وزارة التعليم العالي والبحث العلمي
جامعة عباس لغرور – خنشلة–
كلية الحقوق العلوم السياسية

القسم: الحقوق

الحماية القانونية من جرائم الذكاء الاصطناعي

مذكرة مكملة لنيل شهادة الماستر في شعبة: الحقوق

تخصص: قانون جنائي وعلوم جنائية

إعداد الطالب:
– تريكي منير

إشراف الأستاذة:
– د. مامن بسمة

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
العالية نوال	أستاذ محاضر أ	جامعة عباس لغرور –خنشلة–	رئيسا
مامن بسمة	أستاذ محاضر أ	جامعة عباس لغرور –خنشلة–	مشرفا مقررا
سلامي نادية	أستاذ	جامعة عباس لغرور –خنشلة–	عضوا مناقش

السنة الجامعية:

2026/2025

بسم الله الرحمن الرحيم

شكر وعرفان

الشكرُ أولًا وأخيرًا للهِ عزَّ وجلَّ، الذي بنعمته تتمُّ الصالحات وبفضله تتيسّر الأمور وتُنجز الأعمال له الحمدُ على ما أنعم وأولى وله الشكرُ على توفيقه وإعانته في إتمام هذا العمل.

ثمّ أتقدّم بخالص الشكر وعظيم الامتنان إلى الأستاذة المشرفة "مامن بسمة"، التي تفضّلت بالإشراف على هذا العمل، ولم تبخل عليّ بتوجيهاتها القيّمة ونصائحها السديدة وكان لإرشاداتها الأثر الكبير في إخراجه في صورته النهائية فجزاها الله عني خير الجزاء.

كما أتوجّه بجزيل الشكر إلى أساتذتي الأفاضل، الذين كان لهم الفضل في تكويني العلمي والمعرفي، بما قدّموه من علم وتوجيه وإرشاد خلال مسيرتي الدراسية.

وفي الختام، أسأل الله أن يجعل هذا العمل خالصًا لوجهه الكريم، وأن ينفع به، وأن يجزي كل من ساهم فيه خير الجزاء.

الإهداء

إلى من كان لهم الفضل الأول في كل ما وصلتُ إليه، إلى من حملوا عني مشقة الطريق قبل أن أبدأه.

إلى من جعل الله الجنة تحت أقدامها، إلى نبع الحنان ومصدر الدعاء الذي لا ينقطع، أمي الغالية التي كانت ولا تزال سندي الذي ما انحنى أدامها الله لي نورًا في حياتي.

إلى من أحمل اسمه، إلى رمز العطاء والتضحية، إلى ظلي الذي سبق خطايا، إلى معلم فلسفة الثبات أبي الغالي حفظه الله وأطال في عمره.

إلى إخوتي الأعزاء رفقاء الدرب، شركاء الفرح والتعب، صدورا اتسعت لي حين ضاقت بي الدنيا.

إليهم جميعًا أهدي ثمرة هذا الجهد المتواضع، عرفانًا وامتنانًا، ودعاءً بأن يجزيهم الله خير الجزاء وأن يديم علينا نعمة السند والمحبة والتوفيق.

مقدمة

مقدمة:

شهد العالم خلال العقود الأخيرة تطورًا تكنولوجيًا متسارعًا، في المجالات الرقمية وتقنيات المعلومات والاتصال، الأمر الذي أدى إلى بروز أنظمة ذكية تعتمد على تقنيات الذكاء الاصطناعي والتي أصبحت تمثل ركيزة أساسية في مختلف المجالات مناحي الحياة الاقتصادية، الاجتماعية، الأمنية والعلمية والقانونية.

فقد أدى الانتشار الواسع لهذه التقنيات إلى ظهور أنماط جديدة من الجرائم الإلكترونية التي تختلف في طبيعتها وآلياتها عن الجرائم التقليدية، أين غدت الأنظمة الذكية تستخدم في تنفيذ عمليات اختراق إلكترونية معقدة، التلاعب بالبيانات والمعلومات، وانتحال الشخصيات الرقمية، والتزييف العميق للمحتوى السمعي والبصري والاحتيال الإلكتروني، إضافة إلى تطوير برمجيات خبيثة قادرة على التعلم والتكيف مع وسائل الحماية الأمنية الأمر الذي جعل هذه الجرائم تشكل تحدّياً حقيقياً أمام الأنظمة القانونية التقليدية التي لم تعد قادرة في كثير من الأحيان على استيعاب هذه الأفعال الإجرامية الجديدة أو توفير الحماية الكافية لمواجهتها.

أهمية الموضوع:

ومن هذا المنطلق أصبح موضوع "الحماية القانونية من جرائم الذكاء الاصطناعي" من أهم الموضوعات القانونية الحديثة التي فرضت نفسها بقوة على الساحة التشريعية، الفقهية والقضائية، باعتباره يرتبط بصورة مباشرة بحماية الأمن الرقمي وضمان سلامة المعاملات الإلكترونية والحفاظ على الحقوق والحريات الأساسية للأفراد في البيئة الرقمية، إذ يكتسي هذا الموضوع أهمية بالغة في ظل التطور السريع للتقنيات الرقمية، كما يبرز لمحاولة بيان مدى كفاية التشريعات الحالية لمواجهة الجرائم المرتبطة بالذكاء الاصطناعي والكشف عن أوجه القصور القانونية والإجرائية في مكافحتها.

أسباب اختيار الموضوع:

1. الأسباب الذاتية:

- الرغبة الشخصية في دراسة المواضيع القانونية الحديثة المرتبطة بالتكنولوجيا الرقمية والذكاء الاصطناعي.
- الرغبة في الإسهام العلمي في معالجة موضوع حديث يمس الواقع العملي والتطور التقني المعاصر، وتنمية الرصيد المعرفي في مجال الجرائم الإلكترونية.

2. الأسباب الموضوعية:

- حداثة موضوع جرائم الذكاء الاصطناعي وقلة الدراسات القانونية العربية المتخصصة فيه.
- قصور بعض النصوص القانونية التقليدية عن استيعاب الجرائم المرتبطة بالأنظمة الذكية.

أهداف الموضوع:

تهدف هذه الدراسة إلى تحقيق جملة من الأهداف القانونية المتعلقة بمكافحة جرائم الذكاء الاصطناعي والمتمثلة في:

أهداف علمية:

تسعى هذه الدراسة إلى توضيح مفهوم جرائم الذكاء الاصطناعي وبيان خصائصها وصورها المختلفة، مع تحليل الإطار القانوني المنظم لها وإبراز الإشكالات المرتبطة بالمسؤولية القانونية والحماية الجزائية.

أهداف عملية:

تعمل هذه الدراسة على تقييم مدى نجاعة التشريعات الحالية في مواجهة التحديات التي تفرضها تقنيات الذكاء الاصطناعي، والكشف عن مكامن العجز في النصوص التشريعية

والإجرائية القضائية مع اقتراح حلول وآليات قانونية حديثة من شأنها تعزيز فعالية الحماية الجزائية وضمان التوازن بين مواكبة التطور التكنولوجي وصون الأمن القانوني للأفراد والمجتمع.

إشكالية البحث:

وبناءً على ما تقدم، تبرز الإشكالية الرئيسة لهذه الدراسة على النحو التالي:

- إلى أي مدى استطاعت المنظومة القانونية توفير حماية قانونية فعالة لمواجهة جرائم الذكاء الاصطناعي في ظل التطور التكنولوجي المتسارع وتعدد صور هذه الجرائم؟

وهذه الإشكالية تتضمن في جوانبها أفكاراً مترابطة يمكن تفصيلها في شكل تساؤلات فرعية، يشكل كل واحد منها محوراً من المحاور الأساسية لهذا البحث والتي تجمل فيما يلي:

1. ما هو مفهوم الذكاء الاصطناعي؟ وما أبرز خصائصه التقنية والقانونية؟
2. ما المقصود بجرائم الذكاء الاصطناعي؟ وماهي أهم صورها وأنواعها؟
3. كيف تقوم المسؤولية الجزائية للمستخدم في جرائم الذكاء الاصطناعي؟
4. ما الصعوبات القانونية المرتبطة بإثبات المسؤولية الجزائية في جرائم الذكاء الاصطناعي؟
5. فيم تمثلت النصوص القانونية التي يعتمد عليها التشريع الجزائري في مواجهة جرائم الذكاء الاصطناعي؟
6. ما أبرز النقائص والعيوب التي تعاني منها الحماية الجزائية الحالية في التشريع الجزائري؟
7. كيف عالجت التشريعات المقارنة، خاصة الأوروبية والأمريكية والآسيوية جرائم الذكاء الاصطناعي؟
8. ما الآفاق المستقبلية الكفيلة بتطوير التشريع الجزائري وتعزيز الحماية القانونية من جرائم الذكاء الاصطناعي؟

صعوبات الدراسة:

واجهت هذه الدراسة جملة من الصعوبات، تمثلت أساسًا في حداثة موضوع جرائم الذكاء الاصطناعي وتشعبه بين الجوانب القانونية والتقنية، إضافة إلى قلة المراجع المتخصصة التي تناولت الموضوع بصورة دقيقة ومفصلة، كما شكل التطور السريع للتقنيات الذكية وتعدد صور الجرائم المرتبطة بها صعوبة الإحاطة الشاملة بمختلف جوانب الدراسة.

الدراسات السابقة:

ومن بين أبرز الدراسات التي تناولت هذا الموضوع دراسة الباحثة مشتة نسرين بعنوان "المسؤولية الجزائية عن جرائم الذكاء الاصطناعي" المنشورة في مجلة الدراسات القانونية سنة 2025 حيث استفدت منها في كونها تناولت قواعد المسؤولية الجزائية التقليدية لمواجهة جرائم الذكاء الاصطناعي، كما اتجهت دراسة وليد سعد الدين محمد سعيد بعنوان "المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي" في عنصر التشريعات المقارنة خاصة الأمريكية والأوروبية ما منح الدراسة طابعًا معاصرًا وإضافات ثمينة تستحق التقدير.

منهج البحث:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي باعتباره المنهج الأنسب لدراسة هذا الموضوع، حيث يتم من خلاله وصف ظاهرة جرائم الذكاء الاصطناعي وبيان خصائصها وصورها المختلفة ضف إلى ذلك تحليل النصوص القانونية المرتبطة بها، كما تم الاستعانة بالمنهج المقارن عند دراسة بعض التشريعات الأجنبية والتجارب الدولية المتعلقة بتنظيم الذكاء الاصطناعي ومكافحة الجرائم المرتبطة به بغرض الاستفادة من الحلول التشريعية المقارنة في تطوير المنظومة القانونية الوطنية.

خطة البحث:

اقتضت طبيعة الموضوع تقسيم الدراسة إلى فصلين رئيسيين:

يتناول الفصل الأول الإطار المفاهيمي لجرائم الذكاء الاصطناعي حيث يتم التطرق إلى مفهومها وطبيعتها، ثم بيان أهم أنواعها وصورها المختلفة.

أما الفصل الثاني فعنون بالحماية الجزائية من جرائم الذكاء الاصطناعي وذلك من خلال دراسة آليات الحماية القانونية وسبل تطوير المواجهة التشريعية والإجرائية لهذه الجرائم.

واختتمت هذه الدراسة بخاتمة تحتوي مجموعة النتائج التي تم التوصل إليها بالإضافة إلى مجموعة من التوصيات.

الفصل الأول

الإطار المفاهيمي لجرائم الذكاء الاصطناعي

تمهيد:

يمثل الذكاء الاصطناعي أحد أبرز مظاهر التطور الرقمي المعاصر، لما يقدمه من قدرة على التعلم وتحليل المعطيات، واتخاذ القرارات بصورة شبه مستقلة، إضافة إلى اعتباره أداة تقنية مساعدة في العديد من المجالات كالصحة، الاقتصاد، الأمن، القضاء...

ولكن رغم مزايا هذه التقنية إلا أن هذا لا ينفي وجود سلبيات تتمثل في أنماط مستحدثة من السلوك الإجرامي سواء من خلال استغلال هذا النظام كوسيلة لارتكاب الجرائم أو استهداف هذه الأنظمة بحد ذاتها بالاعتداء أو التخريب أو السرقة.

وأمام هذه المستجدات احتاجت الدراسة لتحديد الإطار المفاهيمي للذكاء الاصطناعي من خلال تحديد مفهومه وكذلك خصائصه، حتى نتمكن من فهم الأساس للحماية الجزائية من جرائم الذكاء الاصطناعي.

بحيث سنتناول هذا الفصل في مبحثين:

المبحث الأول: ماهية الذكاء الاصطناعي:

يعتبر الذكاء الاصطناعي من أبرز التحولات التكنولوجية التي يشهدها العالم، لما يتمتع به من قدرة على تقليد الذكاء البشري القانوني ومحاكاته من حيث: التعلم، التحليل، اتخاذ القرارات، ونظرا لارتباط جرائم الذكاء الاصطناعي بهذه الأنظمة وخصائصها التقنية فإن فهم ماهية الذكاء الاصطناعي يعد أمرا ضروريا لضبط الإطار القانوني له، وعليه ندرس هذا المبحث من حيث مفهوم وخصائص هذا النظام حتى يتم دراسة الجرائم المرتبطة به من حيث مفهومها وأنواعها، وسيتم تقسيم هذا المبحث كما يلي:

المطلب الأول: مفهوم الذكاء الاصطناعي:

مع التطور التكنولوجي المعاصر ظهرت أنظمة ذكية أصبحت قادرة على وظائف كانت صعبة على الإنسان كالتعلم والاستدلال وكذلك اتخاذ قرارات في كثير من المجالات المعرفية وهو ما أطلق عليه "الذكاء الاصطناعي" (إسماعيل ع.، 2017، صفحة 15).

ويقصد به عموما تلك الأنظمة المعلوماتية القادرة على محاكاة القدرات الذهنية البشرية، وهذا اعتمادا على خوارزميات وتحليل بيانات يحملها هذا النظام، غير أن هذا المفهوم يظل محل تطور مستمر تبعا لتطور التكنولوجيا، مما يفرض علينا تناول تعريفه القانوني وخصائصه تمهيدا لدراسة انعكاساته.

في هذا المطلب سنتطرق لتعريف الذكاء الاصطناعي في الفرع الأول، ويتم تناول خصائص أنظمة الذكاء الاصطناعي في الفرع الثاني.

الفرع الأول: تعريف الذكاء الاصطناعي:

يعتبر الذكاء الاصطناعي من أبرز المفاهيم التقنية المعاصرة التي أثارت اهتمام الباحثين في مجالات عدة، منها علوم الحاسوب والقانون ونظرا لتعدد تطبيقاته وتطور

أنظمته، فقد تعددت تعريفاته، وسنقدمه في تعريف لغوي واصطلاحي وكذلك تعريف تقني وقانوني وهذا وفقا لما يلي:

أولا. التعريف اللغوي والاصطلاحي للذكاء الاصطناعي:

1-التعريف اللغوي: يتكون مصطلح الذكاء الاصطناعي من كلمتين:

*الذكاء: يدل على الفطنة وسرعة الفهم والقدرة على الإدراك والاستنتاج.

*الاصطناعي: يقصد به ما يصنعه الإنسان أو ما يكون غير طبيعي (منظور، قاموس لسان العرب، 1994، صفحة 281)، وبذلك فإن الذكاء الاصطناعي لغة يعني الذكاء المصنوع بواسطة الإنسان.

2_التعريف الاصطلاحي: يقصد به فرع من فروع علم الحاسوب يهتم بتصميم وتطوير أنظمة وبرامج قادرة على تقليد القدرات الذهنية للإنسان مثل: التعلم، الاستنتاج، اتخاذ القرارات، حل المشكلات، بهدف تمكين الآلات من أداء مهام تتطلب عادة ذكاءً بشريًا (هاشم رشيدة، ملياني عبد الوهاب، 2024، صفحة 10).

3_التعريف التقني: يعرفه كل من المؤلفين "ستيوارت راسل" و "بيتر نوفيغ" على أنه "فرع من فروع المعلوماتية يهتم بدراسة وتصميم العوامل أو الأنظمة الذكية، بحيث أنها برامج ذكية تستطيع إدراك البيئة التي تعمل فيها، ثم تتخذ قرارات أو أفعال تساعدها على تحقيق أهداف معينة بنجاح" (بيترنورفينغ، صفحة 2).

ثانيا. التعريف القانوني:

يقصد به الأنظمة التقنية التي تعمل بشكل مستقل نسبيا وهذا اعتمادا على بيانات وخوارزميات تهدف إلى تحليل المعلومات واتخاذ القرارات أو تقديم توصيات قد يكون لها أثر قانوني على الأفراد (الأوروبية، مقترح اللائحة الأوروبية بشأن الذكاء الإصطناعي، 2021، صفحة 40)، وهذا يدل على أن الذكاء الاصطناعي جعل الحاسوب أو الآلة قادرين على

التفكير أو التصرف أو اتخاذ قرار كما يفعل العقل البشري الإنساني في بعض المهام كفهم المعلومات أو البيانات، أو التعلم من المكتسبات القبلية والتعلم من التجارب السابقة، واتخاذ قرارات مناسبة وحل مشكلات.

الفرع الثاني: خصائص أنظمة الذكاء الاصطناعي:

تتميز أنظمة الذكاء الاصطناعي بمجموعة من الخصائص التقنية التي تميزها عن برامج المعلوماتية التقليدية، والتي تجعل هذه الأخيرة قادرة على القيام بهمام معقدة وكانت قديما صعبة على العقل البشري، كما أن هذه الخصائص تثير العديد من الإشكالات القانونية خاصة من حيث المسؤولية الجزائية، وسنتناول هذه الخصائص في عدة عناوين:

أولا. الاستقلالية النسبية: تتمتع أنظمة الذكاء الاصطناعي بدرجة من الاستقلالية في أداء المهام واتخاذ القرارات دون تدخل مباشر من الإنسان بعد تشغيلها، حيث تعتمد على خوارزميات متقدمة تمكنها من تحليل المعطيات واختيار أفضل الحلول الممكنة وتختلف هذه الاستقلالية من نظام إلى آخر، فقد تكون محدودة في بعض التطبيقات وقد تصل إلى درجة عالية في الأنظمة المتقدمة مثل السيارات ذاتية القيادة والروبوتات الذكية والبرامج الحاسوبية الذكية الأمر الذي يثير إشكالات قانونية تتعلق بتحديد المسؤولية الجزائية عند وقوع الضرر أو الجريمة (الله ع.، 2018، صفحة 60).

ثانيا. القدرة على التعلم الذاتي: تعد هذه الخاصية من أبرز خصائص أنظمة الذكاء الاصطناعي، حيث يمكن لهذه الأخيرة التعلم من البيانات والتجارب السابقة باستخدام تقنيات التعلم الآلي، مما يسمح لها بتطوير أدائها وتحسين نتائجه مع مرور الوقت دون الحاجة إلى إعادة برمجتها بشكل مباشر من قبل الإنسان (العبد، 2019، صفحة 120).

ثالث. السرعة العالية في معالجة البيانات: تتميز أيضا هذه الأنظمة بقدرتها الكبيرة على معالجة وتحليل كم هائل من البيانات في وقت قصير جدا مقارنة بالقدرات البشرية الأمر

الذي يجعلها فعالة في العديد من المجالات مثل: الطب، الأمن السيبراني، والتحليل المالي (حمودة، 2019، صفحة 110).

رابعا. صعوبة التنبؤ بالسلوك: من الخصائص التي تثير جدلا قانونيا، صعوبة التنبؤ بسلوك أنظمة هذه التقنية في بعض الحالات خاصة تلك التي تعتمد على التعلم الذاتي هذه الأنظمة قرارات أو تقوم بأفعال لم يتوقعها المبرمجون لها نتيجة تحليلها للبيانات وتفاعلها مع البيئة المحيطة (الخطيب، 2020، صفحة 14).

خامسا. القدرة على محاكاة الذكاء البشري: تسعى هذه التقنية إلى محاكاة القدرات الذهنية للإنسان مثل: التفكير، التحليل، الاستنتاج واتخاذ القرارات وتظهر هذه القدرة في العديد من التطبيقات مثل المساعدات الرقمية وأنظمة التعرف على الصوت والصورة والأنظمة الخبيرة (محمد م.، 2015، صفحة 150).

سادسا. الاعتماد على البيانات الضخمة: تعتمد هذه الأنظمة في عملها على كم هائل من البيانات تعرف بالبيانات الضخمة، حيث يتم جمعها وتحليلها واستخلاص الأنماط منها من أجل تحسين أداء النظام ودقة نتائجه فكلما زادت كمية البيانات المتاحة للنظام ازدادت قدرته على التعلم والتنبؤ واتخاذ القرارات بشكل أكثر دقة (الرحيم، 2020، صفحة 90).

سابعا. الطابع غير المادي للذكاء الاصطناعي: يتميز الذكاء الاصطناعي بطابع غير مادي إذ يتمثل أساسا في برامج وخوارزميات رقمية تعمل داخل الأنظمة المعلوماتية، ولا يرتبط وجوده بالضرورة بكيان مادي مستقل، رغم إمكانية تجسيده أحيانا في أجهزة أو روبوتات وهذا الطابع يثير إشكالات قانونية تتعلق بتحديد المسؤولية القانونية عن الأفعال الصادرة عن هذه الأنظمة (إسماعيل م.، 2018، صفحة 160).

ثامنا. القدرة على اتخاذ القرار: تتمتع هذه التقنية بالقدرة على اتخاذ القرارات بناء على تحليل المعطيات والبيانات المتاحة، حيث تقوم الخوارزميات بمعالجة المعلومات واختيار البديل الأكثر ملائمة وفقا للمعايير المبرمجة فيها، وتبرز هذه الخاصية في العديد من التطبيقات

مثل الأنظمة الخبيرة وأنظمة الدعم في اتخاذ القرار، وهو ما يثير إشكالات قانونية تتعلق بمدى مسؤولية الإنسان عن القرارات التي تتخذها هذه الأنظمة (الدايم، 2016، صفحة 70).

تاسعا. القدرة على التكيف مع البيئة: يتميز هذا النظام بقدرته على التكيف مع البيئة المحيطة به، حيث يستطيع تعديل سلوكه واستراتيجياته بناء على التغيرات التي تطرأ على المعطيات أو الظروف المحيطة ويظهر ذلك في العديد من التطبيقات مثل الروبوتات الذكية وأنظمة القيادة الذاتية التي تتفاعل مع محيطها وتتخذ قرارات مناسبة وفقا للظروف المتغيرة (الغني، 2017، صفحة 300).

عاشرا. الطابع التفاعلي للذكاء الاصطناعي: لهذا النظام طابع تفاعلي يسمح له بالتفاعل مع المستخدمين أو مع الأنظمة الأخرى، حيث يمكن استقبال الأوامر أو البيانات والاستجابة لها بطريقة ذكية تحاكي التفاعل البشري وتظهر هذه الخاصية في تطبيقات عديدة مثل المساعدات الرقمية وأنظمة المحادثة الآلية وأنظمة خدمة العملاء الذكية (خليل، 2015، صفحة 21).

المطلب الثاني: المقصود بجرائم الذكاء الاصطناعي:

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى ظهور أنماط جديدة من السلوك الإجرامي، لم تكن مألوفة من ظل الأنظمة التقليدية، حيث أصبحت هذه التقنيات تستعمل كوسيلة حديثة ومتطورة لارتكاب الجرائم أو كفاعل شبه مستقل في بعض الحالات، وإذا كان الذكاء الاصطناعي في جوهره أداة لخدمة الإنسان، فإن سوء استخدامه أو استغلال خصائصه التقنية قد يؤدي إلى نتائج خطيرة تمس بالأمن المعلوماتي والاقتصادي والاجتماعي، وتكمن خصوصية جرائم هذا النظام بأنها قادرة على التعلم الذاتي واتخاذ القرار، مما يدفع إلى طرح إشكالات قانونية تتعلق بتحديد المفهوم الدقيق لهذه الجرائم وتمييزها عن غيرها من جرائم المعلوماتية القديمة، كما يثير تعدد صور استخدام هذه الأنظمة صعوبة في

فهم أنواع الجرائم التي يمكن أن تنشأ عنها، خاصة مع تداخلها مع بعض أنواع الجرائم الإلكترونية كالاعتداء على المعطيات، التزوير الرقمي (إبراهيم، الذكاء الاصطناعي والمسؤولية الجنائية، 2022، صفحة 45).

وعليه يقتضي الأمر الوقوف على المقصود بجرائم الذكاء الاصطناعي ثم تبيان أنواعها وصورها المستحدثة، وسنتناول هذا المطلب في الفرعين التاليين خصصنا الفرع الأول للحديث عن المقصود بجرائم الذكاء الاصطناعي اما الفرع الثاني فخصصناه للحديث عن أنواع جرائم الذكاء الاصطناعي.

الفرع الأول: المقصود بجرائم الذكاء الاصطناعي:

نظرا لحداثة موضوع جرائم الذكاء الاصطناعي وتشعبه بين مجالات متعددة، فقد تعددت التعريفات التي تناولته بحسب الزاوية التي ينظر إليه منها، ويمكن تبيان ذلك من التعريفات التالية:

أولا. المقصود بجرائم الذكاء الاصطناعي لغة واصطلاحا:

أ/ لغة: يقصد بالجريمة كل فعل يخالف القانون أو الخروج عن القواعد والنظم العامة، أما الذكاء الاصطناعي فهو تركيب لغوي يدل على القدرة على الفهم أو الإدراك والمحاكاة والشيء المصنوع.

وعليه يمكن تعريف جرائم الذكاء الاصطناعي لغويا بأنها: "الأفعال غير المشروعة المرتبطة باستخدام الذكاء المحاكي لذكاء الإنسان" (منظور، لسان العرب، 1984، صفحة 89).

ب/ اصطلاحا: تعرف جرائم الذكاء الاصطناعي بأنها كل سلوك غير مشروع يتم باستخدام تقنيات الذكاء الاصطناعي أو موجه ضدها، ويترتب عليه ضرر مادي أو معنوي (حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، صفحة 18).

ج/ تقنيا: من الناحية التقنية تعرف جرائم الذكاء الاصطناعي بأنها كل نشاط غير قانوني يتم باستخدام أنظمة تعتمد على الخوارزميات والتعلم الآلي، والتي تمكن الآلة من تحليل البيانات واتخاذ القرارات بشكل شبه مستقل (نورفينغ، 2021).

ثانيا. المقصود بجرائم الذكاء الاصطناعي قانونيا:

لا يوجد تعريف قانوني موحد لجرائم الذكاء الاصطناعي إلا أنه يمكن استخلاص تعريف عام موحد مفاده: كل فعل مجرم قانونا يتم باستخدام أنظمة الذكاء الاصطناعي أو ينشأ عن تشغيلها ويؤدي إلى المساس بمصلحة محمية قانونا (الأوروبية، قانون الذكاء الإصطناعي، 2021).

كما ترتبط هذه الجرائم بإشكالية المسؤولية القانونية عن أفعال الأنظمة الذكية (منصور، المسؤولية الإلكترونية، 2009، صفحة 45).

الفرع الثاني: أنواع جرائم الذكاء الاصطناعي:

تتعدد جرائم الذكاء الاصطناعي بتعدد مجالات استخدام هذه التقنية وتطورها المستمر إذ يمكن أن تستعمل كوسيلة لارتكاب الجرائم وكأداة مساعدة، بل وقد تسهم في إحداث أنماط إجرامية مستحدثة وعليه يمكن تصنيف جرائم الذكاء الاصطناعي إلى التالي:

أولا. الجرائم المرتكبة بواسطة الذكاء الاصطناعي:

ويقصد بها التي يستخدم فيها الذكاء الاصطناعي كأداة لتنفيذ الفعل الإجرامي دون أن يكون له إرادة مستقلة، وإنما يتم توجيهه من قبل الإنسان ومن أبرز صورها:

. التزييف العميق وانتحال الشخصيات.

. الاختراقات السيبرانية المعتمدة على التعلم الآلي حيث تسهم هذه الأنظمة في زيادة دقة الجريمة وصعوبة اكتشافها، وهو ما يشكل تحديا للسلطات الجنائية (عبد الرزاق بن عبد العزيز المرجان، زياد فايز الجندي، 2024، صفحة 10).

ثانيا. الجرائم الناتجة عن السلوك المستقل للذكاء الاصطناعي:

في بعض الحالات قد تتصرف أنظمة الذكاء الاصطناعي بشكل شبه مستقل نتيجة التعلم الذاتي، مما يؤدي إلى وقوع أفعال ضارة دون تدخل مباشر من الإنسان مثل:

. حوادث السيارات ذاتية القيادة

. أخطاء الخوارزميات في أنظمة التوظيف أو القروض

وهنا يثور إشكال قانوني حول تحديد المسؤولية الجزائية: هل تقع على المبرمج؟ أم المستخدم؟ أم النظام ذاته؟ (حجازي، المسؤولية المدنية عن أضرار الأنترنيت، 2020، صفحة 215).

ثالثا. الجرائم الموجهة ضد أنظمة الذكاء الاصطناعي:

وهي الجرائم التي تستهدف أنظمة الذكاء الاصطناعي ذاتها مثل:

. التلاعب بالبيانات

. سرقة الخوارزميات أو النماذج الذكية

. الهجمات على أنظمة التعلم الآلي

وتمثل هذه الجرائم تهديدا مباشر للأمن المعلوماتي خاصة في القطاعات الحساسة (أحمد أ.، 2025، صفحة 120).

رابعا. الجرائم الناتجة عن إساءة استخدام تطبيقات الذكاء الاصطناعي:

تتمثل في استغلال نتائج الأنظمة الذكية في ارتكاب أفعال غير مشروعة:

. نشر معلومات مضللة أو أخبار زائفة

. انتهاك حقوق الملكية الفكرية

. التلاعب بالرأي العام عبر المنصات الرقمية

وتزداد خطورة هذه الجرائم بسبب الانتشار الواسع للأنظمة الذكية وسهولة الوصول إليها (الأوربية، 2021، صفحة 15).

وهذا المبحث يتناول تعريف للذكاء الاصطناعي باعتباره أنظمة تحاكي القدرات الذهنية للإنسان في التعلم واتخاذ القرار، ويتناول خصائصه كالاستقلالية النسبية، كما يوضح أن جرائم الذكاء الاصطناعي هي أفعال غير مشروعة ترتكب باستخدام هذه التقنيات أو ضدها، وتتنوع أشكالها مما يطرح تحديات قانونية جديدة.

المبحث الثاني: المسؤولية الجزائية الناتجة عن جرائم الذكاء الاصطناعي:

سندرس في هذا المبحث المسؤولية الجزائية عن جرائم الذكاء الاصطناعي، مع بيان تعدد الأطراف المتدخلة فيها كالمستخدم المبرمج والمطور والمزود والأساس القانوني لمسؤولية كل منهما سواء على أساس القصد الجنائي أو الخطأ، إضافة إلى صعوبات الإثبات وإمكانية قيام المسؤولية المشتركة، ومن هنا سنقسم هذا المبحث إلى مطلبين:

المطلب الأول: المسؤولية الجزائية للمستخدم:

تثير المسؤولية الجزائية للمستخدم في نطاق جرائم الذكاء الاصطناعي إشكاليات قانونية دقيقة باعتبار أن هذه الجرائم لا تنفصل عن تدخل العنصر البشري الذي يوجه ويستعمل الأنظمة الذكية، فرغم الطبيعة التقنية لهذه الأنظمة، يظل المستخدم العنصر الأساسي الذي يضفي على الفعل طابعه المشروع، ويحدد مدى وقوع المسؤولية الجزائية عليه، وسنتناول هذا المطلب في فرعين:

الفرع الأول: القصد الجنائي في جرائم الذكاء الاصطناعي:

يشكل القصد الجنائي الركن المعنوي الذي تقوم عليه المسؤولية الجزائية إذ يمكن إرادة الفاعل نحو ارتكاب الفعل المجرم، وفي مجال جرائم الذكاء الاصطناعي يعطي هذا الركن أهمية خاصة نظرا لطبيعة هذه الأنظمة، مما يستدعي بحث مدى توافر القصد الجنائي لدى الفاعل عند القيام بأفعال غير مشروعة بهذه التقنية.

ويتخذ القصد الجنائي في هذا المجال صورتين:

أولا. القصد الجنائي العام:

ويتمثل في العلم بالفعل والإرادة في ارتكابه، كمن يستخدم برنامجا ذكيا لاختراق نظام معلوماتي (حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، 2007، صفحة 40).

ثانيا. القصد الجنائي الخاص:

ويقوم عندما يتطلب نية خاصة، مثل نية الإضرار بالغير أو تحقيق منفعة غير مشروعة كما في جرائم الاحتيال الإلكتروني باستخدام الذكاء الاصطناعي (القانونية، 2019، صفحة 85).

يتحقق القصد الجنائي في جرائم الذكاء الاصطناعي عندما يستخدم الفاعل النظام الذكي عن علم وإرادة لارتكاب الفعل المجرم قانونا (العقوبات، المادة 41، 8 يونيو 1966)، ويعد هذا الركن أساسيا لتقرير المسؤولية الجزائية إذ يميز بين الاستخدام المشروع للنظام وبين الاستخدام الموجه لإحداث أضرار وانتهاك القوانين (العقوبات، المادة 288، 8 يونيو 1966).

وكذلك نرى بأن مجرد تشغيل النظام الذكي أو التعامل معه لا يكفي لإثبات المسؤولية الجزائية بل يجب أن يثبت أن الفاعل كان مدركا للطبيعة المجرمة للفعل وعمد إلى (العام، 1989، صفحة 456) تنفيذه مستخدما الوسيلة الذكية لتحقيق هذا الغرض

وأيضا عنصر القصد الجنائي في جرائم الذكاء الاصطناعي يجب تفسيره بمرونة، بحيث يشمل الإدراك للفعل المجرم وليس الإرادة العامة، فعدم فهم خصائص هذا النظام الذكي قد يخفف المسؤولية، بينما الاستخدام المتعمد للنظام لتحقيق نتائج محظورة قانونا يحقق القصد الجنائي كاملا.

وهنا يمكننا القول إن القصد الجنائي يشكل الركيزة الأساسية للمسؤولية الجزائية في جرائم الذكاء الاصطناعي.

الفرع الثاني: ركن الخطأ وسوء استخدام الأدوات الذكية:

في جرائم الذكاء الاصطناعي، تتحقق المسؤولية الجزائية أيضا عبر الخطأ أو الإهمال مثل سوء استخدام الأنظمة الذكية أو باستعمالها بطريقة غير مشروعة أو غير حذرة، مما يؤدي إلى نتائج ضارة ويجعل الفاعل مسؤولا.

ويعد ركن الخطأ عنصرا أساسيا في المسؤولية الجزائية للمستخدم عند ارتكاب فعل مجرم، ويظهر هذا في الحالات التالية:

أولا. الإهمال: يقصد به التقصير في اتخاذ الاحتياطات اللازمة عند التعامل مع الأنظمة الذكية، مثل عدم متابعة التحديثات الأمنية لنظام أو تجاهل التحذيرات الخاصة بالأمان الرقمي، ويترتب على هذا الإهمال حدوث أضرار قد تكون مادية أو معنوية للغير ويشكل قاعدة لتطبيق المسؤولية الجزائية (نريمان، 2017، صفحة 134_157).

ومثال ذلك عدم حماية خوارزميات التعلم الآلي التي تتحكم في عمليات مالية قد يؤدي إلى اختراقات وسرقة أموال العملاء.

ثانيا. التهور: يعرف بأنه استخدام النظام بطريقة غير مدروسة، دون التحقق من النتائج المحتملة أو المخاطر المصاحبة، مما يترتب عليه وقوع أضرار غير مقصودة.

ويعتبر التهور خطأ جزئيا حتى في غياب القصد الجنائي المباشر (الجزائر، 2020، صفحة 112).

وكأبسط مثال على هذا السماح بتشغيل روبوتات الذكاء الاصطناعي في بيئة حرجة دون اختبارات أمان كافية، مما يؤدي إلى أضرار جسدية أو مادية.

ثالثا. سوء استخدام الأدوات الذكية: يشمل هذا استخدام هذه التقنية لتحقيق أغراض غير مشروعة، مثل التلاعب بالبيانات أو التزوير الإلكتروني، حتى في غياب النية المباشرة

للإضرار بالآخرين (الله م.، دراسة ماجستير الخطأ الجنائي وسوء إستخدام الذكاء الإصطناعي، 2021، صفحة 68.55).

رابعا. العلاقة السببية بين الفعل والنتيجة: تتحقق المسؤولية الجزائية عندما يثبت وجود خطأ مرتبط بالضرر الناتج عن استخدام النظام الذكي إذ يتطلب ذلك تحليلا دقيقا لإمكانية توقع المستخدم لنتيجة الضارة ومدى معرفته بالخطأ المرتكب (ج، 8يونيو 1966، صفحة 41 288).

وقد أشارت الفقهية الحديثة إلى ضرورة تقييم القدرة التقنية للمستخدم ومدى تمكنه من التحكم في النظام أو معرفة مخاطره، باعتباره معيارا لتحديد درجة الخطأ (صالح م.، 2019، صفحة 105.88).

خامسا. الخطأ التقني والفني: لا يقتصر الخطأ على السلوك الشخصي للمستخدم بل يمتد أيضا إلى الإخفاق في الالتزام بالمعايير التقنية، مثل تجاهل بروتوكولات الأمان أو عدم مراقبة الخوارزميات بشكل دوري، يعد هذا النوع من الأخطاء أحد أسباب تحميل المسؤولية الجزائية على المستخدم خاصة إذا أدى إلى نتائج ضارة للغير (أمين، 2024، صفحة 83 85).

وكمثال على ذلك: عدم اختبار خوارزمية الذكاء الاصطناعي قبل نشرها في بيئة حيوية قد يؤدي إلى إخفاق النظام وتضرر الأشخاص.

سادسا. أثر التكرار والاستمرارية في الخطأ: ينظر في القضاء الجزائري والفقه المعاصر إلى تكرار الأخطاء والاستمرار في سلوك يشتمل على تهور وإهمال يعزز المسؤولية الجزائية، ويزيد من شدتها، خصوصا عند التعامل مع أنظمة ذكية حساسة مثل الذكاء الاصطناعي الطبي أو المالي (حمدي، 2020، صفحة 56.33).

وهنا نرى بأن ركن الخطأ في جرائم الذكاء الاصطناعي يتأسس على الإهمال أو التهور أو سوء استخدام الأدوات الذكية، إضافة إلى الأخطاء التقنية وتقوم المسؤولية الجزائية بوجود

علاقة سببية بين الفعل والضرر مع إمكانية توقعه كما يؤدي تكرار الخطأ إلى تشديد هذه المسؤولية خاصة في المجالات الحساسة.

المطلب الثاني: المسؤولية الجزائية للمبرمج والمطور والمزود:

توسع نطاق المسؤولية الجزائية في مجال جرائم الذكاء الاصطناعي، بحيث لا يقتصر على المستخدم فقط، بل يمتد ليشمل المبرمجين والمطورين والمزودين الذين يساهمون في تصميم وتشغيل هذه الأنظمة، وهؤلاء يلعبون دورا جوهريا في تحديد سلوك النظام الذكي، سواء من خلال برمجته أو تحديثه أو توفيره للغير، الأمر الذي قد يؤدي إلى قيام مسؤوليتهم الجزائية متى ثبت وجود خطأ تقني أو إهمال في مراحل التطوير أو النشر، كما تزداد أهمية هذا الطرح بالنظر إلى تعقيد الأنظمة الذكية وصعوبة تتبع مصدر الخطأ، مما يطرح إشكالات قانونية دقيقة تتعلق بالإثبات وتوزيع المسؤولية بين مختلف المتدخلين، وسنتناول هذا المطلب في فرعين:

الفرع الأول: خطأ التصميم والإهمال الرقمي:

يعد خطأ التصميم والإهمال التقني من أبرز صور المسؤولية الجزائية للمبرمج والمطور، إذ تنشأ هذه المسؤولية عند وجود خلل في برمجة النظام أو التقصير في اختباره وتأمينه، مما يؤدي إلى نتائج ضارة أو غير مشروعة، ويترتب عن هذا الخطأ مساءلة جزائية متى ثبت أن الفاعل لم يلتزم بالمعايير التقنية الواجبة أو أهمل في توقع المخاطر المحتملة.

أولا. الأساس القانوني لمسؤولية المبرمج والمطور والمزود: خطأ التصميم والإهمال الرقمي من أهم الأسس التي تبنى عليها المسؤولية الجزائية للمبرمج والمطور والمزود في مجال الذكاء الاصطناعي، نظرا للدور المحوري الذي يلعبه هؤلاء في إنشاء الأنظمة الذكية وتحديد كيفية عملها، وهو ما يفرض عليهم بضمان سلامة هذه الأنظمة واحترامها للقواعد القانونية (سليمان، شرح قانون العقوبات القسم العام: النظرية العامة للمسؤولية الجزائية، 2010، صفحة 312).

ثانيا. مفهوم خطأ التصميم في أنظمة الذكاء الاصطناعي: يتحقق خطأ التصميم عندما يكون النظام الذكي معيبا في بنيته الأساسية، سواء بسبب خلل في الخوارزميات أو قصور في منطق اتخاذ القرار، مما يؤدي إلى نتائج غير مشروعة أو ضارة، كالمساس بالمعطيات الشخصية أو التمييز بين الأفراد، وهو ما يعد إخلال بالمعايير التقنية الواجب احترامها (نصر الله، حوراء عزيز، الزهيري، رشا موسى، 2026، صفحة 7).

ثالثا. صور الإهمال التقني ومعياره المهني: الإهمال التقني يتمثل في تقصير المبرمج أو المطور في أداء واجباته المهنية، كعدم إخضاع النظام للاختبارات اللازمة أو إغفال تحديثه لسد الثغرات الأمنية، ويقاس هذا الإهمال بمعيار الشخص المعتاد في نفس الظروف المهنية (شيماء، 2025، صفحة 45_50).

رابعا. قيام المسؤولية الجزائية على الخطأ الغير عمدي: تقوم المسؤولية الجزائية متى توافرت عناصر الخطأ الغير عمدي من إهمال أو عدم القيام بالاحتياط إلى جانب تحقق الضرر وقيام علاقة سببية بين الخطأ والنتيجة، وفقا للقواعد العامة في قانون العقوبات (مروشن، 2026، صفحة 78.44)

خامسا. صعوبة تحديد المسؤولية في ظل تعقيد الأنظمة الذكية: تزداد صعوبة تحديد المسؤولية في هذا المجال بسبب تعقيد الأنظمة الذكية وتعدد المتدخلين في تصميمها، مما يفرض ضرورة اعتماد معايير دقيقة لتحديد الخطأ وتوزيع المسؤوليات بين مختلف الأطراف (بوسقيعة ل.، الوجيز في القانون الجزائي العام، 2017، صفحة 145).

وهنا نجد أن المسؤولية الجزائية للمبرمج والمطور تقوم على خطأ التصميم والإهمال التقني متى أدى إلى ضرر، ويقدر هذا الخطأ وفق المعيار المهني الحريص مع صعوبة تحديد المسؤولية بسبب تعقيد أنظمة الذكاء الاصطناعي وتعدد المتدخلين فيها.

الفرع الثاني: صعوبة الإثبات والمسؤولية المشتركة:

تعد مسألة إثبات المسؤولية الجزائية في جرائم الذكاء الاصطناعي من أبرز التحديات التي تواجه الأنظمة القانونية الحديثة، نظرا للطبيعة التقنية المعقدة لهذه الأنظمة وتداخل العوامل المؤثرة في عملها، فخلافا للجرائم التقليدية، حيث يمكن تحديد الفاعل والركن المادي بسهولة نسبية، يطرح الذكاء الاصطناعي إشكالات عميقة تتعلق بإمكانية تتبع مصدر القرار وتحديد المسؤول عنه.

وتبرز أولى هذه الصعوبات في ما يعرف بغموض الخوارزميات أو "الصندوق الأسود" حيث تعتمد العديد من أنظمة الذكاء الاصطناعي، خاصة تلك القائمة على التعلم العميق، على نماذج غير شفافة تجعل من الصعب فهم الكيفية التي يتم بها اتخاذ القرار، حتى من قبل المطورين أنفسهم، وهو ما ينعكس سلبا على إمكانية إثبات الخطأ أو تحديد مصدره بدقة (الزهراء، 2022، صفحة 83)، كما أن هذا الغموض ينعكس بشكل مباشر على صعوبة إثبات العلاقة السببية، التي تعد ركنا أساسيا لقيام المسؤولية الجزائية، إذ يصبح من العسير الربط بين الفعل المرتكب والنتيجة الإجرامية في ظل تدخل معطيات تقنية معقدة ومتغيرة (القادر ز.، 2020، صفحة 128).

إلى جانب ذلك، يزداد الأمر تعقيدا بسبب تعدد الأطراف المتدخلة في تصميم وتشغيل أنظمة الذكاء الاصطناعي، حيث تشمل هذه المنظومة كلا من المبرمج والمطور والمزود، إضافة إلى المستخدم النهائي، وهو ما يؤدي إلى تداخل الأدوار وتوزع المسؤوليات، ويجعل من الصعب إسناد الفعل الإجرامي إلى طرف واحد بشكل دقيق (أحمد م.، 2021، صفحة 147)، وفي ظل هذا التداخل، قد يكون الخطأ ناتجا عن خلل في التصميم، أو قصور في البيانات، أو سوء استخدام من قبل المستخدم، مما يعقد عملية الإثبات.

وأمام هذه الإشكالات، اتجه الفقه القانوني إلى تبني فكرة المسؤولية المشتركة كحل عملي، تقوم على توزيع المسؤولية بين مختلف الأطراف بحسب درجة مساهمتهم في إحداث

الضرر، وقد تأخذ هذه المسؤولية طابعا تضامنيا في الحالات التي يتعذر فيها تحديد المسؤول بشكل دقيق (خالد، 2023، صفحة 61)، ويهدف هذا الاتجاه إلى تحقيق نوع من العدالة من خلال عدم إفلات أي طرف ساهم في الخطأ من المساءلة.

كما ظهرت اتجاهات فقهية حديثة تدعو إلى التخفيف من عبء الإثبات الواقع على عاتق الضحية، من خلال اعتماد قرائن قانونية أو افتراض الخطأ في بعض الحالات، خاصة عندما يتعلق الأمر بأنظمة معقدة يصعب فهمها أو التحكم فيها، وهو ما من شأنه تعزيز حماية الضحايا وضمان فعالية المتابعة الجزائية (سمير ب.، 2021، صفحة 218).

وفي الأخير، يتضح أن صعوبة الإثبات في جرائم الذكاء الاصطناعي تفرض ضرورة تدخل تشريعي لتطوير قواعد خاصة تتلاءم مع هذا النوع من الجرائم، سواء من حيث وسائل الإثبات أو من حيث تحديد المسؤوليات، مما يحقق التوازن بين متطلبات العدالة الجنائية وتشجيع الابتكار التكنولوجي.

خلص هذا الفصل إلى تناول الإطار المفاهيمي لجرائم الذكاء الاصطناعي من خلال تعريف هذا النظام وبيان خصائصه القائمة على التعلم الذاتي والاستقلالية وصعوبة التنبؤ بسلوكه، كما يوضح مفهوم جرائمه التي تشمل استخدامه كوسيلة إجرامية أو استهداف أنظمته عبر الاختراق أو التلاعب، ويبين أن هذه الجرائم تتنوع بين جرائم رقمية تقليدية مطورة وجرائم موجهة ضد الأنظمة الذكية نفسها، كما يناقش المسؤولية الجزائية للمستخدم التي تقوم على القصد الجنائي أو الخطأ وسوء الاستخدام، ويخلص إلى إشكالية مسؤولية المبرمج والمطور وصعوبة الإثبات، مما يؤدي إلى تبني فكرة المسؤولية المشتركة.

الفصل الثاني

الحماية الجزائية من جرائم الذكاء الاصطناعي في التشريع الجزائري و آفاق تطويرها

تمهيد:

يشهد الذكاء الاصطناعي تطورا متسارعا أدى إلى بروز أنماط جديدة من الجرائم التي تتطلب تدخلا قانونيا فعالا، وقد سعى المشرع الجزائري إلى مواجهة هذه التحديات من خلال مجموعة من النصوص القانونية ذات الصلة، رغم أنها لم توضع خصيصا لهذا المجال، غير أن هذه الحماية لاتزال تواجه عدة نقائص، أبرزها غياب تنظيم تشريعي دقيق يواكب خصوصية الجرائم المرتبطة بالذكاء الاصطناعي.

لذلك يبرز الاهتمام بدراسة مدى كفاية الإطار القانوني الحالي وتحليل أوجه القصور فيه كما يقتضي الأمر الاستفادة من التجارب المقارنة واقتراح آفاق تطوير تعزز الحماية الجزائية في الجزائر، وسنتناول هذا الفصل في مبحثين:

المبحث الأول: الإطار القانوني للحماية الجزائية:

يعد تحديد الإطار القانوني للحماية الجزائية من جرائم الذكاء الاصطناعي خطوة أساسية لفهم مدى قدرة التشريع الجزائري على مواهة هذه الظاهرة المستحدثة، فقد اعتمد المشرع على مجموعة من القوانين العامة والخاصة لتنظيم الجرائم المرتبطة بالتكنولوجيا الحديثة، غير أن هذه النصوص رغم أهميتها لم تصنع خصيصا لمجال الذكاء الاصطناعي، مما يطرح إشكالات في التطبيق، كما تكشف الممارسة عن وجود ثغرات قانونية تحد من فعالية الحماية الجزائية، لذلك تبرز الحاجة إلى تحليل هذه النصوص وبيان حدودها ونقاط ضعفها، ويقسم هذا المبحث إلى مطلبين:

المطلب الأول: النصوص القانونية المطبقة حاليا:

يدرس هذا المطلب النصوص القانونية المعمول بها في الجزائر لمواجهة الجرائم المرتبطة بالتكنولوجيا الحديثة وتشمل هذه النصوص قانون العقوبات وقانون الجرائم الإلكترونية وحماية البيانات الشخصية، غير أن تطبيقها على جرائم الذكاء الاصطناعي يثير تحديات بسبب عدم تخصيصها لهذا المجال، وسنقسم هذا المطلب في الفرعين التاليين:

الفرع الأول: مواجهة جرائم الذكاء الاصطناعي في قانون العقوبات:

يعالج هذا الفرع دور قانون العقوبات في مواجهة جرائم الذكاء الاصطناعي، ويعد إطارا عاما لتجريم بعض الأفعال المرتبطة بها، إلا أن فعاليته تبقى محدودة لعدم تخصيصه لهذا المجال.

ويعد قانون العقوبات الجزائري الإطار العام الذي ينظم تجريم الأفعال الماسة بنظام العام والأشخاص والممتلكات حيث يشكل المرجع الأساسي في غياب نصوص خاصة بجرائم الذكاء الاصطناعي (الشعبية، 8 يونيو 1966).

وتكمن أهميته في كونه يوفر قواعد عامة يمكن من خلالها تكييف العديد من الأفعال المرتكبة باستخدام التقنيات الحديثة، مما في ذلك تطبيقات الذكاء الاصطناعي ضمن الجرائم التقليدية.

ففيما يتعلق بجرائم الاحتيال الإلكتروني، يمكن تطبيق أحكام نص المادة 372 من قانون العقوبات التي تجرم النصب والاحتيال وهذا على الأفعال التي تتم عبر الوسائل الرقمية أو باستخدام أنظمة ذكية، متى توافرت أركان الجريمة من احتيال وخداع بقصد الاستلاء على مال الغير.

كما يمكن إدراج أفعال انتحال الهوية الرقمية ضمن الجرائم الماسة بالأشخاص خاصة إذا ترتب عنها ضرر مادي أو معنوي (بوسقيعة ل.، الوجيز في القانون الجزائي العام ، 2013، صفحة 215).

ومن جهة أخرى، تطبق نصوص حماية الحياة الخاصة على الأفعال التي تتضمن جمع أو نشر بيانات شخصية دون إذن، حتى وإن تم ذلك باستخدام تقنيات الذكاء الاصطناعي مثل تحليل الصور أو الأصوات أو البيانات الشخصية (القادر ز.، 2019، صفحة 100.85).

ويلاحظ أن القضاء يمكنه توسيع تفسير هذه النصوص لتشمل الأفعال المستحدثة استنادا إلى مبدأ مرونة النص الجنائي في مواجهة التطورات التقنية.

غير أن تطبيق قانون العقوبات في هذا المجال يواجه عدة صعوبات، أبرزها تعقيد الوسائل التقنية وصعوبة تحديد الفاعل الحقيقي، خاصة في ظل استخدام أنظمة ذكية تعمل بشكل شبه مستقل مما يطرح إشكاليات في إسناد المسؤولية الجزائية (محمد ب.، 2021، صفحة 120 . 140).

وعليه رغم أهمية قانون العقوبات في توفير حماية جزائية عامة، إلا أن فعاليته تبقى محدودة في مواجهة جرائم الذكاء الاصطناعي مما يستدعي تدخل المشرع لتحديث النصوص أو سن تشريعات خاصة تراعي خصوصية هذه الجرائم وتطورها المستمر.

الفرع الثاني: مواجهة جرائم الذكاء الاصطناعي في قانون الجرائم الإلكترونية 09ـ04

يعد القانون 09ـ04 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الإطار التشريعي الأساسي في الجزائر لمواجهة الجرائم الإلكترونية وهو يشكل حجر الأساس للحماية الجزائية في مواجهة الأفعال المرتبطة بالذكاء الاصطناعي وإن لم ينظم هذا الأخير بشكل صريح.

أولا. نطاق تطبيق القانون:

يشمل هذا القانون مختلف الجرائم المرتكبة عبر الأنظمة المعلوماتية، مثل الدخول غير المشروع إلى الأنظمة، المساس بسلامة البيانات، عرقلة سير الأنظمة، ونشر أو تداول محتويات غير مشروعة.

وبذلك يمكن تطبيقه على العديد منصور جرائم الذكاء الاصطناعي خاصة عندما يستعمل كوسيلة لارتكاب الجريمة، مثل: الهجمات السيبرانية الذكية أو الاحتيال الرقمي (ش، 05 أوت 2009).

ثانيا. صور التجريم ذات الصلة بالذكاء الاصطناعي:

يتضمن القانون عدة أفعال مجرمة يمكن إسقاطها على جرائم الذكاء الاصطناعي من أبرزها:

ـ الدخول أو البقاء غير المشروع في نظام معلوماتي.

ـ حذف أو تعديل أو إدخال بيانات بطريقة احتيالية.

ـ عرقلة أو تعطيل سير نظام معلوماتي.

ـ نشر أو استخدام بيانات بطرق غير مشروعة.

وتبرز أهمية هذه النصوص في أنها تعطي الأفعال التي قد تنفذ باستخدام تقنيات الذكاء الاصطناعي، مثل: اختراق الأنظمة عبر خوارزميات متقدمة أو التلاعب بالبيانات باستخدام نماذج ذكية (القادر ب.، 2018، صفحة 130.112).

ثالثا. الآليات الإجرائية التي جاء بها القانون:

لم يقتصر هذا القانون على التجريم فقط بل أقر آليات إجرائية خاصة منها:

ـ إنشاء هيئات مختصة بمكافحة الجرائم الإلكترونية.

ـ منح السلطات صلاحيات في المراقبة الإلكترونية واعتراض الاتصالات.

ـ إلزام مزودي خدمات الإنترنيت بالتعاون مع الجهات القضائية.

وهذه الآليات تعد ضرورية في تتبع الجرائم المرتبطة بالذكاء الاصطناعي خاصة بالنظر إلى طابعها العابر للحدود وصعوبة كشف مرتكبيها (محمد ب.، 2020، صفحة 85_102).

رابعا. حدود تطبيق القانون على جرائم الذكاء الاصطناعي:

رغم أهمية القانون إلا أنه يواجه عدة نقائص عند تطبيقه على جرائم الذكاء الاصطناعي، أبرزها:

ـ عدم وجود نصوص صريحة تتناول الذكاء الاصطناعي ككيان قانوني أو كوسيلة إجرامية مستقلة.

ـ صعوبة تكييف بعض الأفعال الحديثة مثل التزييف العميق

ـ عدم مواكبة التطور السريع لتقنيات الذكية.

وبالتالي يبقى هذا القانون إطارا عاما يمكن الاستناد إليه لكنه غير كافي لمواجهة التحديات المستجدة التي يطرحها الذكاء الاصطناعي (فاطمة، 2021، صفحة 55 70).

خامسا. تقييم قانوني:

يمكن القول إن القانون 09ـ04 يوفر حماية جزائية مهمة لكنه تقليدي، إذ يركز على النظام المعلوماتي دون التعمق في خصوصية الذكاء الاصطناعي، مما يستدعي تدخلا تشريعيا لتحديثه أو استكماله بنصوص خاصة (سمير ل.، 2019، صفحة 60 75).

الفرع الثالث: مواجهة جرائم الذكاء الاصطناعي في قانون حماية البيانات الشخصية 18ـ07

يشكل هذا القانون إطارا قانونيا أساسيا لتعزيز الحماية الجزائية في مواجهة الجرائم المرتبطة بالتطورات التكنولوجية، وعلى رأسها تطبيقات الذكاء الاصطناعي التي تعتمد

بشكل كبير على جمع ومعالجة البيانات (الرسمية، 10 جوان 2018، صفحة المادة 2ـ10).

أولا. نطاق تطبيق القانون:

يهدف هذا القانون إلى حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم ذات الطابع الشخصي حيث يشمل جمع المعطيات التي تعمل بها هذه البيانات، مثل: الجمع، التسجيل، التخزين، التعديل أو النقل.

ويطبق على المعالجة الآلية أو غير الآلية وهو ما يجعله وثيق الصلة بأنظمة الذكاء الاصطناعي التي تقوم على التحليل الآلي للمعطيات (الرحمان، 2021، صفحة 120-150).

ثانيا. الضوابط القانونية لمعالجة البيانات:

أقر المشرع الجزائري مجموعة من الشروط التي يجب احترامها من بينها:

ـ مشروعية المعالجة وارتباطها بهدف محدد.

ـ الحصول على رضا صريح من الشخص المعني.

ـ احترام مبدأ التناسب وعدم الإفراط في جمع البيانات.

ـ ضمان حماية المعطيات من الاختراق أو التسريب.

وتعد هذه الضوابط ضرورية للحد من الانحرافات التي قد تنتج عن استخدام الذكاء الاصطناعي في تحليل البيانات الشخصية (أحمد ب.، 2020، صفحة 260-275).

ثالثا. الآليات الجزائية المقررة:

يتضمن القانون 07-18 مجموعة من الجزاءات الجنائية التي تهدف إلى ردع الاعتداءات على البيانات الشخصية ومن أبرزها:

- تجريم المعالجة غير المشروعة للبيانات الشخصية.
- معاقبة كل من يقوم بجمع البيانات بوسائل احتيالية أو غير قانونية.
- تجريم إفشاء أو نشر البيانات دون إذن صاحبها.
- فرض عقوبات على الإخلال بالتزامات أمن المعلومات.

وتتراوح العقوبات بين الحبس والغرامة بحسب خطورة الفعل والضرر الناتج عنها (ليلى، 2022، صفحة 88-105).

رابعا. دور القانون في مواجهة جرائم الذكاء الاصطناعي:

يساهم هذا القانون بشكل غير مباشر في الحد من جرائم الذكاء الاصطناعي من خلال:

- تقييد استخدام البيانات في تدريب الخوارزميات دون موافقة.
- حماية الأفراد من الاستغلال غير المشروع لبياناتهم في الأنظمة الذكية.
- توفير أساس قانوني لمساءلة المسؤولية عن خروقات البيانات في البيئات الرقمية.

غير أن هذا الدور يظل محدودا بسبب عدم تضمين نصوص صريحة تتعلق بالقرارات الآلية أو المسؤولية عن أخطاء الأنظمة الذكية (كمال، 2021، صفحة 55-70).

خامسا. تقييم قانوني:

رغم أن القانون 07ـ18 يمثل خطوة مهمة نحو تعزيز الحماية القانونية للبيانات الشخصية إلا أنه لا يواكب بشكل كامل التطورات السريعة في مجال الذكاء الاصطناعي مما يستدعي تحديثه أو استكماله بنصوص خاصة أو أكثر دقة ومرونة (مراد، 2023، صفحة 14ـ165).

الفرع الرابع: مواجهة جرائم الذكاء الاصطناعي في القوانين المكملة:

إلى جانب قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقانون حماية البيانات الشخصية، توجد مجموعة من القوانين المكملة التي يمكن الاستناد إليها في مواجهة بعض جرائم الذكاء الاصطناعي، وذلك بالنظر إلى الطبيعة المتشعبة لهذه الجرائم وارتباطها بعدة مجالات قانونية وتقنية ومن أهم هذه القوانين:

أولا. قانون التوقيع والتصديق الإلكتروني:

يعد القانون رقم 15ـ04 المتعلق بالتوقيع والتصديق الإلكتروني من النصوص المهمة التي تساهم بصورة غير مباشرة في مكافحة جرائم الذكاء الاصطناعي، خاصة الجرائم المرتبطة بالتزوير الرقمي وانتحال الهوية الإلكترونية والتلاعب بالمحررات الرقمية.

فقد أقر هذا القانون الحجية القانونية للوثائق والتوقيعات الإلكترونية، ووضع آليات تقنية وقانونية للتحقق من صحة المعاملات الإلكترونية وتأمينها (المتعلق بالتوقيع والتصديق الإلكتروني، 2015).

وتظهر أهمية هذا القانون في مواجهة بعض تطبيقات الذكاء الاصطناعي التي قد تستعمل لتقليد التوقيعات أو تزوير المستندات الرقمية أو إنشاء هويات وهمية باستعمال تقنيات التزييف العميق، الأمر الذي يهدد الثقة في المعاملات الإلكترونية ويستوجب حماية قانونية فعالة

ثانيا. قانون التجارة الإلكترونية:

ساهم القانون 18ـ05 المتعلق بالتجارة الإلكترونية في توفير حماية قانونية للمعاملات التجارية الرقمية، خاصة فيما يتعلق بحماية المستهلك الإلكتروني وتأمين المعاملات عبر الإنترنيت (الأمر 18ـ05 المتعلق بالتجارة الإلكترونية، 2018).

وتبرز أهميته في التصدي لبعض الجرائم التي قد ترتكب بواسطة أنظمة الذكاء الاصطناعي، مثل الاحتيال الإلكتروني والإعلانات المضللة وسرقة البيانات البنكية واختراق المنصات التجارية.

كما ألزم هذا القانون الموردين الإلكترونيين باحترام قواعد الشفافية وحماية المعطيات الشخصية، وهو ما يعزز الرقابة القانونية على استخدام تقنيات الذكاء الاصطناعي داخل المنصات الرقمية.

ثالثا. قانون حقوق المؤلف والحقوق المجاورة:

يؤدي القانون 03ـ05 المتعلق بحقوق المؤلف والحقوق المجاورة دورا مهما في حماية المصنفات الفكرية من الاعتداءات التي قد تنتج عن استخدام تقنيات الذكاء الاصطناعي، خاصة مع انتشار البرامج القادرة على انتاج النصوص والصور والأعمال الفنية بصورة آلية (الأمر 03ـ05 المتعلق بحقوق المؤلف والحقوق المجاورة، 2003).

وتثار في هذا المجال عدة إشكالات قانونية تتعلق بنسبة المصنفات المنتجة بواسطة الذكاء الاصطناعي، ومدى اعتبارها محمية قانونا إضافة إلى مسؤولية من يستعمل هذه الأنظمة في تقليد الأعمال الأصلية أو انتهاك حقوق الملكية الفكرية.

رابعا. قانون الإعلام والاتصال:

يمكن الاستناد كذلك إلى أحكام قانون الإعلام في مواجهة بعض المرتبطة بالذكاء الاصطناعي، لاسيما نشر الأخبار الكاذبة والتلاعب بالمحتوى الإعلامي واستعمال تقنيات

التزييف العميق للتأثير على الرأي العام أو المساس بالحياة الخاصة بالأفراد (القانون العضوي 12-05 المتعلق بالإعلام، 2012).

وتزداد أهمية هذا القانون مع تطور أدوات الذكاء الاصطناعي القادرة على انتاج محتويات سمعية وبصرية يصعب التمييز بينها وبين الحقيقة، مما يفرض ضرورة تطوير الإطار القانوني والتنظيم لحماية الأمن الإعلامي والرقمي.

خامسا. النصوص التنظيمية المتعلقة بالأمن السيبراني:

تكمل النصوص التنظيمية المتعلقة بالأمن السيبراني والإجراءات التقنية لحماية الأنظمة المعلوماتية المنظومة القانونية الجزائرية في مكافحة الجرائم المستحدثة، حيث تهدف إلى حماية البنى التحتية الرقمية والأنظمة المعلوماتية من الاختراقات والهجمات الإلكترونية التي قد تعتمد على تقنيات الذكاء الاصطناعي (الامر 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، 2009).

ورغم أهمية هذه القوانين المكملة، إلا أنها تبقى غير كافية لمواجهة التطور السريع لجرائم الذكاء الاصطناعي نظرا لكونها لم توضع أساسا لتنظيم هذه التقنية بشكل مباشر الأمر الذي يستدعي سن تشريع خاص يحدد بدقة الجرائم المرتبطة بالذكاء الاصطناعي وآليات المسؤولية والعقوبات المناسبة لها.

خلص المطلب الأول إلى أن التشريع الجزائري يوفر حماية جزائية لجرائم الذكاء الاصطناعي من خلال مجموعة من النصوص القانونية العامة، كقانون العقوبات وقانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية، إضافة إلى بعض القوانين المكملة المرتبطة بالمعاملات الإلكترونية والملكية الفكرية، غير أن هذه النصوص تبقى غير كافية لمواجهة التطور السريع لجرائم الذكاء الاصطناعي لغياب تنظيم قانوني خاص يعالج هذه الجرائم بصورة دقيقة ومباشرة.

المطلب الثاني: حدود وعيوب الحماية الجزائية الحالية:

رغم تعدد النصوص القانونية التي يمكن تطبيقها على جرائم الذكاء الاصطناعي في التشريع الجزائري، إلا أن هذه الحماية لا تزال تواجه عدة صعوبات ونقائص تحد من فعاليتها، ويرجع ذلك على الطبيعة التقنية المتطورة لهذه الجرائم وسرعة تطور تطبيقات الذكاء الاصطناعي، الأمر الذي جعل النصوص التقليدية عاجزة أحيانًا عن الإحاطة بمختلف صورها المستحدثة سواء من حيث التكييف القانوني أو من حيث الإثبات والمسؤولية الجزائية.

الفرع الأول: غياب نصوص خاصة بالذكاء الاصطناعي:

يعد غياب نصوص قانونية خاصة تنظم جرائم الذكاء الاصطناعي من أبرز النقائص التي يعاني منها التشريع الجزائري في مجال الحماية الجزائية، فرغم وجود مجموعة من النصوص القانونية المتعلقة بالجرائم الإلكترونية وحماية البيانات الشخصية، إلا أنها وضعت أساسًا لمواجهة الجرائم المعلوماتية التقليدية ولم تصمّم خصيصًا لمواكبة الجرائم المستحدثة الناتجة عن تطور الذكاء الاصطناعي.

وتتميز جرائم الذكاء الاصطناعي بطبيعة تقنية معقدة ومتطورة، حيث يمكن ارتكابها بواسطة أنظمة قادرة على التعلم الذاتي واتخاذ القرارات بصورة شبه مستقلة، مثل تقنيات التزييف العميق Deep Fake والبرمجيات الذكية القادرة على اختراق الأنظمة أو تقليد الأصوات والصور، وهو ما يجعل تطبيق النصوص التقليدية عليها أمرًا صعبًا في بعض الحالات (محمد حامد، أحمد عبد الظاهر، 2024، صفحة 52).

كما أن المشرع الجزائري لم يضع إلى حد الآن تعريفًا قانونيًا دقيقًا للذكاء الاصطناعي، ولم يحدد بشكل واضح صور الجرائم المرتبطة به أو المسؤولية الجزائية الناتجة عن استخدامه، سواء تعلقت بمسؤولية المبرمج أو المستخدم أو مالك النظام الذكي مما يؤدي إلى وجود فراغ تشريعي ينعكس سلبًا على فعالية الحماية الجزائية.

ويترتب عن هذا النقص التشريعي أيضًا صعوبة حماية بعض الحقوق السياسية، خاصة الحق في الخصوصية وحماية المعطيات الشخصية، بالنظر إلى قدرة تقنيات الذكاء الاصطناعي على جمع وتحليل كميات ضخمة من البيانات واستغلالها بطرق قد تمس بحرية الأفراد وحقوقهم.

كما يرى جانب من الفقه أن النصوص التقليدية في قانون العقوبات لم تعد كافية وحدها لمواجهة الجرائم الحديثة المرتبطة بالذكاء الاصطناعي، بسبب التطور السريع لهذه التقنية وتنوع صور استخدامها الإجرامي، مما يستوجب تدخلًا تشريعيًا خاصًا يواكب هذه التطورات.

لذلك أصبح من الضروري تدخل المشرع الجزائري لوضع إطار قانوني خاص بجرائم الذكاء الاصطناعي، يحدد المفاهيم الأساسية وصور الجرائم المستحدثة وآليات المسؤولية الجزائية والعقوبات المناسبة، بما يحقق التوازن بين تشجيع التطور التكنولوجي وضمان الحماية القانونية للمجتمع (نسرين، 2025، صفحة 524_552).

الفرع الثاني: صعوبة التكييف القانوني والإثبات:

تعد صعوبة التكييف القانوني والإثبات من أهم التحديات التي تواجه الحماية الجزائية من جرائم الذكاء الاصطناعي، وذلك بسبب الطبيعة التقنية المعقدة لهذه الجرائم وتطور وسائل ارتكابها.

فالقواعد التقليدية في قانون العقوبات وضعت أساسا لجرائم مادية تقليدية، بينما تعتمد جرائم الذكاء الاصطناعي على أنظمة رقمية وخوارزميات قد تعمل بصورة مستقلة أو شبه مستقلة، مما يجعل إخضاعها للتكييف القانوني التقليدي أمرا صعبا.

وتظهر صعوبة التكييف القانوني خاصة عند محاولة تحديد الوصف الجزائي المناسب لبعض الأفعال المرتبطة بالذكاء الاصطناعي، مثل جرائم التزييف العميق، انتحال الهوية الرقمية، والتلاعب بالمحتوى الإلكتروني بواسطة البرامج الذكية ففي كثير من الحالات يصعب تحديد ما إذا كانت هذه الأفعال تدخل ضمن جرائم التزوير أو الاحتيال أو المساس

بالحياة الخاصة أو الجرائم الإلكترونية التقليدية (الظاهر، المواجهة الجنائية للجرائم المعلوماتية، 2010، صفحة 110).

كما تبرز إشكالية أخرى تتعلق بتحديد المسؤولية الجزائية، إذ يثور التساؤل حول الشخص المسؤول عن الجريمة المرتكبة بواسطة نظاما ذكي: هل هو المبرمج، أم المستخدم، أم الشركة المالكة للنظام، أم النظام الذكي ذاته؟ وهو ما يكشف قصور القواعد التقليدية للمسؤولية الجزائية في استيعاب الخصائص الحديثة للذكاء الاصطناعي.

أما من ناحية الإثبات، فتواجه السلطات القضائية صعوبات كبيرة في جمع الأدلة الرقمية وتحليلها، خاصة أن جرائم الذكاء الاصطناعي تتم غالبا في بيئة إلكترونية معقدة تعتمد على التشفير وسرعة تداول البيانات وإمكانية إخفاء الهوية الرقمية للجناة.

كما أن بعض تطبيقات الذكاء الاصطناعي قادرة على انتاج محتويات مزيفة بدرجة عالية من الدقة، مما يصعب التمييز بين الأدلة الحقيقية والمصطنعة، إضافة إلى ذلك فإن نقص الخبرة التقنية لدى بعض جهات التحقيق والقضاء قد يعيق الفهم الدقيق للآليات التقنية المعتمدة في هذه الجرائم الأمر الذي يؤثر على فعالية المتابعة القضائية وتحقيق الردع الجنائي المطلوب (أيت عبد المالك نادية وفلاح عبد القادر، 2021، صفحة 520).

لذلك أصبح من الضروري تطوير وسائل الإثبات الرقمي، وتكوين قضاة وخبراء متخصصين في الجرائم التكنولوجية مع تحديث التشريعات الجزائية بما يتلاءم مع خصوصية جرائم الذكاء الاصطناعي وتطورها المستمر.

وعليه يمكن القول إن التشريع الجزائري يوفر حماية جزائية لجرائم الذكاء الاصطناعي من خلال نصوص قانونية عامة، غير أن هذه الحماية تبقى محدودة بسبب غياب تشريع خاص بالذكاء الاصطناعي، إضافة إلى صعوبة التكييف القانوني والإثبات في الجرائم المرتبطة بالتقنيات الحديثة.

المبحث الثاني: صور الحماية الجزائية والتجربة المقارنة والآفاق المستقبلية:

تفرض جرائم الذكاء الاصطناعي ضرورة توفير حماية جزائية فعالة تشمل العقوبات وآليات الإثبات والإجراءات القانونية، نظرا لخصوصية هذه الجرائم وتعقيدها التقني، كما اتجهت عدة دول إلى تطوير تشريعات حديثة لمواكبة هذه التحديات، ما استدعى تناول هذا المبحث صور الحماية الجزائية، بعض التجارب المقارنة، وآفاق تطوير التشريع الجزائري في هذا المجال، وسيقسم هذا المبحث إلى مطلبين.

المطلب الأول: الحماية الموضوعية والإجرائية:

تقتضي مكافحة جرائم الذكاء الاصطناعي توفير حماية جزائية متكاملة تشمل الجانب الموضوعي من خلال العقوبات والجانب الإجرائي عبر وسائل التحقيق والإثبات، وتبرز أهمية هذه الحماية بسبب الطابع التقني المعقد لهذه الجرائم وصعوبة اكتشافها وتتبع مرتكبيها، ويندرج هذا المطلب ضمن فرعين.

الفرع الأول: الحماية الموضوعية (العقوبات):

يقصد بالحماية الموضوعية في مجال جرائم الذكاء الاصطناعي مجموعة القواعد القانونية التي تهدف إلى تجريم الأفعال غير المشروعة المرتبطة باستعمال تقنيات الذكاء الاصطناعي، مع تقرير العقوبات المناسبة لها قصد حماية النظام العام والأفراد والمؤسسات من أخطار هذه الجرائم.

وقد أصبحت هذه الحماية ضرورية نتيجة التطور التكنولوجي السريع وما نتج عنه من جرائم إلكترونية حديثة تعتمد على الأنظمة الذكية والخوارزميات المتطورة (بوسقيعة أ.، الوجيز في القانون الجزائي الخاص، 2021، صفحة 17).

ويعتمد المشرع الجزائري حاليا على النصوص العامة في قانون العقوبات وبعض القوانين المكملة لمواجهة الجرائم المرتبطة بالذكاء الاصطناعي، وعلى رأسها القانون رقم 09ـــ04

المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لحماية الأنظمة المعلوماتية من الاعتداءات الإلكترونية المختلفة (القانون رقم 09-04، 2009).

وتشمل الحماية الموضوعية تجريم أفعال متعددة، من بينها الدخول غير المشروع إلى الأنظمة المعلوماتية، إتلاف البيانات الرقمية، الاحتيال الإلكتروني، وسرقة المعطيات الشخصية وهي جرائم قد تتم بواسطة برامج الذكاء الاصطناعي أو الخوارزميات الذكية، كما يمكن استعمال هذه التقنيات في نشر الأخبار الكاذبة أو تقليد الأصوات والصور عبر تقنية التزييف العميق، الأمر الذي يشكل خطرا على الحياة الخاصة للأفراد وعلى الأمن المعلوماتي للدولة (كركوب، 2016، صفحة 10_45).

وتتمثل العقوبات المقررة لهذه الجرائم أساسًا في العقوبات الأصلية كالحبس والغرامة المالية، حيث تختلف بحسب خطورة الفعل المرتكب والضرر الناتج عنه فقد شدد المشرّع العقوبات في الجرائم التي تمس بأمن الأنظمة المعلوماتية أو تؤدي إلى تعطيل المرافق العامة أو الإضرار بالمصالح الاقتصادية للدولة (نجم، شرح قانون العقوبات الجزائري، 2019، صفحة 88).

كما تتضمن الحماية الموضوعية عقوبات تكميلية تهدف إلى منع تكرار الجريمة، مثل مصادرة الأجهزة والبرمجيات المستعملة في ارتكاب الجريمة، وغلق المواقع الإلكترونية أو الحسابات الرقمية المستغلة في النشاط الإجرامي، إضافة إلى المنع من ممارسة بعض الأنشطة المرتبطة بالمجال المعلوماتي.

وتبرز أهمية هذه العقوبات في الحد من خطورة الوسائل التقنية المستعملة في الجرائم الإلكترونية (بوسقيعة أ.، الوجيز في القانون الجزائي الخاص، صفحة 56).

ومن جهة أخرى، عزز القانون رقم18ـ07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الحماية الجزائية للبيانات الشخصية، خاصة في

ظل استخدام الذكاء الاصطناعي في جمع وتحليل المعلومات الشخصية دون ترخيص أو بشكل يمس بالحياة الخاصة للأفراد (الجريدة الرسمية ج ج د ش).

ورغم أهمية هذه النصوص، إلا أن الحماية الموضوعية الحالية ماتزال غير كافية لمواجهة التطور المستمر لجرائم الذكاء الاصطناعي وذلك بسبب ظهور أنماط إجرامية جديدة يصعب تكييفها وفق القواعد التقليدية، لذلك أصبح من الضروري سن تشريع خاص ينظم جرائم الذكاء الاصطناعي بشكل دقيق ويحدد المسؤوليات والعقوبات المناسبة لها، مع تطوير المنظومة القانونية بما ينسجم مع التطور الرقمي العالمي.

الفرع الثاني: الحماية الإجرائية من جرائم الذكاء الاصطناعي:

لا تقتصر الحماية الجزائية من جرائم الذكاء الاصطناعي على الجانب الموضوعي المتعلق بتجريم الأفعال وفرض العقوبات، بل تمتد كذلك إلى الحماية الإجرائية التي تهدف إلى تمكين السلطات القضائية والأمنية من اكتشاف هذه الجرائم والتحقيق فيها وإثباتها ومعاقبة مرتكبيها وفق إجراءات قانونية فعالة، إذ تكتسي الحماية الإجرائية أهمية بالغة بالنظر إلى الطبيعة التقنية المعقدة للجرائم المتعلقة بالذكاء الاصطناعي، والتي غالبًا ما تتم عبر الفضاء الرقمي وبوسائل يصعب تتبعها بطرق تقليدية.

وقد سعى المشرّع الجزائري إلى توفير مجموعة من الآليات الإجرائية لمواجهة الجرائم الإلكترونية، خاصة من خلال القانون رقم 09ـ04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي منح السلطات المختصة صلاحيات خاصة للتحري والبحث في الجرائم المعلوماتية (القانون رقم 09ـ04).

وتتمثل أهم وسائل الحماية الإجرائية في إجراءات البحث والتحري الإلكتروني، حيث يمكن للضبطية القضائية القيام بتتبع الأنشطة الإجرامية الرقمية وجمع الأدلة الإلكترونية التي تخص الجريمة، مثل الرسائل الإلكترونية، سجلات الاتصالات والبيانات المخزنة داخل الأنظمة المعلوماتية، كما يسمح القانون باللجوء إلى الخبرة التقنية من أجل تحليل الأنظمة

والبرمجيات المستعملة في ارتكاب الجريمة وكشف كيفية تنفيذها (سليمان، شرح قانون الإجراءات الجزائية الجزائري، 2019، صفحة 140).

كما اعتمد المشرع وسائل خاصة للإثبات تتلاءم مع طبيعة الجرائم الإلكترونية، إذ أصبح الدليل الإلكتروني من أهم وسائل الإثبات الحديثة ويشمل مختلف البيانات والمعلومات الرقمية التي يمكن استخراجها من الحواسيب أو الهواتف أو الشبكات الإلكترونية، ويتميز هذا النوع من الأدلة بكونه سريع الزوال وسهل التعديل مما يفرض ضرورة التدخل السريع للمحققين من أجل المحافظة عليه وضمان سلامته القانونية (بوسقيعة أ.، الوجيز في القانون الجزائي الخاص، صفحة 71).

ومن بين الوسائل الإجرائية الحديثة كذلك إمكانية اعتراض الاتصالات الإلكترونية ومراقبة الشبكات الرقمية بإذن قضائي، خاصة إذا تعلق الأمر بجرائم خطيرة تمس بالأمن العام أو الأمن السيبراني للدولة وتهدف هذه الإجراءات إلى كشف النشاط الإجرامي وتحديد هوية الفاعلين، لاسيما أن جرائم الذكاء الاصطناعي قد ترتكب عن بعد أو بواسطة هويات رقمية وهمية (نجم، شرح ق العقوبات الجزائري ، صفحة 103).

وتلعب الخبرة الفنية دورًا محوريًا في مجال الإثبات، نظرًا للطابع التقني لهذه الجرائم إذ يعتمد القاضي غالبا على خبراء في الإعلام الآلي والأمن السيبراني لتحليل الأدلة الرقمية وتفسير الجوانب التقنية المتعلقة بالجريمة، وتساعد هذه الخبرة في تحديد مصدر الاختراق أو كيفية استخدام أنظمة الذكاء الاصطناعي في تنفيذ الفعل الإجرامي.

ورغم هذه الآليات تواجه الحماية الإجرائية عدة صعوبات، من بينها الطابع العابر للحدود للجرائم الإلكترونية، صعوبة تحديد هوية الجناة، إضافة إلى التطور السريع للتكنولوجيا مقارنة ببطء تطور التشريعات، كما أن بعض وسائل الإثبات الرقمية قد تثير إشكالات تتعلق بحماية الحياة الخاصة وحرية الأفراد مما يفرض ضرورة تحقيق التوازن بين متطلبات الأمن واحترام الحقوق والحريات الأساسية (القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين).

لذلك أصبح من الضروري تطوير المنظومة الإجرائية الجزائية من خلال تعزيز التكوين التقني للقضاة وأعوان الضبطية القضائية، وإنشاء مخابر متخصصة في الأدلة الرقمية وتحديث قواعد الإثبات بما يتلاءم مع خصوصية جرائم الذكاء الاصطناعي، إلى جانب تعزيز التعاون الدولي في مجال تبادل المعلومات ومكافحة الجرائم السيبرانية العابرة للحدود.

وخلاصة القول، إن الحماية الجزائية من جرائم الذكاء الاصطناعي تقوم على تكامل العقوبات مع الإجراءات ووسائل الإثبات الحديثة بما يضمن مواجهة هذه الجرائم بفعالية وتحقيق الحماية القانونية والأمن الرقمي.

المطلب الثاني: التجارب المقارنة والمقترحات المستقبلية:

في ظل التطور السريع للذكاء الاصطناعي اتجهت العديد من التشريعات المقارنة إلى وضع آليات قانونية وتنظيمية لمواجهة الجرائم المرتبطة به، سواء من خلال قوانين خاصة أو عبر تنظيم المسؤولية والرقابة التقنية، ومن هذا المنطلق يهدف هذا المطلب إلى إبراز أهم التجارب المقارنة في المجال مع التطرق إلى آفاق تطوير التشريع الجزائري بما يواكب التحديات التقنية الحديثة ويعزز الحماية الجزائية، وينطوي هذا المطلب تحت ثلاثة فروع.

الفرع الأول: التجربة الأوروبية:

تعد التجربة الأوروبية من أبرز التجارب القانونية الحديثة في مجال تنظيم الذكاء الاصطناعي، حيث سعى الاتحاد الأوروبي إلى وضع إطار قانوني شامل يهدف إلى تحقيق التوازن بين تشجيع الابتكار التكنولوجي وضمان حماية الحقوق والحريات الأساسية للأفراد، وقد تجسد ذلك من خلال إصدار قانون الذكاء الاصطناعي الأوروبي المعروف ب AI ACTيعتبر أول تشريع متكامل ينظم استخدامات الذكاء الاصطناعي وفق مقاربة قائمة على تقييم المخاطر.

وقد اعتمد المشرع الأوروبي على تصنيف أنظمة الذكاء الاصطناعي بحسب درجة خطورتها، فقسمها إلى أنظمة ذات مخاطر غير مقبولة، أنظمة عالية الخطورة، أنظمة

محدودة المخاطر، وأنظمة منخفضة المخاطر، إذ تخضع الأنظمة عالية الخطورة لرقابة صارمة تشمل شروط الشفافية، ضمان جودة البيانات، وإخضاع الأنظمة لتقييم المسبق قبل طرحها للاستعمال وذلك حماية للأمن والحقوق الأساسية للأفراد (الأوروبي ا.، 2024).

كما حضر القانون الأوروبي بعض التطبيقات التي تشكّل تهديدًا مباشرًا للحريات العامة، مثل أنظمة التلاعب السلوكي، تقنيات التصنيف الاجتماعي، وبعض استعمالات التعرف البيومتري الآني في الأماكن العامة لما قد يترتب عنها من مساس بالخصوصية والكرامة الإنسانية، ويبرز ذلك توجه الاتحاد الأوروبي نحو إقرار حماية وقائية قبل وقوع الضرر بدل الاقتصار على العقاب اللاحق (الأوروبية، مقترح لائحة بشأن الذكاء الاصطناعي، 2012، صفحة 9_12).

ومن جهة أخرى، فرض قانون AI ACTالتزامات قانونية على الشركات المطورة والمشغلة لأنظمة الذكاء الاصطناعي من بينها ضرورة توثيق البيانات والخوارزميات، ضمان إمكانية تتبع القرارات الصادرة عن الأنظمة الذكية، إضافة إلى إخضاع بعض الأنظمة لرقابة الهيئات المختصة داخل الاتحاد الأوروبي.

ويعتبر هذا التوجه تطورا مهما في مجال الحماية الجزائية، لأنه يسمح بتحديد المسؤولية القانونية عند وقوع الجرائم أو الأضرار الناتجة عن استخدام الذكاء الاصطناعي (الأوروبي ا.، 2024).

وتظهر أهمية التجربة الأوروبية أيضا في اهتمامها بالجانب الأخلاقي، إذ ربطت بين مشروعية استخدام الذكاء الاصطناعي واحترام حقوق الإنسان ومبادئ الشفافية وعدم التمييز، لذلك اعتبر العديد من الفقهاء أن قانون AI ACTيمثل نموذجا تشريعيا يمكن للدول الأخرى الاستفادة منه عند وضع قوانينها الوطنية الخاصة بالذكاء الاصطناعي.

وعليه، فإن التجربة الأوروبية تبرز اتجاها حديثا يقوم على الوقاية القانونية والرقابة التقنية المسبقة بدل الاكتفاء بالنصوص التقليدية، وهو ما يمكن أن يشكل مرجعا مهما للمشرع الجزائري في إطار تطوير منظومة الحماية الجزائية من جرائم الذكاء الاصطناعي.

الفرع الثاني: التجارب الأمريكية والآسيوية:

قامت على التنظيم المرن والمسؤولية والرقابة التقنية، إذ تتميز هذه التجارب في مجال تنظيم الذكاء الاصطناعي باتباع مقاربة أكثر مرونة مقارنة بالتجربة الأوروبية، حيث تركز هذه الدول على تشجيع الابتكار التكنولوجي وعدم فرض قيود قانونية صارمة قد تعيق تطور الشركات الرقمية.

لذلك اعتمدت هذه الأنظمة على مبادئ المسؤولية التقنية، الرقابة الذكية، ووضع معايير أخلاقية وإرشادات تنظيمية بدل الاكتفاء بالتشريعات التقليدية

ففي الولايات المتحدة الأمريكية، لم يتم إلى حد الآن إصدار قانون فدرالي شامل خاص بالذكاء الاصطناعي، وإنما تعتمد السلطات على مجموعة من القواعد القطاعية المتعلقة بحماية البيانات والأمن السيبراني والمسؤولية المدنية، إلى جانب دور الشركات الكبرى في وضع سياسات الاستخدام الآمن للأنظمة الذكية، كما أصدرت الإدارة الأمريكية عدة توجيهات تؤكد ضرورة تطوير الذكاء الاصطناعي بطريقة تحترم الخصوصية والحقوق الأساسية وتضمن الأمن الرقمي، ويقوم النموذج الأمريكي على فكرة "التنظيم المرن"، أي منح المؤسسات التقنية حرية واسعة في التطوير مع إخضاعها للمساءلة عند حدوث أضرار أو جرائم ناتجة عن استخدام الأنظمة الذكية (سعيد، 2022، صفحة 18_22).

أما في الدول الآسيوية، فقد برزت الصين واليابان وكوريا الجنوبية كنماذج متقدمة في مجال الذكاء الاصطناعي، حيث سعت هذه الدول إلى الجمع بين التطور التكنولوجي والرقابة الحكومية؛ ففي الصين مثلا تفرض السلطات رقابة صارمة على المنصات الرقمية وأنظمة الذكاء الاصطناعي، خاصة فيما يتعلق بالمحتوى الرقمي وحماية الأمن القومي، مع إلزام

الشركات بتسجيل بعض الخوارزميات والإفصاح عن آليات عملها (جمال، 2022، صفحة 325_330).

كما اهتمت اليابان وكوريا الجنوبية بتطوير مواثيق أخلاقية ومعايير تقنية لتنظيم استخدام الذكاء الاصطناعي، مع التركيز على حماية المستخدمين وضمان أمن البيانات وتعزيز الثقة الرقمية؛ وتعتمد هذه الدول على التعاون بين الدولة والشركات والمؤسسات البحثية لوضع آليات فعّالة للرقابة التقنية ومنع إساءة استخدام الأنظمة الذكية (لطفي، 2021، صفحة 144_149).

وتظهر هذه التجارب أن التنظيم المرن قد يكون أكثر قدرة على مواكبة التطور السريع للذكاء الاصطناعي، غير أنه قد يثير صعوبات تتعلق بضعف الحماية القانونية في بعض الحالات، خاصة عند غياب نصوص جزائية واضحة تحدد المسؤوليات والعقوبات؛ لذلك تسعى أغلب الدول اليوم إلى تحقيق توازن بين حرية الابتكار وضمان الحماية القانونية والأمن الرقمي.

الفرع الثالث: آفاق تطوير التشريع الجزائري في مواجهة جرائم الذكاء الاصطناعي:

أدى التطور السريع لتقنيات الذكاء الاصطناعي إلى ظهور أنماط جديدة من الجرائم الإلكترونية التي تتجاوز في كثير من الأحيان نطاق النصوص التقليدية، الأمر الذي يفرض على المشرع الجزائري ضرورة تطوير المنظومة القانونية بما يتلاءم مع طبيعة هذه الجرائم الحديثة فرغم وجود عدة نصوص قانونية متعلقة بالجرائم الإلكترونية وحماية البيانات الشخصية، إلا أن خصوصية جرائم الذكاء الاصطناعي تستوجب وضع إطار قانوني أكثر تخصصا وفعالية.

ومن أبرز آفاق التطور التشريعي سنَّ قانون خاص بالذكاء الاصطناعي يحدد المفاهيم الأساسية، يضبط شروط استخدام الأنظمة الذكية، ويبين المسؤولية القانونية المترتبة عن الأضرار والجرائم الناتجة عنها كما ينبغي أن يتضمن هذا التشريع قواعد خاصة بحماية

البيانات، شفافية الخوارزميات، وآليات الرقابة على الأنظمة عالية الخطورة (بوشنافة، الجرائم المعلوماتية في ظل التشريع الجزائري، صفحة 144).

كما يقتضي تطوير الحماية الجزائية تحديث وسائل الإثبات الإلكتروني بما يسمح بمواكبة الجرائم المرتكبة عبر تقنيات الذكاء الاصطناعي، خاصة وأن هذه الجرائم تعتمد على خوارزميات معقدة ووسائل تقنية يصعب كشفها بالطرق التقليدية؛ لذلك أصبح من الضروري تعزيز الخبرة التقنية واعتماد الأدلة الرقمية الحديثة وتمكين جهات التحقيق من الوسائل التكنولوجية اللازمة لاكتشاف الجرائم وتتبع مرتكبيها (حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، صفحة 203).

ومن جهة أخرى، يتطلب التصدي لجرائم الذكاء الاصطناعي تأهيل القضاة وأعوان الضبطية القضائية والخبراء التقنيين حتى يتمكنوا من فهم الجوانب التقنية المرتبطة بالخوارزميات والأنظمة الذكية، فالتكوين المتخصص أصبح ضرورة لازمة لضمان التطبيق السليم للقانون وتحقيق فعالية المتابعة الجزائية في هذا النوع من الجرائم.

كذلك يعد تعزيز التعاون الدولي من أهم آفاق تطوير التشريع الجزائري لأن جرائم الذكاء الاصطناعي غالبا ما تتجاوز الحدود الوطنية، مما يستوجب تبادل المعلومات والخبرات التقنية والقضائية بين الدول بالإضافة إلى الانضمام إلى الاتفاقيات الدولية المتعلقة بمكافحة الجرائم السيبرانية والأمن الرقمي (الظاهر، المواجهة الجنائية للجرائم المعلوماتية، صفحة 132).

وختاما، فإن تطوير التشريع الجزائري في مجال الذكاء الاصطناعي لا يقتصر على تشديد العقوبات فقط، بل يتعداه ليشمل بناء منظومة قانونية وتقنية متكاملة تقوم على الوقاية، التكوين، الرقابة التقنية، والتعاون الدولي بما يضمن حماية فعالة للمجتمع من مخاطر جرائم الذكاء الاصطناعي.

تبين من خلال ما تم تقديمه أن الحماية الجزائية من جرائم الذكاء الاصطناعي تتطلب تطويرا يتجاوز العقوبات التقليدية ليضم آليات إجرائية وتقنية حديثة، مع الاستفادة من التجارب المقارنة التي اعتمدت التنظيم المرن والرقابة التقنية؛ أما في الجزائر فإن الفعالية تقتضي سن تشريع خاص بالذكاء الاصطناعي، تحديث وسائل الإثبات، تأهيل الجهات القضائية إلى جانب تعزيز التعاون الدولي لمواجهة هذا النوع من الجرائم المتطورة.

خاتمة

خاتمة:

نستنتج من تحليلنا السابق ومحصول القول فيه؛ أن التطور المتسارع لتقنيات الذكاء الاصطناعي أدى إلى بروز تحديات قانونية وجزائية جديدة فرضت نفسها على مختلف التشريعات الحديثة، باعتبار أن هذه التقنيات أصبحت تستعمل في العديد من المجالات الحيوية، سواء بسورة مشروعة أو في إطار أنشطة إجرامية تمس بالأفراد والمؤسسات والدول؛ وقد بينت الدراسة أن جرائم الذكاء الاصطناعي تتميز بخصائص تختلف عن الجرائم التقليدية، من حيث الوسلة المستعملة، وصعوبة اكتشاف الجريمة، وتعقيد إثبات المسؤولية الجزائية، خاصة مع الطابع التقني للخوارزميات والأنظمة الذكية.

كم تبين أن التشريع الجزائري، رغم احتواءه على بعض النصوص القانونية المتعلقة بالجرائم الإلكترونية وحماية البيانات الشخصية، إلا أنه لايزال يفتقر إلى تنظيم قانوني خاص وشامل يواكب التطور السريع لذكاء الاصطناعي وما يرتبط به من مخاطر جزائية مستحدثة؛ وقد أظهرت التجارب المقارنة، خاصة الأوروبية و الأمريكية والآسيوية، أهمية اعتماد مقاربة قانونية تجمع بين تشجيع الابتكار التكنولوجي وضمان الحماية القانونية والجزائية الفعالة.

وانطلاقا من ذلك، فإن مواجهة جرائم الذكاء الاصطناعي تتطلب تطوير المنظومة القانونية والاجرائية، وتحديث وسائل الإثبات الرقمية، وتعزيز التعاون بين الجهات القضائية والتقنية، بما يسمح بتحقيق حماية فعالة للحقوق والحريات في البيئة الرقمية الحديثة.

أهم النتائج:

ـ أن الذكاء الاصطناعي أصبح وسيلة يمكن إستغلالها في إرتكاب جرائم إلكترونية متطورة يصعب إكتشافها وإثباتها.

ـ أن جرائم الذكاء الاصطناعي تتميز بالطابع التقني والعابر للحدود، مما يزيد من صعوبة مكافحتها بالوسائل التقليدية.

ـ أن التشريع الجزائري يعتمد حاليا على نصوص عامة، مثل قانون العقوبات وقانون الجرائم الإلكترونية، دون وجود قانون خاص ينظم الذكاء الاصطناعي.

ـ أن المسؤولية الجزائية في جرائم الذكاء الاصطناعي قد تشمل المستخدم والمبرمج والمطور والمزود، بحسب طبيعة الخطأ المرتكب.

ـ أن إثبات الجرائم المرتبطة بالذكاء الاصطناعي يعد من أبرز الإشكالات العملية بسبب تعقيد الخوارزميات وصعوبة تحديد مصدر القرار الآلي.

ـ أن التجارب المقارنة، خاصة التجربة الأوروبية من خلال قانونها، تمثل نموذجا حديثا يمكن الاستفادة منه في تطوير التشريع الجزائري.

ـ أن فعالية الحماية الجزائية المستقبلية ترتبط بمدى قدرة المشرع الجزائري على إدماج مفاهيم حديثة، مثل المسؤولية الرقمية، والأدلة الالكترونية الذكية، والرقابة عن الخوارزميات.

أهم التوصيات:

ـ ضرورة سن تشريع جزائري خاص بالذكاء الاصطناعي يتضمن تعريفا دقيقا لأنظمته وجرائمه والمسؤولية المترتبة عنه.

ـ تحديث قانون العقوبات وقانون الجرائم الإلكترونية بما يتلاءم مع الجرائم المستحدثة الناتجة عن إستخدام الذكاء الاصطناعي.

ـ تطوير وسائل الإثبات الرقمية واعتماد الخبرة التقنية الحديثة في التحقيقات الجزائية المتعلقة بالأنظمة الذكية.

ـ إنشاء هيئات وطنية مختصة بمراقبة تطبيقات الذكاء الاصطناعي وتقييم مخاطرها القانونية والأمنية.

ـ تعزيز التكوين التقني والقانوني للقضاة وأجهزة الضبطية القضائية والخبراء في مجال الجرائم الرقمية والذكاء الاصطناعي.

ـ دعم التعاون الدولي وتبادل المعلومات والخبرات لمواجهة الجرائم العابرة للحدود المرتبطة بالذكاء الاصطناعي.

ـ تحقيق التوازن بين تشجيع الابتكار التكنولوجي وضمان حماية الحقوق والحريات الأساسية للأفراد.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1. إبراهيم ,خ .م .(2022) .*الذكاء الاصطناعي والمسؤولية الجنائية* .الإسكندرية :دار الفكر الجامعي.

2. إبراهيم ,خ .م .(2022) .*الذكاء الاصطناعي والمسؤولية الجنائية* .الإسكندرية :دار الفكر الجامعي.

3. أحمد ,أ .م .(2025) .*جرائم الذكاء الاصطناعي* .المغرب :دار الآفاق المغربية للنشر والتوزيع.

4. أحمد ,ب .(2020) .*الجرائم المعلوماتية في ظل التشريع الجزائري* .الجزائر :دار الخلدونية.

5. أحمد ,ب .(2022) .*المسؤولية الجنائية في عصر الذكاء الإصطناعي* .الجزائر : مجلة العلوم القانونية جامعة زيان عاشور الجلفة.

6. أحمد ,م .(2021) .*المسؤولية الجنائية عن إستخدام الذكاء الإصطناعي* .الجزائر : رسالة ماجستير.

7. إسماعيل ,ع .ا .(2017) .*الذكاء الإصطناعي و تطبيقاته في التعليم* .éd)الطبعة 1).القاهرة ,مصر :عالم الكتب للنشر والتوزيع.

8. إسماعيل ,م .ع .(2018) .*المنطق الضبابي وتطبيقاته في الذكاء الاصطناعي* . عمان :دار المسيرة.

9. الأمر 18ـ 05المتعلق بالتجارة الإلكترونية ,2018) .ماي .(10*الجريدة الرسمية*.(28)

10. الأمر 03- 05المتعلق بحقوق المؤلف والحقوق المجاورة ,2003) .يوليو 19(.*الجريدة الرسمية*.(44)

11. الامر 09- 04المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ,2009) .أوت .(05*الجريدة الرسمية*.(47)

12. الأوربية ,ا .(2021) .*قانون الذكاء الإصطناعي* .بروكسل بلجيكا :المفوضية الأوروبية.

13. الأوروبي ,ا .(2024) .اللائحة)الاتحاد الأوروبي (المتعلقة بالذكاء الاصطناعي .*الجريدة الرسمية للذكاء الاصطناعي* ,المواد 6_5و .15_8

14. الأوروبي ,ا .ا ,2024) .يوليو .(12اللائحة المتعلقة بالذكاء الاصطناعي رقم .1689*الجريدة الرسمية للاتحاد الأوربي*.(12)

15. الأوروبية ,ا .(2012) .مقترح لائحة بشأن الذكاء الاصطناعي .*قانون الذكاء الاصطناعي*.12_9 ,

16. الأوروبية ,ا .(2021) .*قانون الذكاء الإصطناعي* .بروكسل بلجيكا :أوروبا.

17. الأوروبية ,ا .(2021) .مقترح اللائحة الأوروبية بشأن الذكاء الإصطناعي . *المفوضية الأوروبية*.40 ,

18. الجريدة الرسمية ج ج د ش .(s.d.) .القانون 18- .07*الجريدة الرسمية للجمهورية الجزائرية*.(34)

19. الجزائر ,ك .ا .(2020) .دراسة حول المسؤولية الجنائية للمستخدم في جرائم التكنولوجيا الحديثة .*مجلة العلوم القانونية*112 ,*12* ,..130

20. الخطيب ,م .ع .(2020) .*الذكاء الاصطناعي والقانون دراسة قانونية مقارنة* .قطر :جامعة قطر.

21. الدايم ,ع .ا .(2016) .*نظم دعم القرار والذكاء الاصطناعي* .الاسكندرية مصر :دار الفكر الجامعي.

22. الرحمان ,ع .ع .(2021) .*حماية المعطيات الشخصية في التشريع الجزائري* .الجزائر :دار بلقيس.

23. الرحيم ,م .ع .(2020) .*علم البيانات والذكاء الاصطناعي* .بيروت :دار الكتب العلمية.

24. الرسمية ,ا 10) .جوان .(2018القانون 07ـ 18المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .*الجريدة الرسمية* ,م 10.ـ2

25. الزهراء ,ع .ف .(2022) .*المسؤولية الجزائية عن أنظمة الذكاء الاصطناعي مجلة الباحث للدراسات القانونية والسياسية* .ورقلة الجزائر :جامعة قاصدي مرباح.

26. السنهوري ,ع .ا .(2023) .*الحماية القانونية للتقنيات الحديثة والذكاء الاصطناعي* .القاهرة :دار النهضة العربية .

27. الشعبية ,ا .ا 8) .يونيو .(1966الأمر رقم 66ـ 156المتضمن قانون العقوبات المعدل والمتمم .*الجريدة الرسمية* .

28. الظاهر ,أ .ع .(2010) .*المواجهة الجنائية للجرائم المعلوماتية* .القاهرة , مصر :دار النهضة العربية.

29. الظاهر ,أ .ع .(.s.d) .*المواجهة الجنائية للجرائم المعلوماتية*.

30. العام ,ق .ا .(1989) .القاهرة مصر :دار النهضة العربية.

31. العبد ,م .ع .(2019) .*الذكاء الاصطناعي المفاهيم والتطبيقات* .بيروت :دار الكتب العلمية.

32. العقوبات ,ق 8) .يونيو .(1966*المادة 288.* الجزائر :الأمر رقم 66 156 قانون العقوبات الجزائري .

33. العقوبات ,ق 8) .يونيو .(1966*المادة 41.* الجزائر :الأمر 66 156 المعدل والمتمم قانون العقوبات الجزائري .

34. الغني ,ع .ع .(2017) .*مقدمة في الذكاء الاصطناعي والنظم الخبيرة* . عمان :دار المسيرة.

35. القادر ,ب .ع .(2018) .*الجرائم المعلوماتية في التشريع الجزائري* .الجزائر : دار هومة.

36. القادر ,ز .ع .(2019) .الجريمة المعلوماتية في التشريع الجزائري .*مجلة الدراسات القانونية كلية الحقوق جامعة الجزائر 1,* 85 ..100

37. القادر ,ز .ع .(2020) .*إشكالية إثبات الخطأ في الجرائم المعلوماتية* .باتنة الجزائر :مجلة الحقوق والعلوم السياسية جامعة باتنة 1.

38. القانون 18ـ 07المتعلق بحماية الأشخاص الطبيعيين.(34) .(s.d.) .

39. القانون العضوي 12ـ 05المتعلق بالإعلام ,2012) .يناير .(12*الجريدة الرسمية*.(2)

40. القانون رقم 09ـ.(47) .(s.d.) .04

41. القانون رقم 09ـ 2009, 04اوت .(05*الجريدة الرسمية للجمهورية الجزائرية*.(47)

42. القانونية ,م .ا .(2019) .المسؤولية الجنائية عن جرائم التكنولوجيا الحديثة . 85.

43. الله ,ع .غ .(2018) .*الذكاء الاصطناعي و النظم الذكية* .عمان :دار المناهج للنشر والتوزيع.

44. الله ,م .ب .(2021) .*دراسة ماجستير الخطأ الجنائي وسوء إستخدام الذكاء الإصطناعي* Vol. 55). .(68الجزائر :جامعة قسنطينة.

45. الله ,م .ب .(s.d.) .*الخطأ الجنائي وسوء إستخدام الذكاء الإ.*

46. المتعلق بالتوقيع والتصديق الإلكتروني ,2015) .فيفري .(1*الجريدة الرسمية*.(6)

47. أمين ,ع .ح .(2024) .استعمالات الذكاء الإصطناعي بين الحرية الشخصية و المسؤوليات القانونية دراسة مقارنة .*مجلة العلوم القانونية لكلية الحقوق* , 83 85.

48. أيت عبد المالك نادية وفلاح عبد القادر .(2021) .التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري .*مجلة الأستاذ الباحث*.214 ,

49. بوسقيعة ,أ .(2021) .*الوجيز في القانون الجزائي الخاص* .الجزائر :دار هومة.

50. بوسقيعة ,أ .(s.d.) .*الوجيز في القانون الجزائي الخاص.*

51. بوسقيعة ,أ .(s.d.) .*الوجيز في القانون الجزائي الخاص*.

52. بوسقيعة ,ل .(2013) .*الوجيز في القانون الجزائي العام* .الجزائر :دار هومة لطباعة ونشضر وتوزيع .

53. بوسقيعة ,ل .(2017) .*الوجيز في القانون الجزائي العام* .(Vol. 7)الجزائر : دار هومة.

54. بوشنافة ,أ .(s.d.) .*الجرائم المعلوماتية في ظل التشريع الجزائري*.

55. بيترنورفينغ ,س .ر .(s.d.) .*كتاب الذكاء الاصطناعي مدخل حديث* . الولايات المتحدة :دار بيرسون للتعليم.

56. ج ,ق .ع8) .يونيو .(1966*الجريدة الرسمية* .الجزائر :الجريدة الرسمية الأمر 66..156

57. جمال ,ب .(2022) .الذكاء الاصطناعي :بحث عن مقاربة قانونية .*المجلة الجزائرية للعلوم القانونية والسياسية ,المجلد*)*59*العدد .330_325 ,(5

58. جمال ,ب .(2022) .الذكاء الاصطناعي :بحث عن مقاربة قانونية .*المجلة الجزائرية للعلوم القانونية والسياسية ,المجلد*)*59*العدد .(5

59. حجازي ,ع .ا .(2005) .*الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت* .القاهرة ,مصر :دار الكتب القانونية.

60. حجازي ,ع .ا .(2007) .*الإثبات الجنائي في جرائم الكمبيوتر والإنترنت* .(Vol. 6)القاهرة مصر :دار الكتب القانونية.

61. حجازي ,ع .ا .(2020) .*المسؤولية المدنية عن أضرار الأنترنيت* . الإسكندرية مصر :دار الفكر الجامعي.

62. حجازي ,ع .ا .(s.d.) .*الإثبات الجنائي في جرائم الكمبيوتر والإنترنت*.

63. حجازي ,ع .ا .(s.d.) .*الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت*.

64. حمدي ,ل .(2020) .*الإهمال المتكرر والجرائم الإلكترونية دراسة ماجستير* . وهران الجزائر :جامعة وهران.

65. حمودة ,ع .ا .(2019) .*الذكاء الاصطناعي :المفاهيم والتطبيقات* .بيروت : دار الكتب العلمية.

66. خالد ,ب .د .(2023) .*إشكالية المسؤولية المشتركة في أنظمة الذكاء الاصطناعي* .سطيف الجزائر :مجلة الدراسات القانونية جامعة سطيف.2

67. خليل ,م .إ .(2015) .*تفاعل الإنسان مع الحاسوب والأنظمة الذكية* . الإسكندرية :دار الفكر الجامعي.

68. سعيد ,و .س .(2022) .المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي .*مجلة العلوم القانونية ,المجلد*)*64*العدد .(2

69. سليمان ,ع .ا .(2010) .*شرح قانون العقوبات القسم العام :النظرية العامة للمسؤولية الجزائية* .(Vol. 2)الجزائر :دار الهدى.

70. سليمان ,ع .ا .(2019) .*شرح قانون الإجراءات الجزائية الجزائري* .(éd الطبعة .(4الجزائر :ديوان المطبوعات الجامعية.

71. سمير ,ب .(2021) .*صعوبة إثبات المسؤولية في الجرائم السيبرانية* .بسكرة الجزائر :مجلة الإجتهاد القضائي جامعة بسكرة.

72. سمير ,ل .(2019) .*الإثبات في الجرائم الإلكترونية* .الجزائر :دار بلقيس .

73. ش ,ج .ا 05) .أوت .(2009قانون09ـ 04المتعلق بالقواعد الخاصة للوقاية من اتلجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .*الجريدة الرسمية* , العدد .47

74. شريف ,س .(2021) .*الذكاء الاصطناعي والقانون :التحديات القانونية المعاصرة* .الإسكندرية ,مصر :دار الجامعة الجديدة.

75. شيماء ,ب .(2025) .المسؤولية القانونية الناشئة عن استعمالات الذكاء الاصطناعي .*مذكرة ماستر*.88 ,

76. صالح ,ع .ا .(s.d.) .*الحماية القانونية للمعاملات الالكترونية*.

77. صالح ,ع .ا .(s.d.) .*الحماية القانونية للمعاملات الإلكترونية*.

78. صالح ,م .(2019) .*المسؤولية الجنائية في الجرائم الإلكترونية* .الجزائر : مجلة العلوم القانونية جامعة الجزائر .2

79. عبد الرزاق بن عبد العزيز المرجان، زياد فايز الجندي .(2024) .*مواجهة الجرائم المرتكبة بواسطة الذكاء الاصطناعي* .الرياض :جامعة نايف العربية للعلوم الأمنية.

80. فاطمة ,ز .(2021) .الحماية الجزائية للمعطيات المعلوماتية في القانون الجزائري .*مجلة العلوم القانونية جامعة الجزائر* .75 55 ,*1*

81. كركوب ,ط .ع .(2016) .الحماية الجنائية الموضوعية لحقوق الإنسان وحرياته الأساسية .*رسالة دكتوراه في القانون الجنائي* 144 .p)ـ .(145القاهرة : جامعة القاهرة كلية الحقوق.

82. كمال ,س .(2021) .المسؤولية الجزائية عن إنتهاك البيانات الشخصية . *مجلة الإجتهاد القضائي*55 ,*18* ,ـ.70

83. لطفي ,خ .ح .(2021) .*الذكاء الاصطناعي وحمايته من الناحية المدنية والجنائية* .الإسكندرية ,مصر :دار الفكر الجامعي.

84. ليلى ,ب .ن .(2022) .الإطار القانوني لحماية البيانات الشخصية في الجزائر .*مجلة الدراسات القانونية المقارنة*88 ,*5* ,ـ.105

85. محمد حامد، أحمد عبد الظاهر .(2024) .*المسؤولية الجنائية عن استخدامات الذكاء الاصطناعي* .القاهرة ,مصر :دار النهضة العلمية.

86. محمد ,ب .د .(2020) .*المسؤلية الجزائية عن الجرائم الإلكترونية* .الجزائر : دار الجامعة الجديدة.

87. محمد ,ب .ع .(2021) .تحديات تطبيق قانون العقوبات على جرائم الذكاء الاصطناعي .*مجلة الحقوق جامعة باتنة* 120 ,*1*ـ.140

88. محمد ,م .ع .(2015) .*الذكاء الاصطناعي والنظم الخبيرة* .دار الفكر العربي.

89. مراد ,ز .(2023) .تحديات حماية البيانات في عصر الذكاء الاصطناعي . *مجلة العلوم القانونية جامعة الشهيد حمه لخضر - الوادي - الجزائر* ,*14* , 140ـ165.

90. مروشن ,خ .م .(2026) .المسؤولية القانونية عن أخطاء أنظمة الذكاء الإصطناعي في ضوء حقوق الإنسان .*مجلة ميسان للدراسات القانونية* 44 ,..78

91. مكارثي ,ج .(2007) .*ماهو الذكاء الإصطناعي؟* ,2007 Consulté le . sur stanford.edu_jmc_whatisia.html.

92. منصور ,م .ح .(2009) .*المسؤولية الإلكترونية* .الإسكندرية مصر :دار الجامعة الجديدة.

93. منصور ,م .ح .(2017) .*الاثبات الالكتروني في المواد الجنائية* . الاسكندرية ,مصر :دار الجامعة الجديدة.

94. منصور ,م .ح .(2022) .*المسؤولية القانونية الناشئة عن تطبيقات الذكاء الاصطناعي* .الاسكندرية :دار الجامعة الجديدة .

95. منظور ,ا .(1955) .*لسان العرب* .بيروت لبنان :دار صادر.

96. منظور ,ا .(1984) .*لسان العرب* .بيروت :دار صادر.

97. منظور ,ا .(1994) .*قاموس لسان العرب* .لبنان :دار صادر.

98. نجم ,م .ص .(2019) .*شرح قانون العقوبات الجزائري* .الجزائر :ديوان المطبوعات الجامعية.

99. نجم ,م .ص .(s.d.) .*شرح ق العقوبات الجزائري* .

100. نريمان ,م .ب .(2017) .المسؤولية عن فعل الأنظمة الإلكترونية الذكية . *مجلة Annales de l'université d'alger, 31*(1), 456.

101. نسرين ,م .(2025) .المسؤولية الجزائية عن جرائم الذكاء الاصطناعي في التشريع الجزائري .*مجلة الدراسات القانونية والاقتصادية*)*8* ,العدد .201 ,(2

102. نصر الله، حوراء عزيز، الزهيري، رشا موسى .(2026) .المسؤولية المدنية للمنتج عن تطبيقات الذكاء الاصطناعي المعيبة .*مجلة آشور للعلوم القانونية والسياسية*.211 ,

103. نفسه ,م.(.s.d) .

104. نورفينغ ,س .ر .(2021) .*الذكاء الإصطناعي مدخل حديث* .بريطانيا : بيرسون.

105. هاشم رشيدة، ملياني عبد الوهاب .(2024) .الإطار المفاهيمي للذكاء الاصطناعي .*مجلة التراث*.48 ,(2)*14* ,

فهرس الموضوعات

فهرس الموضوعات

مقدمة: 1

الفصل الأول

الإطار المفاهيمي لجرائم الذكاء الاصطناعي

تمهيد: 7

المبحث الأول: ماهية الذكاء الاصطناعي: 8

المطلب الأول: مفهوم الذكاء الاصطناعي: 8

الفرع الأول: تعريف الذكاء الاصطناعي: 8

الفرع الثاني: خصائص أنظمة الذكاء الاصطناعي: 10

المطلب الثاني: المقصود بجرائم الذكاء الاصطناعي: 12

الفرع الأول: المقصود بجرائم الذكاء الاصطناعي: 13

الفرع الثاني: أنواع جرائم الذكاء الاصطناعي: 14

المبحث الثاني: المسؤولية الجزائية الناتجة عن جرائم الذكاء الاصطناعي: 17

المطلب الأول: المسؤولية الجزائية للمستخدم: 17

الفرع الأول: القصد الجنائي في جرائم الذكاء الاصطناعي: 17

الفرع الثاني: ركن الخطأ وسوء استخدام الأدوات الذكية: 19

المطلب الثاني: المسؤولية الجزائية للمبرمج والمطور والمزود: 21

الفرع الأول: خطأ التصميم والإهمال الرقمي: 21

الفرع الثاني: صعوبة الإثبات والمسؤولية المشتركة: 23

الفصل الثاني

الحماية الجزائية من جرائم الذكاء الاصطناعي في التشريع الجزائري و آفاق تطويرها

تمهيد:.....26
المبحث الأول: الإطار القانوني للحماية الجزائية: 27
المطلب الأول: النصوص القانونية المطبقة حاليا:.....27
الفرع الأول: مواجهة جرائم الذكاء الاصطناعي في قانون العقوبات: 27
الفرع الثاني: مواجهة جرائم الذكاء الاصطناعي في قانون الجرائم الإلكترونية 09ـ04 ...29
الفرع الثالث: مواجهة جرائم الذكاء الاصطناعي في قانون حماية البيانات الشخصية 18ـ07 31
الفرع الرابع: مواجهة جرائم الذكاء الاصطناعي في القوانين المكملة: 33
المطلب الثاني: حدود وعيوب الحماية الجزائية الحالية:.....36
الفرع الأول: غياب نصوص خاصة بالذكاء الاصطناعي:.....36
الفرع الثاني: صعوبة التكييف القانوني والإثبات: 37
المبحث الثاني: صور الحماية الجزائية والتجربة المقارنة والآفاق المستقبلية:.....39
المطلب الأول: الحماية الموضوعية والإجرائية: 39
الفرع الأول: الحماية الموضوعية (العقوبات):.....39
الفرع الثاني: الحماية الإجرائية من جرائم الذكاء الاصطناعي: 41
المطلب الثاني: التجارب المقارنة والمقترحات المستقبلية: 43
الفرع الأول: التجربة الأوروبية:.....43
الفرع الثاني: التجارب الأمريكية والآسيوية: 45

الفرع الثالث: آفاق تطوير التشريع الجزائري في مواجهة جرائم الذكاء الاصطناعي:.....46

قائمة المصادر والمراجع 54

ملخص الدراسة:

تتناول هذه الدراسة موضوع الحماية القانونية من جرائم الذكاء الاصطناعي في ظل التطور السريع للتقنيات الرقمية وظهور جرائم مستحدثة كالتزييف العميق والاحتيال الإلكتروني والهجمات السيبرانية. وتهدف إلى بيان مفهوم هذه الجرائم وتحليل المسؤولية الجزائية الناشئة عنها، مع دراسة مدى كفاية التشريع الجزائري في مواجهتها.

وقد خلصت الدراسة إلى أن التشريع الجزائري يوفر حماية قانونية عامة، إلا أنها تبقى غير كافية بسبب غياب تنظيم خاص بجرائم الذكاء الاصطناعي وصعوبة الإثبات والتكييف القانوني، مما يستدعي تطوير إطار تشريعي متخصص يواكب التطورات التقنية الحديثة.

الكلمات المفتاحية: جرائم الذكاء الاصطناعي، الحماية الجزائية، المسؤولية الجزائية، الإثبات الرقمي، التشريع الجزائري.

Abstract:

This study examines legal protection against artificial intelligence crimes in light of the rapid development of digital technologies and the emergence of new crimes such as deepfakes, cyber fraud, and cyberattacks. It aims to clarify the concept of AI crimes, analyze criminal liability arising from them, and evaluate the adequacy of Algerian legislation in addressing such crimes.

The study concludes that Algerian legislation provides general legal protection; however, it remains insufficient due to the absence of specialized legislation on AI crimes and the difficulties related to legal qualification and digital evidence, which necessitates the development of a modern legal framework adapted to technological advancements.

Keywords: Artificial Intelligence Crimes, Criminal Protection, Criminal Liability, Digital Evidence, Algerian Legislation.