مجلة الدراسات القانونية والاقتصادية ISSN 2602-7321/ EISSN 2773- 2649

السنة: 2024 المجلد: 07 العدد: 02 ص- ص: 345-371



# المسؤولية الجزائية لمسيري الشركات في عصر الذكاء الاصطناعي: تحديات وآفاق قانونية جديدة

# Criminal Liability of Corporate Managers in the Age " of Artificial Intelligence: New Legal Challenges and "Horizons

لوصفان سلمى*[1]، جامعة محمد لمين دباغين، الجزائر، lousfane.selma@gmail.com

أمقران رضوان[2]، جامعة العربي بن مهيدي، الجزائر، amokrane.radhwane@univ-oeb.dz

تاريخ إرسال المقال: 2024/08/10 تاريخ قبول المقال: 2024/10/03

**الملخص:**

يتناول الموضوع المسؤولية الجزائية لمسيري الشركات التجارية في عصر الذكاء الاصطناعي الذي أصبح استخدامه شائعا في إدارة وتسيير الشركة التجارية، مسلطا الضوء على مختلف التحديات القانونية الجديدة المتعلقة بصعوبة استخدام أدوات الذكاء الاصطناعي وضرورة صياغة نصوص قانونية مستحدثة تبين حدود هذا الاستخدام الذي قد يؤدي إلى ارتكاب أفعال مجرمة، حيث تتضمن الدراسة مفهوم الذكاء الاصطناعي، ومختلف أنواع الجرائم المحتملة المرتبطة به والتي تنقسم إلى صنفين أساسين: الأول يكون فيه الذكاء الاصطناعي أداة للجريمة والتي تقوم على الغش والاحتيال، أما في الثاني فيكون الذكاء الاصطناعي هدفا للجريمة مثل إساءة استخدام البيانات، ويخلص الموضوع إلى ضرورة تحديث الأطر القانونية الحالية وتطوير القوانين والأنظمة بما يتناسب مع التطورات التكنولوجية السريعة في مجال الذكاء الاصطناعي، لمواجهة هذه التحديات الجديدة بفعالية.

الكلمات المفتاحية: مسير الشركة التجارية، الذكاء الاصطناعي، جرائم الذكاء الاصطناعي.

## Abstract :

The topic addresses the criminal liability of commercial company managers in the era of artificial intelligence, which has become commonly used in the management and operation of commercial companies. It sheds light on various new legal challenges related to the difficulty of using AI tools and the need to formulate

* لوصفان سلمى

updated legal texts that define the limits of this use, which may lead to committing criminal acts. The study includes the concept of artificial intelligence and various types of potential crimes associated with it, which are divided into two main categories: The first is where AI is a tool for crime, primarily based on fraud and deception, while in the second, AI is the target of the crime, such as data misuse. The topic concludes with the necessity of updating current legal frameworks and developing laws and regulations to keep pace with rapid technological developments in the field of artificial intelligence, in order to effectively address these new challenges.

Keywords: Commercial company manager, Artificial Intelligence, AI crimes.

**المقدمة:**

في ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبح الذكاء الاصطناعي قوة دافعة للتغيير في مختلف القطاعات، بما في ذلك عالم الأعمال والشركات. هذا التطور التكنولوجي الهائل يفرض تحديات جديدة على الصعيد القانوني، خاصة فيما يتعلق بالمسؤولية الجزائية لمسيري الشركات.

يتناول هذا البحث موضوع "المسؤولية الجزائية لمسيري الشركات في عصر الذكاء الاصطناعي: تحديات وآفاق قانونية جديدة". ويهدف إلى دراسة التحولات القانونية والأخلاقية في مجال المسؤولية الجزائية لقادة الأعمال في ضوء التطبيقات المتزايدة لتقنيات الذكاء الاصطناعي في بيئة الشركات. يشمل ذلك تحليل الجرائم المحتملة المرتبطة بالذكاء الاصطناعي، وكيفية تطبيق مفاهيم المسؤولية الجنائية التقليدية على هذه الحالات الجديدة، بالإضافة إلى استكشاف الحاجة إلى تطوير أطر قانونية جديدة.

لقد شهد مفهوم المسؤولية الجزائية لمسيري الشركات تطوراً ملحوظاً عبر الزمن، من المفاهيم التقليدية إلى التحديات الجديدة التي فرضتها الثورة الرقمية. ويأتي الذكاء الاصطناعي ليضيف بعداً جديداً لهذا التطور، مما يستدعي إعادة النظر في الأطر القانونية القائمة.

تكمن أهمية هذا البحث في تسليط الضوء على التحديات القانونية الناشئة التي تواجه مسيري الشركات في عصر الذكاء الاصطناعي، وتحليل الآفاق المستقبلية للتشريعات والأطر القانونية اللازمة لمواجهة هذه التحديات. كما يسعى إلى استكشاف التوازن الدقيق بين الاستفادة من إمكانيات الذكاء الاصطناعي وضمان المساءلة القانونية عن الأضرار المحتملة الناجمة عن استخدامه في بيئة الأعمال.

تتمحور إشكالية البحث حول السؤال الرئيسي التالي: **كيف يمكن تنظيم المسؤولية الجزائية لمسيري الشركات في ظل التحديات والتعقيدات التي يفرضها استخدام تقنيات الذكاء الاصطناعي في بيئة الأعمال المعاصرة؟**

لمعالجة هذه الإشكالية، يعتمد البحث على المنهج التحليلي الوصفي، حيث يتم تحليل الوضع القانوني الراهن فيما يخص المسؤولية الجزائية لمسيري الشركات، ثم دراسة التحديات المستجدة التي يفرضها الذكاء الاصطناعي على هذا الإطار القانوني. كما يتم استقراء الاتجاهات التشريعية والقضائية الحديثة في هذا المجال، بهدف استخلاص رؤى مستقبلية لتطوير الإطار القانوني بما يتلاءم مع متطلبات العصر الرقمي ويضمن التوازن بين الابتكار والمساءلة القانونية.

## المبحث الأول: تحديات تطبيق المسؤولية الجزائية في سياق الذكاء الاصطناعي

يهدف هذا المبحث إلى استكشاف التحديات التي تنشأ عند محاولة تحديد المسؤولية الجنائية في حالات تورط أنظمة الذكاء الاصطناعي في أفعال قد تعتبر جرائم، وقبل التطرق إلى كل هذا لابد أولا من تسليط الضوء على مفهوم الذكاء الاصطناعي.

### المطلب الأول: مفهوم الذكاء الاصطناعي

يعد مصطلح الذكاء الاصطناعي واحدا من المفاهيم الحديثة والتي تلقى اهتماما كبيرا في العالم بأسره، وعليه فقد جاء هذا المطلب ليتناول تعريف الذكاء الاصطناعي وخصائصه الأساسية.

#### أولا: تعريف الذكاء الاصطناعي

تتباين التعريفات الخاصة بمصطلح الذكاء الاصطناعي بين تقنية وقانونية:

#### 1_ التعريفات التقنية للذكاء الاصطناعي:

**أ_** الذكاء الاصطناعي (AI) : هو مجال علوم الكمبيوتر المخصص لحل المشكلات المعرفية المرتبطة عادةً بالذكاء البشري، مثل التعلم والإبداع والتعرف على الصور، تجمع المؤسسات الحديثة كميات كبيرة من البيانات من مصادر متنوعة مثل أجهزة الاستشعار الذكية والمحتوى الذي ينشئه الإنسان وأدوات المراقبة وسجلات النظام، والهدف من الذكاء الاصطناعي هو إنشاء أنظمة ذاتية التعلم تستخلص المعاني من البيانات، الأمر الذي يمكن للذكاء الاصطناعي من تطبيق تلك المعرفة لحل المشكلات الجديدة بطرق تشبه الإنسان، فعلى سبيل المثال يمكن لتقنية الذكاء الاصطناعي الاستجابة بشكل هادف للمحادثات البشرية، وإنشاء صور ونصوص أصلية، واتخاذ القرارات بناء على مدخلات البيانات في الوقت الفعلي، حيث يمكن

لمؤسستك دمج إمكانات الذكاء الاصطناعي في تطبيقاتك لتحسين عمليات الأعمال لديك وتحسين تجارب العملاء وتسريع الابتكار.[1]

هذا التعريف يركز على الجانب العلمي والتطبيقي للذكاء الاصطناعي، مشيراً إلى أنه فرع من علوم الحاسوب، كما يسلط الضوء على قدرة الذكاء الاصطناعي على محاكاة العمليات المعرفية البشرية، مع التركيز على ثلاثة جوانب رئيسية: التعلم، الإبداع، والتعرف على الصور.

**ب_** لقد أصبح الذكاء الاصطناعي مصطلحا شاملا للتطبيقات التي تؤدي مهاما معقدة كانت تتطلب في الماضي إدخالات بشرية مثل التواصل مع العملاء عبر الإنترنت، و يستخدم غالبا هذا المصطلح بالتبادل مع مجالاته الفرعية، والتي تشمل التعلم الآلي (ML) والتعلم العميق.[2]

ومع ذلك، هناك اختلافات فعلى سبيل المثال يركز التعلم الآلي على إنشاء أنظمة تتعلم أو تحسن من أدائها استنادا إلى البيانات التي تستهلكها، ومن المهم أن نلاحظ أنه على الرغم من أن كل سبل التعلم الآلي ما هي إلا ذكاء اصطناعي، فإنه ليس كل ذكاء اصطناعي يعد تعلمًا آليا.[3]

وللحصول على القيمة الكاملة من الذكاء الاصطناعي، تقوم العديد من الشركات باستثمارات كبيرة في فرق علوم البيانات، حيث يجمع علم البيانات بين الإحصاءات وعلوم الكمبيوتر والمعرفة بالأعمال لاستخلاص القيمة من مصادر البيانات المختلفة.[4]

إن هذا التعريف يضيف عنصرا مهما وهو القدرة على التحسين الذاتي المستمر بناء على البيانات المجمعة، هذا يشير ضمنيا إلى مفهوم التعلم الآلي كجزء أساسي من الذكاء الاصطناعي.

## 2_ خصائص الذكاء الاصطناعي:

من خلال التعاريف السابقة يمكن استنتاج جملة من الخصائص التي تميز الذكاء الاصطناعي والتي تنقسم إلى عنصرين:

[1] Amazon Web Services. (n.d.). ما هو الذكاء الاصطناعي :https://aws.amazon.com/ar/what-is /artificial-intelligence/

[2] بلعسل بنت نبي ياسمين، عمروش الحسين، الذكاء الاصطناعي ودوره في تحقيق التنمية المستدامة، مجلة الدراسات القانونية والاقتصادية، جامعة المسيلة، المجلد 05، العدد 01، 2022، ص 1155، 1156.

[3] المرجع نفسه، ص 1157.

[4] George Chapouthier, Frédéric Kaplan, l'homme, l'animal et la machine, Biblis, Paris, 2013, p. 42.

## أ_ الخصائص الأساسية للذكاء الاصطناعي:

الذكاء الاصطناعي يتميز بمجموعة من الخصائص الأساسية التي تميزه عن الأنظمة التقليدية:[5]

–القدرة على التعلم والتكيف: يمتلك الذكاء الاصطناعي القدرة على التعلم من البيانات والتجارب السابقة، وتحسين أدائه بمرور الوقت دون الحاجة إلى برمجة صريحة.

– معالجة اللغات الطبيعية: يمكن لأنظمة الذكاء الاصطناعي فهم وتحليل وإنتاج اللغة البشرية، مما يسمح بالتفاعل الطبيعي بين الإنسان والآلة.

–الرؤية الحاسوبية: القدرة على تحليل وفهم الصور والفيديوهات، مما يمكن الأنظمة من التعرف على الأشياء والوجوه وتفسير المشاهد المرئية.

–الاستدلال والتخطيط: يمكن لأنظمة الذكاء الاصطناعي استخلاص استنتاجات منطقية من المعلومات المتاحة ووضع خطط لتحقيق أهداف محددة.

## ب_ الخصائص المتقدمة والتطبيقية للذكاء الاصطناعي:

إضافة إلى الخصائص الأساسية، يتميز الذكاء الاصطناعي بخصائص متقدمة تجعله قابلا للتطبيق في مجالات متنوعة:[6]

– التعامل مع البيانات الضخمة: قدرة أنظمة الذكاء الاصطناعي على معالجة وتحليل كميات هائلة من البيانات بسرعة وكفاءة تفوق القدرات البشرية.

– الأتمتة الذكية: القدرة على أتمتة المهام المعقدة التي كانت تتطلب تدخلا بشريا في السابق، مما يؤدي إلى زيادة الكفاءة والإنتاجية في مختلف القطاعات.

– التكيف مع الظروف المتغيرة: يمكن لأنظمة الذكاء الاصطناعي التكيف مع البيئات والظروف المتغيرة، واتخاذ قرارات مستقلة بناء على المعطيات الجديدة.

– التعاون والتكامل: القدرة على العمل بشكل تعاوني مع الأنظمة الأخرى والبشر، مما يعزز الإنتاجية ويفتح آفاقا جديدة للابتكار.

[5] Jean François Dortier, le dictionnaire des sciences humaines, Delta, France, 2004, pp 367, 368

[6] هشام عمر خوجلي، سعيد مكيد، "المستقبل المدمج للأتمتة والذكاء الاصطناعي: دراسة بعض ميزات التأثير الاجتماعي والأخلاقي طويل المدى"، مجلة التكنولوجيا في المجتمع، جامعة عبد الحميد مهري، قسنطينة، المجلد 72، 2023، ص 102.

## ثانيا: تطبيقات الذكاء الاصطناعي في الشركات التجارية

تعددت تطبيقات الذكاء الاصطناعي بتعدد المجالات واختلافها، وقد شهدت تزايدا رهيبا ومستمرا، ويمكن تقسيم استخدامات الذكاء الاصطناعي في مجال الشركات التجارية إلى عنصرين أساسيين:

### 1_ استخدامات الذكاء الاصطناعي في مجال الإدارة:

يمكن تلخيص استخدامات الذكاء الاصطناعي في مجال الإدارة في عنصرين رئيسيين:

#### أ- تحسين العمليات الداخلية وزيادة الكفاءة التشغيلية:

- أتمتة المهام الروتينية: يساعد الذكاء الاصطناعي في أتمتة العمليات المعقدة التي كانت تتطلب تدخلا بشريا في السابق[7].

- إدارة البيانات وتحليلها: يقوم الذكاء الاصطناعي بتحليل كميات كبيرة من البيانات وتقديم رؤى قيمة لاتخاذ القرارات الإستراتيجية.[8]

- تحسين إدارة سلسلة التوريد: يستخدم الذكاء الاصطناعي في تحليل البيانات وتوقع المشكلات المحتملة في سلسلة التوريد قبل حدوثها.[9]

- إدارة المخزون والتنبؤ بالطلب: تستخدم الشركات نماذج التعلم الآلي لتحليل البيانات التاريخية للمبيعات والاتجاهات الموسمية، مما يؤدي إلى تنبؤات أكثر دقة للطلب وتحسين إدارة المخزون.[10]

#### ب_ تعزيز تجربة العملاء وتحسين عمليات الموارد البشرية:

[7] محمد علي، دور الذكاء الاصطناعي في تحويل عمليات الأعمال، مجلة التكنولوجيا والابتكار، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 15، العدد3، 2023، ص 45.

[8] حمد محمود، "تطبيقات الذكاء الاصطناعي في تحليل البيانات الضخمة ودعم القرار"، المجلة العربية للعلوم والمعلوماتية، جامعة الامام محمد بن سعيد الاسلامية، المملكة العربية السعودية، المجلد 8، العدد 2، 2022، ص. 78.

[9] المرجع نفسه، ص 78.

[10] سمير الحسيني، "تطبيقات الذكاء الاصطناعي في إدارة سلاسل التوريد: دراسة حالة لشركات التجزئة"، المجلة العربية للإدارة، الجامعة العربية، فلسطين، المجلد 43، العدد 1، 2023، ص. 112.

– تحسين خدمة العملاء: استخدام روبوتات الدردشة والمساعدين الافتراضيين لتوفير دعم للعملاء على مدار الساعة طوال أيام الأسبوع. [11]

– تخصيص تجربة العملاء: تحليل بيانات العملاء لتقديم توصيات منتجات تتوافق مع الأذواق الفردية وتحسين تجربة التسوق. [12]

– تحسين عمليات التوظيف: استخدام الذكاء الاصطناعي في فرز السير الذاتية وتحديد المرشحين المناسبين للوظائف، مما يوفر وقت مدراء التوظيف. [13]

– تقييم أداء الموظفين: استخدام الذكاء الاصطناعي في تتبع وتقييم حضور الموظفين وأدائهم، وتقديم تقارير دقيقة في الوقت المناسب.[14]

من خلال هذه الاستخدامات، يساعد الذكاء الاصطناعي الشركات على تحسين عملياتها الداخلية، وزيادة كفاءتها التشغيلية، وتعزيز تجربة العملاء، مما يؤدي إلى تحسين الأداء العام للمؤسسة وزيادة قدرتها التنافسية في السوق.

## 2_ تأثير الذكاء الاصطناعي على العمليات التجارية:

يعد الذكاء الاصطناعي من أبرز التقنيات التي غيرت وجه العالم التجاري في العصر الحديث، لذلك فإن فهم الآثار الإيجابية والسلبية للذكاء الاصطناعي على العمليات التجارية أمر بالغ الأهمية للشركات التي تسعى للاستفادة من هذه التقنية مع تجنب مخاطرها المحتملة.

## أ_ الأثر الإيجابي للذكاء الاصطناعي على العمليات التجارية:

[11] ليلى عبد الرحمن، "دور الذكاء الاصطناعي في تحسين تجربة العملاء: دراسة تحليلية لتطبيقات روبوتات الدردشة في قطاع الخدمات"، مجلة الاقتصاد والأعمال العربية، جامعة نايف، المملكة العربية السعودية، المجلد 7، العدد 4، 2022، ص. 89.

[12] عبد العزيز الشمسان، "كيف يمكن للذكاء الاصطناعي تحسين تجربة العملاء"، LinkedIn، تم الاطلاع عليه بتاريخ: 09_ 08_ 2024، على الساعة: 15: 15، https://ae.linkedin.com/pulse/كيف-يمكن-للذكاء-الاصطناعي-تحسين-تجربة-العملاء-abdulaziz-alshamsan

[13] نورا السعيد، "دور الذكاء الاصطناعي في تطوير عمليات التوظيف: دراسة تحليلية لتقنيات فرز السير الذاتية"، المجلة العربية لإدارة الموارد البشرية، جامعة نايف العربية للعلوم الأمنية ، المملكة العربية السعودية، المجلد 5، العدد 2، 2023، ص. 67.

[14] نورا السعيد، المرجع السابق، ص 67.

يحدث الذكاء الاصطناعي تأثيرا إيجابيا عميقا على العمليات التجارية، حيث يعمل على تحسين الكفاءة والإنتاجية من خلال أتمتة المهام الروتينية والمعقدة، مما يقلل الأخطاء البشرية ويزيد الإنتاجية. كما يعزز تجربة العملاء عبر تقديم خدمات مخصصة وتحسين التفاعل معهم، ويدعم صنع القرار من خلال تحليل كميات هائلة من البيانات بسرعة ودقة، كما يساهم الذكاء الاصطناعي في تحسين إدارة سلسلة التوريد والتنبؤ بالطلب، ويعزز الابتكار وتطوير المنتجات استجابة لاحتياجات السوق المتغيرة. علاوة على ذلك، يحسن إدارة المخاطر ويعزز الأمن السيبراني، ويمكن التسويق المستهدف بدقة أكبر، يساعد في الصيانة التنبؤية لتقليل وقت التعطل وتكاليف الصيانة، ويدعم جهود الاستدامة البيئية من خلال تحسين كفاءة استخدام الموارد، وأخيرا يعزز التعاون والتواصل الداخلي في المؤسسات، مما يخلق بيئة عمل أكثر كفاءة وإنتاجية. هذه التحسينات المتعددة تمكن الشركات من البقاء تنافسية وتلبي احتياجات عملائها بشكل أفضل في العصر الرقمي.[15]

## ب_ الأثر السلبي للذكاء الاصطناعي على العمليات التجارية:

رغم الفوائد العديدة للذكاء الاصطناعي، إلا أنه يحمل معه بعض الآثار السلبية المحتملة على العمليات التجارية، فقد يؤدي إلى فقدان بعض الوظائف التقليدية، مما يخلق تحديات اجتماعية واقتصادية تتطلب إعادة تأهيل القوى العاملة. كما أن تكاليف تنفيذ وصيانة أنظمة الذكاء الاصطناعي قد تكون مرتفعة، خاصة للشركات الصغيرة والمتوسطة، وتثير عملية جمع وتحليل كميات كبيرة من بيانات العملاء مخاوفا بشأن الخصوصية وأمن البيانات، كما قد يؤدي الاعتماد المفرط على الذكاء الاصطناعي إلى ضعف في المهارات البشرية الأساسية وزيادة الضعف أمام الأعطال التقنية، إضافة إلى أن قرارات الذكاء الاصطناعي قد تتأثر بالتحيزات الموجودة في البيانات التدريبية، مما قد يؤدي إلى نتائج غير عادلة أو غير دقيقة، ناهيك عن امكانية مواجهة الشركات لتحديات في ضمان الشفافية والمساءلة في عمليات صنع القرار المعتمدة على الذكاء الاصطناعي، مما قد يؤثر على ثقة العملاء والموظفين، فضلا عن الأثمان الباهضة التي تفرض على الشركات التجارية مقابل اشتراكها للاستفادة من خدمات الذكاء الاصطناعي، وأخيرا قد تنشأ مخاوف أخلاقية

[15] محمد الصادق، "تأثير الذكاء الاصطناعي على العمليات التجارية: دراسة تحليلية شاملة"، المجلة العربية للإدارة والاقتصاد الرقمي، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 5، العدد 2، 2023، ص. 78–95.

وقانونية جديدة تتطلب تطوير أطر تنظيمية جديدة لضمان الاستخدام المسؤول للذكاء الاصطناعي في بيئة الأعمال.[16]

## المطلب الثاني: إشكالات تطبيق المسؤولية الجزائية في سياق الذكاء الاصطناعي

يثير تطبيق المسؤولية الجزائية في سياق الذكاء الاصطناعي تحديات قانونية وأخلاقية غير مسبوقة، تتجاوز الأطر التقليدية للقانون الجنائي، هذه الإشكالات تنبع من الطبيعة الفريدة لأنظمة الذكاء الاصطناعي، والتي تتميز بقدرتها على التعلم الذاتي واتخاذ القرارات المستقلة، مما يستدعي إعادة النظر في مفاهيم الإرادة والقصد الجنائي والعلاقة السببية.

### أولا: إشكالات مرتبطة بأركان الجريمة

تتلخص إشكالات تطبيق المسؤولية الجزائية في سياق الذكاء الاصطناعي المرتبطة بأركان الجريمة فيما يلي:

#### 1_ صعوبة تحديد الركن المعنوي في جرائم الذكاء الاصطناعي:

تشكل صعوبة تحديد الركن المعنوي في جرائم الذكاء الاصطناعي تحدياً كبيراً للنظم القانونية التقليدية، حيث تتجلى هذه الصعوبة في عدة جوانب متداخلة، فغياب الإرادة والقصد الجنائي التقليدي لدى أنظمة الذكاء الاصطناعي، إلى جانب قدرتها على اتخاذ قرارات مستقلة دون تدخل بشري مباشر، يجعل من الصعب تطبيق مفاهيم المسؤولية الجنائية المعهودة، كما أن تعقيد الخوارزميات وصعوبة فهم عملية صنع القرار في أنظمة التعلم الآلي العميق يزيد من تعقيد المسألة[17]، يضاف إلى ذلك تعدد الأطراف المشاركة في تطوير وتشغيل هذه الأنظمة، مما يصعب تحديد المسؤول الجنائي بدقة، علاوة على ذلك فإن قدرة بعض أنظمة الذكاء الاصطناعي على التعلم والتطور الذاتي قد تؤدي إلى نتائج غير متوقعة، مما يزيد من تعقيد تحديد المسؤولية، هذه العوامل مجتمعة تبرز الحاجة الملحة إلى تطوير أطر قانونية جديدة تتكيف مع طبيعة

[16] سارة المنصوري، "التحديات الأخلاقية والاجتماعية للذكاء الاصطناعي في بيئة الأعمال: دراسة تحليلية نقدية"، المجلة العربية لأخلاقيات الأعمال والتكنولوجيا، المجلد 4، العدد 3، 2023، ص. 112-130.

[17] أحمد محمد، "تحديات تحديد المسؤولية الجنائية في جرائم الذكاء الاصطناعي: دراسة تحليلية مقارنة"، المجلة العربية للعلوم الجنائية والقانونية، جامعة الإسكندرية، المجلد 8، العدد 2، 2023، ص 45.

الذكاء الاصطناعي وتحدياته الفريدة، لضمان تحديد المسؤولية الجنائية بشكل عادل وفعال في عصر التكنولوجيا المتقدمة.[18]

## 2_ إشكالية العلاقة السببية بين فعل المسير وضرر الذكاء الاصطناعي:

تمثل العلاقة السببية بين فعل المسير وضرر الذكاء الاصطناعي تحدياً جوهرياً في تطبيق المسؤولية الجزائية التقليدية، حيث تتجلى صعوبات متعددة في إثبات هذه العلاقة، فاستقلالية القرار التي تتمتع بها أنظمة الذكاء الاصطناعي تجعل من الصعب ربط الضرر الناتج بتوجيهات المسير المباشرة، كما أن تداخل العوامل المؤثرة في إحداث الضرر، من بيانات مدخلة وبيئة محيطة وتفاعلات مع أنظمة أخرى يزيد من تعقيد تحديد المسؤولية، يضاف إلى ذلك التعقيد التقني الذي يواجه المحاكم والخبراء القانونيين في فهم آليات عمل هذه الأنظمة وتحديد نقاط الخلل بدقة، كما أن التطور المستمر للأنظمة وتحديثاتها المتواصلة يجعل من الصعب تحديد اللحظة الدقيقة التي حدث فيها الخطأ، هذه العوامل مجتمعة تشكل تحدياً كبيراً أمام النظم القانونية التقليدية، مما يستدعي إعادة النظر في مفاهيم العلاقة السببية وتطوير أطر قانونية جديدة تتناسب مع طبيعة الذكاء الاصطناعي وخصائصه الفريدة.[19]

## ثانيا: إشكالات مرتبطة بطبيعة المسؤولية الجزائية

تتلخص إشكالات تطبيق المسؤولية الجزائية في سياق الذكاء الاصطناعي المرتبطة بطبيعة المسؤولية الجزائية فيما يلي:

## 1_ توسيع نطاق المسؤولية ليشمل الإشراف على أنظمة الذكاء الاصطناعي

في ضوء التحديات الناشئة عن استخدام الذكاء الاصطناعي، يتعين على المنظومة القانونية تبني نهج أكثر شمولية في تحديد المسؤولية الجزائية. يمكن تحقيق ذلك من خلال توسيع نطاق المسؤولية ليشمل الإشراف على أنظمة الذكاء الاصطناعي، مما يستلزم إعادة تعريف مفهوم المسؤولية في السياق التكنولوجي الحديث. فمن جهة، يمكن تطبيق مبدأ مسؤولية الإشراف،[20] حيث يتحمل المسؤولون عن تشغيل وإدارة الأنظمة عبء الرقابة الفعالة والمتابعة المستمرة لأداء هذه الأنظمة. ومن جهة أخرى، يمكن فرض واجب

[18] المرجع نفسه، ص 52.

[19] فاطمة الزهراء، "إشكاليات تحديد المسؤولية الجنائية في جرائم الذكاء الاصطناعي: نحو إطار قانوني جديد"، المجلة العربية للدراسات القانونية والقضائية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 6، العدد 3، 2023، ص 97.

[20] المرجع نفسه، ص 99.

العناية القانوني على المطورين والمشغلين، مما يلزمهم باتخاذ كافة التدابير اللازمة لضمان سلامة وأمان الأنظمة. كما يمكن توسيع نطاق المسؤولية ليشمل المؤسسات والشركات التي تطور وتستخدم أنظمة الذكاء الاصطناعي، وذلك من خلال تطبيق مفهوم المسؤولية المؤسسية.[21] هذا النهج من شأنه أن يحفز الشركات على تبني سياسات وإجراءات أكثر صرامة في مجال الامتثال والرقابة. علاوة على ذلك، يمكن فرض إجراءات للتدقيق والمراجعة الدورية لأنظمة الذكاء الاصطناعي، مما يضمن امتثالها المستمر للمعايير القانونية والأخلاقية المعمول بها. هذه الإجراءات مجتمعة من شأنها أن تشكل إطارًا قانونيًا متكاملًا يوازن بين تشجيع الابتكار التكنولوجي وضمان المساءلة القانونية، مع مراعاة الطبيعة الديناميكية والمعقدة لأنظمة الذكاء الاصطناعي. وبذلك، يمكن للقانون أن يتكيف مع التحديات الجديدة التي يفرضها عصر الذكاء الاصطناعي، مع الحفاظ على مبادئ العدالة والمسؤولية الأساسية.[22]

## 2_ مبدأ الحيطة والعناية الواجبة في إدارة تقنيات الذكاء الاصطناعي:

يعد تطبيق مبدأ الحيطة والعناية الواجبة في إدارة تقنيات الذكاء الاصطناعي خطوة محورية نحو تأسيس إطار قانوني متكامل يضمن الاستخدام الآمن والمسؤول لهذه التقنيات المتطورة، هذا المبدأ الذي يستند إلى أسس راسخة في القانون البيئي والصحي، يمكن تكييفه بفعالية ليشمل مجال الذكاء الاصطناعي، مما يوفر أساسًا قويًا للتنظيم القانوني،[23] في هذا السياق يبرز تقييم المخاطر كعنصر أساسي حيث يتعين على المطورين والمستخدمين إجراء تحليلات شاملة للمخاطر المحتملة قبل نشر أي نظام ذكاء اصطناعي، مما يسهم في تعزيز الوقاية والحد من الأضرار المحتملة، كما تشكل الشفافية ركيزة أساسية في هذا الإطار، إذ يتوجب على الجهات المعنية الكشف عن آليات عمل أنظمتها وقراراتها، مما يسهل عملية المساءلة ويعزز الثقة العامة، علاوة على ذلك يعد التدريب والتأهيل المناسب للأفراد المسؤولين عن إدارة وتشغيل أنظمة الذكاء الاصطناعي عنصرًا حيويًا في ضمان الاستخدام الأمثل والآمن لهذه التقنيات، وأخيرًا فإن وضع آليات للاستجابة السريعة والفعالة في حالات الطوارئ أو حدوث أخطاء يعد ضرورة قصوى لتقليل الأضرار المحتملة وضمان الاستجابة الفورية لأي مشكلات قد تنشأ. هذا النهج الشامل في تطبيق مبدأ الحيطة

[21] فاطمة الزهراء، المرجع السابق، ص 100.

[22] Soyer, Baris, and Andrew Tettenborn. "Artificial intelligence and civil liability—do we need a new regime?" International Journal of Law and Information Technology 30, no. 4 (Winter 2022): 385

[23] سمير الحسيني، "تطبيق مبدأ الحيطة والعناية الواجبة في إدارة تقنيات الذكاء الاصطناعي: نحو إطار قانوني متكامل"، المجلة العربية للقانون والتكنولوجيا، الجامعة العربية، فلسطين، المجلد 6، العدد 2، 2023، ص. 88.

والعناية الواجبة من شأنه أن يوفر إطارًا قانونيًا متوازنًا يشجع الابتكار مع ضمان الحماية اللازمة للمجتمع، ويمكن أن يشكل أساسًا لتطوير تشريعات وسياسات أكثر تفصيلاً في مجال تنظيم الذكاء الاصطناعي.[24]

من خلال هذه الاستراتيجيات يمكن تكييف مفاهيم المسؤولية الجزائية التقليدية لتتناسب مع التحديات الفريدة التي يفرضها الذكاء الاصطناعي، مع ضمان المساءلة والحماية القانونية في الوقت نفسه.

## المبحث الثاني: تصنيف جرائم مسير الشركة التجارية المرتبطة بالذكاء الاصطناعي

يتناول هذا المبحث تصنيفاً شاملاً لجرائم مسير الشركة التجارية المرتبطة بالذكاء الاصطناعي، حيث يهدف هذا التصنيف إلى توضيح الأنماط المختلفة للجرائم التي قد يرتكبها مسيرو الشركات في سياق استخدام أو إساءة استخدام تقنيات الذكاء الاصطناعي، مع الأخذ بعين الاعتبار الطبيعة المعقدة والمتغيرة لهذه التقنيات والتي يمكن تقسيمها إلى صنفين أساسيين جرائم التي يكون فيها الذكاء الاصطناعي أداة للجريمة، وأخرى يكون فيها هدفاً للجريمة.

### المطلب الأول: الجرائم التي يكون فيها الذكاء الاصطناعي أداة للجريمة

سيتم في هذا الجزء من الدراسة تحديد الجرائم التي يكون فيها الذكاء الاصطناعي أداة للجريمة، من خلال التفصيل في الأركان العامة وخاصة الركن المادي والمعنوي على اعتبار أن موضوع الذكاء الاصطناعي لا يزال حديثا وبالتالي احتمالية غياب الركن الشرعي المتمثل في مختلف النصوص القانونية المجرمة للتلاعب بالأسواق المالية في قانون العقوبات وقوانين الأوراق المالية وقوانين الجرائم الإلكترونية، وكذلك القوانين المتعلقة بحماية الخصوصية والسمعة.

#### أولا_ الاحتيال المالي باستخدام تقنيات الذكاء الاصطناعي للتلاعب بالأسواق المالية:

في هذا الصنف، يستخدم المجرمون تقنيات الذكاء الاصطناعي كوسيلة لارتكاب جرائم تقليدية أو مستحدثة، من خلال الاعتماد على الغش والاحتيال:

#### 1_ الركن المادي:

يتجلى الركن المادي لجريمة الاحتيال المالي باستخدام تقنيات الذكاء الاصطناعي للتلاعب بالأسواق المالية في سلسلة متكاملة من العناصر المترابطة، يبدأ هذا الركن بالسلوك الإجرامي المتمثل في استخدام تقنيات الذكاء الاصطناعي للتلاعب بالبيانات أو الأسعار في الأسواق المالية، وإجراء عمليات تداول

[24] المرجع نفسه، ص 90.

مصطنعة أو وهمية باستخدام خوارزميات متطورة، وبرمجة أنظمة ذكية لتنفيذ استراتيجيات تداول غير مشروعة، هذا السلوك يؤدي إلى نتيجة إجرامية تتمثل في التأثير غير المشروع على أسعار الأوراق المالية أو السلع، وتحقيق أرباح غير قانونية، مع إلحاق الضرر بالمستثمرين وسلامة السوق، وتتحقق العلاقة السببية عندما يكون هناك رابط مباشر بين استخدام هذه التقنيات والتأثير الملموس على الأسواق.[25] تعتمد هذه الجريمة على وسائل تقنية متقدمة كأنظمة الذكاء الاصطناعي، وخوارزميات التداول عالية التردد، وأدوات تحليل البيانات الضخمة، مستهدفة الأسواق المالية بمختلف أنواعها والبيانات المالية والاقتصادية الحساسة، إن تعقيد هذه العناصر وترابطها يجعل من الصعب إثبات الجريمة وتحديد المسؤولية الجنائية بدقة، مما يستدعي تطوير أساليب تحقيق وإثبات متخصصة تتناسب مع الطبيعة التقنية المعقدة لهذه الجريمة المستحدثة.[26]

## 2_ الركن المعنوي:

يتسم الركن المعنوي لجريمة الاحتيال المالي باستخدام تقنيات الذكاء الاصطناعي للتلاعب بالأسواق المالية بتعقيد خاص، نظراً للطبيعة التقنية المتطورة لهذه الجريمة، يتمثل هذا الركن أساساً في القصد الجنائي العام، الذي يتجلى في علم الجاني بعناصر الجريمة وإرادته في تحقيق نتائجها، فالجاني يدرك تماماً أنه يستخدم تقنيات الذكاء الاصطناعي بشكل غير مشروع للتأثير على الأسواق المالية، ويتجه قصده إلى تحقيق مكاسب مالية غير قانونية، كما يتوفر القصد الجنائي الخاص المتمثل في نية الاحتيال والتلاعب بالسوق، حيث يسعى الجاني عمداً إلى خداع المتعاملين في السوق وتضليلهم، ويمتد هذا القصد ليشمل الوعي بالآثار السلبية لأفعاله على سلامة واستقرار الأسواق المالية، ومع ذلك فإن الطبيعة المعقدة لأنظمة الذكاء الاصطناعي قد تثير تحديات في إثبات هذا الركن، خاصة عندما تكون الخوارزميات قادرة على التعلم والتطور الذاتي، فقد يدفع المتهم بأنه لم يكن على دراية كاملة بكيفية عمل النظام أو بالنتائج المحددة لأفعاله، لذا قد يتطلب الأمر توسيع مفهوم القصد الجنائي ليشمل الإهمال الجسيم أو عدم اتخاذ الاحتياطات اللازمة عند استخدام هذه التقنيات المتطورة في الأسواق المالية. وبالتالي، فإن تحديد وإثبات الركن المعنوي

[25] محمد الصادق، "الجرائم المالية المرتكبة باستخدام الذكاء الاصطناعي: دراسة تحليلية للركن المادي"، المجلة العربية للدراسات الأمنية والقانونية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 7، العدد 2، 2023، ص. 123.

[26] المرجع نفسه، ص 125.

في هذه الجريمة يستدعي تطوير معايير قانونية جديدة تتناسب مع التحديات التي تفرضها تكنولوجيا الذكاء الاصطناعي في المجال المالي.[27]

## ثانيا_ التصيد الاحتيالي المتطور باستخدام رسائل مخصصة ومقنعة تم إنشاؤها بواسطة الذكاء الاصطناعي:

يتمثل الركن المادي والمعنوي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة التصيد الاحتيالي المتطور باستخدام الذكاء الاصطناعي في سلسلة من الأفعال المترابطة والمعقدة تقنياً.[28] يبدأ هذا الركن بإنشاء رسائل مخصصة ومقنعة باستخدام تقنيات الذكاء الاصطناعي المتقدمة، حيث يتم جمع وتحليل البيانات الشخصية للضحايا المستهدفين من مصادر متعددة، بما في ذلك وسائل التواصل الاجتماعي والمعلومات المتاحة للعموم. ثم يقوم النظام الذكي بصياغة رسائل فردية تحاكي بدقة أسلوب التواصل الطبيعي، مستخدماً معلومات شخصية ومهنية دقيقة لزيادة مصداقيتها. يشمل السلوك الإجرامي أيضاً إرسال هذه الرسائل المخصصة عبر قنوات متعددة، مثل البريد الإلكتروني أو الرسائل النصية أو تطبيقات التواصل الاجتماعي، مع تضمينها روابط خبيثة أو مرفقات ضارة مصممة لاختراق أنظمة الضحية أو سرقة معلوماتها الحساسة. قد يتضمن الركن المادي أيضاً إنشاء مواقع ويب مزيفة تحاكي بدقة المواقع الشرعية، باستخدام تقنيات الذكاء الاصطناعي لتحسين التصميم والمحتوى. النتيجة الإجرامية تتمثل في الحصول على معلومات حساسة مثل بيانات تسجيل الدخول أو تفاصيل البطاقات الائتمانية، أو تثبيت برمجيات خبيثة على أجهزة الضحايا. تعقيد هذه العملية وتطورها التقني يجعل من الصعب اكتشافها ومكافحتها بالوسائل التقليدية، مما يزيد من خطورتها وفعاليتها.[29]

### 2_ الركن المعنوي:

---

[27] محمد الصادق، "الجرائم المالية المرتكبة باستخدام الذكاء الاصطناعي: دراسة تحليلية للركن المادي"، المجلة العربية للدراسات الأمنية والقانونية، المرجع السابق، ص 93، 94.

[28] المجرمون الإلكترونيون والذكاء الاصطناعي: ليس مجرد تصيد احتيالي أفضل"، تقرير تحليلي، 2024، تم الاطلاع عليه بتاريخ : 08_08_ 2024، على الساعة: 12:19، https://intel471.com/blog/cybercriminals-and-ai-not-just-better-phishing

[29] مركز الأمن السيبراني الوطني (NCSC)، "كيف يمكن للذكاء الاصطناعي أن يغير مشهد التهديدات السيبرانية"، تقرير تحليلي، 2023، تم الاطلاع عليه بتاريخ 08_08_2024،على الساعة:12:19، https://www.ncsc.gov.uk/blog-post/how-ai-could-change-the-cyber-threat-landscape

يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي المتمثل في نية خداع الضحايا والحصول على معلوماتهم بطرق احتيالية مع العلم بأن الرسائل المرسلة هي وسيلة للاحتيال.

## ثالثا_ إنشاء محتوى مزيف (deepfakes) لأغراض الابتزاز أو التشهير:

يتمثل الركن المادي والمعنوي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة إنشاء محتوى مزيف (deepfakes) لأغراض الابتزاز أو التشهير في سلسلة من الأفعال المترابطة والمعقدة تقنياً، يبدأ هذا الركن باستخدام تقنيات الذكاء الاصطناعي المتقدمة، خاصة خوارزميات التعلم العميق، لإنشاء محتوى مرئي أو صوتي مزيف يبدو حقيقياً للغاية، يشمل ذلك جمع صور أو مقاطع فيديو أو تسجيلات صوتية للضحية، ثم معالجتها باستخدام برامج متخصصة لدمجها مع محتوى آخر أو تعديلها بشكل جذري، يتضمن السلوك الإجرامي أيضاً نشر هذا المحتوى المزيف عبر وسائل التواصل الاجتماعي أو المنصات الإلكترونية الأخرى، أو استخدامه كأداة للابتزاز من خلال التهديد بنشره، أما النتيجة الإجرامية فتتمثل في الإضرار بسمعة الضحية أو خصوصيتها، أو إجبارها على الاستجابة لمطالب الجاني تحت تهديد نشر المحتوى المزيف.[30] يتميز هذا الركن المادي بصعوبة اكتشافه وإثباته نظراً للتطور التقني المستخدم في إنشاء المحتوى المزيف، مما يجعل التمييز بينه وبين المحتوى الحقيقي أمراً بالغ الصعوبة حتى للخبراء.

### 1_ الركن المادي:

يتجسد الركن المعنوي في جريمة إنشاء محتوى مزيف (deepfakes) لأغراض الابتزاز أو التشهير في القصد الجنائي المزدوج. يتمثل القصد العام في علم الجاني بطبيعة أفعاله وإرادته في تنفيذها، حيث يدرك تماماً أنه يستخدم تقنيات الذكاء الاصطناعي لإنشاء محتوى مزيف ويتجه إرادياً نحو هذا الفعل. أما القصد الخاص فيتجلى في نية الابتزاز أو التشهير، حيث يهدف الجاني تحديداً إلى الإضرار بسمعة الضحية أو إجبارها على الاستجابة لمطالبه. هذا التلازم بين الوعي التقني والنية الإجرامية يشكل جوهر الركن المعنوي،

[30] محمد سالمة عبد المنعم، "جريمة الانتقام الإباحي عبر تقنية التزييف العميق deepfakes والمسئولية الجنائية عنها"، مجلة الحقوق الاقتصادية للبحوث القانونية، جامعة الإسكندرية، العدد 2 (1)، 2022، ص. 637.

مع ملاحظة أن تعقيد التقنيات المستخدمة قد يثير تحديات في إثبات هذا الركن، خاصة في حالات التطور السريع لتقنيات الذكاء الاصطناعي.[31]

## المطلب الثاني: الجرائم التي يكون فيها الذكاء الاصطناعي هدفا للجريمة

في كل هذه الجرائم، يلاحظ أن استخدام تقنيات الذكاء الاصطناعي يشكل عنصراً أساسياً في الركن المادي، مما يتطلب تحديثاً مستمراً للتشريعات لمواكبة التطورات التكنولوجية وضمان تغطية هذه الأشكال الجديدة من الجرائم.

### أولا_ تعطيل أو اختراق الأنظمة التي تعتمد على الذكاء الاصطناعي:

يتمثل الركن المادي والمعنوي لجريمة تعطيل أو اختراق الأنظمة التي تعتمد على الذكاء الاصطناعي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة تعطيل أو اختراق الأنظمة التي تعتمد على الذكاء الاصطناعي في سلسلة من الأفعال المترابطة والمعقدة تقنياً، يبدأ هذا الركن بالدخول غير المصرح به إلى أنظمة الذكاء الاصطناعي، سواء عن طريق اختراق الحماية الأمنية أو استغلال ثغرات في البرمجيات، ثم يتضمن تنفيذ أوامر أو برامج ضارة تهدف إلى تعطيل عمل النظام أو تغيير وظائفه الأساسية، مما قد يشمل تعديل الخوارزميات، أو التلاعب بقواعد البيانات التي يعتمد عليها النظام في اتخاذ القرارات.[32]
كما قد يتضمن الركن المادي أيضاً إدخال بيانات مضللة أو خاطئة لتشويه مخرجات النظام، أو استخراج معلومات حساسة بطريقة غير مشروعة، وقد يمتد ليشمل منع الوصول المشروع إلى النظام أو تعطيل خدماته.

النتيجة الإجرامية تتمثل في إحداث خلل في أداء نظام الذكاء الاصطناعي أو تعطيله كلياً أو جزئياً، مما قد يؤدي إلى أضرار مادية أو معنوية للجهات المعتمدة على هذه الأنظمة، ويتحقق الركن المادي بمجرد القيام

[31] المرجع نفسه، ص 637.

[32] بوزنون سعيدة، "كيانات الذكاء الاصطناعي في فكر القانون الجنائي"، مجلة المعيار، جامعة عبد الحميد بن باديس، مستغانم، المجلد 28، العدد 4، 2024، ص. 571.

بأي من هذه الأفعال، حتى لو لم تتحقق النتيجة المرجوة من الاختراق أو التعطيل، نظراً لخطورة هذه الأفعال على أمن وسلامة أنظمة الذكاء الاصطناعي.[33]

### 2_ الركن المعنوي:

يتجسد الركن المعنوي في جريمة تعطيل أو اختراق الأنظمة التي تعتمد على الذكاء الاصطناعي في القصد الجنائي بشقيه العام والخاص، يتمثل القصد العام في علم الجاني الكامل بطبيعة أفعاله غير المشروعة وإرادته الحرة في تنفيذها، حيث يدرك تماماً أنه يقوم بالدخول غير المصرح به إلى أنظمة الذكاء الاصطناعي أو يسعى لتعطيلها، أما القصد الخاص فيتجلى في نية الجاني تحقيق هدف محدد، سواء كان ذلك إلحاق الضرر بالنظام، أو الحصول على معلومات سرية، أو إثبات قدراته التقنية، ويمتد هذا القصد ليشمل الوعي بالآثار المحتملة لأفعاله على أداء النظام وسلامته، ومن الجدير بالذكر أن تعقيد أنظمة الذكاء الاصطناعي قد يثير تحديات في إثبات هذا الركن، خاصة في الحالات التي قد يدعي فيها المتهم عدم إدراكه الكامل لعواقب أفعاله نظراً لتعقيد النظام. لذا قد يتطلب الأمر توسيع مفهوم القصد الجنائي ليشمل الإهمال الجسيم أو عدم اتخاذ الاحتياطات اللازمة عند التعامل مع هذه الأنظمة

الحساسة، مما يستدعي تطوير معايير قانونية جديدة لتقييم القصد الجنائي في سياق الجرائم المتعلقة بالذكاء الاصطناعي. [34]

## ثانيا_ تسميم البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي:

يتمثل الركن المادي والمعنوي لجريمة تسميم البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة تسميم البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي في سلسلة من الأفعال المعقدة والمتداخلة تقنياً، يبدأ هذا الركن بالتدخل المتعمد في مجموعات البيانات المستخدمة لتدريب النماذج، سواء عن طريق إدخال بيانات مضللة أو خاطئة، أو تعديل البيانات الموجودة بطريقة تؤثر على نتائج التعلم، قد يشمل ذلك إضافة أمثلة مصممة خصيصاً لإحداث تحيزات معينة في

[33] بوزنون سعيدة، مرجع سابق الذكر، ص 579.

[34] محمد الصادق، "الجرائم المالية المرتكبة باستخدام الذكاء الاصطناعي: دراسة تحليلية للركن المادي"، المجلة العربية للدراسات الأمنية والقانونية، المرجع السابق، ص129.

النموذج، أو إدخال بيانات ضارة تهدف إلى تشويه مخرجات النظام، كما قد يتضمن الركن المادي التلاعب بخوارزميات معالجة البيانات أو تغيير معايير التدريب بشكل يؤدي إلى نتائج مضللة أو متحيزة، ويمتد هذا الركن ليشمل أيضاً أي محاولات لإخفاء هذا التلاعب، مثل استخدام تقنيات متطورة لجعل البيانات المسممة تبدو طبيعية وغير قابلة للاكتشاف بالوسائل التقليدية.[35]

أما النتيجة الإجرامية تتمثل في إنتاج نموذج ذكاء اصطناعي معيب أو متحيز، قادر على اتخاذ قرارات خاطئة أو ضارة عند تطبيقه في العالم الحقيقي، ويتحقق الركن المادي بمجرد القيام بأي من هذه الأفعال، حتى لو لم تظهر آثارها الضارة فوراً، نظراً لخطورة هذه الممارسات على سلامة وموثوقية أنظمة الذكاء الاصطناعي.[36]

إن تعقيد هذه العملية وطبيعتها التقنية المتقدمة تجعل من الصعب اكتشافها ومكافحتها بالوسائل التقليدية، مما يزيد من تأثيرها المحتمل على مجموعة واسعة من التطبيقات التي تعتمد على الذكاء الاصطناعي.[37]

## 2_الركن المعنوي:

يتجلى الركن المعنوي في هذه الجريمة في القصد الجنائي بشقيه العام والخاص. فالقصد العام يتمثل في علم الجاني بطبيعة أفعاله وإرادته في تنفيذها، حيث يدرك تماماً أنه يقوم بالتلاعب بالبيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي بطريقة غير مشروعة، ويتجه إرادياً نحو هذا الفعل، أما القصد الخاص فيتجلى في نية الجاني تحقيق هدف محدد، كإحداث تحيزات معينة في النموذج أو جعله يتخذ قرارات خاطئة أو ضارة. [38]

ويمتد هذا القصد ليشمل الوعي بالآثار المحتملة لأفعاله على أداء النظام وسلامته، وإدراك مدى خطورة هذه الأفعال على موثوقية وأمان أنظمة الذكاء الاصطناعي، ومن الجدير بالذكر أن تعقيد عملية تسميم البيانات وطبيعتها التقنية المتقدمة قد تثير تحديات في إثبات هذا الركن، خاصة في الحالات التي قد يدعي فيها المتهم عدم إدراكه الكامل لعواقب أفعاله نظراً لتعقيد النظام.

---

[35] "ما هو تسميم البيانات (تسميم الذكاء الاصطناعي) وكيف يعمل؟"، TechTarget، تم الاطلاع عليه بتاريخ : 08_08 2024، على الساعة: 16:13

[36] عبد الله الغامدي، "تسميم البيانات: التهديد الخفي لأنظمة الذكاء الاصطناعي"، مجلة الأمن السيبراني، جامعة الملك سعود، المملكة العربية السعودية، المجلد 3، العدد 2، 2023، ص56.

[37] المرجع نفسه، ص 57.

[38] سمير الحسيني، "الركن المعنوي في جرائم تسميم البيانات: دراسة تحليلية في إطار القانون الجنائي"، المجلة العربية للعلوم الجنائية والقانونية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 9، العدد 1، 2024، ص. 80- 81.

وبالتالي قد يتطلب الأمر توسيع مفهوم القصد الجنائي ليشمل الإهمال الجسيم أو عدم اتخاذ الاحتياطات اللازمة عند التعامل مع هذه الأنظمة الحساسة، مما يستدعي تطوير معايير قانونية جديدة لتقييم القصد الجنائي في سياق الجرائم المتعلقة بتسميم بيانات الذكاء الاصطناعي.[39]

## ثالثا_ التحايل على أنظمة التعرف على الوجه أو تقنيات الأمان المعتمدة على الذكاء الاصطناعي:

يتمثل الركن المادي والمعنوي لجريمة التحايل على أنظمة التعرف على الوجه أو تقنيات الأمان المعتمدة على الذكاء الاصطناعي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة التحايل على أنظمة التعرف على الوجه أو تقنيات الأمان المعتمدة على الذكاء الاصطناعي في سلسلة من الأفعال المعقدة والمتداخلة تقنياً، يبدأ هذا الركن بمحاولة خداع النظام من خلال استخدام وسائل متطورة مثل الأقنعة المصممة خصيصاً أو تقنيات التزييف العميق (Deepfake) لإنشاء صور أو فيديوهات مزيفة تحاكي الوجوه الحقيقية، كما قد يشمل التلاعب بالبيانات المدخلة إلى النظام أو محاولة تغيير الخوارزميات المستخدمة في عملية التعرف، ويمتد هذا الركن ليشمل أيضاً استغلال نقاط الضعف في أنظمة الأمان، مثل استخدام تقنيات متقدمة لتجاوز آليات التحقق من الهوية أو اختراق قواعد البيانات التي تحتوي على معلومات القياسات الحيوية، وقد يتضمن السلوك الإجرامي أيضاً محاولات لتشويش أو تعطيل أجهزة الاستشعار والكاميرات المستخدمة في عملية التعرف على الوجه. النتيجة الإجرامية تتمثل في نجاح المتهم في تجاوز نظام الأمان أو الحصول على وصول غير مصرح به إلى أماكن أو معلومات محمية. ويتحقق الركن المادي بمجرد القيام بأي من هذه الأفعال، حتى لو لم تنجح المحاولة في النهاية، نظراً لخطورة هذه الأفعال على سلامة وموثوقية أنظمة الأمان المعتمدة على الذكاء الاصطناعي.[40]

### 2_ الركن المعنوي:

يتجسد الركن المعنوي في جريمة التحايل على أنظمة التعرف على الوجه أو تقنيات الأمان المعتمدة على الذكاء الاصطناعي في القصد الجنائي بشقيه العام والخاص، ويتمثل القصد العام في علم الجاني الكامل بطبيعة أفعاله غير المشروعة وإرادته الحرة في تنفيذها، حيث يدرك تماماً أنه يسعى لخداع أو تجاوز

[39] سمير الحسيني، مرجع سابق الذكر، ص 85.

[40] بن شهيدة محمد، "الملكية الفكرية والتحديات القانونية في تكنولوجيا الذكاء الاصطناعي"، مجلة التراث، جامعة زيان عاشور، الجلفة، المجلد 13، العدد 4، 2023، ص. 27-28.

أنظمة أمنية متطورة، أما القصد الخاص فيتجلى في نية الجاني تحقيق هدف محدد، سواء كان ذلك الوصول غير المصرح به إلى مناطق محظورة، أو الحصول على معلومات سرية، أو إثبات قدراته التقنية في اختراق هذه الأنظمة، ويمتد هذا القصد ليشمل الوعي بالآثار المحتملة لأفعاله على أمن وسلامة الأشخاص أو المؤسسات المحمية بهذه الأنظمة، ومن الجدير بالذكر أن تعقيد تقنيات الذكاء الاصطناعي المستخدمة في أنظمة الأمان قد يثير تحديات في إثبات هذا الركن، خاصة في الحالات التي قد يدعي فيها المتهم أنه كان يختبر أمان النظام دون نية إجرامية. لذا قد يتطلب الأمر تطوير معايير قانونية جديدة لتقييم القصد الجنائي في سياق الجرائم المتعلقة بالتحايل على أنظمة الذكاء الاصطناعي، مع الأخذ بعين الاعتبار مستوى المعرفة التقنية للمتهم ودوافعه المحتملة.

## رابعا_ سرقة أو استغلال الملكية الفكرية المرتبطة بتقنيات الذكاء الاصطناعي:

يتمثل الركن المادي والمعنوي لجريمة سرقة أو استغلال الملكية الفكرية المرتبطة بتقنيات الذكاء الاصطناعي فيما يلي:

### 1_ الركن المادي:

يتجلى الركن المادي في جريمة سرقة أو استغلال الملكية الفكرية المرتبطة بتقنيات الذكاء الاصطناعي في سلسلة من الأفعال المعقدة والمتداخلة تقنياً وقانونياً، يبدأ هذا الركن بالحصول غير المشروع على المعلومات أو التقنيات المحمية بحقوق الملكية الفكرية، سواء كانت خوارزميات، نماذج تعلم آلي، أو برمجيات متخصصة في الذكاء الاصطناعي، وقد يتم ذلك عبر الاختراق الإلكتروني لأنظمة الشركات أو المؤسسات البحثية، أو من خلال التجسس الصناعي، أو حتى عبر استمالة موظفين للحصول على معلومات سرية.

يمتد هذا الركن ليشمل أيضاً نسخ أو تعديل أو إعادة هندسة البرمجيات والخوارزميات المحمية دون إذن، أو استخدام هذه التقنيات في تطوير منتجات منافسة، كما قد يتضمن الاستغلال غير المشروع للبيانات المستخدمة في تدريب نماذج الذكاء الاصطناعي، والتي قد تكون محمية بحقوق الملكية الفكرية.

أما النتيجة الإجرامية فتتمثل في الاستفادة غير المشروعة من هذه الملكية الفكرية، سواء من خلال بيعها لأطراف ثالثة، أو استخدامها في تطوير منتجات منافسة، أو تحقيق مكاسب مالية أو تنافسية غير عادلة. ويتحقق الركن المادي بمجرد القيام بأي من هذه الأفعال، حتى لو لم يتم استغلال المعلومات

المسروقة بشكل فعلي، نظراً لخطورة هذه الأفعال على حقوق الملكية الفكرية وقيمتها الاقتصادية والاستراتيجية في مجال الذكاء الاصطناعي.[41]

إن تعقيد هذه الجريمة يكمن في صعوبة تتبع وإثبات عملية السرقة أو الاستغلال، خاصة عندما يتعلق الأمر بتقنيات متطورة قد يصعب تمييزها عن التطورات المستقلة المشروعة في مجال الذكاء الاصطناعي.

## 2_ الركن المعنوي:

يتجسد الركن المعنوي في جريمة سرقة أو استغلال الملكية الفكرية المرتبطة بتقنيات الذكاء الاصطناعي في القصد الجنائي بشقيه العام والخاص.

القصد العام يتمثل في علم الجاني الكامل بطبيعة أفعاله غير المشروعة وإرادته الحرة في تنفيذها، فالجاني يدرك تماماً أنه يقوم بالحصول على أو استغلال ملكية فكرية محمية قانوناً دون إذن أو حق، سواء كانت خوارزميات، نماذج تعلم آلي، أو برمجيات متخصصة في الذكاء الاصطناعي، وهو على وعي بأن هذه المعلومات أو التقنيات تخضع لحماية قانونية وأن الوصول إليها أو استخدامها بدون ترخيص يعد انتهاكاً للقانون.

أما القصد الخاص فيتجلى في نية الجاني تحقيق منفعة معينة من وراء هذه الأفعال. قد تكون هذه المنفعة مادية، مثل تحقيق أرباح من بيع المعلومات المسروقة أو استخدامها في تطوير منتجات منافسة، أو قد تكون منفعة تنافسية، كتحقيق تقدم تكنولوجي على حساب المنافسين، كما قد تكون الدوافع متعلقة بالتجسس الصناعي أو حتى التجسس على مستوى الدول في حالة التقنيات الإستراتيجية.[42]

يمتد هذا القصد ليشمل الوعي بالآثار السلبية المحتملة لأفعاله على أصحاب الحقوق الشرعيين وعلى سوق الذكاء الاصطناعي ككل. الجاني يدرك أن أفعاله تضر بالابتكار وتقوض الثقة في مجال البحث والتطوير في الذكاء الاصطناعي.

ومن الجدير بالذكر أن إثبات الركن المعنوي في هذه الجريمة قد يواجه تحديات، خاصة في الحالات التي قد يدعي فيها المتهم عدم علمه بأن المعلومات أو التقنيات كانت محمية، أو أنه كان يعتقد أنه يمارس هندسة عكسية مشروعة، لذا قد يتطلب الأمر تطوير معايير قانونية دقيقة لتقييم القصد الجنائي في سياق جرائم

[41] بن شهيدة محمد، المرجع السابق، ص 31.

[42] المرجع نفسه، ص 33.

الملكية الفكرية المتعلقة بالذكاء الاصطناعي، مع الأخذ بعين الاعتبار مستوى الخبرة التقنية للمتهم ومدى وعيه بقوانين الملكية الفكرية في هذا المجال المتخصص.[43]

وتحليلا لما سبق يمكن القول بأن الجرائم المرتبطة بالذكاء الاصطناعي تشكل تحدياً كبيراً وغير مسبوق للأنظمة القانونية والأمنية التقليدية، حيث يبرز الذكاء الاصطناعي كهدف رئيسي للنشاط الإجرامي بأشكال متعددة. فسواء كان الأمر يتعلق بمحاولات تعطيل أنظمة الذكاء الاصطناعي، أو التلاعب بها، أو تجاوز آليات حمايتها، أو حتى سرقة التقنيات المرتبطة بها، فإن هذه الأفعال تكشف عن ضرورة ملحة لتطوير التشريعات القائمة. هذا التطوير يجب أن يشمل توسيع نطاق الحماية القانونية لتغطي أنظمة الذكاء الاصطناعي بشكل صريح، مع تجريم الأفعال التي تستهدفها مباشرة. وتبرز في هذا السياق عدة تحديات قانونية جوهرية، أبرزها صعوبة تحديد المسؤول الجنائي في حالات استقلالية الذكاء الاصطناعي، وإشكالية تطبيق مفاهيم المسؤولية التقليدية على الأنظمة الذكية. كما تظهر تحديات في إثبات هذه الجرائم، نظراً لصعوبة جمع الأدلة وإثباتها في الجرائم المرتكبة باستخدام تقنيات الذكاء الاصطناعي المتطورة. ولمواجهة هذه التحديات، يتعين تحديث القوانين لتشمل الجرائم المستحدثة المرتبطة بالذكاء الاصطناعي، مع ضرورة إيجاد توازن دقيق بين تشجيع الابتكار في هذا المجال وحماية المجتمع من المخاطر المحتملة. وبالنظر إلى الطبيعة العابرة للحدود لهذه الجرائم، فإن التصدي لها يتطلب تعاوناً دولياً وثيقاً في مجالات المكافحة والملاحقة القضائية. إن هذا الواقع المعقد يستدعي تطوير أطر قانونية وتقنية جديدة ومبتكرة، قادرة على التكيف مع التطور السريع لتقنيات الذكاء الاصطناعي وأنماط الجرائم المرتبطة بها، لضمان حماية فعالة للمجتمع مع الحفاظ على مسار التقدم التكنولوجي.

وتحليلا لما سبق يمكن القول بأن الجرائم المرتبطة بالذكاء الاصطناعي تشكل تحدياً كبيراً وغير مسبوق للأنظمة القانونية والأمنية التقليدية، حيث يبرز الذكاء الاصطناعي كهدف رئيسي للنشاط الإجرامي بأشكال متعددة. فسواء كان الأمر يتعلق بمحاولات تعطيل أنظمة الذكاء الاصطناعي، أو التلاعب بها، أو تجاوز آليات حمايتها، أو حتى سرقة التقنيات المرتبطة بها، فإن هذه الأفعال تكشف عن ضرورة ملحة لتطوير التشريعات القائمة.

## خاتمة:

[43] بن شهيدة محمد، المرجع السابق ، ص 34.

لقد استعرضنا مجموعة متنوعة من الجرائم التي يمكن أن ترتكب باستخدام الذكاء الاصطناعي أو ضده، بما في ذلك الاحتيال المالي، التصيد الاحتيالي المتطور، إنشاء محتوى مزيف (deepfakes)، تعطيل أنظمة الذكاء الاصطناعي، تسميم البيانات، والتحايل على أنظمة الأمان. كما ناقشنا بالتفصيل الأركان المادية والمعنوية لهذه الجرائم، مسلطين الضوء على التعقيدات الجديدة التي تفرضها طبيعة الذكاء الاصطناعي، وقد تبين أن تنظيم المسؤولية الجزائية لمسيري الشركات في ظل تحديات الذكاء الاصطناعي يتطلب نهجًا شاملًا ومتوازنًا، يأخذ بعين الاعتبار حداثة هذه التقنية وعدم تمكن الجميع من استخدامها بشكل متساوٍ. فمع تسارع وتيرة التطور التكنولوجي، تبرز إشكالية الفجوة الرقمية بين الشركات القادرة على توظيف تقنيات الذكاء الاصطناعي المتقدمة وتلك التي تفتقر إلى الموارد أو الخبرات اللازمة لذلك. هذا التفاوت يستدعي مراعاة خاصة عند صياغة الأطر القانونية، بحيث تكون المسؤولية الجزائية متناسبة مع مستوى الوعي والقدرة على استخدام هذه التقنيات. ويمكن تحقيق ذلك من خلال تبني سياسات تدريجية في تطبيق القوانين، وتوفير برامج تأهيلية للشركات الصغيرة والمتوسطة، مع التركيز على نشر الوعي القانوني والتقني بين مختلف الفاعلين في القطاع الاقتصادي. كما يجب أن تراعي التشريعات الجديدة الفروقات في مستويات الاستخدام والفهم لتقنيات الذكاء الاصطناعي، مما يضمن عدالة في تطبيق القانون وحماية للمبتكرين في هذا المجال الناشئ.

وقد تم التوصل إلى النتائج الرئيسية لهذه الدراسة تشمل:

- وجود فجوة كبيرة بين التشريعات الحالية والتحديات التي يفرضها الذكاء الاصطناعي.
- صعوبة تحديد المسؤولية الجنائية في حالات استقلالية الذكاء الاصطناعي.
- تعقيد عملية إثبات الجرائم المرتكبة باستخدام تقنيات الذكاء الاصطناعي المتطورة.
- الحاجة إلى إعادة تعريف مفاهيم القصد الجنائي والإهمال في سياق الذكاء الاصطناعي.
- ضرورة التعاون الدولي لمواجهة الطبيعة العابرة للحدود لهذه الجرائم.

بناءً على هذه النتائج، نقدم التوصيات التالية:

- تحديث التشريعات الوطنية لتشمل الجرائم المستحدثة المرتبطة بالذكاء الاصطناعي، مع التركيز على تحديد المسؤولية الجزائية لمسيري الشركات.
- تطوير معايير قانونية جديدة لتقييم المسؤولية الجنائية في حالات استخدام الذكاء الاصطناعي، مع مراعاة مستوى استقلالية النظام.

- إنشاء هيئات متخصصة للتحقيق في الجرائم المرتبطة بالذكاء الاصطناعي، مع تدريب القضاة والمحققين على التعامل مع هذه القضايا المعقدة.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية والجرائم المرتبطة بالذكاء الاصطناعي، بما في ذلك تبادل المعلومات والخبرات.
- فرض التزامات قانونية على الشركات لضمان الشفافية والمساءلة في استخدام أنظمة الذكاء الاصطناعي.
- تشجيع البحث والتطوير في مجال الأخلاقيات والقانون المرتبط بالذكاء الاصطناعي.

ختاماً، إن التحديات التي يفرضها الذكاء الاصطناعي على نظام العدالة الجنائية تتطلب استجابة شاملة ومتعددة الأبعاد. يجب أن تكون هذه الاستجابة مرنة بما يكفي للتكيف مع التطورات التكنولوجية السريعة، مع الحفاظ على المبادئ الأساسية للعدالة والمساءلة. إن مستقبل المسؤولية الجزائية لمسيري الشركات في عصر الذكاء الاصطناعي سيعتمد على قدرتنا على موازنة الابتكار التكنولوجي مع حماية حقوق الأفراد والمجتمع.

## قائمة المصادر والمراجع:

### أولا: الكتب الأجنبية:

1- George Chapouthier, Frédéric Kaplan, l'homme, l'animal et la machine, Biblis, Paris, 2013.
2- Jean François Dortier, le dictionnaire des sciences humaines, Delta, France, 2004.
3- Soyer, Baris, and Andrew Tettenborn. "Artificial intelligence and civil liability—do we need a new regime?" International Journal of Law and Information Technology 30, no. 4 (Winter 2022)

### ثانيا: المقالات:

1. أحمد محمد، "تحديات تحديد المسؤولية الجنائية في جرائم الذكاء الاصطناعي: دراسة تحليلية مقارنة"، المجلة العربية للعلوم الجنائية والقانونية، جامعة الإسكندرية، المجلد 8، العدد 2، 2023.
2. بلعسل بنت نبي ياسمين، عمروش الحسين، الذكاء الاصطناعي ودوره في تحقيق التنمية المستدامة، مجلة الدراسات القانونية والاقتصادية، جامعة المسيلة، المجلد 05، العدد 01، 2022.

3. بن شهيدة محمد، "الملكية الفكرية والتحديات القانونية في تكنولوجيا الذكاء الاصطناعي"، مجلة التراث، جامعة زيان عاشور، الجلفة، المجلد 13، العدد 4، 2023.
4. بوزنون سعيدة، "كيانات الذكاء الاصطناعي في فكر القانون الجنائي"، مجلة المعيار، جامعة عبد الحميد بن باديس، الجزائر، المجلد 28، العدد 4، 2024.
5. حمد محمود، "تطبيقات الذكاء الاصطناعي في تحليل البيانات الضخمة ودعم القرار"، المجلة العربية للعلوم والمعلوماتية، جامعة الإمام محمد بن سعيد الإسلامية، المملكة العربية السعودية، المجلد 8، العدد 2، 2022.
6. سارة المنصوري، "التحديات الأخلاقية والاجتماعية للذكاء الاصطناعي في بيئة الأعمال: دراسة تحليلية نقدية"، المجلة العربية لأخلاقيات الأعمال والتكنولوجيا، المجلد 4، العدد 3، 2023.
7. سمير الحسيني، "الركن المعنوي في جرائم تسميم البيانات: دراسة تحليلية في إطار القانون الجنائي"، المجلة العربية للعلوم الجنائية والقانونية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 9، العدد 1، 2024.
8. سمير الحسيني، "تطبيق مبدأ الحيطة والعناية الواجبة في إدارة تقنيات الذكاء الاصطناعي: نحو إطار قانوني متكامل"، المجلة العربية للقانون والتكنولوجيا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 6، العدد 2، 2023.
9. سمير الحسيني، "تطبيقات الذكاء الاصطناعي في إدارة سلاسل التوريد: دراسة حالة لشركات التجزئة"، المجلة العربية للإدارة، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 43، العدد 1، 2023.
10. عبد الله الغامدي، "تسميم البيانات: التهديد الخفي لأنظمة الذكاء الاصطناعي"، مجلة الأمن السيبراني، جامعة الملك سعود، المملكة العربية السعودية، المجلد 3، العدد 2، 2023.
11. فاطمة الزهراء، "إشكاليات تحديد المسؤولية الجنائية في جرائم الذكاء الاصطناعي: نحو إطار قانوني جديد"، المجلة العربية للدراسات القانونية والقضائية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 6، العدد 3، 2023.
12. ليلى عبد الرحمن، "دور الذكاء الاصطناعي في تحسين تجربة العملاء: دراسة تحليلية لتطبيقات روبوتات الدردشة في قطاع الخدمات"، مجلة الاقتصاد والأعمال العربية، جامعة بيروت العربية، لبنان، المجلد 7، العدد 4، 2022.

13. محمد الصادق، "الجرائم المالية المرتكبة باستخدام الذكاء الاصطناعي: دراسة تحليلية للركن المادي"، المجلة العربية للدراسات الأمنية والقانونية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 7، العدد 2، 2023.
14. محمد الصادق، "تأثير الذكاء الاصطناعي على العمليات التجارية: دراسة تحليلية شاملة"، المجلة العربية للإدارة والاقتصاد الرقمي، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 5، العدد 2، 2023.
15. محمد سالمة عبد المنعم، "جريمة الانتقام الإباحي عبر تقنية التزييف العميق deepfakes والمسئولية الجنائية عنها"، مجلة الحقوق الاقتصادية للبحوث القانونية، جامعة الإسكندرية، العدد 2 (1)، 2022.
16. محمد علي، "دور الذكاء الاصطناعي في تحويل عمليات الأعمال"، مجلة التكنولوجيا والابتكار، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 15، العدد 3، 2023.
17. نورا السعيد، "دور الذكاء الاصطناعي في تطوير عمليات التوظيف: دراسة تحليلية لتقنيات فرز السير الذاتية"، المجلة العربية لإدارة الموارد البشرية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 5، العدد 2، 2023.
18. هشام عمر خوجلي، سعيد مكيد، "المستقبل المدمج للأتمتة والذكاء الاصطناعي: دراسة بعض ميزات التأثير الاجتماعي والأخلاقي طويل المدى"، مجلة التكنولوجيا في المجتمع، جامعة عبد الحميد مهري، قسنطينة، المجلد 72، 2023.

## ثالثا: المواقع الإلكترونية:

- "كيف يمكن للذكاء الاصطناعي تحسين تجربة العملاء"، LinkedIn، تم الاطلاع عليه بتاريخ: 09_08_2024، على الساعة: 15: 15، https://ae.linkedin.com/pulse/كيف-يمكن-للذكاء-الاصطناعي-تحسين-تجربة-العملاء-abdulaziz-alshamsan
- المجرمون الإلكترونيون والذكاء الاصطناعي: ليس مجرد تصيد احتيالي أفضل"، تقرير تحليلي، 2024، تم الاطلاع عليه بتاريخ : 08_08_2024، على الساعة: 12:19، https://intel471.com/blog/cybercriminals-and-ai-not-just-better-phishing
- مركز الأمن السيبراني الوطني (NCSC)، "كيف يمكن للذكاء الاصطناعي أن يغير مشهد التهديدات السيبرانية"، تقرير تحليلي، 2023، تم الاطلاع عليه بتاريخ 08_08_2024،على

الساعة:12:19، https://www.ncsc.gov.uk/blog-post/how-ai-could-change-the-cyber-threat-landscape

- "ما هو تسميم البيانات (تسميم الذكاء الاصطناعي) وكيف يعمل؟"، TechTarget، تم الاطلاع عليه بتاريخ : 08_08 2024، على الساعة: 16:13 https://www.techtarget.com/searchenterpriseai/definition/data-poisoning-AI-poison

Amazon Web Services. https://aws.amazon.com/ar/what-is /artificial-intelligenc