Conference Proceedings: Enhancing the Role of Islamic, Social, and Human Studies in Building Society, Volume 23, July 2026.

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at
https://iasj.rdd.edu.iq/journals/journal/view/247

سوسيولوجية الجريمة السيبرانية في عصر الذكاء الاصطناعي
مقاربة تحليلية للمجتمع الرقمي

د. هناء عبد الحميد إبراهيم عبد الحميد
الجامعة التقنية الوسطى / المعهد الطبي التقني – منصور
م.م إيلاف رائد إسماعيل دباش
الجامعة التقنية الوسطى / المعهد الطبي التقني – منصور

The Sociology of Cybercrime in the Age of Artificial Intelligence: An Analytical Approach to the Digital Network Society

Dr. Hanaa Abdul Hameed Ibrahim Abdul Hameed
hanaa_abdulhameed@mtu.edu.iq
Middle Technical University / Medical Technical Institute – Mansour
Asst Lec Elaph Raeed Ismail Dabash
elaph_raeed@mtu.edu.iq
Middle Technical University / Medical Technical Institute – Mansour

المستخلص :

يسعى هذا البحث إلى تقديم مقاربة سوسيولوجية تحليلية لظاهرة الجريمة السيبرانية في ضوء التحولات البنيوية التي أحدثتها تطبيقات الذكاء الاصطناعي في المجتمع الرقمي المعاصر, وتتبلور مشكلة الدراسة في التناقض القائم بين سرعة التطور الخوارزمي الفائق لأنظمة الذكاء الاصطناعي، مقابل البطء الهيكلي في استجابة المنظومات المؤسسية، التشريعية، والاجتماعية لتوفير الحماية للفضاء الافتراضي, ولتفكيك هذه الإشكالية، اعتمد البحث على المنهج الوصفي التحليلي؛ موظفاً أداة المراجعة المنهجية للأدبيات السوسيولوجية والجنائية المعاصرة، إلى جانب أداة تحليل المضمون الاجتماعي النقدي للإحصاءات والمؤشرات الصادرة عن المنظمات الأمنية الدولية كاليوروبول والإنتربول لعامي 2024 و 2025 .

وقد توصل البحث إلى جملة من النتائج، أبرزها: أن الذكاء الاصطناعي أعاد إنتاج ظاهرة الانحراف الاجتماعي عبر نمذجة الجريمة الرقمية وتحويلها إلى صناعة شبكية مؤتمتة عابرة للحدود (الجريمة كخدمة) تخلّف خسائر فادحة، كما أفرزت التقنيات التوليدية –وفي مقدمتها التزييف العميق– أنماطاً مستحدثة من الابتزاز والوقوع كضحية ترتبط طردياً بكثافة السلوك الروتيني الرقمي للأفراد, وأوصى البحث بضرورة الانتقال نحو سياسات الحوكمة الرقمية الرشيدة التي توظف خوارزميات الذكاء الاصطناعي كأداة استباقية وتنبؤية للضبط الاجتماعي الرقمي، مع إقرار تشريعات جنائية مرنة تصون الحقوق والحريات الرقمية للمستخدمين.

الكلمات المفتاحية: السوسيولوجيا الرقمية، الجريمة السيبرانية الذكية، المجتمع الشبكي، الحوكمة الخوارزمية، التضحية الرقمية، الأتمتة الانحرافية، الضبط الاجتماعي الافتراضي .

Abstract:

This research aims to provide a comprehensive sociological and analytical approach to the phenomenon of cybercrime in light of the structural transformations brought about by artificial intelligence (AI) technologies in the contemporary digital network society. The research problem crystallizes in the stark contradiction between the hyper-acceleration of algorithmic developments in AI systems and the structural lag in institutional, legislative, and social responses required to secure the virtual ecosystem. To unpack this dilemma, the study adopts a descriptive-analytical approach, utilizing a systematic review of contemporary sociological and

criminological literature, alongside a critical social content analysis of recent statistical indicators published by global law enforcement agencies, such as Interpol and Europol, for the years 2024 and 2025 .
The study reveals several key findings: AI has fundamentally reproduced social deviance by modeling cybercrime into an automated, transnational, and highly organized industry (Cybercrime-as-a-Service) that inflicts devastating economic and societal losses. Furthermore, generative technologies, particularly deepfakes, have produced novel patterns of interpersonal blackmail and cyber-victimization, which correlate directly with the density of individuals' routine digital activities. Ultimately, the research recommends a paradigm shift toward proactive algorithmic and digital governance policies that leverage AI as a tool for virtual social control, while robustly safeguarding users' digital rights and fundamental freedoms through updated legal frameworks.
Keywords: Digital Sociology, Cybercrime, Artificial Intelligence, Network Society, Algorithmic Governance, Cyber-Victimization, Virtual Social Control.

المقدمة :

يمر المجتمع الإنساني المعاصر بمرحلة تحول بنيوية غير مسبوقة، تجاوزت في أبعادها حدود التغير الثقافي والنمو الاقتصادي الكلاسيكي، لتطال جوهر التشكيلات الاجتماعية وتفاعلاتها اليومية, ولقد أدى بزوغ المجتمع الشبكي الرقمي إلى إعادة صياغة المفاهيم التقليدية للزمان والمكان، فلم يعد الفضاء السيبراني مجرد بنية تحتية تقنية أو وسيط اتصالي عابر, والفضاء السيبراني أصبح مجالًا اجتماعيًا مستقلاً للتفاعل الاجتماعي, هذا الحقل يتميز بالسيولة الهيكلية، وتتشكل داخله هويات افتراضية مغايرة، وتُعاد فيه هندسة علاقات القوة، وتتصارع عبره المصالح الطبقية والاقتصادية العابرة للحدود القومية والجغرافية .

ومع الانتقال المتسارع نحو تطبيقات الثورة الصناعية الرابعة، وفي مقدمتها الطفرة الفائقة لأنظمة الذكاء الاصطناعي، قفز المجتمع الرقمي من طور التفاعل البشري المعتمد على الآلة إلى طور الأنظمة الخوارزمية المستقلة ذاتياً, أدى الذكاء الاصطناعي إلى إعادة تشكيل بعض الظواهر الاجتماعية وتسريع انتشارها داخل البيئة الرقمية, وفي هذا السياق المعقد، تبرز الجريمة السيبرانية الذكية كأبرز تجليات الانحراف الاجتماعي الرقمي؛ حيث أتاحت الخوارزميات التوليدية والبيانات الضخمة للمجموعات الشبكية المنظمة فرصاً ابتكارية لشن هجمات واختراقات بالغة التعقيد، تتجاوز بطبيعتها الديناميكية قدرات الضبط الاجتماعي التقليدي والمنظومات الجنائية الكلاسيكية الموروثة من عصر المجتمع الصناعي .

تكتسب المقاربة السوسيولوجية للجريمة السيبرانية المعززة بالذكاء الاصطناعي مشروعيتها العلمية من خلال استقراء المؤشرات الكمية والأمبيريقية التي ترصد حجم الظاهرة وتأثيرها الهيكلي المتسار, وتشير البيانات الإحصائية التراكمية الصادرة عن المؤسسات البحثية والمنظمات الأمنية الدولية إلى أن كلفة الجريمة السيبرانية عالمياً تشهد نمواً أسياً غير مسبوق، حيث قفزت الخسائر الاقتصادية الناجمة عن الجرائم الرقمية لتتجاوز عتبة 8 تريليونات دولار سنوياً، مع توقعات تشير إلى تصاعدها المستمر، مما يجعل اقتصاد الجريمة السيبرانية بمثابة أحد أكبر الكيانات الاقتصادية في العالم, وتعكس هذه الكلفة الفلكية تحول الجريمة من مجرد اختراقات عشوائية إلى نظام بيئي إجرامي متكامل يعتمد على أتمتة الهجمات وابتكارها على نطاق واسع .

وفيما يتعلق بوتيرة وكثافة السلوك الانحرافي، تكشف تقارير الرصد الرقمي والمؤشرات الميدانية المقلقة عن أن الفضاء السيبراني يتعرض لمحاولات اختراق وقرصنة بمعدل هجوم واحد كل 39 ثانية, وقد تضاعفت هجمات التصيد الاحتيالي والهندسة الاجتماعية القائمة على الذكاء الاصطناعي التوليدي بنسبة تتجاوز 135%، ويعزى هذا الارتفاع القياسي إلى قدرة الأنظمة الذكية على توليد محتويات تفاعلية ورسائل مخصصة سيكولوجياً لاستهداف الضحايا بدقة شديدة تخدع أدوات الدفاع التقليدية .

أما على المستوى الميداني والبيئات المحلية، تظهر الإحصاءات والدراسات المسحية للضحايا تقسيماً بنيوياً يحكم أبعاد التضحية؛ حيث تأتي الجرائم الشخصية والابتزاز القائم على التزييف العميق وتوليد الهويات المفبركة في مقدمة الأنماط التي تستهدف فئات الشباب وطلبة الجامعات، وتتسبب في أزمات تفكك أسري ووصم اجتماعي عميق. وتليها الجرائم الاقتصادية والمجتمعية كسرقة الهويات الرقمية والاحتيال المالي الذكي الذي يستهدف المؤسسات والأفراد على حد سواء، مما يؤدي إلى زعزعة الثقة في التعاملات البنائية للمجتمع الافتراضي .

أولاً: مشكلة البحث : تتأسس المشكلة البحثية على هذا التناقض الصارخ وغير المتكافئ الذي كشفت عنه المؤشرات الإحصائية منها سرعة التدفق والتطور الخوارزمي الفائق في عالم الذكاء الاصطناعي، مقابل البطء الهيكلي في استجابة البنى الاجتماعية والمؤسسية، التشريعية، الأمنية، والتوعوية، لحماية الأفراد والمؤسسات من إساءة استخدام هذه التقنيات, وإن تغلغل الذكاء الاصطناعي في الأنشطة السيبرانية غير المشروعة أدى إلى نزع الطابع المحلي عن الفعل الانحرافي وعولمته، محولاً الجريمة الرقمية من مجرد سلوك فردي مدفوع بنقص قيمي أو دافع سيكولوجي، إلى

صناعة شبكية منظمة ومؤتمتة تجني أرباحاً فاحشة وتستهدف البناء الاجتماعي, وبناءً على هذه المعطيات تتمحور إشكالية هذه الدراسة حول **كيفية إعادة إنتاج الذكاء الاصطناعي لظاهرة الجريمة السيبرانية، وما هي الأبعاد والديناميات السوسيولوجية والثقافية التي تحكم ممارساتها وتحدد خريطة الضحايا داخل المجتمع الرقمي المعاص؟**, وينبثق عن هذا التساؤل المحوري عدة أسئلة فرعية ومقاربات نقدية :

١. ما هي كفاءة الأطر النظرية في السوسيولوجيا الجنائية وعلم الاجتماع الرقمي، مثل النشاط الروتيني، والأنومي، والمنظور الشبكي، على تفكيك الجريمة السيبرانية الذكية ؟

٢. ما هي الأسباب والبنى التحتية، الاجتماعية، الاقتصادية، والثقافية، التي تساهم في تغذية السلوك الانحرافي الرقمي وتدفع النخب والفاعلين نحو احتراف الجريمة السيبرانية المعززة بالذكاء الاصطناعي ؟

٣. كيف تؤثر الأنماط المستحدثة للجريمة الذكية، مثل التزييف العميق والهندسة الاجتماعية الخوارزمية، على الاستقرار النفس–اجتماعي وتعميق مظاهر الاغتراب الرقمي والوقوع كضحية ؟

٤. ما هي الإشكاليات والأبعاد الأخلاقية والحقوقية المترتبة على استخدام أنظمة الذكاء الاصطناعي نفسها كأداة للضبط الاجتماعي الرقمي والرقابة الأمنية السيبرانية ؟

ثانيًا: أهمية الدراسة وأهدافها المعرفية :

تكتسب هذه الدراسة أهمية علمية وعملية بالغة؛ نظراً لندرة الأدبيات السوسيولوجية العربية التي تقارب قضايا الذكاء الاصطناعي من منظور السوسيولوجيا الرقمية الفائقة وعلم الجريمة السيبراني, حيث تقتصر معظم الدراسات الحالية على المعالجات القانونية البحتة أو التقنية الأمنية, ومن ثمَّ تسعى الدراسة إلى تحقيق الأهداف الآتية :

١. مراجعة وتحيين النظريات السوسيولوجية الكلاسيكية والمعاصرة لتطوير أطر تفسيرية قادرة على استيعاب متغيرات الجريمة السيبرانية الذكية .

٢. رصد وتحليل التحولات الجوهرية التي طرأت على بنية الجريمة الرقمية وأساليب ارتكابها وهويتها التنظيمية في ظل تقنيات الأتمتة والتزييف العميق واختراق الخصوصية .

٣. استكشاف الآثار والتداعيات الاجتماعية والاقتصادية والنفسية العميقة التي تخلّفها هذه الجرائم على الأفراد والمؤسسات والمجموعات داخل الفضاء الافتراضي .

٤. تقديم رؤية نقدية لآليات الأمن السيبراني القائم على الذكاء الاصطناعي، واستشراف آفاق الحوكمة الرقمية الرشيدة التي توازن بين الردع الأمني وصون الحقوق الرقمية والحريات الأساسية للمستخدمين .

ثالثًا: مسلّمات البحث (Research Postulates): يتأسس هذا البحث في معالجته للإشكالية على ثلاث مسلّمات نظرية ومنهجية رصينة :

المسَلّمة الأولى : الجريمة السيبرانية الذكية هي ظاهرة اجتماعية بنيوية في المقام الأول وليست مجرد معضلة تقنية أو ثغرة برمجية؛ فهي تجسيد افتراضي للانحرافات، والصراعات، واللامساواة، وحالة اللامعيارية القائمة في البناء الاجتماعي الواقعي، جرى نقلها وتضخيمها وتوليدها خوارزمياً داخل البيئة الرقمية .

المسَلّمة الثانية : أن تكنولوجيا الذكاء الاصطناعي وخوارزمياته ليست محايدة قيميّاً أو أخلاقياً، بل هي نتاج سياقات سوسيولوجية وثقافية مشحونة برؤى ومصالح مصمميها ومستخدميها، مما يجعل انحراف الآلة الذكية انعكاساً مباشراً لخلل في منظومة الضبط المعياري والقيمي الإنساني .

المسَلّمة الثالثة : عجز المقاربات القانونية الجزائية أو التقنية الأمنية البحتة عن احتواء الظاهرة أو الحد منها، ما لم تتكامل مع فهم سوسيولوجي معمق للجذور الثقافية والاجتماعية التي تُغذّي بيئة السلوك الإجرامي وتصنع هندسة الوقوع كضحية .

رابعًا: منهجية البحث : للوصول إلى غايات البحث وتفكيك أبعاده، يعتمد البحث على المنهج الوصفي التحليلي؛ باعتباره المنهج الأنسب لمقاربة الظواهر الرقمية المستحدثة، حيث يتيح تجاوز الرصد الظاهري للجريمة إلى تحليل العلاقات البنيوية بين التطور الخوارزمي للذكاء الاصطناعي والتحولات القيمية والسلوكية داخل المجتمع الرقمي, وتوظف الدراسة في إطار هذا المنهج أداتين رئيسيتين : أداة المراجعة السوسيولوجية المنهجية للأدبيات والنظريات الجنائية المعاصرة لتأصيل أبعاد الانحراف الرقمي، وأداة تحليل المضمون الاجتماعي النقدي للإحصاءات والمؤشرات الصادرة عن الجهات الأمنية الدولية كالإنتربول، وذلك لقراءة الدلالات الاجتماعية والثقافية الكامنة خلف لغة الأرقام .

ويُصنَّف هذا البحث ضمن الدراسات النظرية (التحليلية) التي تركز على التحليل العلمي للنصوص والأطر المفاهيمية، بما ينسجم مع أهداف البحث وطبيعته .

خامسًا: حدود البحث : يتحدد نطاق هذا البحث ضمن الأبعاد المنهجية التالية :

١. **الحدود الموضوعية (المجال العلمي)** : ينصرف هذا البحث موضوعياً إلى التفكيك السوسيولوجي لظاهرة الجريمة السيبرانية في ظل الطفرة الفائقة لتطبيقات الذكاء الاصطناعي، مع التركيز على دراسة وتحليل آليات إعادة إنتاج الانحراف الرقمي عبر توليفة نظرية تربط التحول التكنولوجي بالإطار المجتمعي, ويركز البحث في شقه التحليلي من منظور علم الاجتماع الرقمي والجنائي على رصد الأنماط المستحدثة للجريمة الذكية (مثل التزييف العميق والهندسة الاجتماعية الخوارزمية)، وقياس كفاءة تدابير الضبط الاجتماعي، واستكشاف ديناميات الوقوع كضحية داخل المجتمع الشبكي المعاصر.

٢. **الحدود الزمانية (المجال الزمني)** : تتحدد الحدود الزمانية للبحث في المرحلة الممتدة من عام 2024 الذي شهد الانفجار المعرفي والتطبيقي الفائق لأنظمة الذكاء الاصطناعي التوليدي، وصولاً إلى عام 2026 مع رصد امتداداتها الإحصائية والتوثيقية المتاحة, وتكتسب هذه المدة أهميتها الاستراتيجية والجنائية كونها تمثل مرحلة التحول الحرجة نحو نمذجة الجريمة السيبرانية كصناعة شبكية مؤتمتة؛ وإن اتخاذ عام 2024 حداً زمنياً في البحث يعود إلى أنه يمثل المنعطف التكنولوجي والتأسيسي العام الذي انبثقت منه وتأسست عليه الأنماط الإجرامية المستحدثة وتحديات الأمن الرقمي الراهنة .

٣. **الحدود المكانية (المجال الجغرافي)** : يتحدد النطاق الجغرافي للبحث في البيئة الافتراضية العالمية والمحلية للمجتمع الرقمي، مع تركيز تحليلي خاص على الفضاء السيبراني العربي والمحلي (العراق والمنطقة المحيطة) من خلال مسح اتجاهات الجريمة الإلكترونية في الواقع الميداني، وجغرافياً يركز البحث على الفضاءات الرقمية الأكثر عرضة للتهديدات (كالمنصات التفاعلية، بوابات المعاملات المصرفية الرقمية، وشبكات التواصل الاجتماعي) التي تمثل بيئة خصبة لعمل الخوارزميات واستهداف الضحايا .

المبحث الأول

المقاربات النظرية والأطر التفسيرية للجريمة السيبرانية الذكية

لغرض ضبط المصطلحات العلمية المستخدمة في هذا البحث، ومنعاً لأي لُبس في التفسير، نستعرض فيما يلي المفاهيم التي اعتمدتها الباحثتان لوصف وتحديد المتغيرات الأساسية داخل السياق الميداني للبحث :

١. **<u>الذكاء الاصطناعي (AI)</u>** : تعددت المعاني والتعريفات المقترحة للذكاء الاصطناعي بمعنى وجود تعريفات متعددة ومنها تعريف الباحث في هذا المجال الذي يعد ابرزها هو الذي اقترحه (جون مكارثي) إذ عرفه بانه (علم وهندسة صنع آلات الذكية), ويعرف بانه (دراسة وتصميم أنظمة ذكية تستوعب بيئتها وتتخذ إجراءات تزيد من فرص نجاحها, وعُرّفْ بأنه (هو خلق وتصميم برامج الحاسبات التي تحاكي أسلوب الذكاء الإنساني لكي يتمكن الحاسوب من اداء بعض المهام بدلا من الإنسان، التي تتطلب التفكير والتفهم والسمع والتكلم والحركة بأسلوب منطقي ومنظم, ومن خلال ما تقدم يتبين لنا أن الذكاء الاصطناعي هو الذي يعده ويصنعه البشر في الحاسوب او الآلة، أي الإمكانية على اكتساب الخبرة وممارسة المعرفة وتطبيقها على ما إبتكره الإنسان، ونحن نرجح ونتفق مع التعريف الاخير لكونه يتلاءم إلى درجة ما مع ما تحتويه كيانات الذكاء الاصطناعي [١] .

وتُعرّف الباحثتان (الذكاء الاصطناعي) إجرائياً في هذا البحث بأنه منظومة من الأنظمة البرمجية والخوارزميات الرقمية المستقلة ذاتياً، والتي تمتلك القدرة على محاكاة العمليات الذهنية البشرية، مثل التعلّم العميق، وتحليل البيانات الضخمة، والتنبؤ بالسلوكيات, ولا يُنظر إليه في هذه الدراسة كأداة تقنية صماء، بل كفاعل بنيوي صامت يُساء توظيفه من قِبل تنظيمات القرصنة والشبكات المنظمة لإعادة هندسة تفاعلات القوة والوقائع الافتراضية، من خلال أتمتة الهجمات السيبرانية وتوليد تقنيات التزييف العميق والهندسة الاجتماعية لتمرير أفعال انحرافية بالغة التعقيد تتجاوز قدرات الضبط الاجتماعي التقليدي .

٢. **<u>الابتزاز الإلكتروني :</u>** قيام شخص أو مجموعة أشخاص ضمن منظمة اجرامية الكترونية بتهديد شخص أخرا أو مجموعة أشخاص على القيام بعمل ما أو ترك فعل ما بأستخدام وسائل ضغط من خلال تقنية المعلومات، أي تطويع شبكة المعلوماتية (الأنترنت او وسائل التزاصل الأجتماعي) لإغراض الضغط على الشخص المُستهدف بدفع مبلغ من لمال أو القيام بفعل مشين يرفضه الواقع الإجتماعي العراقي أو الظهور للجمهور والتنازل عن ملكية معينة [٢] .

وتُعرّف الباحثتان (الابتزاز الإلكتروني) إجرائياً في هذا البحث بأنه سلوك انحرافي وفعل إجرامي سيبراني مؤتمت، يعمد فيه الفاعل الرقمي إلى استغلال تطبيقات وخوارزميات الذكاء الاصطناعي والتقنيات التوليدية للتزييف العميق (فبركة هويات، صور، أصوات، أو مقاطع فيديو) لتهديد الضحية بنشر مواد تمس اعتبارها الاجتماعي أو الشخصي، أو حجب بياناتها الرقمية الحيوية، بغرض إكراهها نفسياً أو مادياً لتقديم تنازلات مالية،

أو جنسية، أو سياسية، يتمظهر هذا السلوك كأداة لا متناظرة لإعادة هندسة تفاعلات القوة والسيطرة الافتراضية، مستهدفاً استقرار البناء الأسري والمجتمعي عبر استغلال السلوك الروتيني الرقمي للأفراد في البيئة الشبكية، مما يخلّف تداعيات بنيوية عميقة كالوصم الاجتماعي والاغتراب الرقمي .

٢. المجتمع الشبكي : المجتمع الشبكي هو المجتمع الذي أصبحت فيه الشبكات، المدعومة بتكنولوجيا المعلومات والاتصالات، الشكل التنظيمي المهيمن الذي تُدار من خلاله العلاقات الاجتماعية والاقتصادية والسياسية والثقافية, ويشير بارني إلى أن المجتمع الشبكي يتميز بسمتين أساسيتين هي انتشار تقنيات المعلومات والاتصالات الرقمية, واعتماد الأفراد والمؤسسات على الشبكات بوصفها النمط الرئيس للتنظيم والتفاعل [٣] .

وتُعرّف الباحثة (المجتمع الشبكي) إجرائياً في هذا البحث بأنه البناء الاجتماعي المستحدث الذي يتشكل من شبكات تفاعلية افتراضية عابرة للحدود الجغرافية والزمانية، وتعتمد بنيته التحتية وقواعده المعيارية على تدفق البيانات والمعلومات الرقمية، يُعد هذا المجتمع بيئة حاضنة وموازية لمجتمع الواقع، تُعاد فيها صياغة الهويات، وتتشكل عبرها علاقات القوة والطبقية، كما يوفر بيئة سيالة تسهل من خلالها أتمتة السلوكيات الانحرافية وتمرير الجرائم السيبرانية الذكية .

الإطار النظري للدراسة (توليفة سوسيولوجية–أمنية) : يُمثّل التراث السوسيولوجي منطلقاً تحليلياً أساسياً لتفكيك الظواهر الانحرافية المستحدثة؛ إذ إن الجريمة السيبرانية المعززة بالذكاء الاصطناعي ليست معزولة عن السياق الاجتماعي البنائي، بل هي امتداد متطور لديناميات السلوك الإجرامي وأشكال الخلل المعياري داخل المجتمع الشبكي المعاصر, ويمكن تقسيم هذه الأطر التفسيرية إلى مستويين متكاملين :

١. **النظريات الكلاسيكية في قراءة الجريمة السيبرانية :** يُمثّل التراث النظري الكلاسيكي لعلوم الاجتماع والجريمة مرجعية تأصيلية متجددة، حيث تتيح إعادة إسقاطها ومحاكاتها في البيئة الرقمية فهم الجذور البنائية للإجرام عبر أربعة محاور:

أ. نظرية الضغط الاجتماعي (روبرت ميرتون): يبرز هذا النموذج تجليّاً صريحاً في المجتمعات الشبكية التي تُعظّم قيم الاستهلاك الرفاهي والثراء الرقمي السريع، في مقابل محدودية السبل المشروعة المتاحة لجميع الطبقات, وهنا يُعاد إنتاج نمط الابتكار الإجرامي، إذ يندفع الأفراد الخاضعون للتهميش الاجتماعي أو الضغوط الاقتصادية، لا سيما في بيئات التحول والخلل الاقتصادي كالواقع العراقي، إلى توظيف خوارزميات الذكاء الاصطناعي كأداة بديلة للاحتيال المالي والابتزاز الإلكتروني كمسار ملتف للحراك الطبقي والمادي خارج الأطر الرسمية والمشروعة للدولة [٤] .

ب. نظرية الارتباط التفاضلي (إدوين سذرلاند): تؤكد النظرية أن السلوك الانحرافي ليس دافعاً غريزياً أو طارئاً، بل هو فعل مكتسب يتم تلقينه عبر التفاعل والاتصال داخل الجماعات الأولية, وفي الفضاء الافتراضي، توسع مفهوم الجماعة ليشمل غرف الإنترنت المظلم (Dark Web) والمنصات المشفرة، والتي تحولت إلى بيئات تنشئة رقمية تفاضلية؛ حيث لا يقتصر التعلم فيها على المهارات التقنية لبرمجة التزييف العميق وصياغة حيل الهندسة الاجتماعية، بل يشمل استدخال مبررات أخلاقية وآليات حياد قيمي تُحيّد بوجدان الفاعل الرقمي عن الشعور بالذنب تجاه الضحايا وتُسهّل اختراق أنظمة الضبط الجنائي والقانوني [٥] .

ج. نظرية الفرصة الروتينية (كوهين وفيلسون): ترى النظرية أن الجريمة نتاج حتمي لتقاطع ثلاثة عناصر في الزمان والمكان: مجرم متحفز، هدف جذاب، وغياب الحراسة الفاعلة, ومن خلال أنظمة الذكاء الاصطناعي، تضاعفت هذه الفرص هندسياً؛ فالخوارزميات باتت تتولى آلياً تحليل السلوك الروتيني الرقمي للمستخدمين وكثافة تفاعلاتهم اليومية لتحديد الأهداف الجذابة بدقة (مثل استخلاص البيانات الشخصية والصور القابلة للفبركة)، مستغلة الفجوة الهيكلية المتمثلة في بطء استجابة منظومات الحماية والتشريعات الأمنية والقانونية في توفير حراسة تقنية استباقية فاعلة للضحايا [٦] .

د. نظرية الوصم والإشكاليات الهوياتية (هوارد بيكر): تكشف النظرية أن الانحراف ليس صفة كامنة في الفعل بل هو بناء اجتماعي تفرضه القوى المهيمنة عبر ردود الفعل المجتمعية, وفي سياق الابتزاز والجرائم السيبرانية، يتمظهر الوصم ببعدين: الأول يرتبط بالضحية التي تتعرض للابتزاز بمحتويات التزييف العميق وتواجه وصماً اجتماعياً بنيوياً يهدد مكانتها الأسرية نتيجة الثقافة السائدة، والثاني يتمثل في سعي شبكات الجريمة المُنظمة لإعادة صياغة هوياتها الانحرافية والالتفاف على الملاحقة القانونية عبر استغلال الفجوات التشريعية لتبرير سلوكياتها الابتزازية [٧] .

٢. **الأطر النظرية الراهنة :** تنتقل السوسيولوجيا المعاصرة إلى تفكيك الظاهرة من خلال ربط البنية التقنية بالتحولات الهيكلية للمجتمع عبر ثلاثة أطر رئيسية :

أ. نظرية المجتمع الشبكي (مانويل كاستلز): تركز على أن بنية المجتمع المعاصر باتت تدار وتتشكل عبر شبكات متداخلة تتدفق فيها المعلومات والقوة؛ ولم تعد السلطة ممركزة في مؤسسات تقليدية بل انتقلت إلى عُقَد الشبكة ومفاصل تدفق البيانات, وتتيح هذه الرؤية مقاربة الجريمة السيبرانية

الذكية وصناعة الابتزاز بوصفها صراعاً بنيوياً محتدماً لفرض السيطرة واستغلال الأصول الرقمية واختراق الخصوصية لتحقيق هيمنة ومكاسب اقتصادية عابرة للحدود السيادية للدول [٨] .

ب. نظرية المراقبة الانضباطية (ميشيل فوكو ومابعد فوكو): تلقي الأطروحة الفوكوية ضوءاً كاشفاً على آليات الضبط الاجتماعي؛ إذ تحول الفضاء الإلكتروني بامتياز إلى مجتمع مراقبة وانضباط شامل تعززت قدراته الرصدية باستخدام الذكاء الاصطناعي والتتبع الخوارزمي, وفي المقابل يخلق الفاعلون المنحرفون ديناميكية صراعية مستمرة عبر تطوير خوارزميات مضادة للتملص والمراوغة والإفلات من أدوات الرقابة الأمنية، مما يولد مواجهة بنيوية مستمرة بين آليات الاستقرار الرقمي وأتمتة السلوك الانحرافي [٩] .

ج. السوسيولوجيا التقنية – الاجتماعية: تؤكد على مبدأ التشكيل المتبادل؛ فالتقنية والمجتمع لا ينفصلان، والذكاء الاصطناعي لا ينتج الانحراف والابتزاز من فراغ تقني محض، بل ينبثق من الثغرات القيمية والخلل المعياري السائد في البناء الاجتماعي ويعيد إنتاجه وتضخيمه افتراضياً, وهذا يستدعي بالضرورة بناء حوكمة رقمية خوارزمية رشيدة توازن بدقة بين متطلبات الردع الأمني وصون البنى الأخلاقية والمجتمعية الرقمية [١٠] .

وترى الباحثتان من خلال القراءة السوسيولوجية التوليفية لهذه الأطر النظرية، أن مقاربة الجريمة السيبرانية الذكية تتطلب تجاوز السرد الكلاسيكي الجاف للنظريات نحو صياغة نموذج تفسيري مركب يأخذ بالحسبان السيولة البنيوية للفضاء الرقمي .

وتؤكد الباحثتان أن خطورة الذكاء الاصطناعي لا تكمن في كونه أداة تقنية معقدة، بل في تحوله إلى فاعل بنيوي مستقل يسلب الضحية قدرتها على الدفاع عن نفسها نتيجة سرعة الأتمتة الخوارزمية، مما يجعل نظرية الفرصة الروتينية ونظرية الضغط الاجتماعي تعملان بالتوازي وبكفاءة فائقة في الفضاء الافتراضي العراقي, فحالة الأنومي الرقمي أو غياب المعيارية الناجم عن الفجوة بين التطور التكنولوجي السريع والبطء التشريعي والمؤسساتي في قانون العقوبات العراقي الحالي (والذي لا يزال يتعامل مع الجريمة الإلكترونية وفقاً لقانون عام 1969 الكلاسيكي)، قد فتحت الباب لشبكات الابتزاز لتعميق الوصم الاجتماعي وهدم البناء القيمي للأسرة تحت غطاء التخفي الخوارزمي .

وتلخص الباحثتان تداخلهما النقدي في أن فك شفرة الانحراف الرقمي يتطلب حوكمة خوارزمية مضادة توظف ذات تقنيات الذكاء الاصطناعي كآلية ضبط اجتماعي وقائي وتنبؤي قادرة على سد الفراغ المعياري وحماية الأمن المجتمعي الرقمي .

الدراسات السابقة : تُمثّل القراءة التحليلية للمنجز العلمي المتراكم ركيزة أساسية لتحديد التطور المعرفي والمنهجي الذي طرأ على مقاربة الانحراف الرقمي؛ إذ حظيت ظاهرة الجريمة السيبرانية باهتمام مطرد في الأدبيات السوسيولوجية والجنائية المعاصرة، وتنوعت الاقترابات البحثية في رصد وتتبع أبعادها, وتتأسس هذه المراجعة المنهجية في دراستنا الحالية على تصنيف الأدبيات السابقة وضبطها ضمن مسارين تحليليين؛ ركز المسار الأول على فحص البيئة الجنائية والتقنية للجريمة الإلكترونية في الواقع الميداني والتشريعي، لا سيما في البيئة العراقية، في حين اتجه المسار الثاني نحو بحث انعكاسات التقنيات المستحدثة والذكاء الاصطناعي على بنية المسؤولية الجنائية والاجتماعية .

وتسعى الباحثتان من خلال هذه القراءة الاستقرائية إلى تجاوز السرد الوصفي التراكمي للدراسات، نحو تفكيك أطرها النظرية وأدواتها المنهجية، وصولاً إلى رصد الفجوة العلمية الكامنة في تلك الأدبيات؛ حيث يلاحظ قصور واضح في الربط السوسيولوجي التوليفي بين الطفرة الفائقة للذكاء الاصطناعي التوليدي (كتقنيات التزييف العميق) وبين هندسة التضحية والابتزاز الإلكتروني في المجتمع الشبكي, وهو ما يمنح هذه الدراسة مشروعيتها العلمية في تقديم إطار تفسيري مركب يتلاءم مع سيولة الجريمة السيبرانية الذكية وتحديات الضبط الاجتماعي الراهنة في العراق, وبناءً على هذا التقسيم الموضوعي يمكن استعراض أبرز تلك الدراسات ومناقشتها على النحو التالي :

الدراسة الأولى: دراسة (العبادي وسعيد وحمدون، 2024): الجريمة الإلكترونية في الواقع العراقي، دراسة وتحليل (Al_Ibadi et al., 2024)، وهدفت إلى الوقوف على حجم وطبيعة الانحرافات الرقمية في البيئة العراقية ورصد التحديات الجنائية والتشريعية التي تواجهها المنظومة الأمنية والقضائية. واعتمدت الدراسة المنهج الوصفي التحليلي وأداة الاستبيان الإلكتروني بالتطبيق على عينة قصدية من طلبة الجامعات العراقية، وصنفت الجرائم المرصودة إلى جرائم شخصية (كالسب والقذف والاحتيال والابتزاز) وجرائم مجتمعية ودولية تمس الأمن الوطني. وتوصلت النتائج إلى تزايد مخيف في معدلات الابتزاز الإلكتروني الموجه ضد الأفراد، وأكدت أن القضاء العراقي لا يزال يواجه معضلة حقيقية تتمثل في غياب قانون خاص ومستقل لمعالجة جرائم المعلوماتية، والاعتماد بدلاً من ذلك على نصوص قانون العقوبات العراقي التقليدي رقم 111 لسنة 1969 المعدل، والذي بات عاجزاً عن استيعاب السيولة والتعقيد المصاحبين للطفرات التقنية المستحدثة [١١] .

تتقاطع دراستنا الحالية مع دراسة العبادي والآخرين (2024) في رصد وتفكيك المعضلة التشريعية للقضاء العراقي واعتماده على نصوص كلاسيكية من القرن الماضي لمواجهة انحرافات القرن الحالي, بيد أن الفجوة البحثية التي تعبر فوقها دراستنا تكمن في أن دراسة العبادي ركزت على

الجرائم الإلكترونية بمفهومها التقليدي العام وأدواتها الافتراضية البسيطة، بينما تتفرد دراستنا الحالية بفحص الجيل الجديد من هذه الجرائم، وهو الجريمة السيبرانية الذكية القائمة على هندسة الابتزاز عبر تقنيات الذكاء الاصطناعي التوليدي، وهو ما لم تلتفت إليه الدراسة السابقة .

الدراسة الثانية : دراسة (العنبكي، 2025): الهندسة الاجتماعية الرقمية وتأثيرها على المنظومة القيمية للمجتمع: دراسة ميدانية اجتماعية في مدينة بعقوبة (Al-Anbaki, 2025), وهدفت الدراسة إلى الكشف عن انعكاسات الهندسة الاجتماعية على أبعاد النسق القيمي والاجتماعي، وتحديد الفروق الإحصائية تبعاً لمتغيرات النوع الاجتماعي والعمر والتحصيل الدراسي, واعتمدت الدراسة منهج المسح الاجتماعي واستخدمت أداة الاستبيان الموزع إلكترونياً على عينة عشوائية بسيطة بلغت 400 مبحوث من سكان مدينة بعقوبة في محافظة ديالى, وتوصلت الدراسة إلى نتائج سوسيولوجية بالغة الأهمية، أبرزها أن أدوات الهندسة الاجتماعية الرقمية تمثل تهديداً مباشراً للمنظومة الأخلاقية والقيمية الموجهة للسلوك، حيث يستغل الجناة التفاعل الاجتماعي الافتراضي لاختراق خصوصيات الضحايا، مما يسهم في تراجع معدلات الثقة الاجتماعية وتضخيم مظاهر الاغتراب والاضطراب الأسري [١٢] .

تلتقي دراستنا مع دراسة العنبكي (2025) في تبني المقاربة السوسيولوجية التي لا تنظر إلى التقنية بمعزل عن قيم المجتمع، وفي التركيز على البعد الجغرافي والاجتماعي العراقي (محافظة ديالى), وتتأسس الفجوة البحثية هنا في طبيعة المتغير التقني المستغل؛ فبينما وقفت دراسة العنبكي عند حدود الهندسة الاجتماعية الرقمية الكلاسيكية القائمة على الخداع البشري اليدوي والنفسي عبر المنصات، تتقدم دراستنا خطوة أبعد لتثبت كيف تحولت الهندسة الاجتماعية في عصر الذكاء الاصطناعي إلى أتمتة خوارزمية ذكية تتولى فيها برمجيات التعلم العميق استخلاص البيانات وصياغة محتويات تزييف عميق مخصصة تزيد من كفاءة التهديد وتسرّع التضحية بالضحايا وتحطيم منظومتهم القيمية .

الدراسة الثالثة: دراسة (خلف، 2025): جاءت تحت عنوان الجريمة السيبرانية وحدود المسؤولية الجنائية في الفضاء الرقمي (Khalaf, 2025)، وهدفت إلى تحليل الأطر القانونية المنظمة للجرائم السيبرانية في العراق وتحديد المسؤولية الجنائية للفاعلين والمساهمين في الفضاء الرقمي (مثل مزودي الخدمة ومشتري المستلزمات التقنية). واعتمدت الدراسة المنهج الوصفي التحليلي القانوني المقارن وتتبع أحكام القضاء العراقي, وخلصت النتائج إلى وجود صعوبات موضوعية وإجرائية بالغة التعقيد تواجه المحاكم العراقية في تكييف القصد الجنائي وإثبات الهوية الرقمية للجناة، نظراً لخصائص التخفي والسيولة واللامركزية التي يوفرها الفضاء السيبراني، مع التوصية بضرورة تطوير أدوات قانونية مرنة وسد الفراغ التشريعي [١٣] .

تشترك دراستنا الحالية مع دراسة خلف (2025) في معالجة إشكالية المسؤولية الإجرامية والقصور الإجرائي في تحديد الفاعل الرقمي وإثبات القصد داخل الفضاء القضائي العراقي, وتتبلور مساهمتنا المضافة وفجوتنا البحثية في انتقال الفاعل من صيغته البشرية التقليدية (القرصان أو المبتز الذي يباشر الفعل يدوياً) إلى الفاعل الخوارزمي البرمجي المستقل (الذكاء الاصطناعي)؛ حيث تناقش دراستنا أبعاداً أكثر حداثة ترتبط بمسؤولية الأنظمة الذكية المستقلة ذاتياً وكيف يسهم هذا التعقيد التقني في تعميق أزمة الإثبات الجنائي أمام القضاء العراقي الحالي .

الدراسة الرابعة : دراسة (الجميلي، 2024): المواجهة الجزائية للجرائم الواقعة باستخدام الذكاء الاصطناعي (Al Jumaily, 2024)، وهدفت إلى تفكيك إشكالية المسؤولية الجنائية والجزائية المترتبة على إساءة استخدام أدوات وأنظمة الذكاء الاصطناعي في إلحاق الضرر بالأفراد والمجتمعات, واعتمد الباحث المنهج التحليلي القانوني المقارن مستنداً إلى التشريعات الجنائية والتحولات الخوارزمية المعاصرة, وتوصلت الدراسة إلى نتائج محورية تؤكد أن التطور المتسارع للتعلم العميق وخوارزميات التوليد الرقمي (مثل الروبوتات المستقلة وتقنيات التزييف) قد أنتجت نمطاً إجرامياً عابر القوانين يرتكز على استخدام التقنية كأداة تنفيذية بالغة الدقة لتمرير أفعال جرمية كالاحتيال والاعتداء على الخصوصية، وأوصت بضرورة إقرار تشريعات جنائية عراقية خاصة تستوعب ماهية الذكاء الاصطناعي وضبط قواعد الإثبات الخوارزمي [١٤] .

تُعد دراسة الجميلي (2024) المرجعية الأقرب لبحثنا من حيث مجال التطبيق والبيئة العراقية الصرفة, إلا أن الفجوة البحثية التي تفصل بين العملين وتمنح دراستنا طابع التجدد، تكمن في أن دراسة الجميلي قادت تحليلاً يغلب عليه الطابع القانوني والجنائي البحت (المسؤولية، العقوبة، الإثبات الخوارزمي الجاف)، بينما تقدم دراستنا الحالية توليفة سوسيوتقنية وجنائية مركبة؛ حيث لا نكتفي ببحث النص القانوني، بل نقوم بإسقاط وتفكيك الظاهرة سوسيولوجياً وعبر النظريات الاجتماعية (كالأنشطة الروتينية الرقمية والأنومي والوصم الباكري) لتوضيح كيف يُعيد الذكاء الاصطناعي هندسة تفاعلات الابتزاز والوصم الاجتماعي للضحية داخل البناء المجتمعي الشبكي العراقي .

الدراسة الخامسة : دراسة (الملا، 2024): جاءت الدراسة بعنوان الجرائم السيبرانية في عصر الثورة الصناعية الرابعة: الواقع والمأمول، دراسة وصفية تحليلية استشرافية في حقل القانون الجنائي (Al-Mulla, 2024), وهدفت إلى استشراف مستقبل السياسة الجنائية الدولية والعربية في مواجهة التهديدات السيبرانية الناشئة عن تكنولوجيات الثورة الصناعية الرابعة (كالذكاء الاصطناعي، إنترنت الأشياء، البيانات الضخمة، والميتافيرس),

واعتمدت الدراسة المنهج الوصفي التحليلي الاستشرافي, وخلصت نتائجها إلى أن المنظومات القانونية والتشريعية التقليدية في معظم دول المنطقة تقع في حالة عجز وقصور هيكلي أمام ديناميكية وتطور تلك الجرائم، وأكدت أن حماية المعلومات والأمن المجتمعي تتطلب استراتيجيات استباقية وقوانين مرنة تتجاوز ردود الفعل الكلاسيكية وتتبنى مفهوم الأمن السيبراني الوقائي الشامل والتنبؤ الخوارزمي بمخاطر الجريمة [١٥] .

تتلاقى دراستنا مع أطروحة الملا (2024) في طابعها الاستشرافي والتنبيه لخطورة تكنولوجيات الثورة الصناعية الرابعة وحالة العجز الهيكلي للمنظومات التشريعية, وتتمظهر الفجوة المعرفية لصالح دراستنا في مستوى التخصيص والتركيز؛ إذ ركزت دراسة الملا على إطار استشرافي عريض وشامل لكافة تقنيات الثورة الرابعة (إنترنت أشياء، بيانات ضخمة، ميتافيرس) على مستوى تحليلي عام، في حين تعمد دراستنا الحالية إلى المجهرية والتركيز السوسيولوجي الميداني، من خلال اقتطاع جزئية تقنية محددة بالغة الخطورة وهي (الذكاء الاصطناعي التوليدي والتزييف العميق) وإسقاطها موضوعياً على ظاهرة اجتماعية وجنائية حساسة ومستشرية في الواقع العراقي وهي (الابتزاز الإلكتروني وهندسة التضحية) .

المبحث الثاني

التحولات البنيوية للجريمة السيبرانية الذكية وديناميات الوقوع كضحية في المجتمع الرقمي

يتناول هذا المبحث التحولات الجوهرية التي أحدثتها تقنيات الذكاء الاصطناعي التوليدي في بنية الجريمة السيبرانية وأساليبها وهويتها التنظيمية، ويستكشف الآثار الاجتماعية والنفسية والاقتصادية العميقة على الأفراد والمؤسسات, ثم يُقدّم رؤية نقدية لآليات الأمن السيبراني المعزز بالذكاء الاصطناعي وآفاق الحوكمة الرقمية الرشيدة, وذلك في ضوء الأطر النظرية التي رُسّخت في المبحث الأول، ومن خلال المؤشرات الإحصائية الصادرة عن اليوروبول والإنتربول لعامَي 2024 و 2025 :

أولًا: التحولات البنيوية في هوية الجريمة السيبرانية الذكية وأساليبها التنظيمية : كشفت المؤشرات الإحصائية والتقارير الميدانية للمنظمات الأمنية الدولية أن الجريمة السيبرانية في عصر الذكاء الاصطناعي لم تتطور كميًا فحسب، بل تحولت نوعيًا في بنيتها وهويتها التنظيمية؛ إذ انتقلت من مرحلة الاختراق الفردي العشوائي إلى مرحلة الصناعة الشبكية المؤتمتة المنظمة، وهو ما يمكن استجلاؤه من خلال المحاور الآتية :

١. نموذج الجريمة- كخدمة (Cybercrime-as-a-Service - CaaS):

أعاد الذكاء الاصطناعي هندسة الجريمة السيبرانية نحو نموذج الاقتصاد الشبكي المؤتمت؛ حيث بات بمقدور أي فاعل، حتى من يفتقر إلى الخبرة التقنية، استئجار أدوات القرصنة والابتزاز جاهزة الاستخدام من خلال منصات الإنترنت المظلم (Dark Web), وتشير تقارير اليوروبول لعام 2024 إلى أن ظاهرة CaaS باتت تُشكّل منظومة اقتصادية إجرامية متكاملة تضم مطوري البرمجيات الخبيثة ومزودي خدمات الاستضافة والموزعين والمتلقين النهائيين لعائدات الابتزاز في سلسلة قيمة إجرامية عابرة للحدود السيادية للدول [١٦], ويُجسّد هذا النموذج بامتياز ما أشارت إليه نظرية الارتباط التفاضلي لسذرلاند من أن السلوك الانحرافي ليس دافعًا غريزيًا، بل هو فعل مكتسب يتم تلقينه عبر التفاعل داخل الجماعات الرقمية المنظمة.

٢. تقنيات التزييف العميق (Deepfake) كسلاح ابتزازي :

تُمثّل تقنيات التزييف العميق القائمة على نماذج الذكاء الاصطناعي التوليدي الأداةَ الأكثر خطورة في منظومة الجريمة السيبرانية الذكية؛ إذ باتت هذه التقنيات قادرة على فبركة محتويات صوتية ومرئية مقنعة تنتحل هوية أشخاص حقيقيين, وقد رصدت تقارير الإنتربول لعام 2025 تضاعفًا في جرائم الابتزاز القائمة على التزييف العميق بنسبة تتجاوز 200% مقارنةً بعام 2023، مع استهداف بنيوي واضح لفئات الشباب وطلبة الجامعات الأكثر كثافةً في السلوك الروتيني الرقمي، مما يُثبت عملياً أطروحة كوهين وفيلسون في نظرية الفرصة الروتينية [١٧], وفي البيئة العراقية تحديدًا، تتمظهر خطورة التزييف العميق في البُعد الثقافي والاجتماعي للمجتمع؛ إذ تُستغل الصور لفبركة مقاطع مزيفة تُوظَّف أداةً للابتزاز الجنسي والمالي، مما يُنتج وصمًا اجتماعيًا بنيويًا مدمرًا يستحضر نظرية الوصم لهوارد بيكر في أوضح صورها .

جدول (1): إحصائيات عالمية للتزييف العميق والهندسة الاجتماعية الخوارزمية 2024-2025 [١٨]

المؤشر الإحصائي	النتيجة
ارتفاع حوادث التزييف العميق المكتشفة عالمياً من 2023 إلى 2024	4 أضعاف (زيادة 400%)
ارتفاع محاولات احتيال التزييف العميق عبر مراكز الاتصال 2024	+1.300% مقارنةً بـ2023
ارتفاع هجمات استبدال الوجه (Face-swap) على أنظمة التحقق	+300% في 2024
معدل تنفيذ هجمات التزييف العميق على أنظمة التحقق من الهوية	محاولة كل 5 دقائق
نسبة المؤسسات التي تعرضت لاحتيال التزييف العميق	1 من كل 3 مؤسسات (33%)

نسبة المؤسسات التي تعرضت لهجوم تزييف عميق خلال 12 شهراً	62% من المؤسسات
أكبر حادثة احتيال بالتزييف العميق موثقة (مكالمة فيديو مزيفة)	25.6 مليون دولار في عملية واحدة
الخسائر الموثقة من احتيال التزييف العميق في مقابلات التوظيف 2025	13 مليون دولار
شكاوى الجرائم ذات الصلة بالذكاء الاصطناعي (أول توثيق رسمي 2025)	22.000+ شكوى / 893 مليون دولار خسائر
ارتفاع خسائر الاحتيال المدعوم بالذكاء الاصطناعي من 2023 إلى 2027	12.3 إلى 40 مليار دولار (32% CAGR)
دقة الإنسان في اكتشاف محتوى التزييف العميق	0.1% فقط (الإنسان عاجز عن الكشف)
ارتفاع هجمات الانتحال الصوتي (Vishing) المدعومة بالذكاء الاصطناعي	+442% في 2024

ولتفكيك المعطيات الإحصائية في الجدول الأول الخاص بخسائر الهجمات السيبرانية والبنى التحتية يظهر انتقالاً بنيوياً في الجريمة الرقمية من الفعل الفردي العشوائي إلى مأسسة الجريمة وتحويلها إلى صناعة شبكية مغلقة تدار كمنظومة عمل تجارية متكاملة ويبرز ذلك بوضوح في ديناميكية صناعة الفدية حيث يكشف النمو الأسّي لمتوسط المبالغ المطلوبة عن عمليات مدروسة تختار ضحاياها بناء على ملاءتهم المالية وقدرتهم على الدفع تحت ضغط الوقت كما أن حدوث هجمات سيبرانية متواترة بمعدل هجوم في ثوان معدودة يعكس إلغاء الحواجز الجغرافية والزمنية بفعل السيولة الرقمية لتصبح الجريمة مستمرة ومستقلة عن الإرادة البشرية المباشرة من خلال برمجيات ذكية تهاجم على مدار الساعة ويلاحظ كذلك تركيز المهاجمين على استهداف القطاعات الحيوية مثل الرعاية الصحية والبنى التحتية وهو استغلال سيكولوجي واقتصادي خبيث لقطاعات لا تملك رفاهية الوقت للمساومة مما يضمن سرعة الاستجابة للمطالب المالية ويمثل عبئاً يستنزف الميزانيات الدفاعية للمؤسسات التي باتت تنفق مبالغ ضخمة لصد الهجمات بدلاً من توجيهها للتطوير والابتكار .

٣. الهندسة الاجتماعية الخوارزمية (Algorithmic Social Engineering) :

تجاوزت الهندسة الاجتماعية في عصر الذكاء الاصطناعي حدود الخداع النفسي اليدوي القائم على الجهد البشري المباشر، لتتحول إلى أتمتة خوارزمية متطورة تعتمد على تحليل ملفات التفاعل الرقمي للضحايا المستهدفين عبر منصات التواصل الاجتماعي، واستخلاص نقاط الضعف النفسية والاجتماعية لصياغة رسائل تصيد مخصصة لكل فرد على حدة, وقد كشف تقرير اليوروبول لعام 2024 أن نسبة نجاح محاولات التصيد الاحتيالي المدعومة بالذكاء الاصطناعي تفوق نظيراتها التقليدية بمضاعفات كبيرة، نظرًا لقدرتها على محاكاة الأسلوب اللغوي والسياق الاجتماعي للضحية بدقة تُعجز أنظمة الدفاع التقليدية [١٩] .

٤. استهداف البنية التحتية الحيوية والمؤسسات :

لم تقتصر الجريمة السيبرانية الذكية على استهداف الأفراد، بل امتدت بصورة منهجية لاستهداف المؤسسات والبنى التحتية الحيوية للدول، من خلال هجمات برامج الفدية (Ransomware) المُدارة ذاتيًا خوارزميًا، والتجسس الصناعي المدعوم بالتعلم الآلي، والهجمات على أنظمة الطاقة والمؤسسات المصرفية. وتُشير الإحصاءات إلى أن الخسائر الاقتصادية الناجمة عن هجمات الفدية الموجهة للمؤسسات وصلت إلى مستويات قياسية في عامَي 2024 – 2025، كاشفةً عن البُعد الطبقي–الاقتصادي لهذه الجريمة وصلتها الوثيقة بمفهوم الصراع على الموارد في المجتمع الشبكي الذي أطّر له كاستلز [٢٠] .

جدول (2): إحصائيات لهجمات الفدية واستهداف المؤسسات والبنى التحتية 2024–2025 [٢١]

المؤشر الإحصائي	النتيجة
خسائر هجمات الفدية (Ransomware) عالمياً 2024	42 مليار دولار
الخسائر المتوقعة من هجمات الفدية بحلول 2031	265 مليار دولار سنوياً
ارتفاع حوادث برامج الفدية الموجهة للبنى التحتية الحيوية 2024	+9% مقارنةً بـ 2023
معدل وقوع هجوم سيبراني على الأعمال عالمياً	هجوم كل 39 ثانية
متوسط تكلفة اختراق بيانات في قطاع الرعاية الصحية 2024	10.93 مليون دولار (الأعلى بين القطاعات)
خسائر الاحتيال في الاستثمار (بما فيها التشفير) 2024	6.4 مليار دولار

خسائر الاختراق عبر البريد التجاري (BEC) 2024	2.77 مليار دولار (21.442 حادثة)
قاعدة مستخدمي منتديات الإنترنت المظلم الكبرى للجريمة كخدمة (CaaS)	أكثر من 400.000 مستخدم نشط
متوسط ارتفاع مدفوعات الفدية في الهجمات المؤسسية 2024	+500% وصلت إلى متوسط 2 مليون دولار
الإنفاق العالمي على الأمن السيبراني 2025	211.6 مليار دولار (+15.1% عن 2024)

وعلى مستوى المعطيات الواردة في الجدول الثاني الخاص بالتكلفة العالمية ومؤشرات التزييف العميق فيكشف التحليل عن أزمة ثقة افتراضية عميقة وظهور نمط من الانحراف الخوارزمي المستند إلى الذكاء الاصطناعي التوليدي إذ إن تضخم الكلفة العالمية السنوية للجريمة يجعل منها أحد أكبر الكيانات الاقتصادية المؤثرة في العالم ويحولها إلى ملاذ آمن لتدفق الأموال غير المشروعة وغسيل الأموال متفوقة على أنماط الجريمة التقليدية وفي ذات السياق يؤدي انفجار تقنيات التزييف العميق وتضاعفها المستمر إلى تآكل الحقيقة وتزييف الهوية والانتقال من مرحلة سرقة البيانات إلى مرحلة فبركة الواقع مما يهدد الأمن السلوكي والقيمي ويسهل عمليات الابتزاز والهندسة الاجتماعية كما يظهر التحليل السوسيولوجي تفاقم أزمة الأمية الرقمية الجيلية من خلال الاستهداف الممنهج للفئات الهشة ككبار السن الذين يعتمدون على آليات إدراك تقليدية تصدق الصوت والصورة بسهولة مما يجعلهم الهدف الأسهل للمجرمين وتتكامل هذه المعطيات لتظهر حالة من العجز في الضبط الاجتماعي والمؤسساتي أمام التدفق الهائل للشكاوى اليومية حيث تعجز الأجهزة الأمنية والتشريعات القانونية بطيئة الحركة عن ملاحقة الجريمة بنفس سرعة ارتكابها الخوارزمية .

ثانيًا: الآثار الاجتماعية والاقتصادية والنفسية للجريمة السيبرانية الذكية على الأفراد والمؤسسات :

تتجاوز تداعيات الجريمة السيبرانية الذكية حدود الأضرار المادية المباشرة، لتُخلّف جروحًا بنيوية عميقة في النسيج الاجتماعي والمنظومة النفسية للضحايا، وتزعزع الثقة في المنظومة المؤسسية برمّتها, وتتكشف هذه التداعيات على ثلاثة مستويات متشابكة :

١. الآثار الاجتماعية: الوصم والتفكك الأسري والاغتراب الرقمي :

يُولّد الابتزاز الإلكتروني القائم على التزييف العميق في السياق العراقي والعربي ظاهرة وصم اجتماعي مزدوج ومعقد؛ إذ لا يقتصر الضرر على الضحية مباشرةً، بل يمتد ليطال الأسرة والمحيط الاجتماعي في بُنية ثقافية تُحمّل الفرد ذنب ما وقع عليه من جريمة, ويترتب على ذلك تراجع حاد في معدلات الثقة الاجتماعية، وارتفاع في مؤشرات الاغتراب الرقمي الذي يتجلى في عزوف شرائح اجتماعية واسعة عن المشاركة الرقمية خشية الوقوع ضحيةً, وكما تُشير الدراسات الميدانية إلى أن حالات التفكك الأسري المرتبطة بجرائم الابتزاز الإلكتروني في تصاعد ملحوظ، لا سيما في ظل ميل الضحايا إلى الصمت وعدم الإبلاغ خشية الوصم، مما يعني أن الأرقام الرسمية لا تعكس الحجم الحقيقي للظاهرة .

٢. الآثار النفسية: الصدمة والاضطراب النفس–اجتماعي:

يُخلّف الوقوع ضحيةً للابتزاز الإلكتروني والتزييف العميق آثارًا نفسية بالغة الخطورة تتجاوز مفهوم الضرر الفردي العابر، لتتضمن أعراض اضطراب ما بعد الصدمة (PTSD)، والقلق الاجتماعي المزمن، والاكتئاب، والتراجع الحاد في مستوى الثقة بالنفس والآخرين, ويتفاقم هذا الأثر النفسي في السياق العراقي بفعل محدودية خدمات الصحة النفسية المتاحة وضعف شبكات الدعم الاجتماعي المؤسسي المخصصة لضحايا الجرائم الإلكترونية, مما يجعل الضحية تواجه محنتها منفردةً في غياب شبه تام للمظلة الحمائية المؤسسية والمجتمعية, وتُبرز هذه الظاهرة ما أسمته السوسيولوجيا التقنية–الاجتماعية بالجرح الرقمي الاجتماعي، حيث يتشابك الضرر التقني مع الضرر الاجتماعي والنفسي في تركيبة بالغة التعقيد .

٣. الآثار الاقتصادية: الخسائر الفردية والمؤسسية وتآكل الثقة :

تُشير التقديرات الاقتصادية المتراكمة إلى أن الجريمة السيبرانية الذكية تُلقي بتكاليف مباشرة وغير مباشرة فادحة على الاقتصادات الوطنية، تشمل الخسائر المالية المباشرة للأفراد والمؤسسات جراء عمليات الاحتيال والفدية والسرقة الرقمية، فضلًا عن التكاليف غير المباشرة المتمثلة في الإنفاق على الأمن السيبراني وإعادة بناء السمعة المؤسسية, والأشد خطورةً من الخسائر المادية هو تآكل ثقة المواطنين في التعاملات البنكية والتجارة الإلكترونية والخدمات الحكومية الرقمية، وهو ما يُعيق مسيرة التحول الرقمي ويُقيّد إمكانات التنمية الاقتصادية في مجتمعات ناشئة كالمجتمع العراقي .

جدول (3): إحصائيات عالمية للجريمة السيبرانية الذكية 2024–2025 [٢٢]

المؤشر الإحصائي	النتيجة
عدد شكاوى الجرائم الإلكترونية المُبلَّغ عنها لدى FBI خلال 2024	859.532 شكوى (2.354 شكوى يومياً)
التكلفة العالمية للجريمة السيبرانية سنوياً 2024	9.5 تريليون دولار
التكلفة العالمية للجريمة السيبرانية سنوياً 2025	10.5 تريليون دولار
التكلفة العالمية المتوقعة بحلول 2029	15.6 تريليون دولار
خدام الذكاء الاصطناعي من قِبل مجرمي الإنترنت لتنفيذ الهندسة الاجتماعي	ارتفاع ملحوظ وتسارع متواصل في 2023
متوسط تكلفة اختراق بيانات واحد على مستوى المؤسسات عالمياً 2024	4.88 مليون دولار (+10% عن 2023)
خسائر كبار السن (60 سنة فأكثر) جراء الجرائم الإلكترونية 2024	4.9 مليار دولار (+43% عن 2023)
ارتفاع محاولات التزييف العميق المرصودة من 2023 إلى 2024	تضاعفت 4 مرات
معدل تنفيذ هجمات التزييف العميق على أنظمة التحقق من الهوية	محاولة كل 5 دقائق

يوضح الجدول الثالث الخاص بتوزيع الجرائم السيبرانية حسب الفئات العمرية ونسب الوعي الأمني والتكلفة العالمية للجرائم السيبرانية يوضح التحليل وجود علاقة طردية واضحة بين التقدم في السن وارتفاع معدلات الوقوع ضحية للاحتيال الرقمي نتيجة للفجوة المعرفية الجيلية في التعامل مع التقنيات الحديثة حيث تسجل الفئات العمرية الأكبر سناً أعلى نسب خسائر مالية نظراً لثقتهم المفرطة في الرسائل والروابط الخبيثة واعتمادهم على أنماط تفاعل تقليدية لا تتناسب مع خبايا الهندسة الاجتماعية وفي المقابل تظهر البيانات أن الفئات الشابة هي الأكثر تعرضاً لجرائم الابتزاز الإلكتروني والتحرش الرقمي نتيجة لارتفاع معدلات بقائهم وتفاعلهم داخل الفضاء الافتراضي ومشاركتهم الكثيفة للبيانات الشخصية بالرغم من امتلاكهم نسب وعي تقني أعلى مقارنة بكبار السن مما يعكس أن الوعي التكنولوجي وحده لا يكفي للحماية دون وجود نضج سلوكي وأمني يقي الأفراد من الوقوع في فخاخ الجريمة المنظمة ويكشف هذا التباين لجوء المجرمين إلى تخصيص واستهداف كل فئة اجتماعية بأسلوب إجرامي يتناسب مع نقاط ضعفها السيكولوجية والتقنية .

ثالثًا: رؤية نقدية لآليات الأمن السيبراني بالذكاء الاصطناعي وآفاق الحوكمة الرقمية الرشيدة :

يستدعي التفكيك السوسيولوجي للجريمة السيبرانية الذكية مراجعةً نقدية للإشكاليات الأخلاقية والحقوقية المتولدة عن توظيف الذكاء الاصطناعي كأداة للضبط الاجتماعي الأمني، وذلك في توازن دقيق يصون الحرية الرقمية للمستخدمين, وتتمحور هذه الرؤية النقدية حول ثلاثة محاور:

١. الإشكاليات الأخلاقية والحقوقية لمنظومات المراقبة الذكية :

تُفرز منظومات المراقبة الأمنية الخوارزمية إشكاليات بنيوية معقدة تتصل بالحقوق الرقمية الأساسية؛ أبرزها خطر الإفراط في المراقبة الشاملة (Mass Surveillance) الذي يطال المواطنين البريئين في سعيٍ لرصد المشتبه بهم، وانحيازات خوارزميات التصنيف التي قد تُنتج أحكامًا مسبقة تمييزية بحق فئات اجتماعية بعينها. ويستحضر هذا السيناريو مفهوم المجتمع الانضباطي الفوكوي، حيث تتمدد آليات المراقبة لتغدو بنية سلطوية شاملة تُقيّد سلوك الفرد في الفضاء الافتراضي خشيةَ أعين الرقيب الخوارزمي، مما قد يُسهم في قمع الإبداع الرقمي والتعبير الحر .

٢. نحو حوكمة خوارزمية رشيدة: التوازن بين الأمن والحرية :

ترى الباحثتان أن المخرج الأمثل من هذه المعضلة لا يكمن في الانسحاب من المجال الأمني الرقمي خشيةَ انتهاك الحريات، ولا في الإذعان الكامل لمنطق المراقبة الخوارزمية الشاملة؛ بل في بناء منظومة حوكمة رقمية رشيدة تُعلي من مبادئ الشفافية الخوارزمية والمساءلة المؤسسية وسيادة القانون على العقل الاصطناعي, وتستلزم هذه المنظومة جملةً من الركائز الأساسية: أولها إطار تشريعي ذكي متجدد يتجاوز نصوص قانون العقوبات العراقي رقم 111 لسنة 1969 نحو تشريعات مخصصة للجريمة السيبرانية الذكية تستوعب متغيرات التزييف العميق والهندسة الاجتماعية الخوارزمية, وثانيها آليات رقابة ديمقراطية على الذكاء الاصطناعي الأمني عبر هيئات مستقلة تُدقق في خوارزميات المراقبة وتضمن توافقها مع معايير حقوق الإنسان الرقمية, وثالثها ثقافة أمنية رقمية استباقية تستهدف تعزيز الوعي المجتمعي بمخاطر الجريمة السيبرانية الذكية من خلال مناهج تعليمية متكاملة .

٣. الذكاء الاصطناعي كأداة للضبط الاجتماعي الاستباقي :

يدعو هذا البحث إلى توظيف الذكاء الاصطناعي ذاته كمنظومة ضبط اجتماعي استباقي تنبؤي تعمل على رصد الأنماط السلوكية الانحرافية قبل تحوّلها إلى أفعال جرمية ناجزة، عبر خوارزميات كشف التهديد المبكر وتحليل شبكات الجريمة المنظمة ورصد تدفق المعاملات المالية المشبوهة

على منصات الإنترنت المظلم. ويستلزم تفعيل هذا التوظيف الأمني بناءَ شراكة استراتيجية متكاملة بين الحكومات والقطاع التقني الخاص والمجتمع المدني الرقمي، في إطار يرسّخ مبدأ صون الكرامة الرقمية للإنسان باعتباره سقفًا أخلاقيًا راسخًا لأي توظيف أمني لتقنيات الذكاء الاصطناعي .

وخلاصة القول، يتبيّن من خلال هذا المبحث أن الجريمة السيبرانية المعززة بالذكاء الاصطناعي باتت ظاهرة اجتماعية بنيوية متجذرة تتشعب آثارها في ثلاثة مستويات متداخلة: التحول في هوية الجريمة نحو النمذجة الشبكية المؤتمتة، والأضرار الاجتماعية والنفسية والاقتصادية الفادحة التي تُخلّفها على ضحاياها، وأخيرًا الإشكاليات الأخلاقية المترتبة على توظيف ذات التقنية في الردع والضبط الأمني, وهو ما يفرض على الفاعلين التشريعيين والمؤسسيين والمجتمعيين ضرورةَ الانتقال من منطق رد الفعل إلى منطق الحوكمة الرقمية الرشيدة الاستباقية التي تُوازن بين صون الأمن المجتمعي وحماية الحقوق الرقمية للمواطن .

من خلال القراءة السوسيولوجية البنائية للمؤشرات والبيانات الأمبيريقية الصادرة عن المنظمات الأمنية الدولية كاليوروبول والإنتربول، إلى أن الطفرة الفائقة لأنظمة الذكاء الاصطناعي أحدثت تحولاً نوعياً تجاوز مجرد الآثار التقنية أو المادية؛ ليمس عمق العلاقات والقوة التشابكية داخل الفضاء الافتراضي, إن السيولة الهيكلية التي تميز البيئة الرقمية أتاحت مأسسة وأتمتة الفعل الانحرافي، ليتجاوز النمط الفردي الكلاسيكي ويستقر كمنظومة اقتصادية واجتماعية موازية ومستقلة تتحدى كفاءة أدوات الضبط الاجتماعي التقليدي والمنظومات الأمنية الموروثة .

وتتأكد خطورة هذا التحول في الكيفية التي أُعيدت بها هندسة "ديناميات الوقوع كضحية"؛ فالذكاء الاصطناعي لم يعد مجرد أداة لتسهيل الجرم، بل بات فاعلاً بنيوياً صامتاً يمتلك قدرة رصدية مستقلة على مسح السلوك اليومي للمستخدمين واستغلال الفجوة الناتجة عن البطء المؤسساتي والتشريعي في توفير الحماية التقنية الاستباقية, هذا التباين الشاسع بين سرعة التدفق الخوارزمي وجمود آليات الردع أنتج حالة حادة من الفراغ المعياري واللامعيارية الرقمية، مما فتح الباب واسعاً أمام قفزات تكنولوجية غير منضبطة تُهدد استقرار الأفراد والمؤسسات على حد سواء .

وعند نقل هذه المقاربة التحليلية من مستواها العالمي العام وإسقاطها نقداً على الواقع المحلي والبيئة العراقية، ترى الباحثتان أن الانعكاسات الحقيقية لجرائم التزييف الخوارزمي والابتزاز الإلكتروني تتخذ أبعاداً ثقافية وسلوكية بالغة الحساسية مقارنةً بالبيئات الغربية, فبينما تقف التقارير الدولية عند حدود رصد الأرقام وحجم الخسائر الاقتصادية، فإن اختراق الخصوصية وفبركة الهويات الرقمية في المجتمع العراقي يصطدم مباشرةً بالمنظومة القيمية والتقاليد السائدة، مما يؤدي إلى إنتاج وصم اجتماعي مزدوج يعمق من تآكل الثقة، ويجبر الضحايا على الانكفاء والصمت تجنباً للمسؤولية الأخلاقية التي غالباً ما يُحمّلها المجتمع للضحية الرقمية بدلاً من الجاني الخوارزمي .

وما يُعقد المشهد محلياً، في رؤية الباحثتين، هو حالة العجز الإجرائي والموضوعي التي تواجهها المنظومة القضائية العراقية؛ حيث يفرض هذا التسارع التقني أزمة حقيقية في تكييف القوانين الكلاسيكية الموروثة –وفي مقدمتها قانون العقوبات لمواجهة فاعل برمجي مستقل أو إثبات قصد جنائي رقمي, وبناءً على ذلك تؤكد الباحثتان أن المواجهة الفعالة لتحديات هذا العصر الرقمي الفائق لا يمكن أن تظل رهينة المقاربات القانونية أو الأمنية الجافة، بل تستوجب الانتقال السريع نحو بناء أطر حوكمة خوارزمية رشيدة ومتوازنة تدمج الذكاء الاصطناعي ذاته كمنظومة ضبط اجتماعي وقائي وتنبؤي قادرة على تحصين الأمن المجتمعي، مع كفالة الحقوق الرقمية وصون الكرامة الإنسانية للمستخدمين .

ختامًا, شهد المجتمع الشبكي المعاصر قفزة بنيوية بالغة التعقيد مع بزوغ الطفرات الفائقة لأنظمة الذكاء الاصطناعي؛ حيث تحولت هذه التكنولوجيا من مجرد أدوات حسابية مساعدة إلى فاعل بنيوي صامت يعيد إنتاج وهندسة الظواهر الاجتماعية وتفاعلات القوة, ولم تكن ظاهرة الجريمة السيبرانية بمعزل عن هذه التحولات؛ إذ كشف هذا البحث، عبر مقاربته السوسيولوجية والنقدية، أن الذكاء الاصطناعي قد أخرج الفعل الانحرافي من دائرته الفردية الكلاسيكية المعتمدة على نقص قيمي أو دافع سيكولوجي محض، ليدمجه في إطار صناعة شبكية مؤتمتة وعابرة للحدود تدار خوارزمياً .

وقد اتضح من خلال المراجعة المنهجية وتحليل المضمون الاجتماعي للمؤشرات الأمنية الدولية لعامي 2024 و 2025 أن حالة الأنومي الرقمي أو غياب المعيارية الناتجة عن الفجوة الزمنية العميقة بين وتيرة التطور الخوارزمي المتسارع وبين البطء الهيكلي في استجابة المؤسسات التشريعية والضبطية، قد خلقت بيئات خصبة لاستهداف الضحايا وتعميق مظاهر الوصم الاجتماعي والاغتراب الرقمي، لاسيما في البيئة المحلية العراقية التي ما زالت تعاني من عجز نصوصها القانونية الكلاسيكية عن استيعاب سيولة الجريمة الذكية, وتؤكد الدراسة في نهايتها أن فك شفرة هذا الانحراف المستحدث وتطويقه لا يمكن أن يتحقق بالمعالجات الأمنية والتقنية الجافة، بل يتطلب رؤية سوسيولوجية–تقنية شاملة تفهم هندسة التضحية وتقيم حوكمة رقمية خوارزمية رشيدة توازن بدقة بين متطلبات الردع الجنائي وصون الحقوق والحريات الرقمية .

الاستنتاجات : من خلال التحليل النقدي للأدبيات السوسيولوجية ومؤشرات الرصد الرقمي، توصل البحث إلى الاستنتاجات البنيوية التالية :

١. أدى الذكاء الاصطناعي التوليدي إلى نزع الطابع المحلي عن الجريمة وعولمتها، حيث أسهمت الخوارزميات في نمذجة الجرائم الرقمية لتصبح صناعة شبكية مؤتمتة تسلب الضحية قدرتها الفورية على الدفاع عن نفسها نتيجة سرعة التدفق الخوارزمي الفائق .

٢. بالتطبيق على نظرية الفرصة الروتينية، تبين أن أنظمة الذكاء الاصطناعي تضاعف فرص التضحية هندسياً عبر تحليل السلوك الرقمي اليومي للمستخدمين واستخلاص بياناتهم الشخصية بدقة لتوليد هجمات مخصصة سيكولوجياً وتمرير حيل هندسة اجتماعية متقدمة .

٣. أفرزت التقنيات التوليدية أنماطاً مستحدثة وغير متناظرة من الابتزاز الإلكتروني؛ حيث تواجه الضحايا (خاصة فئات الشباب وطلبة الجامعات) وصماً اجتماعياً بنيوياً عميقاً يهدد الاستقرار الأسري والمجتمعي نتيجة فبركة الهويات والصور والأصوات التي يصعب إثبات تزييفها بالوسائل الكلاسيكية .

٤. بالتطبيق على نظرية الارتباط التفاضلي، لم يعد تعلم السلوك الانحرافي مقتصراً على الجماعات المادية، بل امتد عبر منصات الإنترنت المظلم (Dark Web) والشبكات المشفرة لتلقين مهارات التزييف والابتزاز خوارزمياً، مع صياغة آليات حياد قيمي تحيد بوجدان الفاعل الرقمي عن الشعور بالذنب .

٥. يعاني الواقع القضائي والأمني العراقي من فجوة معيارية وهيكلية حادة؛ إذ إن الاعتماد على نصوص قانون العقوبات التقليدي رقم 111 لسنة 1969 لمواجهة تحديات القرن الحادي والعشرين الرقمية يقف عاجزاً أمام إثبات القصد الجنائي وتحديد الهوية الرقمية للفاعل الخوارزمي المستقل ذاتياً .

التوصيات : بناءً على الاستنتاجات السابقة، توصي الدراسة بتبني استراتيجية حوكمة مركبة (سوسيوتقنية وقانونية) تتلخص في النقاط الآتية :

١. ضرورة سد الفراغ المعياري الافتراضي عبر توظيف ذات تقنيات الذكاء الاصطناعي كأداة استباقية وتنبؤية للضبط الاجتماعي الرقمي، من خلال بناء أنظمة خوارزمية مضادة قادرة على رصد هجمات الهندسة الاجتماعية وكشف محتويات التزييف العميق قبل استفحال التضحية بالضحايا .

٢. التعجيل بإقرار قانون خاص ومستقل لمعالجة جرائم المعلوماتية والذكاء الاصطناعي في العراق، يتجاوز المعالجات الكلاسيكية ويستوعب مفهوم المسؤولية الجنائية للأنظمة الذكية المستقلة ذاتياً، مع ضبط قواعد مرنة للإثبات الخوارزمي الرقمي أمام المحاكم .

٣. يجب ألا تكون المقاربة الأمنية والرقابة الخوارزمية مبرراً لانتهاك خصوصية المستخدمين؛ بل توصي الدراسة ببناء أطر حوكمة رشيدة توازن بدقة بين متطلبات الردع الجنائي السيبراني وصون الحريات والحقوق الرقمية للمجتمع الافتراضي .

٤. إدماج مفاهيم الأمن السلوكي الرقمي في المناهج التعليمية والجامعية، لرفع وعي الأفراد (ولاسيما الشباب) بكيفية إدارة سلوكهم الروتيني الرقمي، وحماية بياناتهم وحساباتهم التفاعلية لتقليل فرص تقاطع عناصر الجريمة في الفضاء السيبراني .

٥. تأسيس وحدات مشتركة (أمنية، واجتماعية، ونفسية) متخصصة في دعم ضحايا الابتزاز الإلكتروني الناتج عن التزييف العميق، لمواجهة تداعيات الوصم الاجتماعي والاغتراب، وتقديم الإرشاد اللازم للحد من حالات التفكك الأسري والاضطراب المجتمعي .

الهوامش :

(١) الجميلي، جاسم محمد علوان. (٢٠٢٤). المواجهة الجزائية للجرائم الواقعة باستخدام الذكاء الاصطناعي. مجلة العلوم القانونية والسياسية (جامعة ديالى – كلية القانون والعلوم السياسية)، ١٣(٢)، ١٥١–١٨٢.

(٢) العبادي، أسامة نظيم سعدون، وسعيد، طارق م.، وحمدون، صبحي ح. (٢٠٢٤). الجريمة الإلكترونية في الواقع العراقي، دراسة وتحليل. المجلة الدولية للمجالات المتعددة الناشئة: علوم الحاسوب والذكاء الاصطناعي، ٣(١)، ١–٩.

(٣) بارني، دارن. (٢٠١٥). المجتمع الشبكي. ترجمة: أنور الجمعاوي. الدوحة: المركز العربي للأبحاث ودراسة السياسات.

(4) Merton, R. K. (1938). Social Structure and Anomie. American Sociological Review, 3(5), 672–682. https://doi.org/10.2307/2084686

(5) Sutherland, E. H. (1939). Principles of Criminology (3rd ed.). Philadelphia: J. B. Lippincott Company.

(6) Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

(7) Becker, H. S. (1963). Outsiders: Studies in the Sociology of Deviance. New York: Free Press of Glencoe .

(8) Castells, M. (2010). The Rise of the Network Society (2nd ed.). Oxford: Wiley-Blackwell.

(9) Foucault, M. (1975). Discipline and Punish: The Birth of the Prison. New York: Vintage Books .

(10) Wanda Orlikowski, W. J. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science, 3(3), 398-427 .

(١١) العبادي، أسامة ناظم سعدون، وسعيد، طارق، وحمدون، صبحي ح. (٢٠٢٤). الجريمة الإلكترونية في الواقع العراقي، دراسة وتحليل. المجلة الدولية للمجالات المتعددة الناشئة: علوم الحاسوب والذكاء الاصطناعي، ٣(١)، ١-٩.

https://doi.org/10.54938/ijemdcsai.2024.03.1.310

(١٢) العنبكي، حسين إبراهيم حمادي. (٢٠٢٥). الهندسة الاجتماعية الرقمية وتأثيرها على المنظومة القيمية للمجتمع: دراسة ميدانية اجتماعية في مدينة بعقوبة. مجلة واسط للعلوم الإنسانية، ٢١(١)، ٦٤٥-٦٧٠.

(١٣) خلف، أنس محمود. (٢٠٢٥). الجريمة السيبرانية وحدود المسؤولية الجنائية في الفضاء الرقمي. مجلة كلية القانون للعلوم القانونية والسياسية (جامعة كركوك)، ١٤(٥٤)، ١-٣٥.

(١٤) الجميلي، جاسم محمد علوان. (٢٠٢٤). المواجهة الجزائية للجرائم الواقعة باستخدام الذكاء الاصطناعي. مجلة العلوم القانونية والسياسية (جامعة ديالى)، ١٣(٢)، ١٥١-١٨٢.

https://doi.org/10.55716/jjps.2024.13.2.6

(١٥) الملا، معاذ سليمان راشد. (٢٠٢٤). الجرائم السيبرانية في عصر الثورة الصناعية الرابعة: الواقع والمأمول (دراسة وصفية تحليلية استشرافية في حقل القانون الجنائي). مجلة الدراسات الفقهية والقانونية، (ملحق خاص بالعدد ١٩)، ١١٥-١٤٦.

(16) Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publication-events/main-reports/iocta-report

(17) INTERPOL. (2025). Cybercrime: A Threat to People, Profits and Public Services – Global Threat Assessment 2025. International Criminal Police Organization.

https://www.interpol.int/en/Crimes/Cybercrime

(18) Cybersecurity Ventures. (2024). Ransomware damage costs predicted to reach $265 billion by 2031. Cybercrime Magazine. https://cybersecurityventures.com/ransomware-report/

(19) Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/publication-events/main-reports/iocta-report

(20) Castells, M. (2010). The Rise of the Network Society (2nd ed.). Wiley-Blackwell.

(21) Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/internet-

(22) Info Security Magazine. (2024). Ransom payments surge 500% in 2024. https://www.infosecurity-magazine.com/news/ransom-payments-surge-500/