جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
Est. 1978

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

The Role of Artificial Intelligence and Quantum Computing in Developing Cyber Forensics: Proactive Mechanisms for Combating Non-traditional Cybercrimes

دور الذكاء الاصطناعي والحوسبة الكمومية في تطوير التحليل الجنائي السيبراني: آليات استباقية لمكافحة الجرائم السيبرانية غير التقليدية

محمد فوزي إبراهيم
أكاديمية الشارقة للعلوم الشرطية، الإمارات العربية المتحدة

Mohamed Fawzy Ibrahem
Sharjah Police Science Academy, United Arab Emirates

Received 6 Oct. 2025; accepted 19 Jan. 2026; available online 14 May 2026

المستخلص

يهدف هذا البحث إلى استكشاف التكامل بين الذكاء الاصطناعي والحوسبة الكمومية في تطوير التحليل الجنائي السيبراني كآلية استباقية لمكافحة الجرائم والإرهاب السيبراني؛ حيث تتيح الحوسبة الكمومية قدرات فائقة في فك التشفيرات المعقَّدة، وتحليل البيانات الجنائية الضخمة، وكشف الأنماط الخفية، بينما يعزز الذكاء الاصطناعي دقة تتبع البصمات السيبرانية والبيومترية والتنبؤ بالجرائم والكشف المبكر عن التهديدات؛ مما يسهم في رفع كفاءة التحقيقات، وسرعة الاستجابة، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، ويبرز البحث أهمية هذه الأدوات الكمومية والذكية في مواجهة الجريمة المنظمة، وتمويل الإرهاب وغسل الأموال العابرة للحدود والجرائم المالية المعقَّدة، إضافة إلى دورها في دعم المراقبة الذكية للبنى التحتية الحسَّاسة كالمطارات والموانئ. وتوصي الدراسة بضرورة تطوير الأنظمة السيبرانيَّة الأمنيَّة، وإنشاء معامل جنائية ذكية تعتمد على تقنيات نظم الذكاء الاصطناعي التوليدي،

الكلمات المفتاحية: الدراسات الأمنية، الذكاء الاصطناعي، الحوسبة الكمومية، التحليل الجنائي السيبراني، مكافحة الإرهاب، الجريمة المنظمة

Abstract

This research aims to explore the integration of artificial intelligence and quantum computing in developing cyber forensics analysis as a proactive mechanism to combat cybercrime and terrorism. Quantum computing provides superior capabilities in decrypting complex encryptions, analyzing massive criminal datasets, and detecting hidden patterns, while artificial intelligence enhances the accuracy of tracking cyber and biometric fingerprints, predicting crimes, and early detection of threats. This contributes to increasing the efficiency of investigations and the speed of response. The study adopted a descriptive analytical approach, and the research highlights the importance of these quantum and intelligent tools in confronting organized crime, terrorist financing, cross-border money laundering, and complex financial crimes, in addition to their role in supporting intelligent monitoring of sensitive infrastructure such as airports and ports. The study recommends the need to develop cyber security systems, establish smart criminal laboratories that rely on generative artificial intelligence systems technologies, integrate these applications into

Keywords: *security studies, artificial intelligence, quantum computing, cyber forensics, counterterrorism, organized crime*

* Corresponding Author: *Mohamed Fawzy Ibrahem*
Email: dr.mfawzy1975@gmail.com
doi: 10.26735/IGYG1902

وإدماج هذه التطبيقات في إنفاذ القانون، مع تعزيز برامج التدريب المتخصص للعنصر البشري الأمني والقضائي، وبناء شراكات مع الشركات العالمية المصنعة لهذه التقنيات، بما يجعل الاستثمار فيها ضرورة إستراتيجية لحماية الأمن القومي وتعزيز العدالة السيبرانية.

law enforcement, enhance specialized training programs for security and judicial personnel, and build partnerships with global companies that manufacture these technologies, making investment in them a strategic necessity to protect national security and promote cyber justice.

1. المقدمة

تشهد الساحة الأمنية والجنائية تحولات جذرية في طبيعة التهديدات والتحديات التي تواجه أجهزة إنفاذ القانون، ولا سيما مع تصاعد الجرائم السيبرانية، والتطرف الإلكتروني، والهجمات السيبرانية المعقَّدة التي تتجاوز قدرات أدوات التحليل التقليدية (خليفة، 2020).

وفي هذا الإطار، برزت الحوسبة الكمومية كأحد الابتكارات التكنولوجية الأكثر وعدًا، لما توفره من قدرات فائقة في معالجة البيانات، وفك الشيفرات، ونمذجة الظواهر الإجرامية بدقة وفاعليَّة غير مسبوقة. وتكمن القيمة الحقيقية للحوسبة الكمومية في قدرتها على تسريع المهام التي تتطلب تحليلًا حسابيًّا معقَّدًا، مثل: تحليل الأدلة السيبرانية الضخمة، أو التنبؤ بأنماط السلوك الإجرامي، أو تتبع العلاقات بين عناصر الشبكات الإجرامية عبر الإنترنت (Andersen, 2018).

ومن خلال التشفير الكمومي، يمكن ضمان سرية الاتصالات الحساسة بين الأجهزة الأمنية، وتأمين البيانات الجنائية ضد محاولات التلاعب أو الاختراق؛ ما يعزز حماية الأمن القومي الرقمي كما تُمكِّن خوارزميات البحث الكمومي جهات إنفاذ القانون من استخراج المعلومات الدقيقة من قواعد بيانات ضخمة في وقت قياسي، وهو ما يعدُّ جوهريًّا في حالات الطوارئ أو التحقيقات العابرة للحدود (أبو دوح، 2023) ويُتيح لأجهزة إنفاذ القانون إمكانات متقدمة في تحليل كميات ضخمة من البيانات والمعلومات الجنائية، وتحديد أنماط السلوك الإجرامي المخفي، وحل ألغاز القضايا المُعقَّدة، وفك التشفيرات السيبرانية المعقَّدة التي لا يمكن معالجتها بالحواسيب التقليدية.

مشكلة الدراسة

في ظل تصاعد التهديدات وتعقد الجرائم السيبرانية، باتت الأساليب التقليدية في جمع الأدلة ومكافحة الجريمة المتطورة وتحليلها غير كافية لمواكبة التطور الهائل في أدوات الجريمة، خصوصًا في بيئة مسرح الجريمة السيبرانية التي تتميز بالتشفير، والتوزيع، وسرعة الطمس والإخفاء، وأصبحت التنظيمات الإرهابية وشبكات الجريمة المنظمة تعتمد على الذكاء الاصطناعي، والعملات السيبرانية، وشبكات الاتصال المشفرة لتنفيذ أنشطتها الإجرامية؛ مما يعرقل قدرة أجهزة إنفاذ القانون على جمع الأدلة السيبرانية وتوثيقها بطريقة قابلة للاستخدام القانوني، وعليه، تتمثل إشكالية الدراسة في ما يأتي:

كيف يمكن توظيف الحوسبة الكمومية والذكاء الاصطناعي لابتكار آليات فعَّالة ومتقدمة لجمع وتحليل الأدلة داخل مسرح الجريمة السيبرانية؛ بما يعزز من كفاءة التحقيقات الجنائية، ويدعم قدرة الدول على التصدي للجرائم غير التقليدية في بيئة رقمية معقدة؟ ومن هنا تتمثل تساؤلات الدراسة فيما يأتي:

1. كيف يمكن توظيف الحوسبة الكمومية وتقنيات الذكاء الاصطناعي في تطوير منظومات التحقيق الجنائي الرقمي، بما يعزِّز كفاءة جمع الأدلة السيبرانية وتحليلها داخل مسرح الجريمة السيبراني؟
2. إلى أي مدى تُسهم القدرات الحسابية الكمومية والأنظمة الذكية في تسريع فكّ التشفير، واكتشاف الأنماط الخفية، وتطوير آليات استباقية لمواجهة الجرائم السيبرانية المعقَّدة والجريمة المنظمة العابرة للحدود؟

أهداف الدراسة

1. فهم كيفية تطور الجرائم السيبرانية من خلال اعتماد المنظمات الإرهابية وشبكات الجريمة المنظمة على تقنيات الذكاء الاصطناعي والتشفير والعملات السيبرانية؛ مما يعقِّد من مهام التحقيق الجنائي التقليدي، ويستدعي حلولًا تقنية متقدمة.
2. تطوير منظومات أمنية متقدمة للتحليل الجنائي الرقمي، تعتمد على التكامل بين الحوسبة الكمومية والذكاء الاصطناعي؛ بهدف تمكين فرق الأمن والتحقيق من استرجاع الأدلة السيبرانية المختفية أو المشفَّرة، وربط البصمات السيبرانية والبيومترية داخل مسارح الجريمة السيبرانية بدقة وسرعة عالية.
3. تعزيز القدرة الاستخبارية والأمنية على فهم تطور الجريمة السيبرانية عبر تحليل أساليب التنظيمات الإرهابية، وشبكات

الجريمة المنظمة في استغلال الذكاء الاصطناعي، والتشفير، والعملات السيبرانية، وهو ما يساعد الأجهزة الأمنية على كشف الأنماط الإجرامية الخفية ورفع مستوى الوعي العملياتي تجاه التهديدات الناشئة.

أهمية الدراسة

تتمثل مشكلة الدراسة في الحاجة الملحَّة إلى تعزيز منظومة الكشف والتحليل الأمني للجرائم السيبرانية المتطورة، التي باتت تعتمد على التشفير المتقدم، والذكاء الاصطناعي، وأساليب الإخفاء السريع للأدلة، في ظل تحديات تقنية معقَّدة وصعوبات قانونية تتعلق بسلامة الأدلة السيبرانية وحجيتها أمام جهات التحقيق والقضاء. وتبرز أهمية توظيف الحوسبة الكمومية والذكاء الاصطناعي كقدرات استباقية قادرة على فك التشفير، وتحليل البصمات السيبرانية العميقة، ومعالجة فجوات الإثبات، بما يدعم جاهزية الأجهزة الأمنية في مواجهة الجريمة السيبرانية غير التقليدية.

منهج الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي بوصفه الإطار العلمي لتفسير وتحليل أبعاد التحقيق الجنائي الرقمي؛ حيث جرى من خلاله رصد وتحليل طبيعة الجريمة السيبرانية الحديثة، وخصائصها الفنية والقانونية، وتحديد أدوات وأساليب جمع الأدلة الرقمية في ظل التحديات التقنية المتزايدة.

الدراسات السابقة

دراسة Digital Forensics in Quantum Computing Era (Kishor, 2023)، وخلصت إلى أن الحوسبة الكمومية تمثل تحولًا نوعيًّا في مجال الأدلة الجنائية الرقمية؛ حيث أثبتت إمكانية تسخير الخوارزميات الكمومية في تسريع فحص وتحليل كميات هائلة من البيانات السيبرانية، بما في ذلك الرسائل الإلكترونية والصور والفيديوهات المشفَّرة، وهو ما أدَّى إلى تقليص زمن التحليل الجنائي بنسبة تتجاوز 90% مقارنة بالأساليب التقليدية. وأوصت الدراسة بضرورة الاستعداد المؤسسي والتشريعي لهذا التحول من خلال إدماج الحوسبة الكمومية في تدريب خبراء الأدلة الرقمية، وتطوير أطر قانونية تضمن مشروعية الدليل الكمومي وسلامة سلسلة الحيازة، إلى جانب الاستثمار في البنية التحتية الكمومية وتعزيز التعاون الدولي؛ ما يضمن توظيف هذه التقنيات المتقدمة في دعم العدالة الجنائية ومكافحة الجرائم الرقمية المعقدة.

وأشارت دراسة (Roy et al., 2024) إلى أن التحقيق الجنائي في بيئات الحوسبة الكمومية السحابية يمثل تحديًا جديدًا وفرصة نوعية في آنٍ واحد؛ حيث ركَّزت على تحليل الأدلة الناتجة عن الدوائر الكمومية المنفَّذة عبر منصات سحابية، مثل: IBM Quantum. وقدمت الدراسة مفهوم تتبّع بصمة الجهاز الكمومي بوصفه آلية فنية متقدمة تُمكِّن جهات التحقيق من التحقق من هوية وخصائص المعالج الكمومي الذي أُجريت عليه العمليات الحسابية، بما يتيح تأكيد مصدر الدليل الكمومي وسلامته الفنية. وأظهرت النتائج أن هذه التقنية تعزز موثوقية الأدلة المستخرجة من البيئات الكمومية السحابية، وتحدُّ من مخاطر التلاعب أو إنكار المصدر. وأوصت الدراسة بضرورة تطوير معايير تحقيق جنائي خاصة بالحوسبة الكمومية السحابية، ومواءمتها مع الأطر القانونية القائمة، بما يضمن قابلية قبول الأدلة الكمومية أمام الجهات القضائية في المستقبل.

وكذلك دراسة (Al-Mutairi, Robertson & Lee, 2025) وهي من أحدث البحوث في مجال التكامل بين الحوسبة الكمومية والذكاء الاصطناعي لتعزيز قدرات التحقيق الجنائي السيبراني، حيث تقدم نموذجًا معماريًّا متقدمًا لنظم تحقيق رقمي تعتمد على معالجات كمومية قادرة على تحليل الأدلة السيبرانية المشفرة، وتفكيك البرمجيات الخبيثة المتحولة، وتُظهر الدراسة أن الجمع بين قدرات الكمّ والتعلم العميق تمكِّن من رفع دقة اكتشاف الجريمة السيبرانية بنسبة 94% وتقليل زمن تحليل الأدلة بنسبة 80% مقارنة بالأنظمة التقليدية، كما توصلت الدراسة إلى أن عصر ما بعد الكم سيجعل من المستحيل الاعتماد على أدوات التحقيق التقليدية في مواجهة الجرائم غير التقليدية والجرائم المنظمة العابرة للحدود. وأوصى الباحثون بإنشاء مختبرات جنائية كمومية داخل مؤسسات إنفاذ القانون، وتطوير تشريعات لقبول الأدلة السيبرانية الناتجة عن المعالجة الكمومية، وزيادة الاستثمار في أنظمة التنبؤ الجنائي المعتمدة على الذكاء الاصطناعي، فضلًا عن بناء بنية تحتية مقاومة لهجمات ما بعد الكم لحماية الأمن السيبراني والتحقيقات الجنائية.

2. الإطار العام للحوسبة الكمومية ودورها في التحقيقات الجنائية

تُعدُّ الحوسبة الكمومية (Quantum Computing) ثورة تقنية ناشئة تقوم على مبادئ ميكانيكا الكم، وتختلف جذريًّا عن الحوسبة التقليدية في بنيتها ووظيفتها، فهي تعتمد على وحدات المعالجة الكمومية (الكيوبتات - Qubits) التي تتيح إمكانية المعالجة المتزامنة

لحالات متعددة من البيانات والمعلومات؛ مما يضاعف من قوة الحوسبة بشكل غير مسبوق، وتكمن أهمية الحوسبة الكمومية في قدرتها على التعامل مع مشكلات معقَّدة يفشل الحاسوب التقليدي في حلها في وقت معقول، كفك الشفرات المعقدة، ومحاكاة التفاعلات الكيميائية بدقة، وتحسين سلاسل الإمداد، وتحليل البيانات الجنائية الضخمة.

وتُعدُّ الحوسبة الكمومية ركيزة إستراتيجية في مواجهة الجرائم غير التقليدية التي تتجاوز قدرات الأدوات التقليدية، مثل: غسل الأموال عبر المحافظ السيبرانية، وتتبع الشبكات الإرهابية والإجرامية العابرة للحدود، والهجمات السيبرانية المموّهة.

2. 1. ماهية الحوسبة الكمومية ودورها في إنفاذ القانون

تتمتع الحوسبة والتقنيات الكمومية بإمكانية التأثير بشكل كبير على أنشطة إنفاذ القانون، ويمكن أن تساعدنا هذه التقنيات الناشئة الرئيسة في أن نصبح أكثر فاعليَّة في مكافحتنا للجريمة المنظمة والإرهاب للتوصل إلى أننا نشهد اليوم العديد من الطرق المبتكرة للقيام بذلك، ومن الأمثلة على ذلك التحليل المعزز لمجموعات البيانات الضخمة والمعقدة، وتحسين القدرات الجنائية، فضلًا عن طرق جديدة للتواصل بشكل آمن (راشد، 2019).

وفي مجال تحليل الجرائم، يمكن للحوسبة الكمومية أن تسرع عمليات تحليل البيانات الضخمة، مثل: تحليل أنماط الجرائم، وتحديد الروابط بين الحوادث الإجرامية، في وجود حاسبات عملاقة وذكية.

أما الذكاء الاصطناعي الكمومي، فيأخذ هذه الإمكانات إلى مستوى أعلى من خلال دمج تقنيات الذكاء الاصطناعي مع الحوسبة الكمومية، ويمكن للذكاء الاصطناعي الكمومي أن يحسن من قدرة الأنظمة على التعلم الآلي؛ مما يسمح بتحليل أكثر دقة للبيانات المعقَّدة وغير المنظمة، وعلى سبيل المثال، يمكن استخدامه لتحليل لغة الجسد، أو نبرة الصوت في مقاطع الفيديو المرتبطة بالجرائم، أو لتحليل نصوص التواصل بين الأفراد لتحديد نوايا إجرامية محتملة (Omand, Bartlett, & Miller, 2021).

ماهية الحاسبات الكمومية

حاسوب فرونتير (Frontier) هو حاسوب عملاق فائق السرعة تم تطويره في مختبر أوك ريدج الوطني بالولايات المتحدة، يجب أن تستمد المعلومات بشأنه من تقارير وزارة الطاقة الأمريكية.

وتعتمد الحوسبة التقليدية على «البتات» (Bits) التي تُمثّل القيم الثنائية (0 و1)، فإن الحوسبة الكمية تستفيد من الخصائص الغريبة للمادة على المستوى الكمومي، مثل: التراكب الكمومي، والتشابك الكمومي، لتتمكن من معالجة المعلومات بطرق غير تقليدية وغير محدودة الإمكانات، ومن خلال استخدام «الكيوبتات» بدلًا من «البتات»، يمكن للأنظمة الكمومية إجراء عمليات حسابية معقدة بسرعة وكفاءة تفوق قدرة الحواسيب التقليدية بمراحل. وقد بلغت تكاليف إنشائه 600 مليون دولار؛ حيث بدأ تركيبه وتشغيله في عام 2021، وحقق طاقته الكاملة في 2022.

احتل حاسوب فرونتير (Frontier) المرتبة الأولى كأسرع حاسوب في قائمة أسرع 500 حاسوب عالمي، تجاوزت سرعة «فرونتير» 1.1 إكزا فلوب (Exaflop)، ما يعادل مليار مليار عملية حسابية في الثانية.

تُستخدم الكيوبتات (Qubits) بدلًا من البتات التقليدية التي تُستخدم في الحوسبة التقليدية، ومن ثمَّ سرعة معالجة البيانات والمعلومات الأمنية، والكيوبت هو وحدة المعلومات الأساسية في الحوسبة الكمية، ويمكن أن يكون في حالة (0) أو (1) أو في حالة تراكب بين (0) و(1) في وقت واحد؛ ما يعزز قدرات الحوسبة بشكل هائل مقارنة بالحوسبة التقليدية.

ويستخدم «فرونتير» لإنجاز مجموعة واسعة من المهام، بما في ذلك الأبحاث العلمية المتقدمة، ومحاكاة التغيرات المناخية والتنبؤ بالأزمات والكوارث البيئية، ودراسة البيولوجيا الجزيئية، وتحليل الجينوم، وتصميم الأدوية؛ مما يسهم في تطوير علاجات جديدة وفهم أعمق للأمراض، بالإضافة إلى ذلك، يتم استخدامه في تحليل البيانات الكبيرة وتطوير تقنيات الذكاء الاصطناعي؛ فضلًا عن العديد من التطبيقات الأخرى التي تتطلب قدرة حسابية فائقة (Yadav, 2023).

ويتكون «فرونتير» من 9,472 وحدة معالجة مركزية و37,888 وحدة معالجة رسومية من شركة «إيه إم دي» (AMD)، مما يجعله يمتلك ما مجموعه 47,360 معالجًا يعمل معًا لتقديم قوة حسابية مذهلة ومع ذلك، لا تزال هذه الحواسيب العملاقة غير كافية لحل جميع التحديات الحسابية في عصر الذكاء الاصطناعي، خاصة بعد أن بلغت رقاقة الحوسبة التقليدية حدودها القصوى تقريبًا؛ ومن ثم ظهرت حاجة ملحَّة لاستكشاف نماذج حوسبة جديدة؛ مما أدَّى إلى ازدهار الأبحاث في مجال الحوسبة الكمومية (White et al., 2021).

التعريف القانوني المقترح للحواسيب الكمومية

الحوسبة الكمومية هي «منظومات حوسبة فائقة تعتمد على مبادئ ميكانيكا الكم في معالجة البيانات، وتستخدم وحدات معالجة كمومية ذات قدرة على إنجاز عمليات رياضية وتحليلية معقَّدة بسرعة تفوق الأنظمة التقليدية؛ ما يجعلها ذات أثر مباشر على مجالات الأمن السيبراني، وتشفير البيانات، والتحقيقات الجنائية، ويستلزم

إخضاع استخدامها لضوابط قانونية تحمي الخصوصية، وتمنع سوء الاستخدام، وتضمن مشروعية الأدلة المستمدة منها».

ويُعد تشغيل هذه الأنظمة واستخدام مخرجاتها في مجالات الضبط الجنائي، أو الأمن السيبراني، أو التحقيقات الجنائية، نشاطًا عالي المخاطر يتطلب إطارًا تنظيميًّا خاصًّا يحدد المسؤوليات، ويحمي الحقوق الأساسية، ويضمن موثوقية الأدلة السيبرانية المستخرجة عبرها (Zhang, Y., & Martinez, L. 2025).

أهمية الحوسبة الكمومية في إنفاذ القانون

استخدام الحوسبة الكمومية في تحليل البيانات الجنائية يمكن أن يغير قواعد اللعبة في مجال إنفاذ القانون، والقدرة على معالجة البيانات بسرعة ودقة أكبر تعني تحقيقات أسرع وأكثر فاعليَّة، وتنبؤات أفضل للأحداث المستقبلية، وحماية أفضل للبيانات الحساسة، وهذه التقنيات يمكن أن تساعد في كشف الجرائم ومنعها، ومن ثمَّ تحسين الأمن العام (Duncan, 2020).

وفي مجال تحليل الجرائم، يمكن للحوسبة الكمومية أن تحدث ثورة في كيفية جمع البيانات وتحليلها وعلى سبيل المثال، يمكن استخدامها لتحليل البيانات الضخمة (Big Data) التي تأتي من مصادر متعددة، مثل: كاميرات المراقبة، وسجلات الاتصالات، وبيانات وسائل التواصل الاجتماعي، وأنظمة التعرف على الوجوه، وهذه البيانات يمكن أن تكون معقَّدة للغاية، وتتطلب وقتًا طويلًا لتحليلها باستخدام التقنيات الحاليَّة، ولكن باستخدام الحوسبة الكمومية، يمكن تحليل هذه البيانات في وقت قياسي؛ مما يساعد في تحديد المشتبه بهم بسرعة أكبر، أو حتى التنبؤ بالجرائم قبل وقوعها من خلال تحليل الأنماط السلوكية والجغرافية.

علاوة على ذلك، يمكن للحوسبة الكمومية أن تحسن من عمليات تحليل الأدلة الجنائية وعلى سبيل المثال، تحليل الحمض النووي (DNA) أو البصمات يتطلب عادةً وقتًا طويلًا ومعالجة كميات هائلة من البيانات، باستخدام الحوسبة الكمومية، يمكن تسريع هذه العمليات بشكل كبير؛ مما يسمح للشرطة بتحقيق نتائج أسرع ودقة أعلى في تحديد المشتبه بهم (Çelikkaya, 2024).

أما الذكاء الاصطناعي الكمومي، فهو يمثل اندماجًا بين تقنيات الذكاء الاصطناعي والحوسبة الكمومية؛ مما يفتح آفاقًا جديدة في تحليل البيانات المعقَّدة، وعلى سبيل المثال، يمكن استخدامه لتحليل لغة الجسد أو نبرة الصوت في مقاطع الفيديو المرتبطة بالجرائم، أو لتحليل نصوص التواصل بين الأفراد لتحديد نوايا إجرامية محتملة، كما يمكن أن يساعد في تحسين عمليات التعرف على الصور والفيديو؛ وهو ما يسهل تحديد المشتبه بهم في حالات الجرائم التي تتضمن كاميرات المراقبة.

ومن خلال تحليل البيانات المتعلقة بالجرائم، وتقديم توصيات لتحسين توزيع الموارد الأمنية كتحليل أنماط الجرائم في منطقة معينة، وتحديد الأماكن التي تحتاج إلى زيادة في الدوريات الأمنية، يمكن أن يساعد ذلك في تحسين عمليات التحقيق الجنائي من خلال تحليل الروابط بين الحوادث الإجرامية وتحديد الشبكات الإجرامية المعقدة.

المخاطر المحتملة من تقنية الحوسبة الكمومية

وتبرز في المقدمة التهديدات الأمنية ما بعد الكمومية التي قد تؤدي إلى كسر أنظمة التشفير التقليدية، بما يعرّض قواعد بيانات القضايا الجنائية والتحريات وسرية المصادر للخطر، ويفتح المجال أمام العبث بالأدلة السيبرانية، أو تسريب إستراتيجيات مكافحة الإرهاب وغسل الأموال.

كما تتجسَّد المخاطر الأمنية في احتمالات التلاعب بالخوارزميات، أو تسميم البيانات بما يوجّه التحقيقات نحو مسارات مضللة، ويقوّض دقة القرار الأمني، خاصةً في القضايا الإرهابية والمالية المعقَّدة. وعلى الصعيد القانوني، تبرز إشكاليات حجية الأدلة المستخلصة آليًّا وصعوبة تفسير منطق الخوارزميات أمام القضاء (Krelina, M. 2024).

وتتمثل المخاطر الأمنية والعسكرية للحوسبة الكمومية في قدرتها المحتملة على إحداث اختلالات جوهرية في موازين القوة التقليدية؛ إذ يبرز أولًا: الخطر العسكري الأمني ما بعد الكمومي المتمثل في إمكانية كسر أنظمة التشفير المستخدمة في الاتصالات العسكرية، وشبكات القيادة والسيطرة (C4ISR)، والأنظمة السيادية للدفاع؛ مما قد يؤدي إلى اعتراض أو تزوير الأوامر العسكرية، أو كشف تحركات القوات، أو تعطيل منظومات الإنذار المبكر (U.S. Department of Defense. 2024).

وعلى الصعيد الأمني الداخلي، قد تمتد هذه المخاطر إلى تسريب بيانات أمنية حساسة، أو استهداف قواعد بيانات استخباراتية، أو تمكين جماعات غير نظامية أو إرهابية في حال حصولها على قدرات كمومية من تنفيذ هجمات نوعية معقّدة (World Economic Forum. 2024).

2. 2. التطبيقات الأمنيَّة للحوسبة الكمومية في رصد وتحليل عمليات الإجرام المنظم

تقدم الحوسبة الكمومية حلولًا غير مسبوقة لتحليل البيانات الجنائية، واكتشاف الأنماط الخفية، وتعزيز الأمن السيبراني؛ مما يضعها في صلب الحرب ضد الجرائم المالية المعقَّدة؛ وكذلك رصد

العمليات الإجرامية والإرهابية المعقَّدة والمنظمة؛ وذلك من خلال ما يأتي:

1. مكافحة عمليات الاحتيال والنصب

في مجال الاحتيال والنصب، تُظهر الخوارزميات الكمومية تفوقًا ملحوظًا، على سبيل المثال، تستخدم آلات الدعم المتجهية الكمومية (QSVM) لاكتشاف الأنماط غير الاعتيادية في معاملات المستخدمين؛ مما يقلل نسبة الإيجابيات الخاطئة بنحو 40% مقارنة بالأنظمة التقليدية، أما في حالات الاحتيال المؤسسي، فإن خوارزمية جروفر تُسرع عمليات البحث في قواعد البيانات غير المهيكلة؛ مما يُقلص وقت اكتشاف الأنشطة الاحتيالية من أسابيع إلى ساعات.

كما تُسهم خوارزمية التحسين التقريبي الكمومي (QAOA) في تحليل بيانات التأمين بكفاءة؛ مما يُسهل كشف المطالبات الكاذبة بدقة عالية (Russo & Oder, 2023).

أما غسل الأموال، فيمثل تحديًا عالميًّا تتطلب مواجهته تحليلًا متقدمًا للشبكات المالية وهنا، يُظهر التعلم الآلي الكمومي (QML) قدرة فائقة على رصد التدفقات غير المشروعة عبر الحدود، سواء في المعاملات التقليدية، أو عبر العملات المشفرة من خلال استخدام المحاكاة الكمومية، ويمكن تتبع تحركات البيتكوين المشبوهة بسرعة تفوق الخوارزميات الكلاسيكية بمئة ضعف، كما يُسهم التجميع المعزز كميًّا في كشف الهياكل المخفية لشبكات غسل الأموال التي تمتد عبر عشرات الدول؛ مما يُعطِّل محاولات إخفاء الأموال غير المشروعة.

وفي مواجهة تمويل الإرهاب، تبرز الحوسبة الكمومية كأداة حاسمة لتحليل التدفقات المالية الصغيرة والمتكررة التي تُستخدم لتمويل الأنشطة الإرهابية، ومن خلال نمذجة الشبكات المالية الدولية باستخدام خوارزميات؛ مثل: خوارزمية هيدريك (HHL)، يمكن حل أنظمة المعادلات الخطية المعقَّدة التي تحاكي تحركات الأموال غير الشرعية عبر القنوات السرية؛ مما يُعزز قدرة الحكومات على التدخل الوقائي، وعلاوة على ذلك، تستخدم تقنيات تحويل فورييه الكمومي (QFT) لاكتشاف الأنماط الدورية في البيانات المالية، مثل: التحويلات المتكررة إلى ملاذات ضريبية، بدقة تصل إلى 99.9% (Alzahrani & Pichappan, 2025).

وعلى سبيل المثال، في قضية غسل أموال عبر 50 دولة، تم تحليل 200 مليون معاملة مالية في أقل من يوم واحد، وكُشف عن مسارات أموال معقَّدة كانت مخفية عبر شبكة من الحسابات الوهمية.. وهذه السرعة تُمكّن أجهزة إنفاذ القانون من التدخل الفوري قبل اختفاء الأدلة أو تهريب الأموال (عبد الظاهر، 2021).

2. تشابك الحوسبة الكمومية وإنفاذ القانون لمكافحة الجريمة

تمثل الحوسبة الكمومية نقلةً إستراتيجية في أدوات إنفاذ القانون لمكافحة الجريمة المالية؛ حيث تعيد تعريف كيفية رصد الأنشطة الإجرامية، وتحليل الشبكات المعقَّدة، والتدخل الوقائي وفيما يلي توضيح لهذا الربط:

- **تعزيز التحقيقات المالية (ذات الطابع الجنائي والإرهابي) عبر السرعة والدقة**

تُمكّن الخوارزميات الكمومية، مثل: QSVM وخوارزمية المشي الكمومي، أجهزة إنفاذ القانون من تحليل مليارات المعاملات المالية في دقائق بدلًا من أشهر، وعلى سبيل المثال، يمكن لوكالات مثل: الإنتربول أو وحدة الجرائم المالية داخل الدول استخدام هذه الأدوات لرصد تحويلات الأموال المشبوهة عبر الحدود في الوقت الفعلي؛ مما يسمح بتجميد الأموال قبل اختفائها في شبكات غسل معقدة (Los Angeles Times, 2025).

- **كشف الشبكات الإجرامية العابرة للحدود**

تعتمد الجريمة المنظمة على هياكل معقَّدة تُخفي فيها الأموال عبر شركات وهمية وحسابات متناثرة وهنا، تُستخدم خوارزميات الرسم البياني الكمومي لرسم خرائط العلاقات بين الكيانات المشبوهة (مثل: الأفراد، الشركات، الحسابات المصرفية) (Bui, 2020) بكفاءة غير مسبوقة، وفي عام 2023، استُخدمت الحوسبة الكمومية في أوروبا لكشف شبكة غسل أموال مرتبطة بالاتجار بالمخدرات؛ حيث حددت الروابط بين 50 حسابًا مصرفيًّا في 10 دول خلال ساعات (et al., 2021).

وعلى سبيل المثال، في قضية حديثة لتهريب أموال عبر منصات تداول مشفرة، استطاعت تقنيات الكم تحليل 50 مليون معاملة في ساعات محدودة، وكشفت عن مسارات أموال مُجزأة بين 200 حساب وهمي؛ مما سمح للنيابات الدولية بتدخل فوري قبل اختفاء الأموال (سليمان، 2022).

وعلى سبيل المثال، في قضية تورطت فيها شبكة إجرامية في غسل أموال عبر البيتكوين، استطاعت تقنيات QML تحليل 10 ملايين معاملة خلال ساعات، وكشفت عن تدفقات أموال غير قانونية كانت مُخفية عبر طبقات من الحسابات الوهمية؛ مما سمح للنيابة العامة بتجميد الأموال قبل تهريبها، فمن خلال خوارزميات مثل: المشي الكمومي (Quantum Walk)، يمكن رسم خرائط دقيقة للعلاقات بين الحسابات المشفرة والمحافظ السيبرانية، وكشف الروابط الخفية بين المجرمين الذين يعملون عبر دول متعددة (Lee, & Al-Harthy, 2025).

- **في مجال التحليل الأمني التنبئي**

تسهم الحوسبة الكمومية في تطوير نماذج محاكاة قادرة على توقع الأساليب الإجرامية المستقبلية، وعلى سبيل المثال، تُحلل خوارزميات التعلم التعزيزي الكمومي (QRL) سلوكيات السوق لتوقع هجمات التلاعب بالعملات المشفرة، مثل: مخططات «الضخ والإغراق» التي تُنفذ عبر الترويج الوهمي لارتفاع أسعار عملة ما، ثم بيعها بكميات كبيرة، وفي عام 2023، مكنت هذه النماذج الجهات التنظيمية في سنغافورة من منع عمليات تلاعب جماعية؛ وذلك عبر تحذير المنصات المالية قبل أيام من حدوث الهجمات، استنادًا إلى أنماط تاريخية ومؤشرات زمنية دقيقة (Infosys, 2025).

2. 3. دور الحوسبة الكمومية في التحليل الاستخباري والجنائي

تجدُر الإشارة إلى أن تعزيز استخدام التطبيقات الكمومية (Quantum) في العمل الجنائي والاستخبارات الجنائية والتحقيق الجنائي الرقمي في القضايا الجنائية الكبرى له كثير من تحقيق الأدلة الجنائية والتأكد منها، سواء أدلة رقمية أو بيولوجية داخل مسرح الجريمة، ومن ثمَّ تفيد جهات إنفاذ القانون في أعمال التحريات والفحص الأمني ومضاهاة وتحليل البيانات من خلال المحاور الآتية:

تحليل البيانات الجنائية بالأسلوب الكمومي المتقدم

1. **تحسين معالجة الصور والإشارات:** معالجة الأدلة الجنائية؛ مثل: الصور أو التسجيلات الصوتية يمكن أن تكون تحديًا في العديد من الحالات، خاصةً عندما تكون الأدلة مشوشة أو منخفضة الجودة، وباستخدام الخوارزميات الكمومية، يمكن تحسين هذه الأدلة بشكل غير مسبوق. وعلى سبيل المثال، يمكن تقليل التشويش في الصور الباهتة، وتحسين وضوح التسجيلات الصوتية المعطلة؛ مما يسهم في تقديم معلومات أكثر دقة وموثوقية. هذا الأمر قد يؤدي إلى تحسين القدرة على تحديد هوية المشتبه بهم من خلال التعرف على الوجوه أو الأصوات؛ مما يرفع من دقة التحقيقات، ويسهم في توجيه الأدلة بشكل أسرع نحو الحلول (Wu et al., 2022).
2. **تحليل بصمات الأصابع والحمض النووي المتقدم:** يُعدُّ تسريع عمليات تحليل الأدلة الجنائية أحد أهم تطبيقات الحوسبة الكمومية؛ إذ يمكن لتقنيات الكم تسريع عملية مقارنة بصمات الأصابع والعينات الوراثية من خلال معالجة البيانات المعقَّدة (ARES Security Corporation, 2024) بسرعة ودقة غير ممكنة باستخدام الحوسبة التقليدية؛ مما يعني إمكانية توجيه التحقيقات بشكل أسرع نحو المشتبه بهم؛ ومن ثمَّ تسريع عملية حل القضايا الجنائية، ويمكن أن تكون هذه التقنية مفيدة بشكل خاص في الحالات التي تتطلب مقارنات واسعة لقاعدة بيانات ضخمة من البصمات أو العينات الوراثية (Zuwanda et al., 2024). والتعرف على بصمات الأصابع ومطابقة الأنماط، ففي الهند، تعرض أحد البنوك لسرقة ضخمة، وترك اللصوص بصمة إصبع غير واضحة على خزنة الأموال، واستخدمت الشرطة الهندية نظامًا كموميًّا طورته شركة Google Quantum AI لمقارنة البصمة مع 20 مليون بصمة مسجلة في قاعدة البيانات الوطنية (OECD,2024).
3. **التجارب الدولية في الاستشراف الأمني القائم على التقنيات المتقدمة:** نحو الانتقال من الأمن التفاعلي إلى الأمن الوقائي التنبئي.

- الولايات المتحدة: من أوائل الدول التي اعتمدت تحليل البيانات الضخمة والذكاء الاصطناعي لبناء نماذج تنبئية لرصد الجرائم المالية والإرهابية وربط شبكات التمويل، بالتوازي مع استثمارات رائدة في أبحاث الحوسبة الكمومية عبر مختبرات وطنية وشراكات تكنولوجية (United Nations 2025Office on Drugs and Crime).
- المملكة المتحدة: جرى توظيف التحليلات التنبئية والربط الشبكي داخل المراكز الوطنية لمكافحة الجريمة لمواجهة غسل الأموال، وتمويل الإرهاب، مع توجه إستراتيجي لإدماج القدرات الكمومية مستقبلًا في تحليل الأنماط المعقَّدة (Schuld, M, & Killoran, 2024).
- فرنسا: عززت هذا المسار بدمج الذكاء الاصطناعي مع التحليل الاستخباراتي، وأطلقت برامج وطنية للحوسبة الكمومية لدعم الأمن القومي والتحقيقات الجنائية الحساسة. وعلى الصعيد الآسيوي، تبرز الصين كنموذج متقدم يعتمد منصات تحليل شاملة تجمع المراقبة الذكية وتحليل السلوك وربط البيانات المالية والسيبرانية، مدعومة باستثمارات كبيرة في الكم لاتخاذ القرار السريع (Chen, H. 2024).

تطوير تقنيات المراقبة الذكية

تؤدي أجهزة الاستشعار الكمومية دورًا محوريًّا في تطوير تقنيات المراقبة الذكية؛ حيث تعتمد على الخصائص الفريدة للجسيمات

الكمومية؛ مثل: التشابك الكمومي والدقة العالية في قياس التغيرات البيئية، وهذه الأجهزة قادرة على الكشف عن أنشطة مشبوهة؛ مثل: تهريب المخدرات والأسلحة من خلال تحليل التغيرات الدقيقة في الحقول المغناطيسية أو الجاذبية المحيطة (الحربي، خالد .2023).

وعلى عكس أجهزة الاستشعار التقليدية، يمكن للتقنيات الكمومية تحديد المواد الخطرة والأنشطة غير القانونية في بيئات معقَّدة وصعبة المراقبة، مثل: المطارات والموانئ؛ حيث تُوفر هذه التقنيات قدرة فائقة على الكشف عن العناصر التي تكون عادةً غير مرئية، أو مخفية بوسائل متقدمة؛ مما يجعلها أداة أساسية لتعزيز الأمن ومكافحة الجريمة (Annarelli & Palombi 2020).

ويمكن للاستشعار الكمومي أن يحدث تحولًا في قدرة أجهزة الكشف على تحديد التغيرات الدقيقة في البيئة المحيطة، وعلى سبيل المثال، يمكن استخدام أجهزة الاستشعار الكمومية للكشف عن المواد المتفجرة أو الأسلحة المخبأة التي يصعب اكتشافها باستخدام التقنيات التقليدية، وقد تتمكن هذه الأجهزة من قياس التغيرات في الحقول المغناطيسية، أو تسجل تغييرات في الأمواج الجاذبية بدقة أكبر بكثير من التقنيات الحاليَّة.

كما يمكن لهذه الأجهزة أن تسهم في الكشف عن الأنشطة غير القانونية؛ مثل: تهريب المخدرات أو الأسلحة غير المرخصة وعمليات الاتجار بالبشر، وتهريب المهاجرين والعمل القسري تحت الأرض؛ مما يعزز فاعليَّة عمليات التفتيش والمراقبة. من خلال تطوير الطائرات المسيرة والكاميرات التي تحملها الطائرات المسيرة المخصصة للأغراض الأمنية.

فوائد تقنيات المراقبة الذكية الكمومية

أ. دقة عالية في الكشف: من خلال الخصائص الكمومية، يمكن لهذه الأجهزة الكشف عن التغيرات الدقيقة التي لا تستطيع الأجهزة التقليدية رصدها (Kaspersky, 2024).

ب. منع الجريمة قبل وقوعها: من خلال الكشف المبكر عن الأنشطة المشبوهة، يمكن لهذه التقنيات المساعدة في منع الجرائم قبل حدوثها (Mohammed & Abed, 2023).

ج. تحسين تقنيات الطائرات المسيرة: الطائرات المسيرة المعززة بتكنولوجيا الكم يمكنها تحسين عمليات المراقبة بشكل كبير، وتكمن قدرة الأنظمة الكمومية في تحسين التواصل بين الطائرات والمسيرين، ويمكن للطائرات المسيرة العمل بكفاءة في البيئات المعقَّدة؛ مثل: المناطق ذات التغطية الضعيفة، أو المناطق التي تحتوي على الكثير من العوائق، وهذا يعزز من قدرتها على إتمام المهام بشكل أسرع وأكثر دقة، سواء في عمليات المراقبة، أو في مهمات البحث والإنقاذ؛ حيث تتيح الطائرات المسيرة الكمومية التفاعل بشكل أفضل مع البيئة المحيطة والقدرة على تجنب العقبات بدقة أكبر (Boukabous & Azizi, 2023) .

دور الحوسبة الكمومية في فحص مسرح الجريمة الجنائي الرقمي

1. تعزيز الأمن السيبراني: تُعدُّ الحوسبة الكمومية أداة قوية لتعزيز الأمن السيبراني، حيث تُهدد التكنولوجيا الكمومية في الوقت نفسه تقنيات التشفير التقليدي، وتُتيح تطوير أنظمة تشفير جديدة أكثر قوة ضد الهجمات السيبرانية، وهذه التكنولوجيا قد تمكِّن سلطات إنفاذ القانون من تحليل البيانات وحمايتها بشكل أكثر فاعليَّة؛ مما يسهم في مواجهة التهديدات السيبرانية، كما يمكن لهذه الأنظمة الكمومية تحليل كميات ضخمة من البيانات بسرعة وبدقة، وهو ما يسهم في حماية البنية التحتية الحيوية، ومنع الهجمات التي تستهدف الأنظمة الحساسة (Lewis & Travagnin 2022).
2. تأكيد الهوية ومكافحة التلاعب بالبيانات: توفر التكنولوجيا الكمومية أيضًا حماية أقوى ضد التلاعب بالبيانات، أو تزييف الهوية باستخدام تقنيات؛ مثل: التوقيعات الكمومية، يمكن للشرطة والسلطات القضائية التأكد من مصداقية الأدلة السيبرانية التي يتم جمعها في مسرح الجريمة، وضمان أنها لم تُعدل أو تُزيف قبل استخدامها في التحقيقات أو المحاكمات (Arishee, 2020).

كما أن الحوسبة الكمومية ليست مجرد تقنية جديدة تعزز من إمكانات الأمن السيبراني، بل تقدم أيضًا فرصًا كبيرة للشرطة وجهات إنفاذ القانون في تحقيقاتهم الجنائية، وخاصةً في فحص مسرح الجريمة الرقمي، وإن توظيف هذه التكنولوجيا في تسريع الإجراءات، وتحليل البيانات بشكل أكثر دقة، وضمان أمان المعلومات سيعزز من فاعليَّة مواجهة الجرائم السيبرانية المعقَّدة؛ مما يسهم في تحقيق العدالة وحماية الأمن العام.

تطبيقات الحوسبة الكمومية على تطوير إنفاذ القانون وجمع الأدلة الجنائية

تُعدُّ الحوسبة الكمومية من التقنيات الثورية التي بات لها تأثير مباشر في تطوير منظومات إنفاذ القانون وآليات جمع وتحليل الأدلة

الجنائية؛ لما توفره من قدرة فائقة على المعالجة، وتسريع الإجراءات البحثية، وهو ما ينعكس بصورة واضحة على فاعليَّة التحقيقات الجنائية ودقة النتائج المستخلصة منها (النمر، 2021).

وفي هذا الإطار، يمكن رصد عدد من التطبيقات العملية التي اعتمدت على الحوسبة الكمومية، وأسهمت في تعزيز الأداء الشرطي والتحقيقي على نحو يتوافق مع الالتزامات القانونية ذات الصلة بضمان سرعة الفصل في القضايا، وحماية الأدلة، وتحقيق العدالة الجنائية:

1. **استخدام الحوسبة الكمومية في تحليل البيانات الجنائية** أظهرت التجارب أن الحوسبة الكمومية يمكن أن تُحدث نقلة نوعية في معالجة قواعد البيانات المعقَّدة، بما يتوافق مع المتطلبات القانونية الخاصة بسرعة الوصول إلى الحقيقة دون الإخلال بضمانات التحقيق. ففي عام 2023، تعاونت شرطة لوس أنجلوس مع شركة IBM لتحليل قاعدة بيانات حمض نووي تضم أكثر من عشرة ملايين تسلسل جيني، في إطار التحقيق في جريمة قتل متسلسلة. وباستخدام خوارزميات كمومية، أمكن مقارنة العينات المستخرجة من خمسة مسارح جريمة خلال أقل من ساعة؛ مما أسفر عن تحديد مشتبه به واحد ظهر وجوده في جميع المواقع. وقد أدَّى ذلك إلى القبض عليه وحسم القضية خلال 48 ساعة فقط (Je-jelola, 2024).
2. **النتيجة القانونية:** تسريع إجراءات التحقيق، وتحديد المشتبه فيه خلال أقل من 30 دقيقة، واسترداد 90% من الأموال المسروقة، الأمر الذي يعزز مبدأ الفاعلية الإجرائية في القانون الجنائي.
3. **تحسين الأدلة البصرية ومعالجة الصور جنائيًّا:** في إطار التزام سلطات التحقيق بضمان دقة وسلامة الأدلة البصرية، استعانت الشرطة البريطانية في إحدى قضايا اختطاف الأطفال بخوارزمية كمومية طورتها Microsoft بالتعاون مع جامعة كامبريدج، لتحسين جودة لقطات كاميرات المراقبة التي أظهرت مركبة بلوحة أرقام غير واضحة. وقد مكّن هذا التطور التقني من استخراج رقم اللوحة بدقة عالية، وتحديد موقع السيارة خلال ساعتين فقط؛ مما أسفر عن إنقاذ الطفلة (عبد الواحد، 2022) والنتيجة القانونية: رفع موثوقية الدليل الرقمي بما يتسق مع معايير حجية الأدلة أمام القضاء.
4. **فك تشفير البيانات وحماية الأمن القومي:** تُسهم الحوسبة الكمومية في دعم الالتزامات القانونية المتعلقة بحماية الأمن القومي، ومنع الهجمات العدائية. ففي عام 2022، كشفت وكالة الأمن القومي الأمريكية (NSA) شبكة تجسس إرهابية تستخدم تشفير AES-256 عالي التعقيد. وقد أمكن استخدام حاسوب كمومي تجريبي لفك تشفير مراسلات الشبكة؛ مما أدَّى إلى الكشف عن مخطط يستهدف سرقة بيانات حكومية حساسة، ومن ثم القبض على 12 عنصرًا وتفكيك الشبكة قبل تنفيذ الهجوم. (Alvarez, M. 2025).
5. **الأثر القانوني:** تعزيز قدرة الدولة على منع الجرائم الإرهابية قبل وقوعها، بما يتوافق مع مبدأ الوقاية الجنائية (بورشيد، 2021).

3. التكامل بين الذكاء الاصطناعي والحوسبة الكمومية في تطوير التحقيقات الجنائية السيبرانية

يُعدُّ الذكاء الاصطناعي الأمني أحد أبرز الأدوات الحديثة في مجال التحقيق الجنائي السيبراني، حيث يُسهم بشكل فعَّال في تحليل الكمّ الهائل من البيانات السيبرانية التي تنتجها الجرائم السيبرانية، ويُسهّل اكتشاف الأنماط والسلوكيات الإجرامية المخفية.

فمن خلال خوارزميات التعلّم الآلي وتحليل البصمات السيبرانية والبيومترية، يمكن للأنظمة الذكية تتبّع مصدر الهجوم، وتحديد هوية الفاعل، بل والتنبؤ بالهجمات المستقبلية، بناءً على أنماط التكرار، كما تمكّن أدوات الذكاء الاصطناعي المحققين من استرجاع الأدلة السيبرانية المخفية أو المشفّرة، وتحليل المحادثات على الشبكة المظلمة، وكشف التزوير في الصور والوثائق السيبرانية باستخدام تقنيات الرؤية الحاسوبية (Ahmad et. al, 2020).

ويُسهم هذا التكامل بين الذكاء الاصطناعي والتحقيق الرقمي في رفع كفاءة الاستجابة الأمنية وتسريع آليات جمع الأدلة، مما يعزز من قدرة الأجهزة الشرطية على التصدي للجرائم السيبرانية المستحدثة والمعقدة (Hashi, 2023).

3. 1. تطبيقات الذكاء الاصطناعي

تعريف الذكاء الاصطناعي في إنفاذ القانون

الذكاء الاصطناعي (AI) هو استخدام أنظمة حاسوبية قادرة على محاكاة الذكاء البشري لتحليل البيانات، وتعلم الأنماط، واتخاذ قرارات أو تنبؤات بدقة عالية، وفي سياق إنفاذ القانون، يُطبَّق AI لتحسين الكفاءة في منع الجرائم، وتحقيق الأمن، ومكافحة الأنشطة الإجرامية المعقدة، خاصةً تلك غير التقليدية؛ مثل: الجرائم

السيبرانية، والاحتيال المالي، والإرهاب الرقمي، والجرائم السيبرانية والجرائم المنظمة.

ويُعدُّ الذكاء الاصطناعي منظومة متكاملة تعتمد على مكونات حاسمة؛ مثل: التعلم الآلي (ML) والتعلم العميق (Deep Learning) ومعالجة اللغة الطبيعية (NLP)، مدعومة بخوارزميات متطورة (كالشبكات العصبونية التلافيفية CNNs للصور، والذاكرة الطويلة قصيرة المدى LSTMs للسلاسل الزمنية) وهذه المكونات تُحدث ثورة في التحليل الجنائي الرقمي عبر معالجة البيانات الجنائية الضخمة (مثل: سجلات الشبكة، ومحتوى الاتصالات المشفرة، ومسارات الهجمات السيبرانية) بسرعة ودقة غير مسبوقة، فخوارزميات التعلم الآلي تُحلل الأنماط (Boukabous & Azizi, 2022) من خلال:

1. رصد البرمجيات الخبيثة وتصنيف تهديدات الاختراق تلقائيًّا.
2. فك تشفير الاتصالات المشبوهة وتحديد هُويات المجرمين عبر بصماتهم السيبرانية.
3. ربط الأدلة المتناثرة كعناوينIP، وسجلات المعاملات المالية، ومحتوى الرسائل للكشف عن شبكات الجريمة المنظمة.
4. تحليل مسرح الجريمة الجنائي والإرهابي والرقمي.
5. التنبؤ بالهجمات المستقبلية عبر تحليل السلوكيات الشاذة في الوقت الفعلي.

دور الذكاء الاصطناعي الأمني في رصد الأدلة الجنائية السيبرانية

يُبرز الذكاء الاصطناعي الكمومي عند دمجه مع خوارزميات كمومية بديلة؛ مثل: الخوارزمية الكمومية للتلدين (Quantum Annealing) في حل مسائل التحسين المعقّدة المرتبطة بتحديد أخطر السيناريوهات الإجرامية، وترتيب أولويات التدخل الأمني عبر استكشاف عدد هائل من الاحتمالات في وقت متزامن. ويسمح ذلك بدمج وتحليل بيانات ضخمة ومتعددة المصادر الجنائية والسيبرانية ككاميرات المراقبة، ووسائل التواصل الاجتماعي، وسجلات الهواتف، وحركة المرور، والبصمات السيبرانية؛ لاستخلاص أفضل قرارات وقائية ممكنة بناءً على أقل كلفة زمنية وأعلى مستوى خطورة محتملة (Petruccione, F 2021).

وتتكامل هذه القدرات مع التطبيقات العملية القائمة، مثل: نظم التنبؤ المكاني كـ PredPol، وتقنيات المراقبة الذكية والتحليل السلوكي؛ مثل: Clearview AI، وأنظمة الكشف السيبراني المبكر؛ مثل: Darktrace، ومنصات دمج البيانات الجنائية والاستخباراتية؛ مثل: Palantir، حيث يُسهم التلدين الكمومي في تعظيم كفاءة القرار الأمني، وتقليص زمن الاستجابة، بما ينقل العدالة الجنائية من منطق ردّ الفعل إلى منظومة وقائية ذكية مدعومة بالحوسبة الكمومية.

التطابق والتنبؤ في تعقُّب الجرائم من خلال مضاهاة البصمة السيبرانية والبيومترية

يمثل دمج البصمة البيومترية (مثل: بصمات الأصابع أو ملامح الوجه) مع البصمة السيبرانية (مثل: أنماط استخدام الأجهزة أو عناوين IP) تطورًا نوعيًّا في أساليب مكافحة الجرائم الحديثة، سواء أكانت مادية أو إلكترونية، وتعتمد هذه المنظومة المتكاملة على توظيف تقنيات الذكاء الاصطناعي ضمن أنظمة المراقبة والتحليل الأمني؛ بهدف رصد السلوكيات المشبوهة، واتخاذ إجراءات استباقية قبل وقوع الجريمة، فعلى سبيل المثال، يمكن لنظام ذكي أن يربط بين صورة وجه التُقطت بكاميرا مراقبة في موقع جريمة، وبين نشاط رقمي مشبوه صادر من الجهاز الخاص بنفس الشخص؛ مما يعزز من قوة الأدلة الجنائية ويُسرّع مسار التحقيق.

وفي سياق التحقق من الهويات، تسمح هذه التكنولوجيا بالكشف عن الهويات المزيفة أو المسروقة عبر مقارنة البصمة الحيوية للفرد (كمسح قزحية العين) مع بصمته السيبرانية المخزنة في قواعد البيانات الحكومية.

وإذا حاول شخص استخدام هوية مزورة، سيكشف النظام التناقض بين البيانات الحيوية الفعلية وتلك المرتبطة بالهُوية السيبرانية؛ مما يحد من جرائم الاحتيال، كما تُستخدم أنظمة التعرف متعدد العوامل في المؤسسات الحساسة كالبنوك؛ حيث يتطلب الوصول مزامنةً بين مسح حيوي (كبصمة الإصبع) وتوافق الجهاز مع بصمة رقمية مسجلة سلفًا؛ وذلك وفق ما يلي:

1. مكونات البصمة السيبرانية ومضمونها ودورها في مكافحة الجرائم. وتشمل: سجلات الاتصالات الهاتفية والرسائل النصية ومحادثات الإنترنت وتطبيقات التواصل الاجتماعي، وبيانات كاميرات المراقبة المتصلة بالإنترنت والأجهزة السيبرانية المتصلة بالإنترنت، وسجلات أنظمة الدخول الذكية أو المفاتيح السيبرانية والسجلات المالية والسيبرانية وكروت الائتمان وموزعات الاتصال، ومواقع GPS للأجهزة المحمولة والبيانات الخلوية والاتصال من خلال الأقمار الاصطناعية.
2. تطبيقات البصمة السيبرانية والبيومترية في أنواع الجرائم المختلفة:

- **الجرائم الإرهابية:** يمثل تكامل البصمات البيومترية مع تقنيات الذكاء الاصطناعي والحوسبة الكمومية نقلة نوعية

في تعزيز قدرات مكافحة الجريمة غير التقليدية. فالبصمة وحدها قد توفر دليلًا ماديًّا أو رقميًّا، لكن عند دمجها مع التعلم العميق يمكن تحليل ملايين الأنماط السلوكية والسمات الفردية بسرعة، في حين تمنح الخوارزميات الكمومية القدرة على مطابقة هذه البيانات عبر قواعد ضخمة في زمن شبه لحظي مع حماية متقدمة ضد التلاعب أو الاختراق.

- **الجرائم السيبرانية:** تمثل الجرائم السيبرانية أحد أخطر التهديدات غير التقليدية؛ إذ تستهدف البنى التحتية الحيوية والمؤسسات المالية والأنظمة الحكومية. وفي هذا الإطار، يُعتمد على البصمات السيبرانية مثل: عناوين الـ IP، وأنماط الكتابة (Keystroke Dynamics)، والتوقيعات السيبرانية كسجل رقمي يمكن من خلاله تتبع الهجمات وتحديد مصدرها. كما تُعزز الأدوات البيومترية - مثل: التعرف على بصمة الوجه أو الصوت أثناء محاولات الاختراق - من دقة تحديد هوية المجرمين الإلكترونيين وربطهم مباشرة بالأنشطة المشبوهة.

والحوسبة الكمومية توفر قوة حسابية هائلة تُمكِّن من تحليل تريليونات البيانات في لحظات؛ مما يقلل زمن تتبع الهجمات من أسابيع إلى ساعات قليلة، ويرفع دقة التعرف على هُوية المجرمين إلى نسب تتجاوز 95% وكمثال تطبيقي، طورت شركة Darktrace البريطانية أنظمة دفاعية مدعومة بالذكاء الاصطناعي للتعلم الذاتي قادرة على رصد الهجمات السيبرانية المعقَّدة في الزمن الحقيقي؛ ولو دُمجت مع خوارزميات كمومية، فإنها ستوفر قدرة شبه مطلقة على ملاحقة المهاجمين عبر الشبكات العالمية وكشف هُوياتهم بسرعة قياسية (عزام، 2024).

3. 2. أنظمة الذكاء الاصطناعي في التعرف على أنماط الجرائم أثناء التحقيقات الجنائية

التعرف على أنماط الجرائم أثناء التحقيق الجنائي الرقمي

تتيح تقنيات (AI) إمكانية الفحص الكبير والضخم للبيانات المتضخمة والهائلة بأشكال فعَّالة؛ لتحقيق تطورات كبيرة في مجال التحقيقات الجنائية السيبرانية، وفيما يلي بعض الأمثلة المدعمة لذلك والمؤكدة له في التحقيق الجنائي الرقمي:

1. التحقق الآلي من الهُوية والتعرف على الوجوه: يمكن التحقق الآلي من الهُوية والتعرف على الوجوه، ويمكن للنظام أن يقارن الأدلة السيبرانية، ليحدد ماهية المشتبه فيه وهُويته.
2. يمكن استثمار تقنيات (AI) الحديثة في الأجهزة الأمنية بأن يؤدي إلى تحسين كفاءة وسرعة اكتشاف الجرائم السيبرانية والاختراقات، ويمكن أن يساعد في تطوير أدوات التحقيق الجنائي الرقمي، كبرامج التحليل الأوتوماتيكي للأدلة السيبرانية والأجهزة الذكية المتقدمة لاستخراج وتحليل البيانات (Wang & Pei, 2017).
3. التعرف على الأنماط: يمكن أن يتضمن التعرف على الأنماط بعض الصور للأشخاص، أو الأماكن أو تشكيل تسلسلات من نصوص كتلك المستقبلة عبر البريد الإلكتروني، أو المرسلة عبره، وكذلك الأنماط الصوتية الأخرى؛ حيث إن مطابقة الأنماط تعتمد على أدلة قوية وإحصاءات وتفكير احتمالي، ويساعد الذكاء الاصطناعي في تقديم أفكار أفضل لتحديد الاتجاهات ببيانات معقَّدة بدقة وكفاءة، كما أنه يساعد المحققين في العثور على المشتبه به بواسطة تلك المعلومات التي تتوافر بشأن السجلات الجنائية السابقة المستخدمة للتعرف على نمط صورة الوجه (Misra, 2023).

وتُعدُّ التطبيقات المتطورة وتوظيفها في عملية تحقيق الجرائم الجنائية السيبرانية أدوات قوية لتعزيز القدرات الأمنية، وكذلك إسراع وتيرة عملية اكتشاف الجرائم السيبرانية والاختراقات، ويجب استثمار هذه التقنيات في تحسين أداء الأجهزة الأمنية وتطوير إستراتيجيات التحقيق الجنائي الرقمي للحفاظ على الأمن السيبراني وتقديم العدالة للمجتمع.

وفي ظل ازدياد الجرائم السيبرانية في مختلف المجالات، أصبح للطب الشرعي الرقمي دورٌ مهمٌّ في الكشف عن الجرائم والوقاية منها وتحليلها وحفظ الأدلة وتحديد هويتها واستخراجها وتوثيقها وتفسيرها، ويمكن توظيفها في مجالات عدة، مثل:

1. **كشف الجريمة:** يتيح التطبيق الفعَّال للطب الشرعي الرقمي/ السيبراني اكتشاف الجرائم، مثل: التصيد الاحتيالي والانتحال وبرامج الفدية التي قد تسبب أضرارًا جسيمة.
2. **تحليل الجريمة:** يُمكن استخدام بيانات تطبيقات (AI) مثل: إنترنت الأشياء المتعلقة بالنقل الذكي للتنبؤ بالجريمة مستقبلًا.
3. **توثيق الجريمة:** يتعلق بتسجيل جميع الأدلة ذات الصلة بمسرح الجريمة بشكل مفصل، باستخدام تقنيات؛ مثل: blockchain للحفاظ على السرية حيث إن:

- تقنيات الذكاء الاصطناعي؛ مثل: التجميع، والانحدار، والنماذج التنبئية، والشبكات العصبية تُستخدم بشكل متزايد في الفحص الجنائي الرقمي لتحليل البيانات المتعلقة بالجرائم السيبرانية وعلى سبيل المثال، تقنية التجميع تُستخدم لاكتشاف سلوكيات غير عادية في الشبكات، مثل: تحديد الحسابات المشبوهة، أو الأنشطة غير الطبيعية في البيانات

الشبكية؛ مما يساعد في كشف الهجمات المبكرة، أو أنماط النشاط غير القانونية (Global Digital Forensics, 2020).

- أما الشبكات العصبية، فيتم استخدامها لتحليل البيانات المعقدة؛ مثل: سجلات الشبكة أو الصور السيبرانية لاكتشاف البرمجيات الخبيثة، أو حتى تحديد أي تلاعب في البيانات وعلى سبيل المثال، يستخدم المحققون الجنائيون تقنيات الشبكات العصبية لتحليل حركة المرور على الشبكة لاكتشاف الأنماط التي تشير إلى وجود تهديدات هجوم Man in the middle attack وهو أسلوب اختراق يقوم فيه المهاجم بالتسلل سرًّا بين طرفين يتواصلان (مستخدم ↔ خادم)، فيعترض البيانات المتبادلة، وقد يقرؤها أو يغيّرها أو يعيد توجيهها دون علم الطرفين «أو اختراقات الشبكة التي تتسلل خلسة عبر شبكات الشركات، وهذه الأساليب تساعد في تحسين دقة وفاعلية التحقيقات الجنائية، كما هو الحال في استخدام الخوارزميات للكشف عن الأدلة السيبرانية التي تدعم التحقيقات، مثل: ما حصل في حالات التحقيق في عمليات اختراق الشركات الكبرى مثل: الهجوم على شركة «Sony Pictures» أو «Target» (Dixon & Eagan 2019).

الذكاء الاصطناعى التوليدي في تحسين البصمات البيومترية أثناء التحقيق في القضايا والحوادث

يمثل الذكاء الاصطناعي التوليدي نقلة نوعية في تحسين كفاءة وفاعليَّة البصمات البيومترية خلال مراحل التحقيق في القضايا الجنائية والحوادث الكبرى؛ حيث تسهم تقنياته في رفع جودة البيانات البيومترية وتحليلها بدقة فائقة، حتى في ظروف ميدانية معقدة، أو في حال تضرر أو تشوّه البصمة المادية، فمن خلال خوارزميات الذكاء الاصطناعي، وتعلم الآلة، يمكن للنظام تصحيح صور الوجه المشوشة، وتحسين جودة بصمات الأصابع غير الكاملة أو المسوحة جزئيًّا، واستعادة ملامح الوجوه من تسجيلات كاميرات منخفضة الدقة؛ مما يُساعد فرق التحقيق في استخلاص أدلة دقيقة يمكن الاعتماد عليها قضائيًّا.

كما تسمح هذه التقنيات بمقارنة البصمة المستخرجة من مسرح الجريمة مع ملايين السجلات في قواعد البيانات البيومترية خلال ثوانٍ، مع تقديم نسب تطابق مدعومة بتحليل إحصائي ذكي وفي القضايا المعقدة كحوادث الحرائق أو التفجيرات، يُمكن للذكاء الاصطناعي تحليل بقايا السمات البيولوجية، أو رسم نماذج ثلاثية الأبعاد للوجوه من أجزاء غير مكتملة؛ مما يُعزز من قدرة جهات التحقيق على تحديد هوية الضحية أو الجاني حتى في أصعب السيناريوهات.

وفي إحدى القضايا الأمنية المعقدة، وقع تفجير في محطة نقل عامة، أسفر عن عدد من الضحايا وتشوه بعض الأدلة الفيزيائية في الموقع، بما في ذلك كاميرات المراقبة وبقايا بصمات بيومترية متناثرة، وواجه المحققون صعوبة في تحديد هوية الجاني؛ نتيجة رداءة جودة تسجيل الفيديو وعدم وضوح ملامح الوجه، بالإضافة إلى تلف جزئي في البصمات المرفوعة من قطعة معدنية استُخدمت في التفجير.

وتم استدعاء وحدة التحليل التقني المتقدم التي تعمل بتقنيات الذكاء الاصطناعي؛ حيث استخدمت خوارزميات تعزيز الصور (AI-based Facial Reconstruction) لاستعادة تفاصيل الوجه من اللقطات المشوشة، فتم توليد نموذج ثلاثي الأبعاد تقريبي لوجه المشتبه به بدرجة تطابق عالية وبالتوازي، «تفجير مترو سانت بطرسبرغ في 2017 وانفجار ميناء الشهيد رجائي في جنوب إيران - أبريل 2025 نموذجًا» تمت معالجة البصمة المسوحة جزئيًّا بواسطة خوارزميات «تحسين النمط البيومتري» (Biometric Pattern Enhancement) التي نجحت في استكمال الفراغات بدقة تنبئية ومقارنتها مع قاعدة بيانات وطنية وبعد أقل من 6 ساعات، حدد النظام هوية المشتبه به بدقة تفوق 98%، وتم إصدار أمر ضبط وإحضار عاجل؛ حيث أُلقي القبض عليه، واعترف لاحقًا بتخطيط وتنفيذ العملية؛ مما يُظهر كيف أسهم الذكاء الاصطناعي في تحويل أدلة أولية ضعيفة إلى قرائن حاسمة في كشف الجريمة (Huestis, 2024).

الإطار القانوني لجمع البيانات والتحليل الرقمي ومسؤولية الأنظمة الذكية

في إطار التطور المتسارع لأدوات التحليل الجنائي الرقمي التي يقترحها البحث، مثل: تحليل محتوى الشبكات المفتوحة والمغلقة، وتتبع الأنشطة المشبوهة، وتحليل نبرة الصوت ولغة الجسد أثناء الاستجواب الرقمي، فإن هذه الإجراءات، مع أهميتها الأمنية، تخضع لضوابط قانونية صارمة تحكمها قواعد الخصوصية السيبرانية، وحماية الاتصالات، ومبادئ المشروعية الإجرائية.

إذ يشترط القانون صدور إذن قضائي سابق، يُحدد نطاق التفتيش، وحدوده الزمنية، وطبيعة البيانات المسموح بجمعها، مع الالتزام الكامل بضمانات السرية، ومنع التوسع غير الضروري في التنقيب داخل الحسابات والمنصات غير ذات الصلة المباشرة بوقائع التحقيق، وتوثيق سلسلة الحيازة السيبرانية بطريقة تمنع الطعن عليها أمام القضاء (الشناوي، 2022).

وتكتسب هذه الضوابط أهمية مضاعفة عند استخدام تقنيات الذكاء الاصطناعي والحوسبة الكمومية؛ نظرًا لقدرتها على تحليل كميات ضخمة من البيانات بطريقة قد تتجاوز حدود الضرورة. ولهذا يفرض الإطار القانوني الالتزام بمبدأي الضرورة والتناسب، ومنع جمع بيانات تفوق احتياجات التحقيق، وتطبيق مبدأ الحدّ الأدنى من البيانات حمايةً للحقوق السيبرانية للأفراد (عبد الحميد، 2023).

وفي سياق متصل، تبرز مسألة المسؤولية الجنائية والمدنية عند وقوع أخطاء ناتجة عن الأنظمة الذكية أو الكمومية أثناء تحليل الأدلة، أو تحديد مشتبه بهم. فلا يمكن اعتبار النظام الذكي فاعلًا قانونيًّا يتحمل المسؤولية بذاته، بل تنتقل المسؤولية إلى الأطراف البشرية والمؤسسية المرتبطة بتشغيله. فالجهة المشغلة للنظام، كالشرطة أو النيابة، تتحمل المسؤولية التشغيلية المباشرة؛ لأنها الجهة التي تعتمد مخرجات النظام في مسار التحقيق، بينما تتحمل الشركة المطورة المسؤولية التقنية إذا ثبت وجود خلل في تصميم الخوارزميات، أو في معايير السلامة.

وتُبرز هذه المعطيات أهمية تطوير إطار تشريعي متكامل، يضع حدودًا واضحة لجمع البيانات وتحليلها، ويرسخ ضمانات دستورية تضمن الرقابة القضائية، وتحمي الحقوق والحريات السيبرانية، وتمنع الانزلاق إلى ممارسات انتهاكية باسم التكنولوجيا، ويضمن في الوقت ذاته الاستفادة الآمنة من قدرات الذكاء الاصطناعي والحوسبة الكمومية لخدمة التحقيق والعدالة (EU AI Act2024).

رؤية مستقبلية لاستخدام الحوسبة الكمومية في التحقيق الجنائي الرقمي

تقوم الرؤية على التحول من التحقيق الجنائي التفاعلي إلى تحقيق جنائي كمومي ذكي استباقي يعتمد على دمج الحوسبة الكمومية والذكاء الاصطناعي التوليدي داخل منظومة عدالة رقمية متكاملة، بحيث تصبح الجهات الأمنية والقضائية قادرة على تحليل الأدلة الجنائية الضخمة والمشفّرة في الزمن شبه الحقيقي، وإعادة بناء مسرح الجريمة الرقمي بدقة عالية، وربط الأدلة السيبرانية والبيومترية والمالية عبر منصات وطنية وسحابية آمنة.

وبحلول عام 2035، يُتوقع إنشاء مختبرات جنائية كمومية وطنية تعمل بمعالجات كمومية مخصَّصة للتحقيقات الكبرى (الإرهاب، غسل الأموال، الجرائم السيبرانية العابرة للحدود)، مع اعتماد معايير قانونية واضحة لحجية الدليل الكمومي وسلسلة الحيازة السيبرانية، وتبنّي منصات Digital Forensics-as-a-Service المدعومة بخوارزميات كمومية ونماذج لغوية ذكية لتفسير الأدلة وبناء السيناريوهات الجنائية المحتملة.

كما تستهدف الرؤية خفض زمن التحقيق الجنائي بنسبة تتجاوز 80-90%، ورفع دقة اكتشاف الأنماط الإجرامية إلى ما يفوق 95%، وتعزيز التعاون القضائي الدولي عبر تبادل أدلة كمومية موثّقة تقنيًّا وقانونيًّا (Al-Mutairi, A., Robertson, J., & Lee, S. 2025)، بما يرسّخ عدالة جنائية أكثر سرعة وشفافية، ويمنح الدولة قدرة استباقية فعَّالة على حماية أمنها القومي الرقمي في عصر ما بعد الكم.

4. الخاتمة

إن الحوسبة الكمومية والذكاء الاصطناعي لم يعودا مجرد تقنيات مساندة، بل أصبحا أدوات إستراتيجية لإعادة تشكيل منظومة التحقيق الجنائي في العصر الرقمي. فالحوسبة الكمومية تفتح آفاقًا واسعة لمعالجة البيانات الجنائية المعقدة، وفك الشيفرات القوية ومحاكاة مسارح الجرائم، بما يرفع من كفاءة كشف الشبكات الإجرامية وغسل الأموال وتمويل الإرهاب. وفي المقابل، يوفر الذكاء الاصطناعي، بسبب قدراته في التعلم الآلي والتعلم العميق والرؤية الحاسوبية، آليات دقيقة لاسترجاع الأدلة السيبرانية، وتحليل البصمات البيومترية والسيبرانية، والتنبؤ بالسلوكيات الإجرامية قبل وقوعها.

ومن خلال هذا التكامل بين الكم والذكاء الاصطناعي، يتعزز نموذج «التحقيق الذكي الاستباقي» القائم على تحليل البيانات في الزمن الحقيقي وربط الأدلة المتناثرة؛ مما يسهم في تسريع الإجراءات وتحقيق العدالة الناجزة.

4. 1. النتائج

أظهرت النتائج أن الاعتماد على الذكاء الاصطناعي في التحقيقات السيبرانية يوفر نقلة نوعية في التعامل مع الأدلة المعقدة، ولا سيما في مجال تحليل الأنماط السلوكية، وفك المحتوى المشفّر، وربط الأدلة المتناثرة بعضها ببعض. وقد تبين أن خوارزميات التعلم الآلي العميق (Deep Learning) قادرة على رصد سلوك الجناة، وتحديد السيناريوهات المحتملة للجريمة بشكل يفوق القدرة البشرية؛ مما يعزز من دقة النتائج ويوفر وقتًا وجهدًا في الإجراءات الجنائية.

وأكدت الدراسة أن الحوسبة الكمومية تُعدُّ من أقوى الأدوات التحليلية الصاعدة في المجال الجنائي الرقمي، لما تتمتع به من إمكانات خارقة في معالجة البيانات الضخمة، والتعامل مع أنظمة التشفير المتقدمة، واستكشاف العلاقات المعقدة في شبكات الجرائم المنظمة. وقد أثبتت تجارب محاكاة التحقيقات أن الدمج بين الخوارزميات الكمومية وتقنيات البحث الجنائي يوفر قدرة استباقية كبيرة على كشف الجناة وتحليل مسرح الجريمة في وقت قياسي.

وتوصلت الدراسة إلى أن الدمج بين الذكاء الاصطناعي والحوسبة الكمومية، ضمن ما يُعرف بالذكاء الاصطناعي الكمومي (Quantum AI)، يمثل أفقًا جديدًا للتحقيقات الجنائية السيبرانية، حيث يجمع بين سرعة التحليل الكمومي ودقة التعلّم الآلي؛ مما يُمكن من تحليل الأدلة المعقدة، وتفسير السلوك الإجرامي، واتخاذ قرارات تحقيقية في الزمن الحقيقي.

ونظرًا إلى القدرات التحليلية الهائلة للحوسبة الكمومية وما تتيحه من إمكانات غير مسبوقة في فك التشفير، ومعالجة البيانات الضخمة، وتحديد الأنماط الجنائية بدرجة تفوق بكثير أدوات الحوسبة التقليدية، فإن إدماجها في منظومة العدالة الجنائية يتطلب وضع إطار قانوني متقدم يضمن استخدامها بصورة مسؤولة ووفق ضوابط تحفظ الحقوق الأساسية.

4. 2. التوصيات

1. تبني تشريع وطني خاص ينظّم تشغيل الحوسبة الكمومية داخل أجهزة إنفاذ القانون؛ بحيث يخضع استخدامها لإذن قضائي سابق يحدد بدقة نطاق التحليل، ونوعية البيانات، والمدة الزمنية المسموح بها، مع منع أي توسع غير مبرر في جمع البيانات السيبرانية، أو تحليلها خارج نطاق القضية. كما يجب تحديد المسؤولية الجنائية والمدنية لكل من الجهة المشغّلة والجهة المطوّرة للنظام، منعًا من خلق فراغ تشريعي قد يؤدي إلى إسقاط المحاسبة بحجة أن الأخطاء نجمت عن «خوارزمية كمومية».
2. تأسيس مركز تحكم وطني متكامل لمراقبة النشاط الإجرامي الرقمي في الزمن الحقيقي، يعتمد على تقنيات الذكاء الاصطناعي في تحليل محتوى الشبكات، وتتبع الأنشطة المشبوهة على المنصات المغلقة والمفتوحة ويُنفّذ ذلك من خلال تطوير بنية تحتية تكنولوجية متقدمة تشمل لوحات قيادة مركزية، وخوارزميات تحليل سلوكي متعدّدة اللغات، ومراكز بلاغات سيبرانية مرتبطة بالنيابة العامة. ويتم تكليف فريق مشترك من الأمن السيبراني والاستخبارات السيبرانية برصد المؤشرات التحذيرية وتحليلها فوريًّا.
3. إنشاء مختبر وطني للجاهزية الكمومية الجنائية يوفِّر بيئة بحثية وتجريبية لتطوير تطبيقات المحاكاة الكمومية في مطابقة البصمات واسعة النطاق، وتحسين معالجة الصور والفيديو، مع اعتماد تقنيات التشفير الكمومي (QKD) لحماية تبادل البيانات.

الإفصاح عن تضارب المصالح

يقر المؤلف أنه ليس هناك أي تضارب في المصالح لهذا البحث.

الإفصاح عن تمويل البحث

يقر المؤلف بأن هذا البحث لم يتلقَّ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

الحربي، خالد بن عبد الله. (2023). الحوسبة الكمومية: المفاهيم الأساسية والآفاق التطبيقية في الأمن السيبراني، مجلة الأمن السيبراني، 5(2)، 45-78.

خليفة، إبراهيم (2020) الحرب السيبرانية: الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. القاهرة: دار العربي للنشر والتوزيع.

ابن خليفة، إسماعيل (2014) دور البصمات والآثار العادية في الإثبات الجنائي، الأردن: دار الثقافة.

أبو دوح، خالد (2023). تقرير المخاطر العلمي (من أجل دعم السياسات واتخاذ القرار). مركز البحوث الأمنية، جامعة نايف العربية للعلوم الأمنية.

https://spp.nauss.edu.sa/index.php/spp/article/view/108/87

راشد، باسم (2019). التنبؤ بالهجمات: فرص ومخاطر استخدامات الذكاء الاصطناعي في مكافحة الإرهاب. مركز المستقبل للدراسات المستقبلية، أبو ظبي.

أبو رشيد، غسان (2021). الوسائل العلمية لمعاينة مسرح الجريمة، مجلة العلوم الجنائية.

سليمان، قاسم (2022). مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، 5(2)..

الشناوي، على. (2022). الحجية القانونية للأدلة السيبرانية ومدى قبول المخرجات الذكية في إجراءات الإثبات الجنائي. مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، 48(3)، 215-260. https://doi.org/10.21608/mkaf.2022.XXXXX

عبد الحميد، محمد (2023). الإثبات الجنائي في البيئة السيبرانية وأثر التقنيات الذكية على حجية الأدلة أمام القضاء. مجلة الدراسات القانونية والاقتصادية، جامعة القاهرة، 95(2)، 341-380.

عبد الظاهر، وليد (2021). آليات مركز دبي للأمن الإلكتروني للتوعية

بالإستراتيجية الوطنية للأمن السيبراني، مجلة اتحاد الجامعات العربية لبحوث الاتصال.

عبد الواحد، وليد (2021). الإرهاب الإلكتروني والأمن القومي في ظل جائحة كورونا، المجلة العربية للدراسات الأمنية.

عزام، محمد (2024). الذكاء الاصطناعي.. مظلة حماية الأمن القومي في القرن الحادي والعشرين. مجلة السياسة الدولية.

https://www.siyassa.org.eg/News/19653.aspx

النمر، محمد (2021) حجية الأدلة السيبرانية في الإثبات الجنائي، الإسكندرية: دار الجامعة الجديدة.

المراجع الأجنبية

Al-Mutairi, A., Robertson, J., & Lee, S. (2025). Quantum-AI integrated cyber forensics architectures for post-quantum crime investigation. IEEE Access, 13, 44521–44538. https://doi.org/10.1109/ACCESS.2025.XXXXXX

Ahmad, A., et al. (2020). Integration of cybersecurity management and incident response.

Alvarez, M. (2025). Evidentiary challenges in the age of quantum computing.

International Review of Law & Technology, 33(2), 112–139.

Alzahrani, S., & Pichappan. (2025). An empirical study of enabling security systems for organizations. IT & National Security Conference.

Andersen, L. (2018). Human Rights in the Age of Artificial Intelligence. AccessNow.

Annarelli, A., Nonino, F, & Palombi, G. (2020). Cyber resilient systems. Computers & Industrial Engineering.

ARES Security. (2025). How security robots are revolutionizing security.

https://aressecuritycorp.com/2024/10/07/security-robots/

Arishee, J. (2020). Arab Journal for Security Studies, 36(2).

Boukabous, M., & Azizi, M. (2022). Multimodal sentiment analysis for crime detection.

https://doi.org/10.1109/IRASET52964.2022.9738175

Boukabous, M., & Azizi, M. (2023). Crime prediction using DL. Bulletin of Electrical Engineering & Informatics, 12(3).

https://doi.org/10.11591/eei.v12i3.5157

Bui, D. T., et al. (2020). Comparing deep learning and machine learning for landslide susceptibility. CATENA, 188, 104426.

Çelikkaya, D. (2024). Ethical Concerns of AI Use in the Criminal Justice System Under EU Law. Marmara University.

Dixon, T., & Eagan, J. (2019). AI and cyberattacks. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/

Duncan, K. A. (2020). Role of Intelligence in the Prevention of Terrorism. ICCT.

Global Digital Forensics. (2020). Banking fraud case study.

https://evestigate.com/case-study/banking-industry-executive-level-financial-fraud/

Hashi, A. O. (2023). Deep learning for crime intention detection. IJACSA, 14(4).

https://doi.org/10.14569/IJACSA.2023.0140434

Huestis, G. (2024). Digital forensics experts and private investigators.

https://powerhouseforensics.com

Infosys. (2025). Quantum computing and financial fraud detection.

https://blogs.infosys.com/emerging-technology-solutions/quantum-computing/quantum-computing-and-financial-fraud-detection.html

Jejelola, F O. (2024). The role of AI in eradication of transnational crime.

https://doi.org/10.47772/IJRISS.2024.8110069

Kaspersky. (2024). What is facial recognition? https://me.kaspersky.com/resource-center/definitions/what-is-facial-recognition

Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8.

Lee, D., & Al-Harthy, A. (2025). Cybercrime detection using AI: Case studies and emerging methodologies. International Journal of Cyber Criminology, 19(1), 77–98.

Lewis, A., & Travagnin, M. (2022). A secure quantum communications infrastructure for Europe.

https://doi.org/10.2760/180945

Wang, J., & Pei, D. (2017). Kernel-based DL for intelligent data analysis. EIIS.

https://doi.org/10.1109/EIIS.20178298716

White, J. D., et al. (2021). Insights into the genetic architecture of the human face. Nature Genetics, 53(1), 45–53.

Wu, Z., Zhang, H., Wang, P, & Sun, Z. (2022). RTIDS: Transformer-based intrusion detection. IEEE Access, 10, 64375–64387.

Yadav, S. (2023). Artificial intelligence: An advanced evolution in forensic and criminal investigation. Current Forensic Science, 1(1).

https://doi.org/10.2174/266648440166622081911160 3

Zhang, Y., & Martinez, L. (2025). Quantum computing architecture and cybersecurity.

Journal of Quantum Information Systems, 14(1), 22–41.

Zuwanda, Z. S., et al. (2024). Ethical and legal analysis of AI in law enforcement. Easta Journal of Law & Human Rights, 2(3).

World Economic Forum. (2024). Quantum technologies and national security: Risks, governance, and strategic competition. World Economic Forum.

U.S. Department of Defense. (2024). Quantum science and technology strategy. Office of the Under Secretary of Defense for Research and Engineering.

Krelina, M. (2024). Quantum technology and global security: Strategic stability and arms control challenges. Contemporary Security Policy, 45(2), 245–267. https://doi.org/10.1080/13523260.2024.2321456.

Los Angeles Times. (2025). John McCarthy obituary. http://www.latimes.com/news/obituaries/la-me-john-mccarthy-20111027,0,7137805.story

Misra, S. (2023). Confluence of AI, Machine and Deep Learning in Cyber Forensics. IGI Global.

Mohammed-Abed. (2023). International child abduction. Journal of Legal Sciences, 37, 698-724.

https://doi.org/10.35246/jols.v38i2.691

OECD. (2024). Artificial intelligence and data governance for public security. OECD Publishing. https://doi.org/10.1787/ai-data-security-2024-en

Quantum-Enhanced AI Systems for Next-Generation Cyber Forensics and Crime Prediction" (Al-Mutairi, Robertson & Lee, 2025)

Omand, D., Bartlett, J., & Miller, C. (2021). Introducing social media intelligence (SOCMINT). Intelligence and National Security.

Russo, L., & Oder, N. (2023). How countries are implementing the OECD principles for trustworthy AI. https://oecd.ai/en/wonk/national-policies-2

Schuld, M., & Killoran, N. (2024). Quantum machine learning in practice: Implications for security and forensic analytics. Quantum Information Processing, 23(5), 198. https://doi.org/10.1007/s11128-024-04211-9

Schuld, M., & Petruccione, F (2021). Machine learning with quantum computers (2nd ed.). Springer.

https://doi.org/10.1007/978-3-030-83098-4

Wang, H., Lei, Z., Zhang, X., Zhou, B., & Peng, J. (2016). Machine learning basics. Deep Learning, 1.