University of Zawia Journal of Legal and Sharia Sciences (UZJLSS)
Volume 14, Issue 2, 2025, pp 167-193, ISSN 3106-1117

Artificial Intelligence between Enhancing Cybersecurity and Creating New Cybercrimes: A Descriptive Analytical Study in Light of Libyan Law

Manal Al-Zmaim

Department of Criminal Law, Faculty of Law, Al-Jafara University, Al-Sahla, Libya.

*Corresponding author email: Manal Al-Zmaim | E-mail address: aju@aju.edu.ly

Submission: 03-11-2025 | Acceptance: 11-12-2025 | Available online: 30-12-2025 | DOI:10.26629/uzjlss.2025.10

ABSTRACT

This research examines the dual role of artificial intelligence in the field of cybercrime. On the one hand, artificial intelligence has contributed to strengthening cybersecurity and improving mechanisms of crime prevention and detection; on the other hand, it has become a tool for committing sophisticated cybercrimes characterized by technical complexity and difficulties of proof. The research aims to analyze the legal issues related to attributing criminal responsibility for cybercrimes based on artificial intelligence technologies and to identify the challenges facing criminal evidence in this type of crime. The research adopts the descriptive-analytical approach through examining the conceptual framework of artificial intelligence and cybersecurity, analyzing emerging forms of cybercrime, and evaluating the Libyan legal framework, particularly Law No. (5) of 2022 on Combating Cybercrimes, while also benefiting from selected comparative legislations. The research concludes that Libyan legislation, despite its significance, remains insufficient to confront intelligent cybercrimes, whether in terms of criminalization, criminal liability, or evidentiary rules. It further emphasizes the need to develop the Libyan criminal justice system by introducing specific legal provisions concerning artificial intelligence, updating rules of criminal evidence, and strengthening the role of specialized technical expertise in line with contemporary digital transformations.

Keywords: Artificial Intelligence, Cybercrimes, Cybersecurity, Criminal Liability, Digital Criminal Evidence, Digital Evidence, Criminal Policy, Libyan Law, Law No. (5) of 2022.

الذكاء الاصطناعي بين تعزيز الأمن السيبراني وخلق جرائم إلكترونية جديدة: دراسة تحليلية وصفية في ضوء القانون الليبي

منال محمد الزميم

قسم القانون الجنائي، كلية القانون، جامعة الجفارة، السهلة، ليبيا

*المؤلف المراسل: منال محمد الزميم | عنوان البريد الالكتروني: aju@aju.edu.ly

التقديم: 03-11-2025م | القبول: 11-12-2025م | النشر الكترونياً: 30-12-2025م

ملخـــص البحـــث

يتناول هذا البحث دراسة الدور المزدوج للذكاء الاصطناعي في مجال الجرائم الإلكترونية، حيث أسهم من جهة في تعزيز الأمن السيبراني وتطوير آليات الوقاية والكشف عن الجريمة، بينما أصبح من جهة أخرى أداة لارتكاب جرائم

إلكترونية ذكية تتسم بالتعقيد التقني وصعوبة الإثبات. ويهدف البحث إلى تحليل الإشكاليات القانونية المرتبطة بإسناد المسؤولية الجنائية في الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي، وبيان التحديات التي تواجه الإثبات الجنائي في هذا النوع من الجرائم.

واعتمد البحث على المنهج الوصفي التحليلي، من خلال دراسة الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، وتحليل صور الجرائم الإلكترونية المستحدثة، مع تقييم التنظيم القانوني الليبي، ولا سيما القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، إلى جانب الاستفادة من بعض التشريعات المقارنة.

وقد خلص البحث إلى أن التشريع الليبي، رغم أهميته، لا يزال غير كافٍ لمواجهة الجرائم الإلكترونية الذكية، سواء من حيث التجريم أو المسؤولية الجنائية أو قواعد الإثبات. كما انتهى إلى ضرورة تطوير المنظومة الجنائية الليبية عبر استحداث نصوص خاصة بالذكاء الاصطناعي، وتحديث قواعد الإثبات الجنائي، وتعزيز دور الخبرة الفنية المتخصصة، بما يواكب التحولات الرقمية الحديثة.

الكلمات المفتاحية: الذكاء الاصطناعي، الجرائم الإلكترونية، الأمن السيبراني، المسؤولية الجنائية، الإثبات الجنائي الرقمي، الدليل الرقمي، السياسة الجنائية، القانون الليبي، القانون رقم (5) لسنة 2022.

مقدمة

أفرز التطور المتسارع لتقنيات الذكاء الاصطناعي تحولات عميقة في البيئة الرقمية، كان لها أثر بالغ في تعزيز منظومات الأمن السيبراني من خلال تطوير آليات الكشف المبكر عن التهديدات الإلكترونية، وتحسين وسائل حماية الأنظمة المعلوماتية والبيانات الرقمية، غير أن هذا التطور التقني، وعلى الرغم من مزاياه، أسهم في الوقت ذاته في ظهور أنماط جديدة من الجرائم الإلكترونية اتسمت بقدر عالٍ من التعقيد والذكاء، مما أدى إلى تراجع فعالية القواعد القانونية التقليدية في مواجهتها، وقد أدى توظيف تقنيات الذكاء الاصطناعي في ارتكاب الجرائم الإلكترونية إلى بروز إشكاليات قانونية متعددة، لاسيما ما يتعلق بتحديد المسؤولية الجنائية، وإسناد الفعل الإجرامي، ومدى كفاية النصوص التشريعية القائمة لاستيعاب هذا النمط المستحدث من الجرائم. وتزداد هذه الإشكاليات وضوحًا في ظل غياب تنظيم قانوني صريح يحكم استخدام الذكاء الاصطناعي في المجال الجنائي، خاصة في التشريعات التي لم تواكب بعد هذا التطور التكنولوجي.

وانطلاقًا من ذلك، يهدف هذا البحث إلى تسليط الضوء على الدور المزدوج للذكاء الاصطناعي، بوصفه أداة لتعزيز الأمن السيبراني من جهة، ووسيلة محتملة لخلق جرائم إلكترونية جديدة من جهة أخرى، مع التركيز على موقف التشريع الجنائي الليبي ومدى قدرته على مواجهة هذه الجرائم المستحدثة. كما يسعى البحث إلى بيان أوجه القصور التشريعي، واقتراح آليات قانونية من شأنها الإسهام في تطوير المنظومة الجنائية الليبية بما يحقق التوازن بين الاستفادة من التقنيات الحديثة وضمان الحماية الجنائية الفعالة في البيئة الرقمية.

إشكالية البحث

يثير التطور المتسارع لتقنيات الذكاء الاصطناعي إشكاليات قانونية معقدة في مجال الجرائم الإلكترونية، حيث باتت هذه التقنيات تؤدي دورًا مزدوجًا يتمثل في تعزيز منظومات الأمن السيبراني من جهة، وخلق أنماط جديدة من الجرائم

الإلكترونية من جهة أخرى. وقد أفرز هذا الواقع تساؤلات جوهرية حول مدى قدرة القواعد الجنائية التقليدية على استيعاب الجرائم الإلكترونية المستحدثة القائمة على الذكاء الاصطناعي، خاصة فيما يتعلق بإسناد المسؤولية الجنائية وتحديد الفاعل الحقيقي للجريمة، وتتجلى الإشكالية بشكل أوضح في ظل غياب تنظيم تشريعي خاص ينظم استخدام الذكاء الاصطناعي في المجال الجنائي، الأمر الذي يطرح تساؤلًا رئيسيًا حول مدى كفاية التشريع الجنائي الليبي في مواجهة هذا النوع من الجرائم وعليه، تتمحور إشكالية البحث حول التساؤل الآتي:

إلى أي مدى يسهم الذكاء الاصطناعي في تعزيز الأمن السيبراني، وفي المقابل خلق جرائم إلكترونية جديدة، وما مدى كفاية التشريع الجنائي الليبي لمواجهة هذه الجرائم المستحدثة؟

أهمية البحث

تتجلى أهمية هذا البحث فيما يحمله الموضوع من أبعاد علمية وعملية بالغة الأثر، حيث يسعى إلى بيان الدور المزدوج للذكاء الاصطناعي وانعكاساته على السياسة الجنائية المعاصرة، من خلال إبراز إسهامه في تعزيز آليات المكافحة من جهة، وما يفرزه من أنماط جديدة للجرائم الإلكترونية من جهة أخرى. كما يهدف البحث إلى الكشف عن أوجه القصور التي تعتري التنظيم القانوني التشريعي والتطبيقي القائم في مواجهة الجرائم الإلكترونية القائمة على تقنيات الذكاء الاصطناعي ويسهم البحث في دعم الجانب العملي للقانون الجنائي الليبي عبر تقديم مقترحات تشريعية وحلول قانونية قابلة للتطبيق، بما يساعد المشرّع والجهات المختصة على تطوير المنظومة الجنائية لمواكبة التحولات الرقمية المتسارعة ويسهم هذا البحث كذلك في إثراء المكتبة القانونية الليبية بدراسة حديثة تتناول موضوعًا تقنيًا متطورًا، فضلًا عن تقديم مقترحات تشريعية من شأنها مساعدة المشرّع الليبي على تطوير المنظومة الجنائية بما يتلاءم مع التحولات الرقمية المتسارع.

أهداف البحث

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، تتمثل في تحديد الإطار المفاهيمي للذكاء الاصطناعي وبيان دوره في تعزيز الأمن السيبراني، والكشف عن صور الجرائم الإلكترونية المستحدثة الناتجة عن توظيف تقنيات الذكاء الاصطناعي. كما يهدف إلى تحليل الإشكاليات القانونية المتعلقة بإسناد المسؤولية الجنائية عن الجرائم الإلكترونية الذكية، وتقييم مدى كفاية النصوص الجنائية الليبية القائمة في مواجهة هذه الجرائم. ويسعى البحث كذلك إلى تقديم مقترحات وآليات قانونية وتشريعية من شأنها تعزيز الحماية الجنائية في البيئة الرقمية الليبية ومواكبة التطور التقني المتسارع.

منهجية البحث

اعتمد هذا البحث على المنهج الوصفي، من خلال عرض المفاهيم القانونية المرتبطة بالذكاء الاصطناعي والجرائم الإلكترونية، وبيان دورها وانعكاساتها على السياسة الجنائية المعاصرة، كما تم الاستعانة بالمنهج التحليلي في دراسة النصوص الجنائية ذات الصلة، وتحليل الإشكاليات القانونية المتعلقة بإسناد المسؤولية الجنائية في الجرائم الإلكترونية.

وللإجابة عن الإشكالية المطروحة، وتحقيق أهداف هذه الدراسة، سيتم تناول موضوع البحث من خلال ثلاثة مباحث رئيسة؛ يخصص المبحث الأول لبيان الإطار المفاهيمي والقانوني لكل من الذكاء الاصطناعي والأمن السيبراني، بينما يتناول

المبحث الثاني الجرائم الإلكترونية المستحدثة الناتجة عن استخدام تقنيات الذكاء الاصطناعي، أما المبحث الثالث فيُعنى بدراسة المواجهة الجنائية للجرائم الإلكترونية المرتبطة بالذكاء الاصطناعي في ضوء أحكام القانون الليبي. وفي ختام هذه الدراسة سيتم عرض أهم النتائج التي توصلت إليها الدراسة، إلى جانب تقديم مجموعة من التوصيات التي قد تسهم في تعزيز الإطار القانوني لمواجهة هذه الجرائم.

المبحث الأول: الإطار المفاهيمي والقانوني للذكاء الاصطناعي والأمن السيبراني

يعد الذكاء الاصطناعي والأمن السيبراني من أبرز مظاهر التحول الرقمي المعاصر، لما لهما من تأثير مباشر في البنية القانونية والجنائية للدول، وقد فرض هذا التطور التقني المتسارع تحديات جديدة على السياسة الجنائية، سواء من حيث أساليب ارتكاب الجريمة أو وسائل مكافحتها، ويهدف هذا المبحث إلى وضع الإطار المفاهيمي والتحليلي للذكاء الاصطناعي والأمن السيبراني، وبيان دورهما في المجال الجنائي، تمهيدًا لدراسة الجرائم الإلكترونية المستحدثة وآليات مواجهتها.

المطلب الأول: ماهية الذكاء الاصطناعي والأمن السيبراني وتطورهما

يتناول هذا المطلب تحديد مفهوم الذكاء الاصطناعي من الناحية التقنية والقانونية، وبيان خصائصه الأساسية ومراحل تطوره التاريخي، مع الوقوف على مفهوم الأمن السيبراني وأهميته في حماية الأنظمة المعلوماتية والبيانات الرقمية، باعتباره الإطار الحاضن لتطبيقات الذكاء الاصطناعي في البيئة الرقمية.

الفرع الأول: مفهوم الذكاء الاصطناعي وخصائصه

يعد الذكاء الاصطناعي من أبرز التطورات التكنولوجية التي شهدها العصر الحديث، إذ أصبح يلعب دورًا متزايد الأهمية في مختلف المجالات العلمية والاقتصادية والأمنية، وقد أدى التطور السريع في تقنيات الحوسبة والبيانات إلى توسيع نطاق استخدام تطبيقات الذكاء الاصطناعي، الأمر الذي استدعى اهتمام الفقه القانوني بدراسة مفهومه وبيان خصائصه، لما لذلك من أثر في تحديد طبيعته القانونية والآثار المترتبة على استخدامه، ولذا سيتم تناول مفهوم الذكاء الاصطناعي وخصائصه من خلال التقسيم الآتي:

أولا: مفهوم الذكاء الاصطناعي

يقصد بالذكاء الاصطناعي الحاسوبية التي تُصمَّم لمحاكاة القدرات (Artificial Intelligence) مجموعة التقنيات والأنظمة الذهنية للإنسان، مثل التعلم، والاستنتاج، وحل كل المشكلات، واتخاذ القرارات، وذلك اعتمادًا على الخوارزميات المتقدمة وتحليل البيانات الضخمة وقد عرّفه بعض الفقه بأنه «قدرة الآلة على محاكاة السلوك البشري الذكي من خلال أنظمة قادرة على التعلم والتكيّف مع المعطيات المختلفة»، (حجازي، 2020).

ويُنظر إلى الذكاء الاصطناعي من المنظور القانوني بوصفه أداة تقنية ذات طبيعة خاصة، قادرة على إحداث آثار قانونية مباشرة أو غير مباشرة، سواء من خلال دعم اتخاذ القرار أومن خلال تنفيذ مهام قد يترتب عليها مساس بالحقوق أو المصالح المحمية قانونًا، ويزداد الاهتمام القانوني بهذا المفهوم مع توسع مجالات توظيف الذكاء الاصطناعي في المجالين الأمني والجنائي، وما يثيره ذلك من تساؤلات حول حدود استخدامه ومشروعيته.

ثانيًا: خصائص الذكاء الاصطناعي

تميّز الذكاء الاصطناعي بجملة من الخصائص التي تميّزه عن البرمجيات التقليدية، ومن أبرزها قدرته على التعلّم الذاتي من خلال تحليل البيانات السابقة، والتكيّف مع المتغيرات، واتخاذ قرارات شبه مستقلة دون تدخل بشري مباشر، كما يتمتع بقدرة عالية على معالجة كميات ضخمة من البيانات في وقت قياسي، الأمر الذي يجعله أداة فعّالة في المجالات الأمنية ومن خصائصه كذلك القدرة على التنبؤ بالسلوكيات المستقبلية استنادًا إلى الأنماط السابقة، والتفاعل مع البيئة الرقمية المحيطة، فضلًا عن قابليته للتطوير المستمر.

غير أن هذه الخصائص، على الرغم من أهميتها، تثير إشكاليات قانونية متعددة، لا سيما فيما يتعلق بإسناد المسؤولية عن الأفعال الناتجة عن استخدام هذه الأنظمة، وحدود الرقابة البشرية عليها، وهو ما يستدعي تنظيمًا قانونيًا دقيقًا يوازن بين الاستفادة من مزايا الذكاء الاصطناعي وضمان احترام الحقوق والحريات (منصور، 2019).

الفرع الثاني: مفهوم الأمن السيبراني وأهميته في البيئة الرقمية

يعد الأمن السيبراني من المفاهيم الحديثة التي برزت مع التطور المتسارع للتكنولوجيا الرقمية وتزايد الاعتماد على الأنظمة المعلوماتية والشبكات الإلكترونية، الأمر الذي استدعى الاهتمام ببيان مفهومه وإبراز أهميته في حماية البيئة الرقمية، وعليه سيتم تناول ذلك على النحو الآتي:

أولًا: مفهوم الأمن السيبراني

يُقصد بالأمن السيبراني مجموعة التدابير والإجراءات الفنية والتنظيمية والقانونية التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات الإلكترونية والبيانات الرقمية من مختلف صور الاختراق أو الاعتداء أو الاستخدام غير المشروع، ويشمل الأمن السيبراني ضمان سرية المعلومات وسلامتها وتوافرها، بما يكفل استمرارية عمل الأنظمة الرقمية وحمايتها من المخاطر السيبرانية المتزايدة (العبودي، 2021).

ويُعد الأمن السيبراني مفهومًا متطورًا يتجاوز الحماية التقنية البحتة ليشمل أبعادًا قانونية ومؤسسية، نظرًا لما يترتب على الإخلال به من آثار تمس الأمن العام، والاقتصاد الوطني وحقوق الأفراد، الأمر الذي جعله من القضايا الأساسية في السياسات الجنائية المعاصرة.

ثانيًا: أهمية الأمن السيبراني في البيئة الرقمية

تتجلى أهمية الأمن السيبراني في كونه يشكّل الركيزة الأساسية لحماية البيئة الرقمية، ولا سيما في ظل الاعتماد المتزايد على التقنيات الحديثة، بما فيها تقنيات الذكاء الاصطناعي فالأمن السيبراني يضمن حماية البيانات الشخصية والمؤسساتية، ويحدّ من مخاطر الجرائم الإلكترونية، ويسهم في تعزيز الثقة في التعاملات الإلكترونية.

كما تبرز أهميته من المنظور الجنائي في دوره الوقائي، إذ يساهم في الحد من فرص ارتكاب الجرائم الإلكترونية، والكشف المبكر عن الهجمات الرقمية، ودعم جهود الجهات المختصة في مكافحة الجريمة. ويترتب على ذلك ضرورة إيلاء الأمن

السيبراني عناية تشريعية خاصة، بما يحقق التوازن بين متطلبات الحماية الجنائية وضمان احترام الحقوق في البيئة الرقمية.

الفرع الثالث: تطور الذكاء الاصطناعي والأمن السيبراني وأثره على المجال الجنائي

شهد كلٌّ من الذكاء الاصطناعي والأمن السيبراني تطورًا ملحوظًا في ظل الثورة الرقمية المتسارعة، الأمر الذي انعكس بدوره على المجال الجنائي من حيث طبيعة الجرائم ووسائل مكافحتها وعليه سيتم تناول ذلك من خلال ما يأتي:

أولًا: تطور الذكاء الاصطناعي والأمن السيبراني

شهد كل من الذكاء الاصطناعي والأمن السيبراني تطورًا متسارعًا نتيجة التقدم التكنولوجي والثورة الرقمية، حيث انتقل الذكاء الاصطناعي من كونه مجرد برامج تقليدية محدودة الوظائف إلى أنظمة ذكية متقدمة قادرة على التعلّم الذاتي، وتحليل البيانات الضخمة، واتخاذ قرارات شبه مستقلة. وقد أسهم هذا التطور في توسيع مجالات توظيف الذكاء الاصطناعي، ولا سيما في القطاعات الأمنية والقضائية، وفي المقابل، تطور مفهوم الأمن السيبراني من وسائل حماية تقنية بسيطة إلى منظومة متكاملة تشمل أبعادًا تقنية وتشريعية ومؤسسية، تهدف إلى مواجهة التهديدات الرقمية المتزايدة. وقد فرض هذا التطور ضرورة تبني استراتيجيات شاملة للأمن السيبراني، تأخذ في الاعتبار طبيعة المخاطر الجديدة التي أفرزتها التقنيات الذكية (الترهوني، 2022).

ثانيًا: أثر تطور الذكاء الاصطناعي والأمن السيبراني على المجال الجنائي

أدى التطور المتسارع للذكاء الاصطناعي والأمن السيبراني إلى إحداث تغييرات جوهرية في المجال الجنائي، سواء من حيث أساليب ارتكاب الجرائم الإلكترونية أو وسائل مكافحتها. فقد أسهمت التقنيات الذكية في ظهور أنماط إجرامية مستحدثة تتسم بالتعقيد والسرعة وصعوبة الاكتشاف، الأمر الذي شكّل تحديًا حقيقيًا أمام القواعد الجنائية التقليدية.

كما انعكس هذا التطور على آليات الإثبات الجنائي، حيث أضحت الأدلة الرقمية عنصرًا أساسيًا في الكشف عن الجرائم الإلكترونية، وهو ما يستلزم تكييف القواعد الإجرائية الجنائية بما يضمن حجية هذه الأدلة وسلامة إجراءات جمعها. ومن ثم، فإن هذا الواقع يفرض على السياسة الجنائية المعاصرة مواكبة التطور التقني من خلال تحديث التشريعات، وتطوير القدرات المؤسسية، وتحقيق التوازن بين فاعلية المكافحة الجنائية وحماية الحقوق والحريات.

المطلب الثاني دور تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني ومكافحة الجريمة

يهدف هذا المطلب إلى بيان الكيفية التي أسهمت بها تقنيات الذكاء الاصطناعي في دعم منظومات الأمن السيبراني، وتعزيز جهود مكافحة الجرائم الإلكترونية، مع إبراز ما يثيره هذا الدور من إشكاليات قانونية، تمهيدًا لدراستها في المباحث اللاحقة.

الفرع الأول: دور الذكاء الاصطناعي في الوقاية من الجرائم الإلكترونية

أصبحت الوقاية من الجرائم الإلكترونية من أهم أهداف السياسة الجنائية المعاصرة، في ظل التطور المتسارع للتقنيات الرقمية وتنامي الاعتماد على الأنظمة المعلوماتية. وفي هذا الإطار، أسهمت تقنيات الذكاء في إحداث نقلة نوعية في أساليب الوقاية الجنائية، من خلال تعزيز منظومات الأمن السيبراني والحد من فرص ارتكاب الجرائم الإلكترونية قبل وقوعها.

ويتمثل الدور الوقائي للذكاء الاصطناعي أساسًا في قدرته على تحليل كميات ضخمة من البيانات الرقمية، ورصد السلوكيات غير المألوفة داخل الشبكات والأنظمة المعلوماتية، بما يمكّنه من الكشف المبكر عن التهديدات السيبرانية ومحاولات الاختراق. وتساعد هذه القدرة الجهات المختصة على اتخاذ التدابير الوقائية اللازمة في الوقت المناسب، مما يقلل من احتمالات وقوع الجريمة الإلكترونية أو يحد من آثارها السلبية.

كما تُسهم تقنيات الذكاء الاصطناعي في تطوير أنظمة الحماية الرقمية، من خلال تحديث قواعد البيانات الأمنية بصورة مستمرة، والتكيّف مع الأساليب الإجرامية المستحدثة ويعد هذا التطور بالغ الأهمية، نظرًا لما تتسم به الجرائم الإلكترونية من سرعة في التنفيذ وصعوبة في الاكتشاف، الأمر الذي يجعل الوقاية أداة أكثر فاعلية من المعالجة اللاحقة.

ومن المنظور الجنائي، يُعد توظيف الذكاء الاصطناعي في الوقاية من الجرائم الإلكترونية تجسيدًا عمليًا للسياسة الجنائية الوقائية، التي تهدف إلى حماية المصالح المحمية قانونًا قبل المساس بها. وقد أشار الفقه الليبي إلى أن تعزيز الإجراءات الوقائية في المجال الرقمي يُعد ضرورة حتمية لمواجهة الجرائم المستحدثة، خاصة في ظل محدودية القواعد التقليدية في التصدي لها (قاسم، 2024).

غير أن هذا الدور الوقائي، على الرغم من أهميته، يثير جملة من التساؤلات القانونية، ولا سيما فيما يتعلق بمدى مشروعية المراقبة الرقمية القائمة على تقنيات الذكاء الاصطناعي، وحدود استخدامها بما لا يمس الحقوق والحريات الأساسية للأفراد. ومن ثم، فإن نجاح الدور الوقائي للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية يظل مرهونًا بوجود إطار قانوني منضبط يوازن بين متطلبات الأمن السيبراني وضمانات الشرعية الجنائية.

الفرع الثاني: دور تقنيات الذكاء الاصطناعي في كشف الجرائم الإلكترونية وجمع الأدلة الرقمية.

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إحداث تحول ملحوظ في أساليب مكافحة الجرائم الإلكترونية، حيث أصبحت هذه التقنيات تُسهم في كشف الأنشطة الإجرامية وتحليل البيانات الرقمية بصورة أكثر دقة وسرعة. كما برز دورها في دعم جهات التحقيق في جمع الأدلة الرقمية وتعزيز كفاءة الإجراءات الجنائية في مواجهة هذا النوع من الجرائم.

وعليه سيتم تناول ذلك على النحو الآتي:

أولاً: إسهام تقنيات الذكاء الاصطناعي في كشف الجرائم الإلكترونية

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى إحداث نقلة نوعية في أساليب كشف الجرائم الإلكترونية، حيث لم يعد الاكتفاء بالوسائل التقليدية للتحري كافيًا لمواجهة الجرائم الرقمية المعقدة التي تتسم بالخفاء والسرعة والتشابك التقني. وقد أسهمت تقنيات الذكاء الاصطناعي، ولا سيما خوارزميات التعلم الآلي وتحليل البيانات الضخمة، في تمكين

الجهات المختصة من رصد الأنماط غير المشروعة للسلوك الإجرامي داخل الفضاء السيبراني، والكشف المبكر عن الهجمات الإلكترونية قبل وقوع آثارها الضارة.

وتتمثل أهمية هذه التقنيات في قدرتها على تحليل كميات هائلة من البيانات الرقمية في زمن قياسي، ومقارنة السلوكيات الجارية بالأنماط الإجرامية المعروفة، بما يسمح بتحديد محاولات الاختراق وعمليات الاحتيال الإلكتروني، والجرائم الماسة بأنظمة المعلومات كما تسهم الأنظمة الذكية في دعم عمل جهات الضبط الجنائي من خلال تقليل الاعتماد على العنصر البشري وحده، والحد من احتمالات الخطأ أو القصور في كشف الجريمة الإلكترونية. ويُلاحظ أن هذا الدور الوقائي-الكشفي ينسجم مع التوجه الحديث للسياسة الجنائية المعاصرة، التي لم تعد تقتصر على رد الفعل بعد وقوع الجريمة، بل تسعى إلى اعتماد آليات استباقية تعتمد على التحليل الذكي للمخاطر الإجرامية في البيئة الرقمية.

ثانياً: دور الذكاء الاصطناعي في تسهيل إجراءات التحقيق وجمع وتحليل الأدلة الرقمية

إلى جانب دوره في كشف الجرائم الإلكترونية، يضطلع الذكاء الاصطناعي بدور محوري في مجال جمع وتحليل الأدلة الرقمية، التي تُعد من أكثر المسائل تعقيدًا في الإثبات الجنائي المعاصر، فالأدلة المستخلصة من النظم المعلوماتية تتسم بطبيعتها الفنية، وسهولة العبث بها أو إخفائها، الأمر الذي يفرض الاستعانة بتقنيات متقدمة لضمان سلامتها ومصداقيتها وتُستخدم تطبيقات الذكاء الاصطناعي في تتبع مصدر البيانات الرقمية، وتحليل سجلات الدخول، وفك تشفير بعض الأنماط المعقدة من المعاملات الإلكترونية، فضلًا عن إعادة بناء مسار الجريمة الرقمية بصورة دقيقة. كما تسهم هذه التقنيات في تصنيف الأدلة الرقمية وفرزها وربطها ببعضها البعض، بما يعين سلطات التحقيق على تكوين قناعة موضوعية بشأن الوقائع محل الاتهام، غير أن هذا التطور التقني يثير في المقابل جملة من الإشكاليات

القانونية، لا سيما فيما يتعلق بمدى مشروعية الاعتماد على الأدلة المستخلصة بواسطة أنظمة ذكية، وضمان احترام الضمانات الإجرائية، وحقوق الدفاع، وهو ما يستدعي تدخل المشرّع لوضع إطار قانوني واضح ينظم استخدام هذه التقنيات في مرحلتي الاستدلال والتحقيق (السنوسي،2020).

ومن هنا لا يقتصر دور الذكاء الاصطناعي على مرحلة الكشف عن الجرائم الإلكترونية، بل يمتد ليشمل مرحلة التحقيق الجنائي، ولا سيما فيما يتعلق بجمع الأدلة الرقمية وتحليلها. إذ تُستخدم التطبيقات الذكية في تتبع مصادر البيانات، وتحليل سجلات الأنظمة، وفك تشفير بعض المعاملات الرقمية، إضافة إلى فرز الأدلة وربطها زمنياً وموضوعياً بوقائع الجريمة ويسهم هذا الاستخدام في تسريع إجراءات التحقيق، وتقليل الجهد البشري المطلوب لفحص البيانات الرقمية المعقدة، فضلًا عن الحد من احتمالات الخطأ الفني. غير أن الاعتماد على هذه التقنيات يثير في المقابل إشكاليات قانونية تتعلق بمدى حجية الأدلة الرقمية المستخلصة بواسطة أنظمة ذكية، وضمان احترام الضمانات الإجرائية وحقوق الدفاع، وهو ما يستدعي إخضاع استخدام الذكاء الاصطناعي في التحقيق الجنائي لإطار قانوني واضح يوازن بين متطلبات الفعالية الجنائية وحماية الحقوق والحريات.

الفرع الثالث: حدود فاعلية الذكاء الاصطناعي والتحديات القانونية المرتبطة باستخدامه في المجال الجنائي

على الرغم من الأهمية المتزايدة لتقنيات الذكاء الاصطناعي في دعم الجهود الرامية إلى مكافحة الجرائم الإلكترونية وتعزيز كفاءة الإجراءات الجنائية، إلا أن استخدامها في المجال الجنائي يثير جملة من التحديات التقنية والقانونية التي قد تحد من فاعليته. ومن ثم يقتضي الأمر الوقوف على حدود هذه الفاعلية وبيان أبرز الإشكالات المرتبطة بتوظيف هذه التقنيات، وعليه سيتم تناول ذلك من خلال ما يأتي:

اولاً: حدود فاعلية تقنيات الذكاء الاصطناعي في مواجهة الجر ائم الإلكترونية

على الرغم من الدور المتنامي الذي تؤديه تقنيات الذكاء الاصطناعي في دعم الجهود الجنائية الرامية إلى مواجهة الجرائم الإلكترونية، إلا أن فاعلية هذه التقنيات تظل نسبية ومقيدة بجملة من العوامل التقنية والعملية. إذ يرتبط أداء الأنظمة الذكية ارتباطًا وثيقًا بجودة البيانات الرقمية التي تُغذّى بها، من حيث دقتها وحداثتها وشمولها، الأمر الذي قد يؤثر في نتائج التحليل ويؤدي إلى احتمالات الخطأ أو القصور في الكشف عن السلوك الإجرامي (الميري، 2024).

كما أن التطور المستمر في أساليب ارتكاب الجرائم الإلكترونية، ولا سيما لجوء الجناة أنفسهم إلى استخدام تقنيات متقدمة، يحدّ من قدرة أنظمة الذكاء الاصطناعي على مواكبة هذه الجرائم بصورة دائمة، ويُضاف إلى ذلك ما تعانيه بعض الدول ومنها ليبيا، من تحديات تتعلق بضعف البنية التحتية التقنية ونقص الكفاءات المتخصصة، وهو ما يقلل من الاستفادة العملية من هذه التقنيات في المجال الجنائي.

ثانياً: التحديات القانونية المترتبة على استخدام الذكاء الاصطناعي في الإجراءات الجنائية

يثير استخدام تقنيات الذكاء الاصطناعي في المجال الجنائي جملة من التحديات القانونية التي تمس جوهر الشرعية الإجرائية وضمانات المحاكمة العادلة، فاعتماد جهات الضبط والتحقيق على أنظمة ذكية في كشف الجرائم أو تحليل الأدلة الرقمية يطرح تساؤلات جدية حول مدى مشروعية هذه الإجراءات، وحدود الرقابة القضائية على عمل هذه الأنظمة، وإمكانية مناقشة نتائجها والطعن فيها من قبل المتهم.

كما تبرز إشكالية حماية الخصوصية والبيانات الشخصية، في ظل اعتماد تقنيات الذكاء الاصطناعي على جمع وتحليل كمٍّ واسع من البيانات الرقمية، بما قد يؤدي إلى مساس غير مبرر بالحياة الخاصة للأفراد، إذا لم يُضبط ذلك بضوابط قانونية واضحة. ويُضاف إلى ذلك غياب تنظيم تشريعي صريح يحدد المسؤولية القانونية عن الأخطاء الناتجة عن عمل الأنظمة الذكية، سواء من حيث الجهة المستخدمة لها أو القائمين على تصميمها وتطويرها.

وفي هذا الإطار، تؤكد الدراسات المقارنة ضرورة إخضاع استخدام الذكاء الاصطناعي في المجال الجنائي لمعايير قانونية وأخلاقية دقيقة، تضمن تحقيق التوازن بين متطلبات الفعالية في مكافحة الجريمة، واحترام الحقوق والحريات الأساسية، وهو ما يبرز الحاجة إلى تدخل تشريعي يواكب هذه التحولات التقنية.

المطلب الثالث: العلاقة بين الذكاء الاصطناعي والسياسة الجنائية المعاصرة

يُعنى هذا المطلب ببيان الكيفية التي أثّر بها تطور تقنيات الذكاء الاصطناعي في توجهات السياسة الجنائية المعاصرة، سواء على مستوى الوقاية من الجريمة، أو على مستوى التجريم والعقاب، أو من حيث إعادة صياغة أدوات المكافحة الجنائية بما يتلاءم مع التحولات الرقمية

الفرع الأول: تأثير الذكاء الاصطناعي في توجهات السياسة الجنائية الوقائية

أفرز التطور المتسارع لتقنيات الذكاء الاصطناعي تحولًا ملحوظًا في مفهوم السياسة الجنائية، إذ لم تعد هذه الأخيرة تقتصر على مواجهة الجريمة بعد وقوعها، بل اتجهت نحو تعزيز البعد الوقائي والاستباقي. وقد أسهم الذكاء الاصطناعي في دعم هذا التوجه من خلال قدرته على تحليل البيانات الضخمة، والتنبؤ بالمخاطر الإجرامية، ورصد الأنماط السلوكية التي قد تنذر بوقوع الجريمة الإلكترونية قبل تحققها فعليًا. (القويري، 2019).

ويُلاحظ أن اعتماد هذه الآليات الوقائية ينسجم مع فلسفة السياسة الجنائية الحديثة، التي تسعى إلى تقليل فرص ارتكاب الجريمة والحد من آثارها الاجتماعية والاقتصادية. غير أن هذا التوسع في استخدام الوسائل الذكية يثير تساؤلات حول مدى توافقه مع مبدأ الشرعية، وحدود تدخل الدولة في الحياة الخاصة للأفراد، وهو ما يستدعي ضبط هذه الوسائل بإطار قانوني.

الفرع الثاني: أثر الذكاء الاصطناعي في تطوير أدوات التجريم والعقاب

يكتسب بحث أثر الذكاء الاصطناعي في تطوير أدوات التجريم والعقاب أهمية خاصة في ظل التحولات المتسارعة التي تشهدها البيئة الرقمية، وهو ما يقتضي الوقوف على أبرز ملامح هذا التأثير على النحو الآتي:

أولاً: دور الذكاء الاصطناعي في إعادة تشكيل نطاق التجريم الجنائي

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى بروز أنماط جديدة من السلوك الإجرامي لم تكن مألوفة في الإطار التقليدي للجريمة، الأمر الذي فرض على السياسة الجنائية المعاصرة إعادة النظر في نطاق التجريم القائم، فقد أصبحت بعض الأفعال الاجرامية باستخدام تقنيات ذكية، تشكل خطرًا حقيقيًا على المصالح المحمية جنائيًا، رغم عدم النص عليها صراحة في التشريعات الجنائية التقليدية.

وفي هذا السياق، اتجهت السياسة الجنائية الحديثة إلى توسيع دائرة التجريم لتشمل افعالا مستحدثة، كإساءة استخدام الأنظمة الذكية، والاعتداء على أمن البيانات، والتلاعب بالخوارزميات، بما يحقق حماية فعالة للمجتمع في البيئة الرقمية، مع ضرورة الالتزام بمبدأ الشرعية الجنائية وعدم التوسع غير المبرر في التجريم.

ثانياً: إسهام الذكاء الاصطناعي في تطوير أساليب العقاب وتنفيذ الجزاء

لم يقتصر تأثير الذكاء الاصطناعي على مرحلة التجريم، بل امتد ليشمل مرحلة العقاب وتنفيذ الجزاء الجنائي، حيث أتاح استخدام تقنيات ذكية في تقييم خطورة الجناة، ومتابعة سلوك المحكوم عليهم، بما يسهم في تحقيق أهداف العقوبة، ولا سيما الإصلاح وإعادة الإدماج الاجتماعي (الميري، 2024).

غير أن هذا التطور يفرض في المقابل ضرورة مراعاة الضمانات القانونية للمحكوم عليهم وعدم تحويل الوسائل التقنية إلى أدوات رقابة مفرطة تمس بالحقوق والحريات الأساسية، الأمر الذي يستدعي إخضاع استخدام الذكاء الاصطناعي في مجال العقاب لإطار قانوني منضبط يوازن بين الفعالية الجنائية واحترام الكرامة الإنسانية.

الفرع الثالث: حدود التكيّف التشريعي للسياسة الجنائية مع تطورات الذكاء الاصطناعي

يثير التطور المتسارع في تقنيات الذكاء الاصطناعي تحديات متزايدة أمام التشريعات الجنائية التقليدية الأمر الذي يفرض على السياسة الجنائية إعادة النظر في بعض أدواتها التقليدية بما يضمن تحقيق التوازن بين متطلبات الفعالية في مكافحة الجريمة وضمان حماية الحقوق والحريات.

أولاً: قصور التشريعات الجنائية التقليدية عن استيعاب الجرائم الذكية

تكشف دراسة تطور الجرائم المرتبطة بالذكاء الاصطناعي عن وجود فجوة تشريعية بين النصوص الجنائية التقليدية والواقع التقني المتجدد، حيث لم تُصمَّم هذه النصوص لمواجهة جرائم تتسم بالتعقيد الفني، وسرعة التطور، والطابع العابر للحدود. ويؤدي هذا القصور إلى صعوبات في التكييف القانوني، وإلى تباين في التطبيق القضائي، بما قد يضعف من فعالية السياسة الجنائية.

ويُلاحظ أن هذا التحدي يبرز بوضوح في النظم القانونية التي لم تُحدِّث تشريعاتها الجنائية بما يواكب التحولات الرقمية، الأمر الذي يستدعي إعادة تقييم الإطار التشريعي القائم في ضوء التطورات التقنية الحديثة.

ثانياً: متطلبات التكيّف التشريعي وضمانات الشرعية الجنائية

يفرض التكيّف التشريعي مع تطورات الذكاء الاصطناعي على السياسة الجنائية المعاصرة تبنّي مقاربة متوازنة، تقوم على تحديث النصوص الجنائية بما يحقق الفعالية في مواجهة الجرائم الرقمية، دون الإخلال بمبادئ الشرعية الجنائية، واليقين القانوني، وضمانات المحاكمة العادلة. وفي هذا الإطار، تبرز أهمية وضع ضوابط قانونية واضحة لاستخدام الذكاء الاصطناعي في المجال الجنائي، تحدد نطاق استخدامها، والمسؤولية الناشئة عنها، وآليات الرقابة القضائية ما يضمن توافق السياسة الجنائية مع متطلبات دولة القانون في العصر الرقمي.

المبحث الثاني: الجرائم الإلكترونية المستحدثة الناتجة عن استخدام تقنيات الذكاء الاصطناعي

أفرز التطور المتسارع لتقنيات الذكاء الاصطناعي واقعًا إجراميًا جديدًا تجاوز الأطر التقليدية للجريمة الإلكترونية، حيث لم تعد هذه التقنيات مجرد أدوات مساعدة في ارتكاب الفعل الإجرامي، بل أضحت في بعض الأحيان عنصرًا جوهريًا في تكوينه وتنفيذه. وقد أسهم هذا التحول في ظهور أنماط إجرامية مستحدثة تتسم بدرجة عالية من التعقيد والذكاء، سواء من حيث أساليب التنفيذ، أو من حيث صعوبة الكشف والإثبات، أو من حيث تحديد المسؤولية الجنائية عنها.

وإزاء هذا الواقع، برزت الحاجة إلى دراسة الجرائم الإلكترونية المرتبطة بالذكاء الاصطناعي دراسة تحليلية معمقة، تهدف إلى استجلاء صورها المختلفة، وبيان خصائصها المميزة، وتحليل أركانها القانونية، فضلًا عن إبراز التحديات التي تطرحها هذه الجرائم على منظومة العدالة الجنائية، ولا سيما في مرحلتي التجريم والملاحقة الجنائية.

وانطلاقًا من ذلك، يتناول هذا المبحث تحليل أبرز الجرائم الإلكترونية المستحدثة الناتجة عن استخدام تقنيات الذكاء الاصطناعي، وذلك من خلال تقسيمه إلى مطالب وفروع تُعالج الجوانب الموضوعية والإجرائية لهذه الجرائم، تمهيدًا لتقييم مدى كفاية المواجهة الجنائية لها وبما يمهّد لاحقًا لدراسة الإطار القانوني الليبي في هذا المجال (الترهوني، 2022).

المطلب الأول: ماهية الجرائم الإلكترونية المرتبطة باستخدام تقنيات الذكاء الاصطناعي

أفرز التطور المتسارع لتقنيات الذكاء الاصطناعي تحولات جوهرية في طبيعة الجريمة الإلكترونية، حيث لم تعد هذه الجرائم تعتمد فقط على الوسائل التقنية التقليدية، بل أصبحت تقوم في جوهرها على أنظمة ذكية قادرة على التعلم والتحليل واتخاذ القرار، وقد أدى هذا التحول إلى ظهور أنماط إجرامية مستحدثة تتسم بقدر كبير من التعقيد والخفاء، الأمر الذي يفرض إعادة النظر في المفاهيم التقليدية للجريمة الإلكترونية، وبيان خصائص هذه الجرائم وصورها العملية، تمهيدًا لتقييم مدى كفاية المواجهة الجنائية لها.

الفرع الأول: مفهوم الجرائم الإلكترونية القائمة على الذكاء الاصطناعي

يُقصد بالجرائم الإلكترونية تلك الجرائم المستحدثة المرتبطة باستخدام تقنيات الذكاء الاصطناعي تلك الأفعال غير المشروعة التي تُرتكب في البيئة الرقمية، ويكون للذكاء الاصطناعي دور أساسي في تنفيذها أو التخطيط لها أو إخفاء آثارها، من خلال أنظمة أو تطبيقات قادرة على التعلم الذاتي أو معالجة البيانات وتحليلها بصورة مستقلة. وتمتاز هذه الجرائم عن الجرائم الإلكترونية التقليدية بكونها تعتمد على خوارزميات ذكية تحاكي السلوك البشري أو تتجاوزه، بما يمنحها قدرة أكبر على التكيف مع أنظمة الحماية الرقمية.

ولا يقتصر هذا النوع من الجرائم على الاعتداء على نظم المعلومات أو البيانات، بل يمتد ليشمل المساس بالثقة الرقمية، والاعتداء على الخصوصية، والتلاعب بالمعاملات الإلكترونية، بل وقد يصل أثره إلى تهديد الأمن الاقتصادي والاجتماعي. وهو ما يجعل هذه الجرائم تمثل تحديًا حقيقيًا أمام السياسة الجنائية المعاصرة، التي باتت مطالبة باستيعاب هذا التطور التقني في بنيتها التشريعية.

ومن هنا يمكن القول بأن الجرائم الإلكترونية من الجرائم الحديثة والخطيرة التي ظهرت مع تطور التقدم التكنولوجي في العصر الحديث، وهي جرائم عابرة للحدود لا تقف عند القيود الجغرافية للدول (الزوي، 2022).

ومن مخاطرها فهي تمسّ الحياة الخاصة للأفراد والمؤسسات، ويترتب عليها أضرار جسيمة قد تلحق باقتصاد الدول، فضلًا عن كونها خسائر غالبًا ما تكون غير مسبوقة، ولا تتطلب هذه الجريمة جهدًا عضليًا، وإنما تعتمد أساسًا على مستوى عالٍ من الذكاء والمهارة الذهنية، الأمر الذي يجعل من السهل ارتكابها دون حاجة إلى استخدام القوة المادية، كما يمكن للجاني تنفيذ الجريمة دون امتلاك وعي تقني متقدم، وذلك عبر الاستعانة بالحاسوب والوسائل التكنولوجية الحديثة.

وتبرز خطورة هذه الجريمة في إمكانية ارتكابها بصورة خفية وناعمة، إذ لا يُشترط وجود الجاني في مسرح الجريمة، بل يمكن تنفيذها عن بُعد، وهو ما يتيح للمجرمين تحقيق منافع مالية كبيرة. ولذلك تُعدّ الجريمة الإلكترونية عامل جذب للمجرمين لاستغلال التكنولوجيا الحديثة في ارتكاب الأفعال الإجرامية، ولاسيما إذا كان الجاني يعمل في مؤسسة تعتمد في نشاطها

على أنظمة الحاسوب، حيث تتوافر لديه المعلومات اللازمة لإجراء اختراقات متكررة ومتتابعة لأنظمة الشركة، بما يحقق له أرباحًا غير مشروعة وطائلة، وهو ما تؤكده الوقائع العملية المعاصرة. (حجازي، 2019).

الفرع الثاني: صور الجرائم الإلكترونية باستخدام تقنيات الذكاء الاصطناعي

تتعدد صور الجرائم الإلكترونية المستحدثة المرتبطة بالذكاء الاصطناعي، ومن أبرزها جرائم التزييف العميق (Deep fake) التي تُستخدم فيها الخوارزميات الذكية لإنتاج محتوى صوتي أو مرئي مزيف يصعب تمييزه عن الحقيقي، ويُستغل في التشهير أو الابتزاز أو الاحتيال أو

التأثير على الرأي العام. كما تشمل هذه الجرائم الهجمات السيبرانية الذكية القادرة على تحليل أنظمة الحماية الرقمية والتكيف معها لاختراقها بكفاءة أعلى.

ومن الصور المستحدثة كذلك استخدام الروبوتات البرمجية الذكية في تنفيذ عمليات احتيال إلكتروني واسعة النطاق، أو في اختراق الحسابات المصرفية، في التلاعب بالبيانات والأسواق الرقمية. وتعكس هذه الصور تحول الجريمة الإلكترونية من أفعال فردية محدودة إلى أنشطة إجرامية منظمة تعتمد على تقنيات عالية التطور، مما يزيد من خطورتها وصعوبة مكافحتها.

الفرع الثالث: التطبيقات العملية وخطورة الجرائم الإلكترونية الذكية

لا تقتصر خطورة الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي على مجرد تطوير وسائل ارتكاب الجريمة فحسب، بل تمتد لتشمل زيادة قدرتها على التخفي وصعوبة اكتشافها، نظرًا لما تتمتع به هذه التقنيات من قدرة على التعلم الذاتي وتحليل كميات هائلة من البيانات في وقت قصير، الأمر الذي يضاعف من حجم الأضرار التي قد تلحق بالأفراد والمؤسسات على حد سواء.

أولاً: التطبيقات العملية للجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

أفرز الاستخدام المتزايد لتقنيات الذكاء الاصطناعي تطبيقات عملية متعددة في مجال الجرائم الإلكترونية، حيث استُخدمت الأنظمة الذكية في تنفيذ عمليات احتيال إلكتروني معقدة، وتزوير المستندات الرقمية، وانتحال الهوية عبر تقنيات التزييف العميق، فضلًا عن اختراق الأنظمة المصرفية وقواعد البيانات الحساسة. وقد ساهمت القدرة العالية لهذه الأنظمة على تحليل البيانات الضخمة والتعلّم الذاتي في رفع كفاءة السلوك الإجرامي، وجعل اكتشافه أكثر صعوبة مقارنة بالجرائم الإلكترونية التقليدية.

كما أظهرت التطبيقات العملية اعتماد بعض الجناة على برامج ذكية قادرة على محاكاة السلوك البشري في التواصل الإلكتروني، مما أدى إلى تضليل الضحايا وإضفاء مظهر المشروعية على الأفعال الإجرامية. ويُبرز ذلك تحوّل الجريمة الإلكترونية من نماذج بسيطة إلى ممارسات تقنية متقدمة تتسم بالدقة والتنظيم، وهو ما يستدعي أدوات مواجهة جنائية أكثر تطورا.

ثانياً: خطورة الجرائم الإلكترونية الذكية على المصالح المحمية جنائيًا

تتجلى خطورة الجرائم الإلكترونية الذكية في تعدد المصالح القانونية التي تمسّها، حيث لا تقتصر آثارها على الإضرار بالأموال أو البيانات، بل تمتد لتشمل الاعتداء على الخصوصية الرقمية، وزعزعة الثقة في المعاملات الإلكترونية، وتهديد الأمن الاقتصادي والاجتماعي. كما أن الطابع العابر للحدود الذي تتسم به هذه الجرائم يُعقّد من إجراءات الملاحقة والتحقيق، ويُضعف من فعالية وسائل الردع التقليدية.

وتزداد خطورة هذه الجرائم نتيجة لاعتمادها على أنظمة ذاتية التعلم قادرة على تغيير أساليبها وتطويرها بما يُمكّنها من تفادي آليات الرصد والكشف، الأمر الذي يُلقي على عاتق المشرّع والسلطات المختصة مسؤولية تحديث السياسة الجنائية، وتطوير الإطار التشريعي والإجرائي بما يحقق حماية فعالة للمصالح القانونية في البيئة الرقمية (العجمي 2014).

المطلب الثاني: الإشكاليات القانونية لإسناد المسؤولية الجنائية في الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

يتناول هذا المطلب تحليل الإشكاليات القانونية التي يثيرها استخدام تقنيات الذكاء الاصطناعي في ارتكاب الجرائم الإلكترونية، ولا سيما ما يتعلق بتحديد الفاعل الجنائي، وإسناد المسؤولية الجنائية، في ظل الطبيعة التقنية المعقدة لهذه لأنظمة.

الفرع الأول: إشكالية تحديد الفاعل الجنائي في الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

تُعد مسألة تحديد الفاعل الجنائي من أبرز الإشكاليات التي تثيرها الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي، نظرًا للطابع التقني المعقد لهذه الجرائم، وتعدد الأطراف المتدخلة في تصميم وتشغيل واستخدام الأنظمة الذكية، بما يُلقي بظلاله على إمكانية تطبيق القواعد التقليدية للمسؤولية الجنائية.

أولًا: تعدد أطراف النشاط الإجرامي وصعوبة تحديد الفاعل الأصلي

تتميز الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي بتعدد الأطراف المحتملة التي قد تسهم، بصورة مباشرة أو غير مباشرة، في وقوع الفعل الإجرامي، إذ قد يكون الفعل ناتجًا عن تدخل المبرمج الذي صمّم النظام، أو المستخدم الذي استغله في غرض غير مشروع، والمشغل الذي أهمل في الرقابة، أو حتى نتيجة خلل تقني ذاتي ناتج عن خاصية التعلّم الذاتي التي تتمتع بها بعض الأنظمة الذكية (الفيتوري،2018).

ويؤدي هذا التعدد إلى إرباك عملية تحديد الفاعل الجنائي بالمعنى التقليدي، خاصة في الحالات التي ينفذ فيها النظام الذكي أفعالًا لم تكن متوقعة على نحو مباشر من الشخص القائم على تشغيله، وهو ما يثير تساؤلًا جوهريًا حول مدى إمكانية إسناد الفعل الإجرامي إلى شخص طبيعي بعينه، في ظل غياب السلوك الإنساني المباشر أو صعوبة إثبات العلاقة السببية بين الفعل والنتيجة.

وفي هذا السياق تبدو القواعد العامة في قانون العقوبات الليبي، القائمة على فكرة السلوك الإرادي الصادر عن شخص طبيعي مميّز، قاصرة عن استيعاب هذه الصورة المستحدثة من النشاط الإجرامي، الأمر الذي يستدعي إعادة النظر في آليات تحديد الفاعل الجنائي في الجرائم الإلكترونية الذكية (الهادي، 2020).

ثانيًا: أثر الطبيعة الذاتية لأنظمة الذكاء الاصطناعي على إسناد الفعل الجنائي

تُسهم الخصائص التقنية لأنظمة الذكاء الاصطناعي، ولا سيما خاصية الاستقلال النسبي والتعلّم الذاتي، في تعقيد مسألة إسناد الفعل الجنائي، إذ قد يتصرف النظام على نحو يتجاوز الأوامر

البرمجية الأولية، مستندًا إلى خوارزميات تحليل البيانات واتخاذ القرار ويترتب على ذلك إشكال قانوني دقيق يتمثل في التساؤل حول مدى إمكانية اعتبار الفعل الصادر عن النظام الذكي فعلًا منسوبًا إلى الإنسان، أم أنه يُعد نتاجًا لتفاعل تقني مستقل لا يمكن مساءلة شخص بعينه عنه مساءلة جنائية تقليدية. وقد ذهب جانب من الفقه المقارن إلى ضرورة البحث عن «الفاعل المسيطر» الذي يملك سلطة التوجيه أو الرقابة على النظام، باعتباره الأقرب لتحمل المسؤولية الجنائية، ولو على أساس الخطأ أو الإهمال.

وفي الإطار الليبي، لا يزال التشريع الجنائي يفتقر إلى نصوص صريحة تُعالج هذه الإشكالية، مما يفرض على القضاء اللجوء إلى القواعد العامة، وهو حل لا يخلو من قصور في مواجهة الجرائم الإلكترونية الذكية، خاصة تلك التي تتسم بدرجة عالية من التعقيد التقني والاستقلال البرمجي (ابوشناف، 2017).

الفرع الثاني: مدى قابلية تطبيق القواعد التقليدية للمسؤولية الجنائية على الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

يثير تطور الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي تساؤلات جوهرية حول مدى صلاحية القواعد التقليدية للمسؤولية الجنائية لاستيعاب هذا النمط المستحدث من الجرائم، خاصة في ظل الخصائص التقنية التي تميّز الأنظمة الذكية، والتي قد تُضعف من فعالية المفاهيم الجنائية الكلاسيكية.

أولًا: قصور الأركان التقليدية للمسؤولية الجنائية في مواجهة الجرائم الإلكترونية الذكية

تقوم المسؤولية الجنائية في التشريع الليبي، شأنها شأن أغلب التشريعات الجنائية، على توافر أركان أساسية تتمثل في الركن المادي، والركن المعنوي، وصدور الفعل عن شخص طبيعي يتمتع بالإرادة والتمييز، غير أن الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي تطرح إشكالية حقيقية في تطبيق هذه الأركان، لا سيما في الحالات التي يتم فيها تنفيذ الفعل الإجرامي بواسطة نظام ذكي يعمل بصورة شبه مستقلة (المقريف،2021).

ففيما يتعلق بالركن المادي، قد يصعب تحديد السلوك الإجرامي المنسوب إلى شخص معين، خاصة إذا كان الفعل نتيجة تفاعل خوارزمي مع معطيات رقمية متغيرة. أما الركن المعنوي، المتمثل في القصد الجنائي أو الخطأ، فيُعد أكثر الأركان تأثرًا بهذه الجرائم، نظرًا لصعوبة إثبات توافر النية الإجرامية لدى شخص طبيعي، عندما يكون الفعل قد صدر عن نظام ذكي لم يُبرمج صراحة لارتكاب الجريمة.

ويكشف ذلك عن قصور واضح في القواعد التقليدية للمسؤولية الجنائية عن استيعاب الجرائم الإلكترونية الذكية، وهو قصور لا يمكن تجاوزه بالاكتفاء بالتفسير الموسّع للنصوص الجنائية القائمة.

ثانيًا: الاتجاهات الفقهية في تكييف المسؤولية الجنائية عن الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

أمام هذا القصور، اتجه الفقه الجنائي إلى طرح عدة تصورات لتكييف المسؤولية الجنائية في الجرائم الإلكترونية الذكية، من أبرزها الاتجاه الذي يدعو إلى إسناد المسؤولية إلى الشخص الأكثر سيطرة على النظام الذكي، سواء كان المبرمج أو المستخدم أو المشغّل، وذلك بحسب طبيعة الدور الذي أدّاه كل منهم في وقوع الجريمة.

وظهر اتجاه فقهي آخر يدعو إلى تطوير مفهوم الخطأ الجنائي ليشمل حالات الإهمال في تصميم أو تشغيل أو مراقبة أنظمة الذكاء الاصطناعي، بما يسمح بإسناد المسؤولية الجنائية على أساس الخطأ غير العمدي. وفي المقابل، يُبدي جانب من الفقه تحفظه على هذه الاتجاهات، محذرًا من المساس بمبدأ شخصية المسؤولية الجنائية، وضرورة بقاء الإنسان محور المساءلة الجنائية (الفرجاني، 2016).

وفي الإطار الليبي، يظل الاعتماد على القواعد العامة دون تدخل تشريعي صريح حلًا مؤقتًا، لا يرقى إلى مواجهة التحديات التي تفرضها الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي، الأمر الذي يستدعي إعادة النظر في السياسة الجنائية بما يحقق التوازن بين حماية المجتمع وضمانات المسؤولية الجنائية.

الفرع الثالث: المسؤولية الجنائية عن أفعال أنظمة الذكاء الاصطناعي (المبرمج – المستخدم – المشغّل)

تثير الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي إشكالية جوهرية تتعلق بتحديد نطاق المسؤولية الجنائية للأشخاص المرتبطين بالنظام الذكي، ولا سيما المبرمج والمستخدم والمشغّل، في ظل تداخل الأدوار التقنية وتفاوت درجات السيطرة على النظام.

أولًا: المسؤولية الجنائية للمبرمج والمشغّل عن الأفعال الإجرامية للنظام الذكي

يُعد المبرمج من الفاعلين الرئيسيين في منظومة الذكاء الاصطناعي، باعتباره المسؤول عن تصميم الخوارزميات وتحديد حدود عمل النظام. وتُثار مسؤوليته الجنائية متى ثبت أن الفعل الإجرامي كان نتيجة مباشرة لعيب في البرمجة، أو لإدخال أوامر أو تعليمات تُسهِم في تمكين النظام من ارتكاب الجريمة، سواء على نحو عمدي أو نتيجة إهمال جسيم.

أما المشغّل، فتقوم مسؤوليته الجنائية في الحالات التي يثبت فيها إخلاله بواجب الرقابة أو الإشراف على النظام الذكي، لا سيما إذا كان على علم بإمكانية استخدام النظام في أغراض غير مشروعة، أو تجاهل مؤشرات الخطر التي تنذر بوقوع الفعل الإجرامي. ويُمكن في هذه الحالة إسناد المسؤولية إليه على أساس الخطأ الجنائي، وفقًا للقواعد العامة في القانون الجنائي الليبي.

ويُلاحظ أن التشريع الليبي، في صيغته الحالية، لا يتضمن نصوصًا خاصة تُحدد بدقة مسؤولية المبرمج أو المشغّل عن أفعال الأنظمة الذكية، الأمر الذي يضطر القضاء إلى الاعتماد على القواعد العامة، وهو ما قد يؤدي إلى تباين في التفسير والتطبيق.

ثانيًا: المسؤولية الجنائية للمستخدم وإشكالية مساءلة أنظمة الذكاء الاصطناعي ذاتها

تتجه الغالبية العظمى من الفقه الجنائي إلى إسناد المسؤولية الجنائية للمستخدم متى ثبت أنه استغل النظام الذكي عن علم وإرادة في ارتكاب الجريمة الإلكترونية، باعتباره صاحب القرار الفعلي في توجيه النظام نحو السلوك الإجرامي، وتُعد

هذه الصورة الأقرب للتكييف التقليدي للمسؤولية الجنائية، نظرًا لتوافر السلوك الإرادي والقصد الجنائي لدى المستخدم (أبو عامر، 2018).

وفي المقابل، يُثار جدل فقهي حول مدى إمكانية مساءلة أنظمة الذكاء الاصطناعي ذاتها عن الأفعال الإجرامية، خاصة تلك التي تتمتع بدرجة عالية من الاستقلال الذاتي، وقد رفض الاتجاه الغالب هذا التصور، تأسيسًا على افتقار هذه الأنظمة إلى الإرادة والتمييز، وهما ركنان جوهريان للمسؤولية الجنائية. في حين ذهب اتجاه فقهي محدود إلى اقتراح منح الأنظمة الذكية شخصية قانونية خاصة، وهو اتجاه لا يزال محل نقاش نظري ولم يجد له تطبيقًا تشريعيًا فعليًا.

وفي الإطار الليبي، يبقى إسناد المسؤولية الجنائية حكرًا على الأشخاص الطبيعيين، مما يؤكد ضرورة تطوير التشريع الجنائي لمواكبة التحولات التقنية، دون الإخلال بالمبادئ الأساسية للمسؤولية الجنائية.

المطلب الثالث: تحديات الإثبات الجنائي في الجرائم الإلكترونية الذكية

يسعى هذا المطلب إلى تحليل أبرز تحديات الإثبات الجنائي في الجرائم الإلكترونية الذكية، من خلال دراسة طبيعة الدليل الجنائي الرقمي، وبيان الصعوبات التقنية والقانونية التي تعترض جمعه وتحليله، وصولًا إلى بحث حجية الأدلة الرقمية ودور الخبرة الفنية في دعم قناعة القاضي الجنائي، وذلك تمهيدًا لربط هذه الإشكاليات بالواقع القضائي الوطني في موضعه المخصص من البحث.

الفرع الأول: طبيعة الدليل الجنائي الرقمي في الجرائم الإلكترونية الذكية

تفرض الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي طبيعة خاصة للدليل الجنائي، تختلف في خصائصها عن الأدلة التقليدية، الأمر الذي ينعكس مباشرة على إجراءات الإثبات الجنائي وقواعده (حجازي، 2020).

أولًا: مفهوم الدليل الجنائي الرقمي وخصائصه في الجرائم الإلكترونية الذكية

يقصد بالدليل الجنائي الرقمي كل معلومة ذات طابع إلكتروني يتم استخراجها أو تحليلها أو تخزينها باستخدام الوسائل التقنية، ويُستدل بها على وقوع الجريمة أو نسبتها إلى فاعلها، ويشمل ذلك البيانات المخزنة على الحواسيب، وسجلات الخوادم، والبصمات الرقمية، ومخرجات أنظمة الذكاء الاصطناعي ذاتها، وتتسم الأدلة الرقمية في الجرائم الإلكترونية الذكية بعدة خصائص، من أبرزها قابليتها للتغيير أو الإتلاف بسهولة، واعتمادها على وسائط غير مادية، فضلًا عن تعقيد بنيتها التقنية، لا سيما عندما تكون ناتجة عن خوارزميات تعلم آلي أو نظم ذاتية القرار(عبد الرحيم، 2021).

ويؤدي ذلك إلى صعوبة التعامل معها وفق القواعد التقليدية للإثبات الجنائي، التي تقوم في الأصل على أدلة مادية محسوسة.

وفي هذا الإطار، يواجه القضاء الجنائي تحديًا يتمثل في ضرورة فهم الطبيعة التقنية لهذا النوع من الأدلة، وضمان سلامة إجراءات جمعها وتحليلها، بما يحافظ على قيمتها القانونية والاثباتية.

ثانيًا: أثر الاعتماد على أنظمة الذكاء الاصطناعي في تكوين الدليل الجنائي

يُسهم استخدام أنظمة الذكاء الاصطناعي في تكوين الدليل الجنائي الرقمي من خلال تحليل كميات هائلة من البيانات، واستخلاص أنماط سلوكية إجرامية، وربط الوقائع الرقمية ببعضها البعض، غير أن هذا الدور، على أهميته، يثير إشكاليات قانونية تتعلق بمدى شفافية هذه الأنظمة، وإمكانية التحقق من سلامة النتائج التي تُنتجها.

ففي كثير من الحالات، تعتمد الأنظمة الذكية على خوارزميات معقدة يصعب تتبع آلية عملها وهو ما يُعرف بمشكلة «الصندوق الأسود»، الأمر الذي قد يُضعف من إمكانية مناقشة الدليل أمام القضاء، ويُثير تساؤلات حول مدى احترام ضمانات المحاكمة العادلة وحق الدفاع.

وفي السياق الليبي، لا يزال التعامل مع الأدلة الرقمية يخضع في الغالب للقواعد العامة في قانون الإجراءات الجنائية، دون تنظيم خاص يراعي خصوصية الأدلة الناتجة عن أنظمة الذكاء الاصطناعي، مما يفرض ضرورة تدخل تشريعي يحدد ضوابط قبول هذا النوع من الأدلة وحجيته (الورفلي، 2021).

الفرع الثاني: الصعوبات التقنية والقانونية في جمع وتحليل الأدلة الرقمية

تُعد مرحلة جمع وتحليل الأدلة الرقمية من أكثر المراحل تعقيدًا في الجرائم الإلكترونية الذكية نظرًا للطبيعة الفنية الخاصة لهذه الجرائم، وما تفرضه من تحديات تقنية وقانونية تؤثر في سلامة الدليل وفي قيمته الإثباتية.

أولًا: الصعوبات التقنية المرتبطة بجمع وتحليل الأدلة الرقمية

تواجه الجهات المختصة صعوبات تقنية متعددة عند جمع الأدلة الرقمية في الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي، من أبرزها سهولة محو البيانات أو تعديلها في زمن قياسي واستخدام تقنيات التشفير المتقدمة التي تحول دون الوصول إلى محتوى المعلومات محل الجريمة. كما أن اعتماد بعض الأنظمة الذكية على التخزين السحابي أو الخوادم الخارجية يُعقّد من عملية تحديد مكان الدليل وضمان سلامة سلسلة حيازته. (حسني، 2014).

وتزداد هذه الصعوبات تعقيدًا عندما يكون الدليل ناتجًا عن أنظمة ذكاء اصطناعي ذاتية التعلّم، إذ قد تتغير البيانات أو النتائج بمرور الوقت نتيجة تحديث الخوارزميات أو إعادة تدريب النماذج، مما يثير إشكاليات تتعلق بثبات الدليل وإمكانية إعادة فحصه.

غير أن خصوصية الدليل الرقمي، من حيث طبيعته غير المادية وقابليته للتغيير، تفرض ضرورة التحقق من سلامة إجراءات جمعه وحفظه، وضمان عدم العبث به، حفاظًا على قيمته الإثباتية، كما يقتضي الأمر التأكد من ارتباط الدليل بالواقعة محل الاتهام، وتوافر العلاقة السببية بينه وبين الفعل الإجرامي.

ثانيًا: الصعوبات القانونية في مباشرة إجراءات جمع وتحليل الأدلة الرقمية

إلى جانب التحديات التقنية، تبرز صعوبات قانونية تتعلق بإجراءات جمع الأدلة الرقمية وتحليلها، خاصة في ظل غياب تنظيم تشريعي خاص يُراعي خصوصية الجرائم الإلكترونية الذكية، ويُعد احترام مبدأ المشروعية الإجرائية من أبرز هذه الصعوبات، إذ قد يؤدي أي إخلال بضوابط التفتيش أو الضبط الإلكتروني إلى بطلان الدليل.

كما تثير الطبيعة العابرة للحدود للجرائم الإلكترونية إشكاليات تتعلق بالاختصاص القضائي والتعاون الدولي، لا سيما في الحالات التي تكون فيها البيانات محل الجريمة مخزنة خارج الإقليم الوطني. ويضاف إلى ذلك ما يفرضه استخدام الوسائل التقنية الحديثة من ضرورة التوفيق بين مقتضيات مكافحة الجريمة وضمان احترام الحقوق والحريات الفردية وعلى رأسها الحق في الخصوصية (الهلول، 2022).

وفي الإطار الليبي، يظل الاعتماد على القواعد العامة في قانون الإجراءات الجنائية غير كافٍ لمواجهة هذه التحديات، الأمر الذي يستدعي تطوير النصوص الإجرائية بما يتلاءم مع طبيعة الأدلة الرقمية المستحدثة.

الفرع الثالث: حجية الأدلة الرقمية ودور الخبرة الفنية في الإثبات الجنائي

تُثير الأدلة الرقمية في الجرائم الإلكترونية الذكية إشكاليات دقيقة تتعلق بحجيتها أمام القضاء الجنائي، ومدى اعتماد المحكمة عليها في تكوين عقيدتها، فضلًا عن الدور المحوري الذي تؤديه الخبرة الفنية في تفسير هذا النوع من الأدلة. (نجم، 2017).

أولًا: حجية الأدلة الرقمية في الإثبات الجنائي

تُعد حجية الدليل الجنائي الرقمي مسألة جوهرية في مجال الجرائم الإلكترونية الذكية، إذ يتوقف عليها مدى إمكانية اعتماد المحكمة على هذا الدليل في إثبات الواقعة الإجرامية ونسبتها إلى المتهم. ورغم عدم النص صراحة في التشريع الليبي على الأدلة الرقمية، فإن القواعد العامة في قانون الإجراءات الجنائية تجيز للمحكمة الأخذ بجميع الأدلة التي تطمئن إليها، متى كانت قد جُمعت بطرق مشروعة.

وفي هذا الإطار، يتجه الفقه الجنائي إلى الاعتراف بحجية الأدلة الرقمية متى استوفت الضوابط الفنية والقانونية، مع التأكيد على ضرورة تطوير الإطار التشريعي بما يواكب تطور وسائل الإثبات الحديثة (سرور، 2016).

ثانيًا: دور الخبرة الفنية في تفسير الأدلة الرقمية وتقييمها

تلعب الخبرة الفنية دورًا محوريًا في الجرائم الإلكترونية الذكية، نظرًا لتعقيد الأدلة الرقمية وصعوبة فهمها من قبل القاضي الجنائي دون الاستعانة بذوي الاختصاص الفني. ويظهر ذلك وضوح في تحليل البيانات الرقمية، وفحص مخرجات أنظمة الذكاء الاصطناعي، وبيان مدى موثوقيتها وسلامتها.

وتُسهم الخبرة الفنية في مساعدة المحكمة على تكوين عقيدتها، دون أن تُقيّدها برأي الخبير، إذ يظل القاضي صاحب السلطة التقديرية في الأخذ بنتائج الخبرة أو طرحها. غير أن الاعتماد المفرط على الخبرة الفنية، دون وجود معايير قانونية واضحة، قد يُثير مخاوف تتعلق بتغليب الجانب التقني على الضمانات القانونية.

وفي السياق الليبي تبرز الحاجة إلى تأهيل الخبراء الفنيين، ووضع ضوابط قانونية دقيقة تنظيم أعمال الخبرة في الجرائم الإلكترونية، بما يحقق التوازن بين فعالية الإثبات وضمان حقوق الدفاع.

ويستلزم تجاوز هذه الصعوبات توفر كفاءات تقنية متخصصة، واعتماد أدوات فنية دقيقة تضمن سلامة الدليل منذ لحظة جمعه وحتى عرضه أمام القضاء (حجازي 2018).

المبحث الثالث: الإطار القانوني لمواجهة الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي في التشريع الليبي

أفرز التطور المتسارع لتقنيات الذكاء الاصطناعي أنماطًا إجرامية مستحدثة اتسمت بطابع تقني معقد، تجاوز في كثير من صوره الإطار التقليدي للجريمة الجنائية. وقد فرض هذا الواقع تحديات تشريعية وقضائية متزايدة، لا سيما في مجال الجرائم الإلكترونية التي باتت تُرتكب باستخدام أنظمة ذكية قادرة على التعلم الذاتي والتصرف شبه المستقل.

وفي هذا السياق، يبرز التساؤل حول مدى كفاية الإطار القانوني الليبي القائم لمواجهة هذا النوع من الجرائم، ومدى قدرة النصوص الجنائية التقليدية والتشريعات الخاصة على استيعاب الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي. وانطلاقًا من ذلك، يُخصص هذا المبحث لدراسة التنظيم القانوني الليبي لمواجهة الجرائم الإلكترونية، وتحليل مدى ملاءمته للتطورات التقنية الحديثة، تمهيدًا لاستخلاص أوجه القصور واقتراح سبل التطوير التشريعي (بن عودة، 2022).

المطلب الأول: التنظيم القانوني للجرائم الإلكترونية في التشريع الليبي

يُعنى هذا المطلب بدراسة الإطار التشريعي الذي اعتمده المشرّع الليبي لمواجهة الجرائم الإلكترونية، مع التركيز على تطوره من الاعتماد على القواعد العامة في قانون العقوبات والإجراءات الجنائية، إلى تبني تنظيم تشريعي خاص تمثّل في صدور القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، وذلك بهدف بيان مدى كفاية هذا التنظيم في مواجهة الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي.

الفرع الأول: الأساس التشريعي لمواجهة الجرائم الإلكترونية قبل صدور قانون خاص

قبل صدور تشريع خاص يُنظّم الجرائم الإلكترونية، اعتمد المشرّع الليبي على القواعد العامة الواردة في قانون العقوبات وقانون الإجراءات الجنائية لمواجهة الأفعال الإجرامية المرتكبة باستخدام الوسائل الإلكترونية. وقد جرى تكييف هذه الأفعال وفق أوصاف تقليدية، مثل جرائم الاحتيال، والتزوير، والاعتداء على الأموال

أو على الحرية الشخصية، متى توافرت أركان الجريمة وشروطها القانونية (حسني، 2015).

غير أن هذا الأسلوب، القائم على القياس والتكييف، كشف عن قصوره في مواجهة الجرائم الإلكترونية ذات الطبيعة التقنية الخاصة، لا سيما تلك التي تعتمد على أنظمة ذكية معقدة، يصعب إخضاعها للمفاهيم التقليدية للسلوك الإجرامي والفاعل الجنائي. وقد أدى هذا القصور إلى تباين في التطبيقات القضائية، وإلى إثارة إشكاليات تتعلق بمبدأ الشرعية الجنائية ووضوح النصوص (الفيتوري، 2018).

الفرع الثاني: دور القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم إلكترونية

جاء صدور القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية استجابةً للتطور المتزايد في أنماط الجريمة الرقمية، ومحاولةً من المشرّع الليبي لسد الفراغ التشريعي الذي كان قائمًا في هذا المجال. وقد تضمّن هذا القانون تجريم

عدد من الأفعال التي تمس أمن نظم المعلومات، وسلامة البيانات الإلكترونية، وسرية الاتصالات، كما قرر لها عقوبات جنائية تتناسب مع خطورتها.

ويمثل هذا القانون خطوة تشريعية متقدمة مقارنة بالمرحلة السابقة، إذ أرسى إطارًا قانونيًا خاصًا لمكافحة الجرائم الإلكترونية، ووفّر أساسًا تشريعيًا يمكن من خلاله ملاحقة الأفعال الإجرامية المرتكبة عبر الوسائط الرقمية. غير أن الملاحظ أن نصوص القانون جاءت بصياغة عامة، ولم تُعالج بصورة صريحة الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي، ولا الأفعال التي تُرتكب بواسطة أنظمة ذاتية التعلّم، الأمر الذي يُبقي على عدد من الإشكاليات القانونية دون حل (المقريف، 2021).

الفرع الثالث: تقييم كفاية التنظيم القانوني الليبي في مواجهة الجرائم الإلكترونية الذكية

من خلال تحليل القواعد العامة والقانون رقم (5) لسنة 2022، يتبيّن أن التنظيم القانوني الليبي قد حقق تقدمًا ملحوظًا في مجال مكافحة الجرائم الإلكترونية، إلا أنه لا يزال قاصرًا عن استيعاب الجرائم الإلكترونية الذكية بكافة صورها. فغياب نصوص صريحة تُحدّد المسؤولية الجنائية عن الأفعال الصادرة عن أنظمة الذكاء الاصطناعي، وتُبيّن مركز كل من المبرمج والمستخدم والمشغّل، يُضعف من فعالية المواجهة الجنائية.

كما أن عدم تخصيص قواعد إجرائية خاصة بالإثبات الرقمي المتعلق بالأنظمة الذكية يُلقي بعبء كبير على القضاء في تكييف الوقائع وتقدير الأدلة، وهو ما قد يؤثر في تحقيق العدالة الجنائية. ومن ثم، تبرز الحاجة إلى تطوير التشريع الليبي، سواء بتعديل القانون رقم (5) لسنة 2022، أو باستحداث نصوص مكملة له، بما يواكب التطورات التقنية ويُحقق حماية جنائية فعالة في البيئة الرقمية (سعيد، 2022).

المطلب الثاني: أوجه القصور في التنظيم القانوني الليبي وموقف التشريعات المقارنة من الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي

يهدف هذا المطلب إلى تحليل أوجه القصور التي تعتري التنظيم القانوني الليبي في مواجهة الجرائم الإلكترونية المعتمدة على تقنيات الذكاء الاصطناعي، وذلك في ضوء القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، مع الاستعانة بالتجارب التشريعية المقارنة لاستخلاص أوجه التباين والاستفادة من الحلول التي تبنّتها بعض التشريعات الحديثة. ويُسهم هذا التحليل في تقييم مدى قدرة التشريع الليبي على مواكبة التطورات التقنية المتسارعة، تمهيدًا لاقتراح سبل تطويره.

الفرع الأول: أوجه القصور التشريعي في القانون الليبي لمكافحة الجرائم الإلكترونية

رغم ما مثّله القانون رقم (5) لسنة 2022 من نقلة نوعية في مجال مكافحة الجرائم الإلكترونية، إلا أن نصوصه تكشف عن عدد من أوجه القصور عند إسقاطها على الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي. ويأتي في مقدمة هذه القصور غياب تعريف تشريعي واضح لمفهوم الذكاء الاصطناعي، وعدم التمييز بين الجرائم الإلكترونية التقليدية وتلك التي تُرتكب بواسطة أنظمة ذكية قادرة على التعلّم الذاتي واتخاذ القرار. (القانون رقم (5) لسنة 2022).

كما يُلاحظ أن المشرّع الليبي لم يُحدّد على نحو دقيق نطاق المسؤولية الجنائية في حال تدخل أنظمة الذكاء الاصطناعي في ارتكاب الفعل الإجرامي، وهو ما يثير إشكالات عملية تتعلق بإسناد الجريمة، وتحديد الفاعل أو الشريك، خاصة في الحالات التي يتراجع فيها الدور البشري المباشر. ويُضاف إلى ذلك أن القانون لم يُخصّص أحكامًا إجرائية مميزة تتلاءم مع طبيعة الأدلة الرقمية الذكية، مكتفيًا بالقواعد العامة، الأمر الذي قد يُضعف من فعالية الملاحقة الجنائية.

الفرع الثاني: موقف التشريعات المقارنة من الجرائم الإلكترونية الذكية

اتجهت بعض التشريعات المقارنة إلى تبني مقاربة أكثر مرونة وشمولًا في مواجهة الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي، فقد سعى المشرّع الفرنسي، على سبيل المثال، إلى تطوير منظومته الجنائية من خلال توسيع نطاق التجريم المرتبط بالأنظمة المعلوماتية، وإدماج مفاهيم حديثة تتعلق بالمعالجة الآلية للبيانات، مع إسناد المسؤولية الجنائية إلى الشخص الطبيعي أو المعنوي الذي يسيطر فعليًا على النظام الذكي (السنوسي 2023).

كما اهتمت التشريعات الأوروبية بوجه عام، من خلال توجيهات الاتحاد الأوروبي، بوضع إطار قانوني يُنظّم استخدام الذكاء الاصطناعي، ويربط بين الابتكار التقني ومتطلبات الحماية الجنائية، مع التأكيد على ضرورة ضمان الشفافية وقابلية تتبع القرارات الصادرة عن الأنظمة الذكية[4]. ويُظهر هذا الاتجاه التشريعي وعيًا متزايدًا بخطورة الجرائم الإلكترونية الذكية، وحرصًا على تكييف النصوص القانونية بما يحدّ من إفلات مرتكبيها من العقاب.

الفرع الثالث: تقييم المقاربة الليبية في ضوء التجارب المقارنة

من خلال المقارنة بين التشريع الليبي وبعض التشريعات المقارنة، يتبيّن أن المشرّع الليبي لا يزال في مرحلة أولية من تنظيم الجرائم الإلكترونية، ولم يصل بعد إلى معالجة خصوصية الجرائم المعتمدة على الذكاء الاصطناعي بصورة شاملة. فبينما اتجهت التشريعات المقارنة إلى إدماج مفاهيم تقنية حديثة وتطوير قواعد المسؤولية الجنائية، ظل القانون الليبي محافظًا على صياغات عامة قد لا تستوعب التعقيد التقني لهذه الجرائم ا وعليه، تبرز الحاجة إلى مراجعة القانون رقم (5) لسنة 2022، سواء من خلال إدخال تعديلات تشريعية تُعنى صراحةً بالذكاء الاصطناعي، أو عبر سنّ تشريع مكمّل ينظم استخدام هذه التقنيات في المجال الجنائي، مستفيدًا من التجارب المقارنة، وبما يُحقق التوازن بين حماية المجتمع وتشجيع التطور التكنولوجي .

المطلب الثالث: الآليات التشريعية المقترحة لتطوير المواجهة الجنائية للجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي في ليبيا

يُعدّ تطوير المواجهة الجنائية للجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي ضرورة تشريعية تفرضها التحولات الرقمية المتسارعة، وتعقيد الأساليب الإجرامية الحديثة. وانطلاقًا من أوجه القصور التي تم رصدها في التنظيم القانوني الليبي، ولا سيما في القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، يسعى هذا المطلب إلى اقتراح جملة من الآليات التشريعية التي من شأنها تعزيز الحماية الجنائية في البيئة الرقمية الليبية، بما يحقق التوازن بين متطلبات الأمن السيبراني وضمانات الشرعية الجنائية.

الفرع الأول: تطوير السياسة التجريمية واستحداث نصوص خاصة بالجرائم الإلكترونية الذكية

يُقترح، في إطار تطوير السياسة التجريمية، أن يتجه المشرّع الليبي إلى استحداث نصوص جنائية صريحة تُجرّم الأفعال التي تُرتكب باستخدام تقنيات الذكاء الاصطناعي، مع وضع تعريف تشريعي واضح لهذه التقنيات يحدّد نطاقها وحدودها القانونية. ويُسهم هذا التحديد في تفادي الغموض التشريعي، وضمان احترام مبدأ الشرعية الجنائية القائم على الوضوح والتحديد (الورفلي، 2025).

كما يقتضي الأمر التمييز بين الجرائم الإلكترونية التقليدية والجرائم الإلكترونية الذكية، من حيث طبيعة السلوك الإجرامي ودرجة الخطورة، بما يسمح بتدرج العقوبة وتناسبها مع جسامة الفعل. ويُعدّ هذا التوجه من شأنه تمكين القضاء من تطبيق النصوص الجنائية بفعالية أكبر، والحد من التوسع غير المبرر في التفسير.

الفرع الثاني: إعادة تنظيم قواعد المسؤولية الجنائية في الجرائم المعتمدة على الذكاء الاصطناعي

تُثير الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي إشكاليات معقدة تتعلق بإسناد المسؤولية الجنائية، خاصة في الحالات التي تتراجع فيها سيطرة الإنسان على النظام الذكي.

ومن ثم، يُقترح أن يُعيد المشرّع الليبي تنظيم قواعد المسؤولية الجنائية، من خلال تحديد المركز القانوني لكل من مصمّم النظام، ومبرمجه، ومشغّله، والمستخدم النهائي، بحسب درجة السيطرة والتدخل في النشاط الإجرامي.

كما يُستحسن الأخذ بفكرة المسؤولية الجنائية القائمة على السيطرة الفعلية أو الإشراف التقني، على غرار ما ذهبت إليه بعض التشريعات المقارنة، وذلك بما يضمن عدم إفلات الجناة من العقاب، دون الإخلال بالمبادئ العامة للمسؤولية الجنائية القائمة على الخطأ الشخصي (الترهوني، 2022).

الفرع الثالث: تعزيز القواعد الإجرائية والإثبات الجنائي في البيئة الرقمية

لا يكتمل تطوير المواجهة الجنائية دون تحديث القواعد الإجرائية المرتبطة بالإثبات الجنائي في الجرائم الإلكترونية الذكية. ومن ثم، يُقترح إدراج نصوص إجرائية خاصة تُنظّم جمع الأدلة الرقمية، وتحليلها، وحفظها، مع الاعتراف الصريح بحجية الدليل الرقمي المستمد من الأنظمة الذكية، متى توافرت فيه شروط السلامة الفنية والقانونية (السنوسي، 2023).

كما تبرز أهمية تعزيز دور الخبرة الفنية المتخصصة في مجال الذكاء الاصطناعي والأمن السيبراني، من خلال إنشاء وحدات فنية مساعدة للنيابة العامة والقضاء، وتكريس التعاون بين الجهات القضائية والخبراء التقنيين، بما يُسهم في رفع كفاءة التحقيق والإثبات، وتحقيق العدالة الجنائية في البيئة الرقمية الحديثة (بن عودة، 2022).

الخاتمة

تناول هذا البحث موضوع الذكاء الاصطناعي في علاقته بالجرائم الإلكترونية، من زاوية قانونية جنائية، في ظل التحولات الرقمية المتسارعة التي يشهدها العالم المعاصر، وما أفرزته من أنماط إجرامية جديدة تتجاوز الأطر التقليدية للتجريم

والإثبات، وقد سعى البحث إلى بيان الدور المزدوج لتقنيات الذكاء الاصطناعي، سواء في تعزيز الأمن السيبراني ومكافحة الجريمة، أو في استغلالها كوسيلة لارتكاب جرائم إلكترونية ذكية تتسم بالتعقيد والخفاء.

ومن خلال التحليل الوصفي للنصوص القانونية، ولا سيما القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، إلى جانب المقارنة ببعض التشريعات العربية والأجنبية، توصّل البحث إلى أن التنظيم القانوني الليبي يُعد خطوة إيجابية، إلا أنه لا يزال قاصرًا عن استيعاب الخصوصية التقنية للجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي، سواء من حيث التجريم أو المسؤولية الجنائية أو قواعد الإثبات.

وقد خلص البحث إلى أن مواجهة هذا النوع من الجرائم تقتضي تبنّي مقاربة تشريعية شاملة، تجمع بين تحديث النصوص الجنائية، وتطوير القواعد الإجرائية، وتعزيز الخبرة الفنية، بما يضمن تحقيق التوازن بين متطلبات الحماية الجنائية وضمانات الشرعية وسيادة القانون في البيئة الرقمية.

النتائج:

أسفر البحث عن جملة من النتائج، من أبرزها:

1- أن الذكاء الاصطناعي أصبح عنصرًا فاعلًا في تطور الجريمة الإلكترونية، وأسهم في استحداث صور إجرامية جديدة يصعب كشفها بالوسائل التقليدية.

2- أن الجرائم الإلكترونية الذكية تتسم بخصوصية تقنية تجعل من الصعب تطبيق القواعد العامة للمسؤولية الجنائية عليها دون تعديل أو تفسير موسّع.

3- أن القانون الليبي رقم (5) لسنة 2022، رغم أهميته، لم يتناول صراحة الجرائم لمعتمدة على الذكاء الاصطناعي، ولم يضع تعريفًا تشريعيًا لهذه التقنيات.

4- أن قواعد الإثبات الجنائي التقليدية لا تكفي وحدها لمواجهة تحديات الإثبات في الجرائم الإلكترونية الذكية، خاصة فيما يتعلق بحجية الدليل الرقمي.

5- التشريعات المقارنة قطعت شوطًا متقدمًا في تنظيم استخدام الذكاء الاصطناعي وربط المسؤولية الجنائية بدرجة السيطرة التقنية والإشراف الفعلي.

التوصيات:

في ضوء ما انتهى إليه البحث من نتائج، يُوصى بما يلي:

1- تعديل القانون رقم (5) لسنة 2022 أو سنّ تشريع مكمّل، يتضمن نصوصًا صريحة تُعالج الجرائم الإلكترونية المعتمدة على الذكاء الاصطناعي.

2- إعادة تنظيم قواعد المسؤولية الجنائية بما يراعي خصوصية الأنظمة الذكية، من خلال ربط المسؤولية بدرجة السيطرة أو الإشراف أو التدخل البشري في النظام.

3- تطوير القواعد الإجرائية للإثبات الجنائي عبر الاعتراف الصريح بحجية الأدلة الرقمية الذكية، ووضع ضوابط قانونية لجمعها وتحليلها وحفظها.

4- تعزيز دور الخبرة الفنية المتخصصة في مجالي الذكاء الاصطناعي والأمن السيبراني، وإنشاء وحدات تقنية مساعدة للنيابة العامة والقضاء.

5- تأهيل القضاة وأعضاء النيابة وأجهزة الضبط القضائي من خلال برامج تدريبية متخصصة في الجرائم الإلكترونية الذكية.

6- الاستفادة من التجارب التشريعية المقارنة مع مراعاة خصوصية النظام القانوني الليبي ومتطلبات الواقع العملي.

المراجع

بو عامر، محمد زكي. (بدون تاريخ). الحماية الجنائية للمعلومات. الإسكندرية: دار الجامعة الجديدة.

أبوشناف، علي محمد. (2017). أصول المسؤولية الجنائية في القانون الليبي. بنغازي: منشورات جامعة قاريونس.

البحثل، علي محمد. (2022). التحقيق الجنائي في الجرائم الإلكترونية. طرابلس: دار الفرجاني.

الترهوني، سالم محمد. (2022أ). إسناد المسؤولية الجنائية في الجرائم المعلوماتية. مجلة العلوم القانونية، جامعة بنغازي،

الترهوني، سالم محمد. (2022ب). الجرائم الإلكترونية وإشكالات المسؤولية الجنائية. مجلة الدراسات القانونية، جامعة بنغازي، (3).

الزوي، مفتاح محمد. (2022). الجريمة الإلكترونية وإشكالات المواجهة الجنائية في التشريع الليبي. مجلة الدراسات القانونية، جامعة مصراتة.

السعيد، نجاة سالم عبد الرحمن. (2025). التعدي الإلكتروني والأمن المعلوماتي في ظل قانون الجرائم الإلكترونية الليبي رقم (5) لسنة 2022: دراسة مقارنة. مجلة جامعة الزيتونة، (53).

السنوسي، عادل عبد الكريم. (2020). الجريمة المعلوماتية وإشكالات الإثبات الجنائي. مجلة الدراسات القانونية، جامعة مصراتة، (4).

السنوسي، عادل عبد الكريم. (2023أ). الشرح العملي لقانون مكافحة الجرائم الإلكترونية الليبي. طرابلس: دار الجامعة الجديدة.

السنوسي، عادل عبد الكريم. (2023ب). نطاق التجريم في قانون مكافحة الجرائم الإلكترونية الليبي. مجلة الدراسات القانونية، جامعة طرابلس.

العبودي، صالح عبد الله. (2021). الجرائم الإلكترونية في ضوء التطور التقني. عمّان: دار الثقافة للنشر.

العجمي، عبد الله الدغش. (2014). المشكلات العملية والقانونية للجرائم الإلكترونية: دراسة مقارنة [رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط.

الفرجاني، عبد الله سالم. (2016). المسؤولية الجنائية في القانون الليبي. طرابلس: منشورات جامعة طرابلس.

الفيتوري، الصادق عبد الرحمن. (2018). شرح قانون العقوبات الليبي – القسم العام. بنغازي: دار الكتب الوطنية.

القانون رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، الجريدة الرسمية الليبية (2022).

القويري، مفتاح عبد السلام. (2019). الإثبات الجنائي في الجرائم المعلوماتية. مجلة القانون، جامعة طرابلس، (2).

المقريف، سالم عبد السلام. (2021أ). الجرائم المعلوماتية في التشريع الليبي. مجلة القانون، جامعة مصراتة، (1).

المقريف، سالم عبد السلام. (2021ب). الجرائم المعلوماتية وإشكالية التكييف القانوني في التشريع الليبي. مجلة القانون، جامعة مصراتة، (2).

الميري، عبد الرزاق محمد. (2024). المسؤولية الجنائية عن جرائم الذكاء الاصطناعي. المركز الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، (1).

الهادي، محمد علي. (2020). المسؤولية الجنائية عن الجرائم المعلوماتية. مجلة العلوم القانونية، جامعة طرابلس، (2).

الورفلي، علي حسين. (2021). الأدلة الرقمية في القانون الجنائي الليبي. بنغازي: دار الكتب الوطنية.

الورفلي، نهلة محمد مفتاح. (2025). قانون الجرائم الإلكترونية في الميزان: قراءة نقدية للقانون رقم (5) لسنة 2022. المجلة القانونية، بنغازي، (31).

بن عودة، محمد أمين. (2022أ). دور الخبرة الفنية في إثبات الجرائم الإلكترونية. المجلة الجزائرية للعلوم القانونية، (1).

بن عودة، محمد أمين. (2022ب). الذكاء الاصطناعي وتحديات السياسة الجنائية المعاصرة. المجلة الجزائرية للعلوم القانونية، (4).

حجازي، عبد الفتاح بيومي. (2018). الأدلة الإلكترونية وحجيتها في الإثبات الجنائي. الإسكندرية: دار الفكر الجامعي.

حجازي، عبد الفتاح بيومي. (2019). الجرائم الإلكترونية وحماية المعلومات. الإسكندرية: دار الفكر الجامعي.

حجازي، عبد الفتاح بيومي. (2020). الذكاء الاصطناعي والمسؤولية القانونية. الإسكندرية: دار الفكر الجامعي.

حسني، محمود نجيب. (2014). شرح قانون الإجراءات الجنائية. القاهرة: دار النهضة العربية.

حسني، محمود نجيب. (2015). شرح قانون العقوبات – القسم العام. القاهرة: دار النهضة العربية.

سرور، أحمد فتحي. (2016). الوسيط في قانون الإجراءات الجنائية. القاهرة: دار الشروق.

عبد الرحيم، أحمد شوقي. (2021). المسؤولية الجنائية عن أفعال الآلات الذكية. مجلة القانون والاقتصاد، جامعة القاهرة، (1).

قاسم، مراد محمد غالب محمد. (2024). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة مقارنة. المجلة العصرية للدراسات القانونية، جامعة تعز، (2).

منصور، محمد حسين. (2019). الأمن السيبراني وحماية المعلومات. القاهرة: دار النهضة العربية.

نجم، محمد صبحي. (2017). الإثبات الجنائي في الجرائم المعلوماتية. عمّان: دار الثقافة.