

دور الذكاء الاصطناعي في محاربة الغش المالي

The role of artificial intelligence in combating financial fraud

بن علو حورية¹، واضح حورية²Benallou houria¹, Ouadah horiya²¹ مخبر STRTEV، جامعة مستغانم (الجزائر)، houria.benallou.etu@univ-mosta.dz² مخبر STRTEV، جامعة مستغانم (الجزائر)، horiya.ouadah.etu@univ-mosta.dz

تاريخ النشر: 2025/07/01

تاريخ القبول: 2025/05/01

تاريخ الاستلام: 2025/03/23

ملخص:

يهدف هذا البحث إلى دراسة دور الذكاء الاصطناعي في مكافحة الغش المالي، حيث أصبحت المؤسسات المالية تعتمد بشكل متزايد على التقنيات الذكية للكشف عن الأنشطة الاحتيالية والحد من المخاطر المرتبطة بها. يتناول البحث مختلف تقنيات الذكاء الاصطناعي المستخدمة في هذا المجال، مثل التعلم الآلي، وتحليل البيانات الضخمة، والشبكات العصبية العميقة، التي تتيح التعرف على الأنماط المشبوهة والتنبؤ بالسلوكيات الاحتيالية قبل وقوعها.

ورغم الفوائد العديدة التي يوفرها الذكاء الاصطناعي في مكافحة الاحتيال المالي، إلا أن هناك تحديات متعددة تواجه تطبيقه، أبرزها المخاطر الأخلاقية المتعلقة بالشفافية والتحيز في القرارات ومعالجة البيانات المالية. كما تطرق البحث إلى الإطار القانوني والتشريعي المنظم لاستخدام هذه التقنيات، مشيراً إلى الحاجة إلى وضع سياسات واضحة تحكم توظيف الذكاء الاصطناعي في المجال المالي لضمان التوازن بين الفعالية والحماية القانونية. من النتائج الدراسة: عدم وجود قوانين خاصة بالذكاء الاصطناعي في مجال مكافحة الغش المالي في الجزائر لأن الموضوع لا يزال جديداً.

كلمات مفتاحية: الذكاء الاصطناعي، الغش المالي، الاحتيال.

تصنيفات JEL : O170، G03

¹ المؤلف المرسل: بن علو حورية، الإيميل: houria.benallou.etu@univ-mosta.dz

Abstract:

This research aims to examine the role of artificial intelligence in combating financial fraud, as financial institutions increasingly rely on intelligent technologies to detect fraudulent activities and mitigate associated risks. The research examines various AI techniques used in this field, such as machine learning, big data analytics, and deep neural networks, which enable the identification of suspicious patterns and the prediction of fraudulent behavior before it occurs.

Despite the numerous benefits AI offers in combating financial fraud, there are multiple challenges facing its implementation, most notably ethical risks related to transparency, bias in decisions, and the processing of financial data. The study also addressed the legal and legislative framework governing the use of these technologies, highlighting the need to establish clear policies governing the use of AI in the financial sector to ensure a balance between effectiveness and legal protection. Among the study's findings: The absence of specific laws on AI in combating financial fraud in Algeria, as the subject is still new.

JEL Classification Codes: Artificial Intelligence, Financial Fraud, Scam

1. مقدمة:

أصبح الغش المالي أحد التحديات الكبرى التي تواجه الأنظمة المالية العالمية، حيث يؤدي إلى خسائر اقتصادية ضخمة ويهدد استقرار المؤسسات المالية. ومع تطور التكنولوجيا الرقمية، بات من الضروري اعتماد تقنيات متقدمة للكشف عن الأنشطة الاحتيالية والحد من مخاطرها. في هذا السياق، أثبت الذكاء الاصطناعي فعاليته في مكافحة الغش المالي من خلال تحليل البيانات الضخمة، واكتشاف الأنماط المشبوهة، وتعزيز أنظمة الأمان المالي. تعتمد المؤسسات المصرفية وشركات التأمين على تقنيات مثل التعلم الآلي، والشبكات العصبية العميقة، وتحليل المعاملات في الوقت الفعلي للكشف عن الاحتيال المالي قبل وقوعه. ورغم الفوائد الكبيرة لهذه التقنيات، إلا أن هناك تحديات عديدة تتعلق بالخصوصية، والأخلاقيات، والإطار القانوني المنظم لاستخدام الذكاء الاصطناعي في المجال المالي.

تطرح الإشكالية التالية: ما هو دور الذكاء الاصطناعي في مكافحة الغش المالي؟

2 المحور الأول: الإطار النظري والمفاهيمي للذكاء الاصطناعي والغش المالي

2.1 تعريف الذكاء الاصطناعي: يُعرّف الذكاء الاصطناعي (Artificial Intelligence - AI)

على أنه فرع من علوم الحاسوب يُعنى بتطوير أنظمة وبرمجيات قادرة على محاكاة الذكاء البشري، من خلال التعلم من البيانات، والتكيف مع الأنماط المختلفة، واتخاذ قرارات مستقلة بناءً على التحليل الفوري للمعلومات. يعتمد الذكاء الاصطناعي على عدة تقنيات مثل التعلم الآلي (Machine Learning)، والتعلم العميق (Deep Learning)، ومعالجة اللغات الطبيعية (Natural Language Processing)، ورؤية الحاسوب (Computer Vision)، مما يجعله قادرًا على التعامل مع كميات ضخمة من البيانات وتحليلها بسرعة ودقة عالية. (مارجريت إيه بودين، 2015، ص. 45).

في القطاع المالي، يلعب الذكاء الاصطناعي دورًا محوريًا في تحسين الكفاءة التشغيلية، وتعزيز الأمن، وتحليل المخاطر، والتنبؤ بالتوجهات المستقبلية. من أبرز مجالات استخدامه في هذا القطاع: (عادل عبد النور، 2007، ص. 102).

2.2 مجالات استخدام الذكاء الاصطناعي في القطاع المالي:

إدارة المخاطر المالية: يساعد الذكاء الاصطناعي في تحليل بيانات الأسواق والتنبؤ بالمخاطر المحتملة بناءً على أنماط البيانات التاريخية، مما يساعد المؤسسات المالية على اتخاذ قرارات استثمارية أكثر دقة.

مكافحة الغش المالي والاحتيال: من خلال خوارزميات التعلم الآلي، يمكن كشف المعاملات المشبوهة، وتحديد الأنشطة الاحتيالية، مثل الاحتيال في بطاقات الائتمان أو غسيل الأموال، وذلك من خلال تحليل السلوكيات غير العادية للمعاملات المالية.

الخدمات المصرفية الرقمية: تعتمد البنوك والمؤسسات المالية على الذكاء الاصطناعي لتقديم خدمات مخصصة للعملاء، مثل تحليل أنماط الإنفاق، وتقديم توصيات مالية، وتطوير روبوتات الدردشة (Chatbots) لخدمة العملاء على مدار الساعة.

إدارة الأصول والاستثمار: يساعد الذكاء الاصطناعي في اتخاذ قرارات استثمارية دقيقة عبر تحليل الأسواق المالية والتنبؤ بأداء الأصول المالية المختلفة، مما يساهم في تحسين العوائد الاستثمارية.

تحليل الائتمان والتقييم المالي: تعتمد المؤسسات المالية على الذكاء الاصطناعي لتقييم الجدارة الائتمانية للعملاء، من خلال تحليل البيانات المالية والتاريخ الائتماني، مما يساهم في تقليل مخاطر القروض .

الأتمتة في العمليات المالية: يُستخدم الذكاء الاصطناعي لأتمتة العديد من العمليات المالية والإدارية، مثل مراجعة العقود، والتدقيق المالي، وإعداد التقارير، مما يساعد على تقليل الأخطاء البشرية وتحسين الكفاءة التشغيلية .

بفضل هذه التطبيقات، أصبح الذكاء الاصطناعي أداة لا غنى عنها في القطاع المالي، حيث يُساهم في تعزيز الشفافية، وتحسين الأمان، وتقليل الاحتيال، مع تحقيق تجربة مستخدم أكثر ذكاءً وسلاسة.

مفهوم الغش المالي وأشكاله المختلفة في المؤسسات المالية

3.2 تعريف الغش المالي: يُعرّف الغش المالي (Financial Fraud) بأنه أي نشاط غير قانوني أو غير أخلاقي يهدف إلى تحقيق مكاسب مالية غير مشروعة من خلال التلاعب بالمعلومات أو البيانات أو الأنظمة المالية. يتضمن الغش المالي عمليات خداع وتضليل تهدف إلى انتهاك القوانين أو السياسات المالية لتحقيق أرباح غير مشروعة، مما يؤدي إلى خسائر اقتصادية كبيرة للمؤسسات المالية والأفراد على حد سواء. يعتبر الغش المالي من أكبر التحديات التي تواجه الأنظمة المصرفية والمالية، حيث يؤدي إلى زعزعة الثقة في الأسواق المالية، ويؤثر سلبًا على الاقتصاد العالمي. (محمد الغامدي، 2024، ص. 88).

4.2 أشكال الغش المالي في المؤسسات المالية: تتنوع أشكال الغش المالي في المؤسسات المالية، وتشمل عدة ممارسات غير قانونية تؤثر على المعاملات المالية والنزاهة الاقتصادية، ومن أبرز هذه الأشكال: (أحمد عبد الله، 2023، ص. 67).

الاحتيال في بطاقات الائتمان (Credit Card Fraud): يتمثل في استخدام بطاقات ائتمان مسروقة أو مزورة لإجراء معاملات غير مشروعة، أو استخدام بيانات البطاقات المسروقة عبر الإنترنت لإجراء عمليات شراء غير قانونية.

الاحتيال في القروض (Loan Fraud): يحدث عندما يقوم الأفراد أو الشركات بتقديم معلومات مزيفة أو مضللة للحصول على قروض أو تسهيلات مالية لا يستحقونها، مما يؤدي إلى خسائر كبيرة للبنوك.

غسيل الأموال (Money Laundering) وهو عملية تحويل الأموال الناتجة عن أنشطة غير قانونية مثل تجارة المخدرات أو الفساد إلى أموال تبدو قانونية، من خلال مجموعة من المعاملات المالية المعقدة التي تهدف إلى إخفاء المصدر الحقيقي لهذه الأموال.

التلاعب في الأسواق المالية (Market Manipulation) يشمل التلاعب في أسعار الأسهم أو العملات أو السندات من خلال نشر معلومات مضللة، أو تنفيذ عمليات تداول وهمية للتأثير على العرض والطلب في الأسواق المالية.

الاختلاس المالي (Embezzlement) يتمثل في استيلاء الموظفين أو المسؤولين الماليين في المؤسسات المالية على أموال الشركة أو العملاء بطريقة غير قانونية، مثل تحويل الأموال إلى حساباتهم الشخصية دون إذن.

التلاعب في التقارير المالية (Financial Statement Fraud) يتم من خلال تزوير أو تعديل البيانات المالية للمؤسسات بهدف تضليل المستثمرين أو الجهات التنظيمية حول الوضع المالي الحقيقي للشركة، مثل تضخيم الأرباح أو إخفاء الديون.

الاحتيال الإلكتروني المالي (Cyber Financial Fraud) يشمل عمليات الاختراق الإلكتروني وسرقة البيانات المالية أو تنفيذ هجمات قرصنة لاختراق أنظمة الدفع الإلكتروني وسرقة الأموال.

الاحتيال في التأمين المالي (Insurance Fraud) يتمثل في تقديم مطالبات تأمين مزيفة أو مبالغ فيها للحصول على تعويضات مالية غير مستحقة من شركات التأمين.

سرقة الهوية المالية (Identity Theft) تحدث عندما يستخدم شخص غير مصرح له بيانات شخصية أو مصرفية لشخص آخر للوصول إلى حساباته البنكية أو إجراء معاملات مالية باسمه دون إذنه.

العمولات والرشاوى غير القانونية (Bribery and Kickbacks): تتضمن دفع أو تلقي رشاوى للحصول على مزايا مالية غير مشروعة، مثل التلاعب في العقود أو تسهيل العمليات المصرفية بطرق غير قانونية.

5.2 العلاقة بين الذكاء الاصطناعي ومكافحة الغش المالي: يشكل الذكاء الاصطناعي أداة أساسية في مكافحة الغش المالي، حيث يعتمد على تقنيات متقدمة لتحليل البيانات والتنبؤ بالاحتيال واتخاذ إجراءات

فورية للحد من المخاطر. تعتمد المؤسسات المالية على الذكاء الاصطناعي لتحليل كميات ضخمة من المعاملات المالية وتحديد الأنماط غير الطبيعية التي قد تشير إلى عمليات غش محتملة، مما يساهم في منع الاحتيال قبل وقوعه. كما يتيح الذكاء الاصطناعي إمكانية كشف الأنشطة المشبوهة في الوقت الحقيقي، حيث تقوم الأنظمة الذكية بتحليل البيانات المصرفية فور حدوث المعاملة، وعند اكتشاف أي سلوك غير مألوف، يتم إرسال إشعارات تحذيرية أو إيقاف العمليات تلقائيًا لحماية العملاء. (محمد العارضة، 2024، ص. 53).

يساهم الذكاء الاصطناعي أيضًا في تطوير خوارزميات التعلم العميق التي تعتمد على الشبكات العصبية الاصطناعية لفهم الأنماط الاحتمالية التي قد لا تكون واضحة من خلال الأساليب التقليدية. وتستخدم المؤسسات المالية هذه التقنيات لمراقبة سلوك العملاء، حيث يتمكن النظام من اكتشاف أي تغير مفاجئ في طريقة استخدام الحسابات المصرفية، مثل تسجيل الدخول من مواقع غير معتادة أو تنفيذ عمليات مالية غير مألوفة. يساعد الذكاء الاصطناعي في تحليل النصوص المالية باستخدام تقنيات معالجة اللغات الطبيعية، مما يتيح رصد التلاعب في العقود والمستندات المالية واكتشاف الاحتيال في المراسلات الإلكترونية، مثل رسائل البريد الاحتمالية التي تحاول سرقة بيانات المستخدمين. (أحمد محمد، 2022، ص. 120).

يعزز الذكاء الاصطناعي أنظمة المصادقة والأمان الإلكتروني من خلال تقنيات مثل التعرف على الوجه وبصمة الصوت والمصادقة متعددة العوامل، مما يجعل من الصعب على المحتالين اختراق الحسابات المالية أو انتحال هوية العملاء. إضافة إلى ذلك، تلجأ البنوك إلى الذكاء الاصطناعي لرصد عمليات غسيل الأموال من خلال تتبع التدفقات المالية وتحليل الأنشطة المصرفية غير المعتادة، مما يساعد في الحد من الجرائم المالية التي تهدف إلى إخفاء مصادر الأموال غير المشروعة. (خالد علي، 2021، ص. 95).

يقلل الذكاء الاصطناعي من الأخطاء البشرية في عمليات كشف الاحتيال، حيث تتميز الأنظمة الذكية بالدقة العالية في تحليل البيانات المالية مقارنة بالطرق التقليدية. كما يساهم في تطوير أنظمة رقابية ذكية تراقب مدى التزام المؤسسات بالقوانين المالية، مثل لوائح مكافحة تمويل الإرهاب والفساد، مما يضمن امتثال الشركات والمصارف للأنظمة القانونية ويقلل من المخاطر التنظيمية.

3 المحور الثاني: تقنيات الذكاء الاصطناعي في كشف الغش المالي:

1.3 دور الشبكات العصبية العميقة في التنبؤ بالسلوكيات الاحتمالية: يشكل الذكاء الاصطناعي، وخاصة الشبكات العصبية العميقة، أداة رئيسية في التنبؤ بالسلوكيات الاحتمالية في القطاع المالي، حيث تعتمد هذه الشبكات على نماذج متقدمة لمحاكاة عمل الدماغ البشري في معالجة البيانات واكتشاف الأنماط غير الطبيعية. تعتمد المؤسسات المالية على الشبكات العصبية العميقة لقدرتها على تحليل كميات هائلة من البيانات المالية والتعرف على الاحتيال بناءً على سلوكيات المستخدمين والتغيرات الطارئة في المعاملات. تقوم هذه الأنظمة بتعلم العلاقات المعقدة بين المتغيرات المالية، مما يجعلها قادرة على الكشف عن الاحتيال الذي قد يكون غير واضح عبر الطرق التقليدية. (سارة أحمد، 2020، ص. 110).

تُستخدم الشبكات العصبية العميقة في أنظمة مكافحة الغش المالي في مجالات متعددة، مثل اكتشاف عمليات الاحتيال في البطاقات الائتمانية، حيث يتم تحليل نمط إنفاق العملاء للكشف عن أي معاملات غير طبيعية. على سبيل المثال، عند تنفيذ معاملة مالية كبيرة من موقع جغرافي غير مألوف، يمكن للنظام التنبؤ بإمكانية وقوع احتيال وإرسال تنبيه فوري إلى البنك أو العميل. وقد أظهرت دراسة أجرتها Zhang et al. (2021) أن استخدام الشبكات العصبية العميقة في تحليل بيانات البطاقات المصرفية ساهم في تقليل عمليات الاحتيال بنسبة 30% مقارنة بالأساليب التقليدية. (عبد الرحمن حسن، 2019، ص. 75).

إضافة إلى ذلك، تلعب الشبكات العصبية العميقة دورًا بارزًا في كشف عمليات غسيل الأموال، حيث تعتمد البنوك على هذه التقنية لتحليل تدفقات الأموال والكشف عن الأنماط المشبوهة. من خلال تحليل التحويلات المالية المعقدة، يمكن للشبكة العصبية التعرف على الحسابات التي يتم استخدامها لتحويل الأموال بطرق غير مشروعة. وفقًا لتقرير صادر عن (Financial Action Task Force (FATF, 2022)، تمكنت بعض المؤسسات المالية من خفض حالات غسيل الأموال بنسبة 40% بعد تطبيق تقنيات الذكاء الاصطناعي العميق في أنظمة الامتثال المالي.

تعد تطبيقات الذكاء الاصطناعي في الأسواق المالية أيضًا من أبرز المجالات التي تستفيد من الشبكات العصبية العميقة، حيث يتم استخدامها لرصد التلاعب بأسعار الأسهم أو تنفيذ عمليات تداول مشبوهة. على سبيل المثال، يتمكن النظام من التعرف على أنماط التداول غير العادية، مثل عمليات البيع والشراء

المتكررة خلال فترة قصيرة، مما قد يشير إلى محاولات التلاعب في السوق. ووفقًا لدراسة نشرتها Li et al. (2020)، فقد ساعدت تقنيات التعلم العميق في كشف 85% من عمليات التلاعب في سوق الأسهم الصيني، مما يعزز شفافية الأسواق المالية. (محمد علي، 2023، ص. 130).

علاوة على ذلك، يتم استخدام الشبكات العصبية العميقة في تحليل السلوكيات الاحتيالية في التجارة الإلكترونية والخدمات المصرفية الرقمية. تعتمد بعض المنصات على الذكاء الاصطناعي لتحليل سلوك المستخدمين أثناء تصفحهم للمواقع الإلكترونية، بحيث يتم التعرف على محاولات الاحتيال مثل استخدام حسابات وهمية أو محاولة اختراق الحسابات البنكية. أشارت دراسة (Nguyen et al. 2021) إلى أن تطبيق الشبكات العصبية في منصات التجارة الإلكترونية أدى إلى تقليل حالات الاحتيال عبر الإنترنت بنسبة 50% خلال عام واحد. (أحمد سعيد، 2022، ص. 145).

3. 2 التعلم الآلي وتحليل البيانات الضخمة في التعرف على الأنماط المشبوهة: يُعتبر التعلم الآلي أحد أبرز تقنيات الذكاء الاصطناعي المستخدمة في كشف الغش المالي، حيث يعتمد على تحليل البيانات الضخمة لاستخراج الأنماط المشبوهة وتحديد المؤشرات التي تدل على وجود عمليات احتيالية. مع تزايد حجم المعاملات المالية الرقمية، أصبح من الضروري توظيف أنظمة ذكية قادرة على التعلم من البيانات التاريخية والتنبؤ بالسلوكيات غير الطبيعية. يساعد التعلم الآلي في التمييز بين العمليات المالية العادية والمشبوهة، مما يقلل من الأخطاء البشرية ويعزز دقة عمليات الكشف عن الغش المالي. (خالد محمود، 2024، ص. 60).

تعتمد المؤسسات المالية على تقنيات تحليل البيانات الضخمة لرصد أي تغيرات غير متوقعة في سلوك المستخدمين، حيث تتم مقارنة العمليات المالية الحالية مع بيانات سابقة للتعرف على أي أنماط غير اعتيادية. على سبيل المثال، عند تنفيذ معاملة بمبلغ كبير من موقع غير مألوف أو تكرار عمليات سحب الأموال بسرعة، يقوم النظام الذكي برصد هذه السلوكيات وإرسال إشعار تحذيري. وفقًا لدراسة أجرتها Nguyen et al. (2021)، فإن البنوك التي اعتمدت على أنظمة تحليل البيانات الضخمة باستخدام التعلم الآلي شهدت انخفاضًا في معدلات الاحتيال المالي بنسبة 35% مقارنة بالأساليب التقليدية.

من أبرز خوارزميات التعلم الآلي المستخدمة في كشف الغش المالي، نجد خوارزمية Random Forest التي تعتمد على بناء عدة نماذج تحليلية لاتخاذ قرارات دقيقة بشأن المعاملات المالية، حيث تقوم

هذه الخوارزمية بتقسيم البيانات إلى مجموعات صغيرة وتحليل كل مجموعة على حدة للكشف عن أي مؤشرات تدل على الاحتيال. كما أن خوارزمية (Support Vector Machines (SVM تُستخدم بشكل واسع في تصنيف العمليات المالية إلى فئات طبيعية أو مشبوهة بناءً على خصائصها، مما يساعد في التعرف على حالات الاحتيال بسرعة وكفاءة عالية. (محمد حسن، 2023، ص. 25).

إضافة إلى ذلك، يتم استخدام تقنيات التعلم العميق مثل Long Short-Term Memory (LSTM) لتحليل سلاسل زمنية طويلة من المعاملات المالية، مما يتيح اكتشاف الأنماط غير الطبيعية التي تتطور على مدى فترات زمنية طويلة. وقد أظهرت دراسة نشرتها (Zhang et al. (2022 أن هذه التقنيات ساعدت في تحسين قدرة الأنظمة المصرفية على التنبؤ بالاحتيال بنسبة 40%، حيث أصبحت أكثر دقة في تمييز العمليات المالية الحقيقية من الاحتيالية. (عبد الله يوسف، 2024، ص. 80).

تعتمد شركات التأمين وشركات الدفع الإلكتروني أيضاً على تقنيات التعلم الآلي لرصد الاحتيال في طلبات التعويض وعمليات الدفع عبر الإنترنت. على سبيل المثال، يمكن للنظام تحليل بيانات العملاء وسجلات المطالبات السابقة لتحديد أي أنماط تشير إلى محاولات احتيال في طلبات التأمين. ووفقاً لتقرير صادر عن McKinsey & Company (2022)، فإن شركات التأمين التي تبنت التعلم الآلي في أنظمتها تمكنت من تقليل الخسائر المالية الناتجة عن الاحتيال بنسبة 25%، مما يعكس فعالية هذه التقنية في كشف السلوكيات الاحتيالية. (سامي محمد، 2021، ص. 140).

4 المحور الثالث: تطبيقات الذكاء الاصطناعي في المؤسسات المالية لمكافحة الغش:

4.1 أنظمة التصنيف والتنبؤ بالاحتيال في المصارف وشركات التأمين: أصبحت المصارف وشركات التأمين تعتمد بشكل متزايد على أنظمة الذكاء الاصطناعي في التصنيف والتنبؤ بعمليات الاحتيال، حيث توفر هذه الأنظمة قدرة تحليلية متقدمة لرصد المعاملات المشبوهة والكشف عن السلوكيات الاحتيالية قبل حدوثها. تعتمد هذه الأنظمة على تقنيات التعلم الآلي والتعلم العميق لتحليل كميات ضخمة من البيانات المصرفية والتأمينية، مما يمكن المؤسسات المالية من اتخاذ إجراءات استباقية لمنع الاحتيال وتقليل الخسائر المالية. (هند سعيد، 2020، ص. 95).

تعتمد أنظمة التصنيف على خوارزميات التعلم الآلي مثل Random و Decision Trees و Forest لتصنيف العمليات المالية إلى معاملات طبيعية أو مشبوهة بناءً على مجموعة من المعايير، مثل تكرار العمليات، وقيمتها، والموقع الجغرافي للمستخدم. يتم تدريب هذه النماذج على بيانات تاريخية لمعاملات مالية تم تصنيفها مسبقاً، مما يسمح للنظام بتحديد أي سلوك غير طبيعي عند حدوثه. وفقاً لدراسة أجرتها (Nguyen et al. (2022)، فإن استخدام خوارزميات التصنيف في المصارف ساعد في تقليل عمليات الاحتيال بنسبة 40% من خلال تحسين دقة الكشف عن المعاملات غير الشرعية.

أما أنظمة التنبؤ بالاحتيال، فتعتمد على تقنيات أكثر تعقيداً مثل الشبكات العصبية العميقة Deep Neural Networks (DNNs)، والتي تستطيع تحليل العلاقات المعقدة بين المعاملات المالية لاكتشاف الأنماط المخفية التي قد تشير إلى عمليات احتيالية. تستخدم المصارف هذه الأنظمة لرصد المعاملات المشبوهة في الوقت الفعلي، مما يسمح باتخاذ إجراءات فورية مثل تجميد الحسابات أو إرسال تنبيهات للعملاء. أظهرت دراسة (Zhang et al. (2021 أن تطبيق الشبكات العصبية العميقة في أنظمة التنبؤ بالاحتيال المصرفي أدى إلى تحسين دقة الاكتشاف بنسبة 30% مقارنة بالأساليب التقليدية. (هند سعيد، 2020، ص. 95).

في قطاع التأمين، تلعب أنظمة التصنيف والتنبؤ بالاحتيال دوراً حيوياً في الحد من المطالبات الاحتيالية، والتي تُعدّ من أكبر التحديات التي تواجه شركات التأمين. تعتمد هذه الأنظمة على تحليل سجلات المطالبات السابقة والتعرف على الأنماط المشبوهة، مثل تقديم طلبات تعويض متكررة أو المطالبة بتعويضات غير متناسبة مع طبيعة الضرر. على سبيل المثال، يتم استخدام خوارزميات Support Vector Machines (SVM) لتحليل تفاصيل المطالبات والتنبؤ بإمكانية وقوع احتيال. وفقاً لتقرير صادر عن McKinsey & Company (2022)، فإن شركات التأمين التي اعتمدت على الذكاء الاصطناعي في التنبؤ بالاحتيال تمكنت من تقليل الخسائر بنسبة 25% وتحسين كفاءة عمليات التحقيق في المطالبات.

إضافة إلى ذلك، تساعد أنظمة التصنيف والتنبؤ بالاحتيال في تحسين استراتيجيات إدارة المخاطر داخل المؤسسات المالية. فالبنوك التي تعتمد على هذه الأنظمة تستطيع مراقبة الحسابات المصرفية باستمرار والتنبؤ بأي سلوكيات غير اعتيادية، مثل عمليات السحب المتكررة أو التحويلات المالية الضخمة التي تتم في

وقت قصير. كما تساهم هذه الأنظمة في الكشف عن عمليات غسيل الأموال من خلال تحليل تدفقات الأموال بين الحسابات المختلفة، مما يعزز الامتثال للوائح مكافحة غسل الأموال. (عبد الله يوسف، 2024، ص. 80).

رغم الفوائد العديدة لهذه الأنظمة، فإنها تواجه بعض التحديات، مثل الحاجة إلى بيانات ضخمة ومتنوعة لتدريب النماذج بكفاءة، بالإضافة إلى خطر التحيز في التصنيف، حيث قد تؤدي النماذج غير المتوازنة إلى تصنيف خاطئ لبعض المعاملات المالية. لذلك، تسعى المؤسسات المالية إلى تحسين هذه الأنظمة من خلال تحديث البيانات باستمرار واعتماد تقنيات أكثر تطورًا لضمان دقة التنبؤات وتقليل معدلات الإنذارات الكاذبة.

4. 2 تحليل المعاملات المالية في الوقت الفعلي لاكتشاف الأنشطة الاحتيالية: أصبح تحليل المعاملات المالية في الوقت الفعلي باستخدام تقنيات الذكاء الاصطناعي أداة أساسية لمكافحة الأنشطة الاحتيالية في المؤسسات المالية. تعتمد هذه الأنظمة على خوارزميات متقدمة قادرة على معالجة كميات ضخمة من البيانات فور حدوثها، مما يسمح بالكشف عن العمليات المشبوهة خلال ثوانٍ قليلة، وبالتالي تقليل الخسائر المالية الناجمة عن الاحتيال. تساعد هذه التقنيات في تحسين أمان المعاملات وتعزيز ثقة العملاء في الأنظمة المصرفية وشركات الدفع الإلكتروني.

تعتمد المؤسسات المالية على تقنيات مثل التعلم الآلي والشبكات العصبية العميقة لتحليل التدفقات المالية وكشف الأنماط غير الطبيعية. تقوم هذه الأنظمة بمراقبة جميع المعاملات المالية الواردة والصادرة، وتقارنها مع البيانات التاريخية للمستخدمين لتحديد أي سلوكيات مشبوهة. على سبيل المثال، إذا قام أحد العملاء بإجراء معاملة مالية بمبلغ كبير من موقع جغرافي غير معتاد بالنسبة له، فإن النظام يقوم بتحليل هذا الحدث بسرعة ويقرر ما إذا كان يجب تنبيه العميل أو حظر المعاملة مؤقتًا. وفقًا لدراسة أجرتها . Nguyen et al (2022)، فإن المؤسسات المالية التي تعتمد على التحليل الفوري للمعاملات باستخدام الذكاء الاصطناعي قللت من معدلات الاحتيال بنسبة 45% مقارنة بالمؤسسات التي تعتمد على مراجعات يدوية لاحقة. (هند سعيد، 2020، ص. 95).

تستخدم المصارف وشركات الدفع الإلكتروني تقنيات Natural Language Processing (NLP) لمعالجة وتحليل البيانات النصية المرتبطة بالمعاملات المالية، مثل أوصاف العمليات المالية ورسائل التحذير. تساعد هذه التقنيات في التعرف على العمليات المشبوهة من خلال تحليل السياق المحيط بالمعاملات، مما يزيد من دقة أنظمة الكشف عن الاحتيال. إضافة إلى ذلك، تعتمد شركات التأمين على الذكاء الاصطناعي في تحليل المطالبات التأمينية في الوقت الفعلي، حيث يتم مقارنة بيانات المطالبة مع نماذج الاحتيال المعروفة لتحديد مدى مصداقيتها.

من أبرز التقنيات المستخدمة في تحليل المعاملات المالية في الوقت الفعلي، نجد خوارزميات Anomaly Detection التي تعتمد على تقنيات مثل Isolation و Autoencoders و Forest لاكتشاف الأنماط غير الطبيعية في البيانات. تعمل هذه الخوارزميات من خلال تحديد القيم المتطرفة داخل المعاملات المالية، مما يساعد في كشف أي عمليات قد تكون مرتبطة بالاحتيال. وفقاً لدراسة نشرتها (Zhang et al. 2021)، فإن استخدام خوارزميات الكشف عن الشذوذ في الوقت الفعلي ساعد في تحسين دقة اكتشاف الاحتيال بنسبة 35%، حيث أصبحت الأنظمة أكثر قدرة على التمييز بين المعاملات الطبيعية والمشبوهة دون الحاجة إلى تدخل بشري مستمر. (أحمد علي، 2019، ص. 115).

في مجال الامتثال المالي، تُستخدم تقنيات التحليل الفوري للكشف عن عمليات غسل الأموال وتمويل الإرهاب. تعتمد المؤسسات المالية على الذكاء الاصطناعي لتحليل سلاسل المعاملات المالية المعقدة، والبحث عن أي روابط غير طبيعية بين الأطراف المتعاملة. على سبيل المثال، إذا أظهرت البيانات وجود تدفقات مالية متكررة بين حسابات متعددة خلال فترة قصيرة، فقد يشير ذلك إلى محاولة لغسيل الأموال. وفقاً لتقرير صادر عن (Financial Action Task Force (FATF, 2022)، فإن تطبيق تقنيات التحليل الفوري أدى إلى تقليل عدد الإنذارات الكاذبة بنسبة 50%، مما حسن من كفاءة فرق الامتثال المالي.

5 المحور الرابع: التحديات والقيود في استخدام الذكاء الاصطناعي لمكافحة الغش المالي:

5.1 التحديات التقنية والبرمجية في تطوير أنظمة كشف الغش المالي: يواجه استخدام الذكاء الاصطناعي في مكافحة الغش المالي عدة تحديات تقنية وبرمجية، تؤثر على دقة وكفاءة هذه الأنظمة. من بين أبرز التحديات التقنية هو صعوبة تحليل البيانات الضخمة والمعقدة، حيث تتطلب أنظمة الذكاء الاصطناعي

قدرة عالية على معالجة كميات هائلة من البيانات في الوقت الفعلي. تحتاج هذه الأنظمة إلى خوارزميات تعلم آلي متطورة قادرة على التمييز بين المعاملات المشروعة وتلك الاحتمالية دون التسبب في معدلات خطأ مرتفعة، مثل رفض العمليات المالية السليمة أو السماح بعمليات احتيالية.

كما أن تطوير نماذج ذكاء اصطناعي فعالة يتطلب بيانات تدريبية دقيقة ومحدثة باستمرار. يعتمد الذكاء الاصطناعي في كشف الغش المالي على أنماط البيانات السابقة، مما يعني أن أي نقص أو تحيز في البيانات المدخلة قد يؤدي إلى قرارات غير دقيقة. على سبيل المثال، إذا كانت البيانات التاريخية تحتوي على أمثلة محدودة عن عمليات احتيالية معينة، فقد تفشل الأنظمة في التعرف على طرق الاحتيال الجديدة التي لم تكن مأخوذة بعين الاعتبار أثناء التدريب. (محمد عبد الرحمن، 2022، ص. 130).

من الناحية البرمجية، يعد تحسين أداء الخوارزميات وتقليل معدلات الخطأ تحديًا كبيرًا، حيث يجب أن تكون الأنظمة قادرة على التكيف مع التطورات المستمرة في أساليب الغش المالي. المختالون يعتمدون على تقنيات معقدة مثل التلاعب في هويات العملاء والاحتيال عبر الشبكات، مما يستوجب تطوير خوارزميات قادرة على اكتشاف هذه الأنماط بفعالية. بالإضافة إلى ذلك، تواجه المؤسسات المالية صعوبة في دمج تقنيات الذكاء الاصطناعي مع أنظمتها التقليدية، حيث أن الكثير من البنوك وشركات التأمين تعتمد على بنى تحتية قديمة قد لا تتوافق بسهولة مع حلول الذكاء الاصطناعي الحديثة.

5. 2 القوانين والتشريعات المنظمة لاستخدام الذكاء الاصطناعي في مكافحة الغش المالي: تعد الأطر القانونية والتشريعية من العوامل الحاسمة في تنظيم استخدام الذكاء الاصطناعي لمكافحة الغش المالي، حيث تهدف هذه القوانين إلى ضمان الشفافية، حماية خصوصية العملاء، وتحديد المسؤوليات القانونية في حال وقوع أخطاء. من أبرز القوانين المؤثرة في هذا المجال اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تفرض قيودًا صارمة على كيفية استخدام المؤسسات المالية للذكاء الاصطناعي في معالجة بيانات العملاء. تنص هذه اللائحة على ضرورة توفير آليات تتيح للأفراد الاعتراض على القرارات التي تتخذها الأنظمة الذكية، مما يعزز الشفافية والمساءلة القانونية.

في الولايات المتحدة، تراقب هيئة الأوراق المالية والبورصات (SEC) ومكتب مراقبة العملة (OCC) تطبيق تقنيات الذكاء الاصطناعي في المؤسسات المالية، لضمان الامتثال للقوانين التي تحمي

العملاء من القرارات غير العادلة. كما أن العديد من الدول بدأت بوضع لوائح خاصة لاستخدام الذكاء الاصطناعي في القطاع المالي، مثل الإمارات العربية المتحدة ضمن استراتيجيتها الوطنية للذكاء الاصطناعي 2031، والتي تحدد ضوابط صارمة لاستخدام الذكاء الاصطناعي في المؤسسات المالية لضمان الامتثال للمعايير الدولية.

أحد أكبر التحديات القانونية هو مسألة المسؤولية القانونية في حال حدوث أخطاء. فإذا قامت أنظمة الذكاء الاصطناعي بحظر حسابات عملاء دون مبرر واضح أو اتخذت قرارات غير عادلة، فمن يتحمل المسؤولية؟ هل هي المؤسسة المالية أم الجهة المطورة للخوارزمية؟ هذا التساؤل يثير جدلاً قانونياً واسعاً، ويتطلب تطوير أطر قانونية واضحة تحدد المسؤوليات بدقة. (خالد سعيد، 2021، ص. 105).

5. 3 القوانين والتشريعات المنظمة لاستخدام الذكاء الاصطناعي في مكافحة الاحتيال: تعد القوانين والتشريعات المنظمة لاستخدام الذكاء الاصطناعي في مكافحة الاحتيال عاملاً حاسماً في تحديد إطار العمل القانوني الذي يضمن استخدام هذه التقنيات بطرق تتسم بالشفافية والعدالة، مع الحفاظ على حقوق الأفراد والمؤسسات. تعتمد هذه التشريعات على تحقيق توازن بين تعزيز الابتكار التكنولوجي وحماية البيانات الشخصية، بالإضافة إلى تنظيم المسؤوليات القانونية عند حدوث أخطاء أو قرارات غير عادلة ناتجة عن الأنظمة الذكية.

تتنوع الأطر القانونية بين الدول، إلا أن هناك بعض التشريعات العالمية التي تؤثر بشكل مباشر على كيفية استخدام الذكاء الاصطناعي في القطاع المالي لمكافحة الاحتيال. على سبيل المثال، تفرض اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي قيوداً صارمة على معالجة البيانات باستخدام تقنيات الذكاء الاصطناعي. تشترط هذه اللائحة أن تكون قرارات الأنظمة الذكية شفافة وقابلة للتفسير، مما يعني أن المؤسسات المالية مطالبة بتوفير آليات تسمح للعملاء بفهم كيفية اتخاذ القرارات المالية، خاصة تلك المتعلقة بكشف الاحتيال وحظر الحسابات المشبوهة. (سارة محمد، 2023، ص. 90).

في الولايات المتحدة، تقوم هيئة الأوراق المالية والبورصات (SEC) ومكتب مراقبة العملة (OCC) بالإشراف على استخدام الذكاء الاصطناعي في الأنظمة المالية، حيث يتم التأكد من أن هذه التقنيات لا تؤدي إلى تمييز غير عادل ضد فئات معينة من العملاء. كما أن بعض الولايات الأمريكية، مثل كاليفورنيا،

بدأت بوضع قوانين خاصة بالذكاء الاصطناعي، مثل "قانون الشفافية في اتخاذ القرارات المؤتمتة"، الذي يفرض على المؤسسات المالية الإفصاح عن كيفية استخدام الذكاء الاصطناعي في عمليات كشف الاحتيال.

في الدول العربية، بدأت بعض الحكومات بوضع تشريعات تحكم استخدام الذكاء الاصطناعي في القطاع المالي، مثل الإمارات العربية المتحدة من خلال استراتيجيتها الوطنية للذكاء الاصطناعي 2031، والتي تتضمن لوائح تضمن الاستخدام الأخلاقي والأمن للذكاء الاصطناعي في المؤسسات المصرفية. كما أن بعض الدول مثل السعودية والبحرين بدأت في تطوير قوانين تنظم استخدام الذكاء الاصطناعي في المعاملات المالية، مع التركيز على الامتثال لمعايير مكافحة غسل الأموال والاحتيال المالي.

إحدى القضايا القانونية المهمة في هذا المجال هي مسألة المسؤولية القانونية عند حدوث أخطاء في قرارات الذكاء الاصطناعي. إذا قامت الأنظمة الذكية بحظر حسابات عملاء دون مبرر، أو تسببت في خسائر مالية بسبب قرارات خاطئة، فمن يتحمل المسؤولية؟ هل هي المؤسسة المالية التي تستخدم الذكاء الاصطناعي، أم الشركة المطورة للخوارزميات؟ هذا السؤال لا يزال محل جدل قانوني، ما يستدعي تطوير قوانين تحدد المسؤوليات بوضوح. (سارة محمد، 2023، ص. 90).

5.4 المخاطر الأخلاقية والخصوصية في تحليل البيانات المالية: تعتبر المخاطر الأخلاقية والخصوصية في تحليل البيانات المالية من أبرز التحديات التي تواجه استخدام الذكاء الاصطناعي في مكافحة الغش المالي. تعتمد أنظمة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات المالية لاكتشاف الأنماط الاحتيالية، مما يثير مخاوف بشأن انتهاك خصوصية الأفراد والمؤسسات، خاصة مع غياب لوائح تنظيمية موحدة تحكم كيفية جمع هذه البيانات ومعالجتها.

أحد أبرز المخاطر الأخلاقية يتمثل في إمكانية التمييز والقرارات غير العادلة. قد تؤدي خوارزميات الذكاء الاصطناعي، عند تدريبها على بيانات غير متوازنة، إلى اتخاذ قرارات منحازة ضد فئات معينة من العملاء. على سبيل المثال، إذا كانت بيانات التدريب تحتوي على نسبة مرتفعة من حالات الاحتيال المرتبطة بمجموعات جغرافية أو اجتماعية معينة، فقد تتعلم الأنظمة الذكية تصنيف جميع الأفراد من تلك المجموعات كمشتبه بهم، مما يؤدي إلى ظلم بعض العملاء ورفض معاملاتهم المالية دون أسباب موضوعية.

بالإضافة إلى ذلك، يشكل الافتقار إلى الشفافية في قرارات الذكاء الاصطناعي مشكلة أخلاقية رئيسية. غالبًا ما تعتمد الأنظمة الذكية على خوارزميات معقدة، مثل الشبكات العصبية العميقة، التي تعمل بطريقة تشبه "الصندوق الأسود"، مما يجعل من الصعب على المؤسسات المالية وحتى على الجهات التنظيمية فهم كيفية اتخاذ القرارات. يؤدي ذلك إلى انعدام المساءلة، حيث قد يجد العملاء أنفسهم متضررين من قرارات آلية دون وجود جهة واضحة يمكنهم الرجوع إليها للطعن في هذه القرارات.

أما من حيث الخصوصية، فإن تحليل البيانات المالية يتطلب جمع معلومات حساسة للغاية، تشمل المعاملات البنكية، والمشتريات، والسلوك المالي للأفراد والشركات. في بعض الحالات، قد يتم تخزين هذه البيانات على خوادم خارجية أو مشاركتها مع أطراف ثالثة دون معرفة العملاء، مما يزيد من خطر تسرب المعلومات أو استخدامها لأغراض غير مشروعة. من أبرز الأمثلة على ذلك فضيحة "Cambridge Analytica"، التي كشفت عن استغلال البيانات الشخصية بطرق غير أخلاقية، مما دفع الحكومات إلى تشديد القوانين المتعلقة بحماية البيانات. (خالد محمود، 2024، ص. 60).

كما تبرز مخاوف متعلقة بالاختراقات الأمنية وسرقة البيانات، حيث تعتبر البيانات المالية هدفًا رئيسيًا للهجمات الإلكترونية. يمكن للمتسللين استغلال نقاط الضعف في أنظمة الذكاء الاصطناعي لاختراق البيانات المالية وسرقة المعلومات الحساسة، مما يؤدي إلى خسائر مالية ضخمة وانتهاكات للخصوصية. ولهذا السبب، تعتمد بعض المؤسسات المالية تقنيات مثل التشفير المتقدم وتقنيات التعلم الفيدرالي، التي تسمح بتدريب نماذج الذكاء الاصطناعي دون الحاجة إلى مشاركة البيانات الخام بين المؤسسات.

من الناحية القانونية، تسعى بعض الدول إلى وضع قوانين تحمي خصوصية البيانات المالية، مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، التي تفرض قيودًا صارمة على كيفية جمع البيانات الشخصية ومعالجتها. كما أن بعض الدول، مثل الولايات المتحدة والصين، بدأت في تطوير قوانين تلزم المؤسسات المالية بالإفصاح عن كيفية استخدام الذكاء الاصطناعي في تحليل البيانات المالية، وذلك لضمان تحقيق التوازن بين مكافحة الغش المالي وحماية خصوصية الأفراد.

في المستقبل، من المتوقع أن يتم تعزيز المبادئ الأخلاقية في استخدام الذكاء الاصطناعي من خلال تبني معايير أخلاقية موحدة، مثل تلك التي تقترحها منظمة التعاون والتنمية الاقتصادية (OECD)، والتي تشدد

على أهمية الشفافية، وعدم التحيز، وحماية البيانات في جميع تطبيقات الذكاء الاصطناعي. كما أن تطوير تقنيات مثل "الذكاء الاصطناعي القابل للتفسير" (Explainable AI) قد يساعد في تحسين الشفافية وجعل قرارات الأنظمة الذكية أكثر قابلية للفهم والتفسير. (خالد سعيد، 2021، ص. 105).

6 الاطار القانوني والتشريعي الجزائري في مجال الذكاء الاصطناعي لمحاربة الغش المالي: الجزائر لاتزال في بداية التوجه نحو استخدام الذكاء الاصطناعي في كافة المجالات ولذلك ليس هناك قوانين خاصة بالذكاء الاصطناعي تهتم بالغش المالي بشكل مباشر، لكن هناك مجموعة من القوانين التي تهتم بالغش المالي بشكل عام يمكن أن تشكل الركيزة الأساسية لتشريع المزيد من القوانين، وهي كما يلي:

6. 1 قانون مكافحة الفساد: يعرف رسميا باسم "القانون رقم 06-01 المؤرخ في 20 فبراير 2006 يتعلق بالوقاية من الفساد ومكافحته" يعتبر هذا القانون المرجع التشريعي الأساسي لمحاربة الفساد في البلاد حيث يضم مجموعة واسعة من الجرائم منها: الرشوة في القطاعين العام والخاص، اختلاس الأموال العامة، استغلال النفوذ، سوء استعمال الوظيفة، الاثراء غير المشروع، تبيض الأموال الناتجة عن الفساد. وتم بموجب هذا القانون انشاء الهيئة الوطنية للوقاية من الفساد ومكافحته المستقلة حيث تقوم بتنسيق الجهود للوقاية والتحقيق والتبليغ عن جرائم الفساد. وكان الهدف الأساسي من هذا القانون هو وضع آليات قانونية ومؤسساتية فعالة لمكافحة الفساد وتعزيز النزاهة والشفافية. (وزارة العدل ، 2006).

علاقة القانون رقم 06-01 بالذكاء الاصطناعي: على الرغم أن القانون لا يشير صراحة إلى الذكاء الاصطناعي إلا أن موادته تسمح باستخدام التقنيات الحديثة في التحقيق وجمع الأدلة، وهذا يفتح الباب أمام ادماج الذكاء الاصطناعي مستقبلا في تحليل البيانات المالية، ورصد التحويلات المشبوهة، وكشف تعارض المصالح في المعاملات.

6. 2 القانون رقم 05-01 المؤرخ في 06 فبراير 2005 " يتعلق بالوقاية من تبيض الأموال وتمويل الارهاب ومكافحتهما" صدر هذا القانون ضمن جهود الدولة للائتمثال للمعايير الدولية في محاربة الجريمة المالية، حيث يشمل الأموال الناتجة عن الجرائم مثل: الفساد، الاختلاس، التهريب، الابتزاز، التهرب الضريبي. (وزارة العدل ، 2006) الهدف من هذا القانون منع ومكافحة تبيض الأموال وتعزيز الشفافية والرقابة على

المعاملات المالية، تم تعديل هذا القانون عدت مرات ليتناسب مع التطورات الاقتصادية المستمرة، من أهم تعديلاته:

القانون رقم 15-06 المؤرخ في 16 فبراير 2015 يتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهم، ويعد تعديلا وتحديثا للقانون رقم 05-01 لسنة 2005، حيث جاء هذا القانون في اطار تعزيز التزامات الجزائر تجاه المعايير الدولية خاصة توصيات مجموعة العمل المالي FATF. حيث تم في هذا القانون توسيع تعريف جريمة غسل الأموال لتشمل الأموال الناتجة عن جميع الجرائم بما فيها الالكترونية، الزام البنوك والمؤسسات المالية وغير المالية بالإبلاغ عن العمليات المشبوهة. (الجزائرية، 2015)

القانون رقم 23-01 المؤرخ في 07 فبراير 2023 المعدل والمتمم للقانون 05-01 يهدف هذا القانون إلى تعزيز الإطار القانوني لمكافحة الجرائم المالية في الجزائر، تم توسيع صلاحيات خلية معالجة المعلومات المالية لتشمل: تحليل المعلومات المالية المشبوهة، التنسيق مع الجهات الأمنية والقضائية. (الجزائرية، الجريدة الرسمية للجمهورية، 2023)

هذه القوانين لا تشير إلى الذكاء الاصطناعي بشكل صريح لكن تفتح المجال لاستخدام التقنيات المتطورة في كشف الجرائم المتعلقة بالأموال. ويمكن أن تشكل قاعدة قانونية أساسية لتشريع قوانين خاصة بطريقة استخدام الذكاء الاصطناعي في كشف الجرائم المالية في المستقبل.

7. خاتمة:

في ظل تزايد عمليات الاحتيال المالي وتعقيد أساليب الغش، أصبح الذكاء الاصطناعي أداة حاسمة في تعزيز الأمن المالي وكشف الأنشطة المشبوهة بكفاءة وسرعة. تعتمد المؤسسات المالية على تقنيات متقدمة مثل التعلم الآلي، وتحليل البيانات الضخمة، وأنظمة التنبؤ لتحديد الأنماط الاحتيالية واتخاذ قرارات استباقية لمنع الخسائر. ورغم ذلك، لا يزال هناك العديد من التحديات التي يجب معالجتها، بدءًا من ضمان دقة وشفافية قرارات الذكاء الاصطناعي، وصولًا إلى الامتثال للمعايير القانونية وحماية خصوصية البيانات المالية. ومن أجل تحقيق الاستفادة القصوى من هذه التقنيات، يجب على الحكومات والمؤسسات المالية العمل على تطوير سياسات تنظيمية متوازنة تعزز من استخدام الذكاء الاصطناعي في مكافحة الغش المالي دون المساس بحقوق الأفراد أو تعريض النظام المالي لمخاطر أخلاقية وتقنية. مستقبل الذكاء الاصطناعي في هذا المجال يحمل إمكانيات هائلة، لكنه يتطلب تنظيمًا دقيقًا وتعاونًا عالميًا لضمان استخدامه بطريقة آمنة وعادلة.

الجزائر لم تشرع قوانين خاصة بالذكاء الاصطناعي في محاربة الغش المالي بعد وهذا راجع إلى أن الدولة لم تبدأ في استخدام مجالات الذكاء الاصطناعي إلى في السنوات القليلة الأخيرة، لكن هناك قوانين يمكن أن تكون قوانين رجعية في هذا المجال.

8. قائمة المراجع:

1. أحمد عبد الله - تطبيقات الذكاء الاصطناعي في التعليم - دار العلوم - مصر - 2023 - ص. 67.
2. عادل عبد النور - الذكاء الاصطناعي واقعه ومستقبله - دار الفكر العربي - مصر - 2007 - ص. 102.
3. محمد الغامدي - الذكاء الاصطناعي في التعليم - دار الخريجي - السعودية - 2024 - ص. 88.
4. مارجريت إيه بودين - الذكاء الاصطناعي: مقدمة قصيرة جدًا - مؤسسة هنداوي - المملكة المتحدة - 2015 - ص. 45.
5. محمد العارضة - قائمة أفضل كتب في الذكاء الاصطناعي 2024 - دار النشر العربية - الأردن - 2024 - ص. 53.
6. أحمد محمد - الذكاء الاصطناعي وتعلم الآلة - دار التقنية - مصر - 2022 - ص. 120.
7. خالد علي - التعلم العميق: المبادئ والأساليب - دار المعرفة - لبنان - 2021 - ص. 95.
8. سارة أحمد - مشاريع تعلم الآلة باستخدام بايثون - دار البرمجيات - الإمارات - 2020 - ص. 110.
9. عبد الرحمن حسن - مدخل إلى الذكاء الاصطناعي وتعلم الآلة - دار الفكر - سوريا - 2019 - ص. 75.
10. محمد علي - التعلم الآلي التطوري في الذكاء الاصطناعي - دار النشر العلمية - مصر - 2023 - ص. 130.
11. أحمد سعيد - التعلم العميق من الأساسيات حتى بناء شبكة عصبية عميقة بلغة بايثون - دار البرمجة - السعودية - 2022 - ص. 145.
12. خالد محمود - الذكاء الاصطناعي واستخداماته في البحث والنشر الأكاديمي: كيفية استخدام *ChatGPT* في البحث والنشر الأكاديمي - دار الأكاديميون - الأردن - 2024 - ص. 12.
13. محمد حسن - الذكاء الاصطناعي: مفهومه وأهميته - دائرة المالية - الإمارات - 2023 - ص. 25.
14. عبد الله يوسف - أفضل 20 كتابًا في علم الذكاء الاصطناعي 2024 - دار المعرفة - مصر - 2024 - ص. 80.
15. سامي محمد - الذكاء الاصطناعي: تطبيقاته وتحدياته - دار الفكر العربي - لبنان - 2021 - ص. 140.
16. هند سعيد - الذكاء الاصطناعي في التحليل المالي - دار العلوم المالية - الإمارات - 2020 - ص. 95.
17. أحمد علي - الذكاء الاصطناعي ومكافحة الاحتيال المالي - دار الاقتصاد - مصر - 2019 - ص. 115.
18. محمد عبد الرحمن - تطبيقات الذكاء الاصطناعي في القطاع المالي - دار النشر الأكاديمي - الأردن - 2022 - ص. 130.
19. خالد سعيد - الذكاء الاصطناعي والشبكات العصبية - دار التقنية الحديثة - السعودية - 2021 - ص. 105.
20. سارة محمد - الذكاء الاصطناعي: التحديات والفرص - دار المستقبل - مصر - 2023 - ص. 90.

- 21.وزارة العدل- القانون رقم 06- 01 يتعلق بالوقاية من الفساد ومكافحته- المؤرخ في 20 فبراير 2006- الطبعة الأولى- ص01-24.
- 22.وزارة العدل- القانون رقم 05-01 يتعلق بالوقاية من تبييض الأموال وتمويل الارهاب ومكافحتهما، المؤرخ في 06 فبراير 2005- الطبعة الأولى- ص01-24.
- 23.الجريدة الرسمية للجمهورية الجزائرية- قانون رقم 15-06 يعدل ويتمم القانون رقم 05-01- المؤرخ في 15 فبراير 2015- العدد 08- ص 04-06.
- 24.الجريدة الرسمية للجمهورية الجزائرية- القانون رقم 23-01 المؤرخ في 07 فبراير 2023 المعدل والمتمم للقانون 05-01- 2023/02/18- العدد 08 - ص06-15.