، الموسوعة الفقهية الكويتية، 1427/1404هـ.

ثالثاً: الرسائل العلمية:

5. بوكراع، محمد ياسين، "التحريض على الجريمة في التشريع الجزائري"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2021م.
6. صالح، ليلى، "جريمة التحريض عبر مواقع التواصل الاجتماعي"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، 2021م.

رابعاً: الأبحاث والتقارير والمؤتمرات:

7. إمبابي، بسمة سعد الله، "القصد الجنائي الاحتمالي في ضوء الفقه والقضاء المصري والفرنسي"، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، المجلد 13، العدد 84، يونيو 2023م.
8. حسن، شريهان ممدوح، "الجرائم المعلوماتية وسبل مواجهتها على المستويين الوطني والدولي"، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية (MECSJ)، العدد 21، يناير 2020م.

9. سعيد، وليد سعد الدين محمد، "المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي"، مجلة العلوم القانونية والاقتصادية، مجلد 64، عدد 2، 2022م.
10. الشمري، إبراهيم بن ممدوح، "التكليف الفقهي وأثر تغيره: دراسة تأصيلية، وتطبيقية على منتجات مالية إسلامية"، مجلة العلوم الشرعية، جامعة الإمام محمد بن سعود الإسلامية، مج 5، ع 67، 1444هـ.
11. الشريف، محمود سلامه، "الجرائم المرتكبة عبر 'الشات بوت' Chatbot - والمسؤولية الجنائية عنها"، بحث مقدم في المؤتمر العلمي الثامن: التحديات القانونية في العصر الرقمي، كلية الحقوق، جامعة السلطان قابوس، 2024م.
12. المجلس الأطلسي (Atlantic Council)، القرصنة باستخدام الذكاء الاصطناعي: استخدام الذكاء الاصطناعي التوليدي في الأنشطة السيبرانية الخبيثة، 2024م، متاح على الرابط:
<https://dfrlab.org/wp-content/uploads/sites/3/2024/02/csi-report-hacking-with-ai.pdf>
13. مايكروسوفت (Microsoft)، تقرير الدفاع الرقمي لمايكروسوفت 2024، 2024م، متاح على الرابط:
<https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>
14. محمود، عباس إبراهيم أحمد، "الضروريات الخمس وأثرها في تحقيق الأمن الاجتماعي"، مجلة كلية الشريعة والقانون - جامعة أم درمان الإسلامية، مج 3، ع 3، 2018م.
15. يوروبول (Europol)، اسرق، تعامل، وكرر - كيف يتاجر مجرمو الإنترنت ببياناتك ويستغلونها، تقرير تقييم تهديدات الجريمة المنظمة عبر الإنترنت "IOCTA"، لوكسمبورغ، مكتب منشورات الاتحاد الأوروبي، 2025م، متاح على الرابط:
<https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data>.

خامساً: المواقع الإلكترونية:

16. الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، "مبادئ التزييف العميق"، متاح على الرابط:

<https://sdaia.gov.sa/ar/SDAIA/eParticipation/consulting/SDAIADeepfakesGuidelinesAr.pdf>



مجلة الأندلس للعلوم الإنسانية والاجتماعية

مجلة دولية شهرية علمية محكمة

الترقيم الدولي الإلكتروني : ISSN : 2410- 521X

الترقيم الدولي الورقي : ISSN : 2410- 1818

البريد الإلكتروني : journal@andalusuniv.net

المجلة مفهرسة في المواقع الآتية :



2024	2023	2022	2021	2020	العام
0.3068	0.3759	0.1954	0.2692	0.0366	معامل أرسيف
1.55	1.25	1.73	1.60	1.60	معامل التأثير العربي