Professeur Kelly Mua Kingsly
PhD/MBA, MPA, CFA, CFI, PMP, ISO
Ingénieur financier (juricomptabilité finance et audits)
(4) Professeur Kelly M Kingsley | Université Harvard - Academia.edu
blog :www.kellykingsly.com
Mes articles : SSRN
https://www.linkedin.com/in/kelly-kingsley-ph-d-2a5a1416/

L'analyse prédictive dans le domaine de la finance forensique : utiliser l'IA pour anticiper les crimes financiers

1. Présentation

Dans le monde dynamique de la finance, le potentiel d'exploitation par les individus, les entreprises et le crime organisé reste toujours présent. Qu'il s'agisse de fausses déclarations et de dissimulation de dettes par le biais de manipulations boursières, de systèmes de Ponzi ou de cybercriminalité plus sophistiquée d'aujourd'hui, un jeu du chat et de la souris existe entre les transgresseurs et les personnes chargées de la surveillance et de la conformité. La prolifération exponentielle des données et leur complexité inhérente au secteur financier, notamment la banque, l'investissement, l'assurance et les finances personnelles, ont suscité de nouvelles techniques de calcul pour soutenir l'analyse et l'intervention humaine. L'intégration de l'intelligence artificielle (IA) dans l'analyse des données promet des prédictions et découvertes fiables de ce qui n'est pas détecté, ce qui est caché, ce qui est invraisemblable et ce qui est impossible [1]. Par conséquent, les informations dérivées des données peuvent aider à anticiper les scénarios futurs et à soutenir les processus de prise de décision. L'identification des modèles émergents dans l'évolution temporelle des données financières est cruciale, en particulier dans les situations à forts enjeux impliquant des investissements ou des risques importants. Les progrès récents de l'apprentissage automatique intensif ont révolutionné cette capacité dans divers domaines d'application, notamment la reconnaissance vocale et d'image, la sécurité, les médias sociaux et la finance.

Le développement bancaire contemporain met l'accent sur l'expansion et l'amélioration des services bancaires de détail et l'adoption de nouvelles technologies. L'évolution rapide des marchés, l'intensification de la concurrence et la mondialisation ont fait apparaître divers risques dans le secteur bancaire. Les prêts non performants sont une préoccupation majeure pour les banques, car ils affectent la performance et la durabilité. La croissance économique, l'inflation et

les taux d'intérêt ont été examinés en fonction de leur impact sur les prêts non performants des banques [2]. Les pays où les prêts improductifs sont élevés sont plus susceptibles de connaître une croissance atone, et la crise financière mondiale en cours a eu des répercussions négatives sur le secteur bancaire de la plupart des pays.

1.1. Contexte et importance

La croissance exponentielle des crimes financiers après l'effondrement mondial de 2008 a alarmé les auditeurs judiciaires et les organismes d'application de la loi du monde entier. Les crimes financiers majeurs, y compris les systèmes de Ponzi, les délits d'initiés, les fausses déclarations, la corruption internationale et le blanchiment d'argent, sont souvent commis par des professionnels à « QI élevé », invoquant une chasse au chat et à la souris entre eux et les agences de protection des investissements. Bien qu'elles soient techniquement solides, les équipes d'audit de conformité et d'audit judiciaire n'ont pas l'agilité des technologies d'intelligence artificielle (IA), d'apprentissage automatique (ML) et d'apprentissage profond (DL), qui peuvent analyser de nombreuses données financières historiques en quelques secondes et retracer la piste financière criminelle [3]. L'analyse prédictive utilisant les technologies de l'IA permet de prévoir d'éventuels scénarios de criminalité financière sur la base de phénomènes criminels passés. Ce document souligne le besoin crucial de l'analyse prédictive dans le financement judiciaire pour anticiper les crimes financiers avant qu'ils ne se perpétruent. Il analyse également les différentes caractéristiques de la criminalité financière qui peuvent être prédites et les technologies prédictives disponibles dans les domaines non financiers applicables au financement judiciaire. Le modèle complet proposé profitera énormément aux organismes de protection des investissements et aux cabinets d'audit judiciaire à l'échelle mondiale.

1.2. Objectif de l'étude

La criminalité financière est un problème grave et croissant dans le monde entier. À mesure que les marchés financiers deviennent plus complexes, opaques et accessibles, les criminels s'adaptent rapidement et exploitent les lacunes des régulateurs et des organismes d'application de la loi. La criminalité financière est souvent multinationale, multijuridictionnelle, très sophistiquée et complexe à détecter. En raison de cette complexité, de nombreux organes législatifs ont mis en place des équipes d'investigation au sein des autorités financières pour repérer les nouveaux cas de malversations financières, élaborer des réponses politiques

réglementaires et mener des enquêtes criminelles. Les analystes financiers judiciaires examinent la production quotidienne de milliers de séries de données sur les marchés financiers, à la recherche d'activités anormales. L'analyse prédictive est bénéfique dans la prévention de la criminalité opérationnelle et pourrait jouer un rôle similaire dans le financement judiciaire [2]. Malheureusement, les résultats expérimentaux ne sont généralement pas accessibles au public. Par conséquent, l'efficacité des signaux prédictifs (et les conséquences imprévues possibles) des crimes financiers émergents est totalement inconnue.

Le financement judiciaire a un coût très élevé associé aux faux positifs, car il entraîne un examen coûteux et chronophage des données de marché par des experts en finance judiciaire. De plus, toute menace perçue pour le marché peut nuire au système économique dans son ensemble. Compte tenu de ces défis, il est essentiel de s'assurer que toute technologie prédictive proposée est efficace (en termes de sensibilité) et qu'elle présente de faibles niveaux de faux positifs [3]. Ce document est la première étape de l'évaluation de la question de savoir si l'analyse prédictive peut avoir un impact positif sur les efforts de financement judiciaire pour identifier les crimes financiers émergents. La recherche empirique utilise des données de marché artificielles pour inclure des cas connus de crimes financiers émergents. Les anomalies de marché déclenchées de manière aléatoire sont utilisées pour émuler les données de marché des « lanceurs d'alerte » qui résulteraient de la criminalité financière émergente.

1.3. Champ d'application et limites

Cet article examine le potentiel de l'application de l'analyse prédictive basée sur l'IA à la finance judiciaire. L'IA et l'analyse prédictive offrent une occasion unique d'améliorer l'efficacité des stratégies de financement judiciaire, à l'instar des progrès observés actuellement dans des domaines tels que les soins de santé, l'assurance, l'application de la loi et la sécurité nationale. Les raisons sous-jacentes à cette opportunité sont examinées, et les résultats d'un modèle d'analyse prédictive de preuve de concept récent développé en Python sont pris en compte. Étant donné que l'accent est mis sur l'intégration de l'IA et de l'analyse prédictive dans la finance judiciaire, les résultats de cette recherche sont considérés dans le contexte d'une discussion plus large sur l'IA et les systèmes d'analyse prédictive, par opposition à une focalisation plus étroite sur les aspects purement techniques du modèle de preuve de concept lui-même [3]. Cette introduction comprend un aperçu de haut niveau du financement judiciaire, examine l'impact de la pandémie

de COVID sur la criminalité financière et présente des prévisions sur l'état futur de la criminalité économique qui soulignent la nécessité d'améliorer les capacités de jurifinancement.

Le financement judiciaire est la discipline qui enquête sur les comportements anormaux au sein des systèmes financiers afin de déterminer la présence, la nature et l'étendue de la criminalité financière. La criminalité financière implique généralement un comportement déguisé visant à manipuler un système financier afin d'extraire, de détourner ou de dissimuler des fonds illicitement. Les systèmes financiers étudiés par le financement judiciaire impliquent généralement des transactions de données financières entre plusieurs parties qui sont enregistrées dans un format structuré et séquencé dans le temps [1]. L'exemple le plus connu est celui du système bancaire, qui dispose d'un large éventail de données financières enregistrées dans des formats de données ou des bases de données hautement structurées à l'aide d'un protocole de transaction interbancaire mondial standardisé. D'autres systèmes financiers sont moins structurés mais imposent tout de même une certaine structure dans les données financières, tels que les échanges de titres, les systèmes comptables et les systèmes de planification des ressources de l'entreprise.

2. Fondements théoriques

La conformité à la lutte contre le blanchiment d'argent et la détection des fraudes sont des exemples de tâches de juricomptabilité financière qui impliquent de passer au crible les transactions financières pour trouver des modèles indiquant des crimes économiques. Les approches traditionnelles des tâches judiciaires reposent en grande partie sur l'expertise des enquêteurs et des statisticiens en matière de criminalité financière. Cependant, les institutions financières souhaitent automatiser certaines parties des enquêtes judiciaires où les données sont abondantes, mais il est nécessaire d'enquêter de manière proactive sur les finances. L'analyse prédictive peut être utilisée pour rechercher une activité nuisible probable au lieu d'attendre passivement l'arrivée d'une activité suspecte [4].

Les institutions financières réalisent fréquemment des audits de l'activité de leurs clients ou contreparties. Cela se traduit généralement par l'examen de nombreuses transactions par des équipes d'investigation. Une approche plus efficace consisterait à utiliser l'analyse prédictive pour sélectionner un ou plusieurs clients ou contreparties à auditer en fonction de la suspicion déduite du modèle. Comme pour de nombreux autres domaines d'application en finance, les modèles

apprenants pourraient être ajustés à un enregistrement historique d'activité auditée, en tenant compte de l'équité du modèle si certains clients ou homologues se sont livrés à des activités néfastes [2].

2.1. Financement judiciaire et criminalité financière

L'évolution rapide de la technologie et de l'économie mondiale a modifié le profil de nombreux crimes. Les crimes financiers se sont multipliés et sont devenus la menace la plus grave pour l'économie mondiale et la sécurité financière. Les crimes financiers transgressent les frontières et les territoires nationaux, ce qui rend l'application de la loi difficile. De plus, l'intelligence et la sophistication des criminels financiers se sont considérablement améliorées, ce qui rend difficile l'enquête et la poursuite des crimes financiers. Récemment, certains pays ont tenté d'établir un régime de juricomptabilité similaire à celui de la juricomptabilité pour enquêter et prévenir les crimes financiers [1].

Le financement judiciaire fait référence à la combinaison de la finance et du droit pour enquêter sur les crimes financiers. Le financement judiciaire consiste à recueillir et à analyser des preuves financières liées aux crimes financiers et à élaborer des scénarios capables de prédire les intentions des criminels financiers et leurs éventuels crimes futurs, ce qui est généralement appelé profilage criminel ou analyse des modèles de criminalité en criminologie. La finance judiciaire utilise couramment des modèles de prévision financière pour reconstruire le passé et prévoir l'avenir de paramètres financiers spécifiques. Cependant, les modèles de prévision financière existants ne peuvent répondre passivement aux crimes financiers qu'après leur survenance et ne peuvent pas les anticiper activement. Il est souhaitable d'analyser les activités financières de manière proactive, de trouver d'éventuels crimes financiers et de prédire les futurs modèles de criminalité financière [3].

2.2. Analyse prédictive et apprentissage automatique

L'analyse prédictive est devenue une méthode populaire pour les organisations qui cherchent à appréhender les comportements criminels avant qu'ils ne se produisent. L'émergence de l'intelligence artificielle et de l'apprentissage automatique permet des modèles prédictifs plus sophistiqués. Les techniques d'IA et de ML peuvent analyser le big data pour reconnaître des modèles et des tendances, en identifiant les comportements au-delà des seuils normatifs. L'analyse prédictive est utilisée dans divers secteurs, y compris les services de police et les écoles, pour prévoir les crimes futurs et déterminer les élèves à risque.

Il peut examiner les données historiques pour découvrir des associations entre les crimes et les lieux, les périodes ou les personnes impliquées.

La criminalité financière, y compris le blanchiment d'argent, l'évasion fiscale, la fraude en valeurs mobilières et la fraude comptable, mine l'intégrité et la stabilité du système financier et a des conséquences sociétales de grande portée, notamment le financement du terrorisme et la traite des personnes. La pandémie a exacerbé les conditions de la criminalité financière, de plus en plus de personnes à domicile devenant vulnérables à la fraude en ligne. Reconnaissant l'urgence, plusieurs organismes de réglementation et d'application de la loi ont élaboré des documents stratégiques pour lutter contre la criminalité financière. Cependant, la prévention, la détection et les enquêtes sur la criminalité financière sont difficiles en raison de l'évolution technologique rapide du système financier. Le suivi et la reconstitution des activités financières pour constituer un dossier de crime nécessitent une analyse approfondie des données transactionnelles volumineuses dans l'ensemble du système financier, qui repose actuellement sur des ressources humaines manuelles.

2.3. Applications de l'IA dans la finance

L'expansion spectaculaire de la recherche, du développement et des applications de l'intelligence artificielle (IA) a créé de nouvelles opportunités et des défis sans précédent. Dans les affaires, la finance, la science et la société, la vague d'IA changera tôt ou tard les règles du jeu en matière de modélisation financière, d'investissement et de gestion des risques. Les grandes universités et les entreprises financièrement fortunées sont souvent le fer de lance de la recherche et du développement de l'IA. Les pays et les régions où la finance de haute technologie joue un rôle de premier plan se tiendront sur les épaules de géants qui déploient des efforts pluriannuels dans la recherche sur l'IA. Alors que le secteur financier s'appuie de plus en plus sur une modélisation complexe basée sur des données, les impacts socio-économiques et politiques des systèmes d'IA financière doivent être étudiés et surveillés.

La promesse des technologies financières, c'est-à-dire l'application de nouvelles technologies aux services financiers, est de stimuler la concurrence et l'innovation dans un secteur qui a pris du retard par rapport aux autres en matière d'utilisation de la technologie. De nouveaux acteurs, qui ne sont pas encombrés par les systèmes informatiques existants, peuvent offrir des services financiers à moindre coût et plus efficacement que les institutions existantes. Les consommateurs devraient bénéficier de meilleurs produits, services et prix. Cependant, les progrès

technologiques peuvent souvent stimuler la concentration du marché. La finance a une telle tendance à attirer l'attention, ce qui pourrait accroître l'attention portée à la stabilité financière [5]. Les institutions financières traditionnelles et émergentes consacrent des sommes importantes à la technologie. Rien qu'en Europe, les banques ont dépensé 67 milliards d'euros en technologie en 2019 ; aux États-Unis, les dépenses ont dépassé 28 milliards de dollars en 2020.

3. Méthodologie

L'environnement du financement judiciaire regorge de séquences d'événements horodatées susceptibles d'indiquer des crimes financiers imminents. De tels événements doivent être catalogués, analysés et étudiés, souvent à grands frais, par des analystes judiciaires. Cette charge de travail des analystes ne peut être compensée en raison de la rareté des professionnels de la finance légale. L'objectif de cette recherche est d'explorer si l'analyse prédictive pourrait être utilisée pour créer des systèmes qui automatisent la détection de la manipulation potentielle du marché à terme en classant les séquences d'actions de marché horodatées comme « innocentes » ou « manipulatrices » [4]. Le produit final vise à fournir aux équipes de surveillance du financement judiciaire un mécanisme d'alerte automatisé pour examiner les séquences d'action du marché potentiellement manipulatrices avant qu'elles ne dégénèrent en enquêtes financières.

Cette recherche de preuve de concept a été entreprise en trois volets : (1) la génération de données de manipulation de marché semi-synthétiques dans lesquelles l'intention de manipulation est connue, (2) le développement et l'évaluation d'une méthode semi-supervisée basée sur l'apprentissage profond pour détecter la manipulation de marché sur les marchés à terme, et (3) une analyse de sensibilité sur la longueur des séquences d'action de marché nécessaires pour atténuer une stratégie de détection d'évasion réussie [2]. Chaque composant s'appuie sur le précédent. Les utilisateurs finaux visés par cette recherche, les équipes de surveillance financière judiciaire, ont besoin d'une automatisation qui pourrait être appliquée aux données transactionnelles quotidiennes dès leur arrivée. Les systèmes d'apprentissage en ligne sont appelés systèmes automatisés qui génèrent des prédictions à partir de données nouvellement arrivées. Par conséquent, les preuves de concept présentées dans cette recherche sont conçues comme des systèmes d'apprentissage en ligne.

3.1. Collecte et prétraitement des données

Le potentiel de l'analyse prédictive dans le domaine de la criminalistique financière et de la lutte contre le blanchiment d'argent ou la déclaration des

transactions suspectes (STR) a été exploré, en analysant les STR financières grâce à la validation d'un module d'analyse d'intelligence artificielle de preuve de concept. La création de modules d'intelligence artificielle rapides et peu coûteux pour anticiper et inhiber les opérations de continuité des opérations financières, similaires aux antivirus existants, est nécessaire en raison de l'augmentation de la fraude et de la criminalité financières. Actuellement, les DOD sont effectuées manuellement, ce qui facilite l'adoption de nouvelles voies financières [1]. Par conséquent, la possibilité de créer des modules d'intelligence artificielle pour prédire les STR financières est cruciale. Une étude pilote sur la fraude au crédit a été réalisée, et les taux prédictifs élevés ont été validés avec succès par plusieurs méthodes d'apprentissage automatique, ce qui a nécessité des études plus approfondies. La réalisation d'une analyse médico-légale des STR financières sur un ensemble de données STR plus large provenant d'une banque et des résultats permet de prédire les probabilités de détection des STR financières grâce à l'intelligence artificielle en général. Ainsi, le module d'intelligence artificielle de preuve de concept permettant de prévoir les trajectoires de la criminalité financière à travers les DOD financières attendues et anticipées est discuté, en se concentrant sur la collecte de données, la structuration, la modélisation et les modules d'intelligence artificielle STR financiers prédits à partir d'autres ensembles de données STR bancaires.

3.2. Sélection et ingénierie des fonctionnalités

La sélection de caractéristiques pertinentes ou capables de définir des indicateurs appropriés pour comprendre si une entreprise nécessite une enquête plus approfondie est cruciale. Les fonctionnalités sélectionnées pour construire les modèles sont basées sur la littérature antérieure appliquant des techniques d'intelligence artificielle pour détecter la fraude, mais sont complétées par d'autres fonctionnalités pertinentes. Vingt-quatre caractéristiques sont incluses, réparties en quatre catégories : performance de l'entreprise, chiffres comptables, activité du marché et gouvernance d'entreprise. Les variables sélectionnées sont généralement liées à des changements de contexte qui pourraient signaler une fraude potentielle. Par exemple, un changement significatif de la capitalisation boursière pourrait indiquer qu'une entreprise tente de cacher quelque chose et devrait faire l'objet d'une enquête [6]. Toutes les fonctionnalités sont calculées sur la base des données agrégées de l'entreprise par rapport à l'année précédant l'année cible, où la prédiction a lieu. Cela signifie que toutes les caractéristiques sont statiques par rapport à l'année cible.

Les fonctionnalités de performance d'une entreprise visent à analyser l'évolution de la performance d'une entreprise par rapport aux périodes précédentes. À l'instar de la situation où la faillite d'une entreprise est prévue, les changements significatifs dans des variables telles que les bénéfices, le total des actifs et la capitalisation boursière doivent être surveillés par rapport aux années précédentes. En général, la plupart de ces fonctionnalités signalent qu'une entreprise essaie de cacher quelque chose au fur et à mesure que le changement est important. Par exemple, des variations plus importantes des bénéfices peuvent indiquer des bénéfices ajustés entre les exercices, dans le but d'induire les investisseurs en erreur [7]. Alternativement, une entreprise pourrait être impliquée dans un délit d'initié s'il y a des changements soudains dans les cours des actions ou une croissance anormale de l'activité de négociation.

3.3. Élaboration et évaluation du modèle

Une fois que les indicateurs potentiels de criminalité financière ont été identifiés, des modèles d'apprentissage automatique peuvent être développés pour prédire l'occurrence de ces crimes. Les modèles peuvent adopter diverses approches, telles que la classification, la régression ou la détection d'anomalies, et peuvent utiliser des algorithmes allant de simples arbres de décision à des réseaux neuronaux complexes. Les considérations clés comprennent l'équilibre entre la sensibilité et la spécificité (le compromis entre les vrais positifs et les faux positifs) et l'impact de tout ajustement de modèle [8].

Les modèles doivent également être évalués pour s'assurer qu'ils fonctionnent correctement et qu'ils produisent des prédictions précieuses. Un bon point de départ est la matrice de confusion, qui montre les résultats d'un modèle de classification par rapport aux résultats réels. Plusieurs indicateurs de performance peuvent être calculés à partir de cette matrice. Les mesures standard comprennent l'exactitude (la proportion de résultats précis par rapport au nombre total de cas) et le score F1 (la moyenne harmonique de la précision et de la mémorisation). Un autre outil standard pour l'évaluation des modèles est la courbe ROC, qui trace le taux de positivité réel par rapport au taux de faux positifs. Le score AUC résume le graphique ROC en un seul nombre (0,5 représente la performance aléatoire et 1,0 la performance parfaite).

4. Études de cas

Dans le paysage financier moderne, l'essor de la technologie a non seulement transformé la façon dont les transactions financières sont effectuées, mais a également introduit de nouveaux défis dans les crimes économiques tels que la

fraude, le blanchiment d'argent et les délits d'initiés. L'analyse prédictive, alimentée par l'intelligence artificielle (IA), est devenue un outil crucial pour les professionnels de la finance judiciaire qui souhaitent anticiper et atténuer ces crimes. Cette étude de cas explore l'application de l'analyse prédictive dans le financement judiciaire à travers un exemple pratique impliquant les efforts d'une banque multinationale pour lutter contre le blanchiment d'argent.

Arrière-plan

En 2021, une banque multinationale centrale, Global Bank, a fait l'objet d'une surveillance réglementaire accrue en raison d'affaires de blanchiment d'argent très médiatisées liées à ses activités. Le service de conformité de la banque a été submergé par le volume de transactions, ce qui a rendu difficile l'identification des activités suspectes en temps réel. Global Bank a mis en œuvre un système d'analyse prédictive basé sur l'IA pour résoudre ce problème et améliorer ses capacités de financement judiciaire.

Mise en œuvre de l'analyse prédictive

Collecte et intégration des données :

Global Bank a commencé par agréger de grandes quantités de données historiques sur les transactions, de profils de clients et de sources externes telles que des documents publics et des articles de presse. Ces données ont été nettoyées et normalisées pour assurer la cohérence et l'exactitude.

Développement de modèles d'apprentissage automatique :

Les scientifiques des données de Global Bank ont développé des modèles d'apprentissage automatique à l'aide de techniques d'apprentissage supervisées. Ils ont entraîné les modèles sur des données historiques, y compris des cas de blanchiment d'argent connus, afin d'identifier les modèles et les anomalies associés aux activités illicites. Des caractéristiques telles que la taille des transactions, la fréquence, les emplacements géographiques et le comportement des clients ont été incluses dans le modèle.

Détection d'anomalies :

Le système d'IA a été conçu pour surveiller en permanence les transactions en temps réel et signaler les anomalies qui s'écartent des modèles établis. Par exemple, si un client qui effectuait habituellement de petites transactions initiait soudainement un transfert important vers une juridiction à haut risque, le système générerait une alerte pour une enquête plus approfondie.

Évaluation des risques :

Chaque transaction s'est vue attribuer un score de risque basé sur l'analyse du modèle prédictif. Les transactions dépassant un certain seuil étaient

automatiquement signalées pour examen par l'équipe de conformité. Cette approche a permis d'accorder la priorité aux enquêtes sur les activités potentiellement suspectes, ce qui a permis une allocation plus efficace des ressources.

Application pratique : un scénario de cas

Au début de l'année 2022, le système d'analyse prédictive piloté par l'IA a signalé une série de transactions impliquant une entreprise cliente basée dans une région à haut risque connue pour ses activités de blanchiment d'argent. Le système a détecté que le client avait effectué des transferts importants à diverses sociétés fictives dans différentes juridictions sur une courte période.

Ouverture de l'enquête :

L'équipe de conformité a reçu des alertes du système d'IA et a lancé une enquête. Ils ont examiné les transactions signalées et ont constaté que la société cliente n'avait aucune justification commerciale légitime pour de tels transferts.

Diligence raisonnable renforcée :

L'équipe de conformité a effectué une diligence raisonnable accrue, qui comprenait l'examen des activités commerciales, des états financiers et de la structure de propriété du client. Ils ont découvert que des personnes ayant des liens avec des organisations criminelles connues possédaient l'entreprise cliente.

Collaboration avec les forces de l'ordre :

Forte des conclusions de l'enquête, Global Bank a collaboré avec les organismes d'application de la loi pour fournir des preuves d'activités potentielles de blanchiment d'argent. Cette collaboration a donné lieu à une enquête plus vaste qui a permis de découvrir un réseau d'entreprises impliquées dans le blanchiment de fonds pour le compte d'entreprises criminelles.

Rapports réglementaires :

À la suite de l'enquête, Global Bank a déposé des rapports d'activité suspecte (SAR) auprès des autorités réglementaires compétentes, détaillant les conclusions et les mesures prises pour atténuer les risques associés à l'entreprise cliente.

Résultats et avantages

- Détection proactive : Le système d'analyse prédictive basé sur l'IA a permis à Global Bank d'identifier et de traiter de manière proactive les activités potentielles de blanchiment d'argent avant qu'elles ne s'intensifient, réduisant ainsi considérablement son exposition aux sanctions réglementaires.

- Optimisation des ressources : en automatisant le processus de détection des anomalies, l'équipe de conformité peut se concentrer sur les cas à haut risque, améliorant ainsi l'efficacité globale.
- Amélioration de la réputation : L'engagement de Global Bank à lutter contre la criminalité financière au moyen d'une technologie novatrice a renforcé sa réputation dans l'industrie, attirant de nouveaux clients qui appréciaient des mesures de conformité robustes.

Le cas de la Global Bank illustre le potentiel transformateur de l'analyse prédictive dans le domaine de la finance judiciaire. Les organisations peuvent renforcer leurs efforts de conformité en tirant parti de l'IA pour anticiper les crimes financiers et contribuer à la lutte plus large contre la criminalité économique. À mesure que la technologie évolue, l'intégration de l'analyse prédictive deviendra probablement une pratique courante dans le secteur des services financiers, permettant aux entreprises de garder une longueur d'avance sur les menaces émergentes et de protéger l'intégrité du système financier.

4.1. Détection de la fraude dans le secteur bancaire

La complexité croissante des transactions financières et la sophistication des crimes financiers ont rendu les méthodes traditionnelles de détection des fraudes insuffisantes. L'analyse prédictive, alimentée par l'intelligence artificielle (IA), offre au secteur bancaire de nouvelles opportunités pour améliorer ses capacités d'anticipation et d'atténuation des crimes financiers. Ce document explore le rôle de l'analyse prédictive dans le financement judiciaire, en se concentrant sur la manière dont l'IA peut être exploitée pour la détection des fraudes.

Comprendre l'analyse prédictive

L'analyse prédictive implique l'utilisation d'algorithmes statistiques et de techniques d'apprentissage automatique pour identifier des modèles dans les données historiques et prédire les résultats futurs. Dans le contexte du financement judiciaire, il peut aider les institutions à identifier les activités potentiellement frauduleuses avant qu'elles ne se produisent.

Le rôle de l'IA dans l'analyse prédictive

1. Exploration de données : Les algorithmes d'IA peuvent analyser de grandes quantités de données structurées et non structurées provenant de diverses sources, notamment les enregistrements de transactions, le comportement des clients et les

données externes (par exemple, les médias sociaux et les articles de presse). Cette analyse complète permet d'identifier les anomalies qui peuvent indiquer des activités frauduleuses.

2. Modèles d'apprentissage automatique : Les techniques d'apprentissage automatique, telles que l'apprentissage supervisé et non supervisé, peuvent être utilisées pour créer des modèles qui classent les transactions comme légitimes ou suspectes. Ces modèles peuvent apprendre en permanence à partir de nouvelles données, ce qui améliore leur précision.

3. Traitement du langage naturel (NLP) : Le NLP peut analyser les données textuelles, telles que les e-mails et les notes de transaction, pour détecter des modèles ou un langage pouvant indiquer une fraude. Cette capacité améliore la capacité de découvrir les comportements frauduleux cachés.

4. Modélisation prédictive : En créant des modèles prédictifs, les banques peuvent estimer la probabilité que la fraude se produise dans des transactions spécifiques ou des comportements des clients. Ces modèles peuvent être basés sur des cas de fraude historiques, ce qui permet aux institutions de traiter les vulnérabilités de manière proactive.

Applications dans la détection des fraudes

1. Surveillance des transactions : Les systèmes pilotés par l'IA peuvent surveiller les transactions en temps réel, en signalant celles qui s'écartent des modèles établis. Cela permet une enquête et une réponse immédiates aux activités potentiellement frauduleuses.

2. Profilage des clients : Les banques peuvent créer des profils qui aident à identifier les activités inhabituelles en analysant le comportement des clients et l'historique des transactions. Par exemple, un pic soudain de transactions ou des changements dans les habitudes de dépenses peuvent déclencher des alertes pour une enquête plus approfondie.

3. Évaluation des risques : L'analyse prédictive peut attribuer des scores de risque aux transactions ou aux clients en fonction de divers facteurs, tels que la taille des transactions, la fréquence et le comportement historique. Les scores à haut risque peuvent entraîner un examen plus approfondi ou des interventions automatisées.

4. Analyse du réseau : L'IA peut analyser les relations entre les entités (par exemple, les clients, les comptes et les transactions) pour identifier les réseaux

d'activités frauduleuses. Cette approche permet de découvrir des stratagèmes de fraude organisés qui, autrement, pourraient passer inaperçus.

Défis et considérations

1. Confidentialité des données : L'utilisation de l'IA et de l'analyse prédictive soulève des inquiétudes quant à la confidentialité des données et à la conformité aux réglementations telles que le RGPD. Les banques doivent s'assurer qu'elles traitent les données des clients de manière responsable et transparente.

2. Faux positifs : L'un des défis de l'analyse prédictive dans la détection des fraudes est le potentiel de faux positifs, lorsque des transactions légitimes sont signalées comme suspectes. Il est essentiel de trouver un équilibre entre sensibilité et spécificité pour minimiser les désagréments pour les clients.

3. Biais du modèle : Les modèles d'IA peuvent hériter de biais dans les données d'entraînement, ce qui entraîne un traitement injuste de segments de clientèle spécifiques. Une surveillance et un ajustement continus des modèles sont nécessaires pour garantir l'équité et l'exactitude.

4. Intégration avec les systèmes existants : La mise en œuvre de l'analyse prédictive basée sur l'IA nécessite une intégration avec les systèmes et processus bancaires existants, qui peuvent être complexes et gourmands en ressources.

L'analyse prédictive, alimentée par l'IA, représente une avancée significative dans la lutte contre les crimes financiers et la fraude dans le secteur bancaire. En s'appuyant sur des informations basées sur les données, les banques peuvent améliorer leur capacité à anticiper et à atténuer les activités frauduleuses, protégeant ainsi leurs actifs et maintenant la confiance des clients. À mesure que la technologie évolue, il sera essentiel d'investir dans l'IA et l'analyse prédictive pour garder une longueur d'avance sur des crimes financiers de plus en plus sophistiqués.

4.2. Prédiction d'un délit d'initié

Le délit d'initié, c'est-à-dire la pratique illégale de négocier en bourse à son avantage en ayant accès à des informations confidentielles, présente des risques importants pour l'intégrité des marchés et la confiance des investisseurs. Avec l'avènement des technologies de pointe, notamment l'intelligence artificielle (IA) et l'analyse prédictive, le secteur financier se tourne de plus en plus vers ces outils pour détecter et prévenir les activités de délit d'initié. Ce document explore comment l'IA peut

prédire les délits d'initiés, améliorer les efforts de conformité et renforcer les stratégies de financement judiciaire.

Le rôle de l'analyse prédictive dans le financement judiciaire

L'analyse prédictive implique l'utilisation d'algorithmes statistiques et de techniques d'apprentissage automatique pour identifier la probabilité de résultats futurs sur la base de données historiques. Dans le contexte de la finance judiciaire, l'analyse prédictive peut aider les institutions financières et les organismes de réglementation à :

Identifier les modèles : En analysant les données de trading historiques, l'IA peut découvrir des modèles indiquant un délit d'initié, tels que des volumes de transactions inhabituels ou des mouvements de prix précédant des annonces d'entreprise importantes.

Signaler les anomalies : Les algorithmes d'apprentissage automatique peuvent être entraînés à reconnaître les écarts par rapport au comportement de trading typique, ce qui permet de signaler automatiquement les transactions suspectes.

Améliorer les processus d'enquête : les modèles prédictifs peuvent hiérarchiser les cas d'enquête en fonction des scores de risque, ce qui permet aux équipes d'investigation de concentrer leurs ressources sur les cas les plus probables de délit d'initié.

Techniques d'IA pour la prédiction des délits d'initiés

Algorithmes d'apprentissage automatique :

- Apprentissage supervisé : les données historiques sur les cas connus de délit d'initié peuvent être utilisées pour entraîner des modèles à reconnaître les caractéristiques de ces transactions. Des algorithmes tels que la régression logistique, les arbres de décision et les machines à vecteurs de support peuvent être utilisés.

- Apprentissage non supervisé : Des techniques telles que le clustering peuvent identifier des groupes de transactions qui présentent des caractéristiques similaires, ce qui peut justifier une enquête plus approfondie.

Traitement du langage naturel (NLP) :

- NLP peut analyser les articles de presse, les médias sociaux et les communications d'entreprise pour évaluer le sentiment et identifier les fuites potentielles d'informations non publiques qui pourraient influencer le comportement de trading.

Analyse de réseau:

L'analyse des réseaux cartographie les relations entre les individus, les entreprises et les transactions, révélant les liens qui peuvent indiquer une collusion ou des activités coordonnées de délit d'initié.

Analyse de séries chronologiques :

- L'analyse des modèles de trading au fil du temps peut aider à détecter les anomalies qui s'écartent des normes historiques, telles que les pics de volume de transactions avant les annonces importantes. Défis de mise en œuvre

Bien que le potentiel de l'IA dans la prédiction des délits d'initiés soit important, plusieurs défis doivent être relevés :

Qualité et disponibilité des données : L'accès à des ensembles de données complets est crucial pour une modélisation prédictive efficace. Des données incomplètes ou biaisées peuvent conduire à des prédictions inexactes.

Conformité réglementaire : les institutions financières doivent s'assurer que leurs efforts d'analyse prédictive sont conformes aux réglementations en matière de confidentialité et de sécurité des données.

Interprétabilité du modèle : De nombreux modèles d'IA fonctionnent comme des « boîtes noires », ce qui rend difficile pour les enquêteurs de comprendre la raison d'être des prédictions. Il est essentiel d'assurer la transparence pour l'examen réglementaire.

Évolution des tactiques : À mesure que les méthodes de détection s'améliorent, les tactiques employées par les délits d'initiés s'améliorent également. Des mises à jour et une formation continue du modèle sont nécessaires pour suivre le rythme de ces changements.

Études de cas et applications

Plusieurs institutions financières et organismes de réglementation ont commencé à mettre en œuvre l'analyse prédictive basée sur l'IA pour la détection des délits d'initiés :

FINRA (Financial Industry Regulatory Authority) : La FINRA a adopté des techniques d'apprentissage automatique pour analyser les modèles de trading et détecter les activités potentielles de délit d'initié.

Goldman Sachs : La banque d'investissement a investi dans les technologies d'IA pour améliorer ses systèmes de surveillance de la conformité, permettant une analyse en temps réel des données de trading.

NASDAQ : La bourse a développé des algorithmes qui surveillent l'activité de trading pour détecter des signes de délit d'initié à l'aide de données historiques et d'analyses en temps réel.

L'intégration de l'analyse prédictive et de l'IA dans le financement judiciaire représente une approche transformatrice pour lutter contre les délits d'initiés. En tirant parti des technologies de pointe, les institutions financières peuvent améliorer leur capacité à détecter les activités suspectes, à assurer la conformité et à maintenir l'intégrité du marché. Alors que le paysage de la criminalité financière continue d'évoluer, la recherche et le développement continus en matière d'analyse prédictive seront essentiels pour garder une longueur d'avance sur les pratiques illicites et protéger les investisseurs et les marchés.

4.3. Détection du blanchiment d'argent

Dans le domaine de la finance légale, la détection et la prévention des crimes financiers, tels que le blanchiment d'argent, sont devenues de plus en plus sophistiquées en raison de l'avènement de l'analyse prédictive et de l'intelligence artificielle (IA). Ces technologies permettent aux institutions financières et aux organismes de réglementation d'analyser de vastes données, d'identifier des modèles et d'anticiper les activités illicites potentielles.

Comprendre le blanchiment d'argent

Le blanchiment d'argent est le processus qui consiste à faire en sorte que de l'argent obtenu illégalement semble légitime. Il comporte généralement trois étapes :

Placement : Introduire des fonds illicites dans le système financier.

Superposition : Effectuer une série de transactions pour masquer l'origine de l'argent.

Intégration : Réintroduire l'argent blanchi dans l'économie, ce qui rend difficile la traçabilité.

Le rôle de l'analyse prédictive

L'analyse prédictive fait appel à des techniques statistiques et à des algorithmes d'apprentissage automatique pour analyser les données historiques et prédire les résultats futurs. Cela peut être appliqué dans le domaine du financement judiciaire pour détecter les anomalies et les activités suspectes liées au blanchiment d'argent.

Collecte de données : Les institutions financières recueillent des données à partir de diverses sources, notamment des relevés de transactions, des profils de clients et des données externes (p. ex., des articles de presse et des médias sociaux).

Traitement des données : Des algorithmes avancés traitent ces données pour identifier des modèles et des corrélations qui peuvent indiquer des activités de blanchiment d'argent.

Détection des anomalies : les modèles d'apprentissage automatique peuvent être entraînés à reconnaître les comportements normaux des transactions. Lorsqu'une transaction s'écarte considérablement de ces normes, elle peut être signalée pour une enquête plus approfondie.

Évaluation des risques : les modèles prédictifs peuvent attribuer des scores de risque aux transactions ou aux clients en fonction de divers facteurs, tels que la taille des transactions, la fréquence, l'emplacement géographique et le comportement historique.

Analyse de réseau : L'IA peut analyser les relations et les connexions entre les entités (individus, entreprises, comptes) pour découvrir les réseaux cachés impliqués dans le blanchiment d'argent.

Techniques utilisées dans l'analyse prédictive pour la détection du blanchiment d'argent

Apprentissage supervisé : Les algorithmes sont entraînés sur des ensembles de données étiquetés contenant des cas de blanchiment d'argent antérieurs. Le modèle apprend à identifier les caractéristiques indiquant une activité suspecte.

Apprentissage non supervisé : cette technique est utilisée pour identifier des modèles dans des données non étiquetées. Les algorithmes de clustering peuvent regrouper des transactions similaires, ce qui permet de révéler les valeurs aberrantes qui peuvent justifier une enquête.

Traitement du langage naturel (NLP) : le NLP peut analyser des données non structurées, telles que des articles de presse et des publications sur les réseaux sociaux, afin d'identifier les mentions d'activités ou d'entités suspectes.

Analyse des séries chronologiques : Cette technique permet d'analyser les tendances des transactions au fil du temps, ce qui permet de détecter des pics ou des baisses inhabituels d'activité pouvant indiquer du blanchiment d'argent.

Défis et considérations

Qualité des données : L'efficacité de l'analyse prédictive dépend fortement de la qualité et de l'exhaustivité des données. Des données inexactes ou incomplètes peuvent entraîner des faux positifs ou des détections manquées.

Conformité réglementaire : Les institutions financières doivent s'assurer que leurs pratiques d'analyse prédictive sont conformes aux réglementations telles que la loi sur le secret bancaire (BSA) et les lois anti-blanchiment d'argent (AML).

Biais et équité : les modèles d'IA peuvent incorporer par inadvertance des biais dans les données d'entraînement, ce qui entraîne un traitement injuste de certains groupes. La surveillance et l'ajustement continus des modèles sont essentiels.

Évolution des tactiques : Les blanchisseurs d'argent adaptent continuellement leurs méthodes pour échapper à la détection. Les modèles prédictifs doivent être régulièrement mis à jour pour tenir compte des nouvelles tactiques et tendances.

L'analyse prédictive alimentée par l'IA représente une approche transformatrice de la lutte contre les crimes financiers tels que le blanchiment d'argent. En exploitant la puissance de l'analyse des données, les institutions financières peuvent identifier et atténuer les risques de manière proactive, contribuant ainsi à un système financier plus sûr. À mesure que la technologie évolue, l'innovation et la collaboration continues entre les parties prenantes seront essentielles pour garder une longueur d'avance sur les criminels financiers.

5. Défis et considérations éthiques

L'intégration de l'IA et de l'apprentissage automatique dans le financement judiciaire offre aux organismes d'enquête et d'audit des opportunités sans précédent pour atténuer les crimes financiers de manière préventive. Cependant, l'application de ces technologies dans des contextes réels pose également des défis et des préoccupations à multiples facettes, couvrant les dimensions techniques, opérationnelles et éthiques. Étant donné la nature insidieuse des crimes financiers contemporains, qui exploitent les vulnérabilités des technologies à venir et impliquent des réseaux complexes, une méthodologie réactive est intrinsèquement inadéquate. Une prévoyance proactive par le biais de l'analyse prédictive est impérative [9].

L'obscurcissement des données associées aux activités criminelles constitue un défi technique important dans la mise en œuvre de modèles financiers prédictifs. Les auteurs de crimes financiers sont susceptibles d'employer des stratégies sophistiquées pour déformer les modèles analytiques intégrés dans les données, atténuant ainsi l'efficacité des modèles d'enquête judiciaire. Par conséquent, la robustesse du modèle contre la perturbation intentionnelle des données devient une considération cruciale. Alors que la recherche sur la robustesse des modèles financiers prédictifs n'en est qu'à ses balbutiements, l'examen d'études analogues en matière de cybersécurité et de fraude informatique judiciaire peut fournir des informations précieuses. De plus, la plupart des modèles prédictifs actuels dans les scénarios de post-audit de juricomptabilité financière dépendent implicitement de la survenance de crimes similaires antérieurs. Les criminels pourraient exploiter cette dépendance en concevant méticuleusement de nouveaux crimes qui intègrent diverses opportunités, les rendant méconnaissables par les modèles de mise en œuvre. Par conséquent, la conception de modèles prédictifs d'investigation financière prédictive avant l'audit doit également être examinée en profondeur.

5.1. Confidentialité et sécurité des données

La mise en œuvre de l'analyse prédictive dans le domaine de la finance judiciaire nécessitera des investissements importants dans l'infrastructure de protection des données. L'analytique multipartite exigera le partage des données entre les organisations et les secteurs. Par conséquent, les organisations de forensic finance doivent investir dans des mesures de sécurité pour protéger les données en transit. Les violations de données peuvent entraîner de lourdes amendes, des atteintes à la réputation et une perte de confiance des parties prenantes.

D'autre part, les organisations financières qui envisagent d'utiliser des données partagées pour l'analyse prédictive dans la prévention de la fraude voudront s'assurer que leurs données ne peuvent pas être rétro-conçues pour obtenir des informations commercialement sensibles sur leurs opérations principales. De nombreuses protections peuvent être appliquées lors de l'analyse des données pour préserver la confidentialité des présentations de données, allant du partage de secrets aux techniques basées sur le cryptage homomorphe [10]. Cependant, ces méthodes ont tendance à être complexes à mettre en œuvre, ce qui compromet le déploiement de l'analyse financière médico-légale multipartite.

Comme pour tous les paramètres, l'option la plus simple pour la protection des données consiste à préserver la confidentialité des données, en veillant à ce que

chaque organisation de juri-finance n'utilise que ses données. Malheureusement, l'analytique appliquée aux données privées a une utilisation limitée, en particulier dans le cas de la détection de la fraude et de la lutte contre le blanchiment d'argent (AML), où les crimes s'étendent généralement à plusieurs organisations et où le partage d'informations est primordial [11]. Sans données partagées, les performances de modélisation se dégradent rapidement avec des ensembles de données plus petits. Par conséquent, toute solution de partage de données adoptée doit s'efforcer de maintenir les données en transit aussi sécurisées que possible pour se protéger contre les attaques externes.

5.2. Biais et équité dans l'IA

Le recours croissant à l'intelligence artificielle (IA) et aux algorithmes (A)/apprentissage automatique (ML) pour la détection de la criminalité financière (FC) a suscité des craintes légitimes de « discrimination algorithmique » (ou de « racisme automatisé », de « sexisme », etc.). Les grands réseaux criminels exploitent les technologies de pointe et la finance numérique, ce qui nécessite des contre-mesures efficaces. Une grande promesse des algorithmes (A)/intelligence artificielle (IA)/apprentissage automatique (M) est leur capacité à traiter des données massives et à détecter des modèles pertinents, améliorant potentiellement la détection de la criminalité financière (FC) [12]. Cependant, au cours des deux dernières décennies, un domaine de débat en plein essor a émergé, avertissant que les systèmes de décision basés sur les algorithmes (A)/l'intelligence artificielle (IA) pourraient apprendre, renforcer et exacerber les préjugés sociaux existants trouvés dans les données qu'ils traitent, conduisant à des décisions particulièrement préjudiciables sur les groupes sociaux touchés de manière disproportionnée. Les recherches initiales se sont concentrées sur des audits post-mortem de systèmes publics largement utilisés, exposant les conséquences dramatiques pour les populations à faible revenu et les populations minoritaires et déclenchant des protestations et des poursuites judiciaires contre le déploiement de systèmes injustes, cherchant à réparer les dommages individuels et à forcer un examen minutieux.

Les systèmes de détection des FC déployés dans les services financiers publics (FS) peuvent nécessairement être imparfaits et biaisés à l'égard de groupes sociaux spécifiques. Le contrat entre la société et l'Autorité de surveillance financière (FSA) publique exige la précision de la prédiction, l'audibilité et la robustesse des systèmes de détection des FC qui ne peuvent pas nuire aux membres « innocents » de la société. Ils s'exposent donc à une responsabilité. Cependant, de tels

systèmes peuvent nuire de manière disproportionnée à des groupes sociaux spécifiques, par exemple les personnes ayant un faible volume de transactions ou une faible capacité sociale. Les caractéristiques, le déploiement et les préoccupations en matière de responsabilité sociale des systèmes publics d'IA diffèrent de ceux que l'on trouve dans le système de justice pénale et la sécurité publique, ce qui nécessite une reconstitution nuancée du débat sur le domaine de détection des FC et une contre-mesure adaptée. Les recherches actuelles (R) se concentrent sur la conception de modèles algorithmiques (A)/intelligence artificielle (IA)/apprentissage automatique (M) et les audits post-mortem de systèmes injustes, nécessitant des efforts correspondants pour garantir l'équité, la responsabilité et la transparence (FAT) dans les systèmes de détection FC.

5.3. Conformité réglementaire

L'analyse prédictive est utilisée pour évaluer la conformité aux réglementations. Il peut être déterminé que les particuliers ou les entreprises présentent une forte probabilité de non-conformité et qu'ils nécessitent une enquête plus approfondie de la part du personnel chargé de la conformité. Plusieurs modèles ont été élaborés pour prédire le comportement en matière de conformité. Ces modèles sont généralement mis en œuvre dans des produits logiciels qui aident le personnel de conformité dans ses enquêtes. Pourtant, ils ont également été appliqués avec succès à des processus d'entreprise en dehors du secteur financier [1]. Par exemple, certains modèles ont été utilisés pour prédire si une affaire judiciaire serait réglée, rejetée ou donnerait lieu à un résultat particulier dans le contexte de la conformité judiciaire.

L'apprentissage automatique identifie en permanence les points d'intervention qui influencent les comportements. Ce principe peut également s'appliquer dans les affaires financières. L'utilisation de l'apprentissage automatique pour prédire un comportement manipulateur pourrait entraîner des interventions réglementaires, par exemple la réduction des pouvoirs discrétionnaires d'un négociant dans des plateformes spécifiques de valeurs mobilières ou de courtiers [13].

6. Orientations futures

L'analyse prédictive dans le domaine de la finance judiciaire n'en est qu'à ses débuts, mais elle progresse rapidement et évolue de manière décisive. Les cadres technologiques de pointe qui sous-tendent le financement judiciaire sont centrés sur le paradigme de l'intelligence artificielle, en se concentrant principalement sur l'exploration de données, la découverte de connaissances et les innovations en matière d'apprentissage automatique. La détection des fraudes financières est un

domaine en pleine évolution. Il existe encore des facettes de la détection intelligente des fraudes qui n'ont pas été étudiées [1]. Le juricomptabilité est un domaine spécialisé qui examine, analyse et reconstitue des événements financiers passés afin de fournir des preuves dans un cadre juridique. La technologie de l'intelligence artificielle est cruciale pour détecter, prévenir et enquêter sur les fraudes et les irrégularités financières.

Les systèmes innovants de détection d'accidents les plus récents adoptés par la communauté de la recherche automobile s'appuient principalement sur les données des capteurs embarqués pour concevoir des détecteurs d'anomalies en temps réel à l'aide de diverses méthodes d'apprentissage automatique basées sur les données. De plus, ces approches ne tiennent pas compte de la disponibilité de modèles et de données évolutifs de haut niveau lorsque les véhicules entrent dans la zone de recherche automobile sur la piste d'essai. La finance judiciaire peut bénéficier considérablement de l'analyse prédictive et de la technologie de l'intelligence artificielle. Les stratagèmes de fraude financière sont plus complexes à identifier en raison de leur secret et de leur complexité croissants. De plus, il devient plus difficile de détecter la fraude sans connaissance préalable des activités de fraude. La fraude financière a tendance à être plus compliquée en raison de la quantité massive d'informations impliquées dans les activités économiques. L'information impliquée est massive mais hétérogène, accompagnée d'une densité de valeur inférieure. Le graphe de connaissances sera l'un des outils les plus essentiels pour une détection complète à l'avenir.

6.1. Technologies et tendances émergentes

Les progrès des mécanismes de défense proactive basés sur l'IA pour prédire et atténuer l'impact des cyberattaques sur les infrastructures critiques sont essentiels au développement des technologies émergentes. En 2019, une nouvelle vague de scénarios de cyberattaques industrielles en technologie multi-agents et en théorie des jeux a été présentée. Par la suite, l'IA d'apprentissage profond a été déployée pour la défense active afin d'atténuer l'impact potentiel de ces attaques. L'effet des cyberattaques potentiellement perturbatrices sur les infrastructures critiques et le développement de l'apprentissage automatique a ensuite été étudié. Les algorithmes d'apprentissage automatique ont été analysés comme une alternative aux arbres de décision pour suivre l'impact potentiel de la description d'un système de satellites dissipatifs distribués quasi-homogènes. Enfin, des réseaux d'apprentissage profond à mémoire longue et à court terme ont été développés pour surveiller l'effet de la modélisation des scénarios possibles de cyberattaques

à impact intermédiaire et élevé [1]. Nouvelles technologies des TIC, tendances émergentes et implications judiciaires Les nouvelles technologies telles que l'Internet des objets (IoT), l'analyse des mégadonnées et l'IA offrent de nouvelles opportunités et de nouveaux défis en matière de cybercriminalité et d'inconduite financière. L'IoT offre de nouveaux mécanismes et outils de collecte, de partage et de gestion des données. Les défis nouveaux et émergents en matière de cybercriminalité ciblent les infrastructures critiques basées sur l'IoT, non seulement contre les groupes criminels graves, mais aussi contre les États-nations et les acteurs parrainés par l'État. Le protocole Internet v6 (IPv6) est une autre tendance émergente importante offrant de vastes implications pour les enquêtes médico-légales IoT [3]. Ces technologies et tendances créeront un nouveau paradigme de la criminalité financière. Comme tout est interconnecté, la convergence technologique sera militarisée et le retour sur investissement dans les crimes financiers augmentera, ce qui entraînera une plus grande sophistication des cybercrimes financiers.

6.2. Possibilités de recherche

Il est nécessaire d'effectuer des recherches sur les techniques d'enquête médico-légale préventive sur la criminalité financière. La détection et l'intervention précoces des crimes financiers auraient d'énormes avantages pour la société, mais sont généralement difficiles en raison de la déclaration tardive et de l'évolution constante des méthodologies des auteurs. Les choix d'actions influencent fortement les résultats, d'où la nécessité de modèles clairs et concis. Les modèles d'IA entraînés sur des tentatives d'enquête historiques pourraient éclairer des pistes pratiques à explorer, avec une opportunité centrale de minimiser le temps d'analyse des données exploratoires. Les modèles peuvent ne jamais trouver de chemins d'investigation parfaits, mais ils peuvent être suffisamment bons pour justifier une considération et une utilisation plus larges [1]. De plus, les réglementations et les attentes sociales en matière de convergence des capacités préventives incitent fortement la concurrence dans ce domaine entre les organisations publiques et privées. L'introduction de méthodes préventives améliorerait considérablement les capacités d'enquête médico-légale en matière de criminalité financière.

Avant d'appliquer ces méthodes à la criminalistique financière, les domaines de recherche pertinents sont identifiés comme des observables de système d'intérêt clé pour la modélisation des urgences de sûreté et de sécurité, des choix, des politiques, de la planification et des techniques de prédiction et de diagnostic

optimales. L'unité de modélisation de base des observables d'événements émergents de sûreté et de sécurité et des prédictions temporelles est décrite, qu'elle soit exogène, bonne, mauvaise ou neutre, nécessitant la prise en compte de l'état, des actions et des connaissances d'un système [3].

7. En conclusion

Le financement judiciaire est une discipline scientifique qui traite des crimes liés à l'économie. Il applique une analyse prédictive ex-ante basée sur les événements financiers qui se sont déjà produits. Une analyse rétrospective des données historiques est utilisée pour dériver un modèle à partir de l'estimation et de la projection de différents états économiques. Les fondements théoriques de ces modèles sont discutés, et les implications et les applications potentielles dans le financement judiciaire sont esquissées. Accompagnés du développement technologique et d'une disponibilité accrue des données de transaction, les outils d'analyse prédictive peuvent devenir un élément indispensable de la boîte à outils de l'enquêteur judiciaire et financier. Dans un contexte plus large, le potentiel de la physique appliquée et en particulier des approches de finance quantitative au-delà des applications actuellement standardisées peut être illustré par la finance forensique à titre d'étude de cas. La création d'un cadre disciplinaire complet de crimes financiers et d'outils d'analyse possibles démontre comment une technique perfectionnée dans un domaine peut être adaptée à des domaines intentionnellement et technologiquement similaires pour favoriser l'enquête et la responsabilité. Compte tenu de la prolifération mondiale continue des crimes et des fraudes financiers, cette adaptabilité entre les domaines est d'une importance cruciale.

7.1. Principales constatations et contributions

Cette étude visait à déterminer s'il est possible de développer des modèles d'analyse prédictive capables d'anticiper la criminalité financière dans les entreprises du marché grec en utilisant des techniques d'intelligence artificielle. Les crimes financiers ont été collectés pour atteindre cet objectif, et une série de modèles (forêt aléatoire, arbres de décision C5.0, réseaux neuronaux et machines à vecteurs de support) utilisant des ratios financiers comme variables indépendantes ont été développés. Les résultats ont montré qu'il est possible de détecter la criminalité financière avec un niveau de réussite raisonnable, ce qui souligne l'importance de l'adéquation des données utilisées pour la construction des modèles et de l'évaluation des résultats de chaque modèle à l'aide de plusieurs paramètres d'évaluation. Cette étude contribue à la littérature sur le financement

judiciaire et l'utilisation des techniques d'intelligence artificielle en a) fournissant un cadre théorique sur lequel de nouvelles applications peuvent être construites, b) fournissant une description détaillée des procédures requises pour collecter des données sur les crimes financiers, une tâche qui s'est avérée assez délicate, c) fournissant une application comparative de diverses techniques d'intelligence artificielle sur un ensemble de données nouvellement créé, et d) discuter des caractéristiques financières des entreprises avant la commission de crimes financiers, ce qui peut intéresser même un public non technique [3]. Cette étude devrait servir de point de départ à d'autres recherches sur l'analyse prédictive en finance légale et l'utilisation des techniques d'intelligence artificielle.

7.2. Implications pour l'industrie

Les implications de l'analyse prédictive utilisant l'intelligence artificielle dans le financement judiciaire sont cruciales pour les institutions financières, les organismes d'application de la loi et les régulateurs. En utilisant des outils d'analyse prédictive basés sur l'IA, ces organisations peuvent identifier les transactions potentiellement frauduleuses avant qu'elles ne se produisent, plutôt que de s'appuyer sur des méthodes traditionnelles qui analysent les données passées après coup. Cette recherche souligne l'importance des processus d'enquête proactifs dans le financement judiciaire et souligne le potentiel de la technologie de l'IA en tant que changeur de jeu dans ce domaine [3].

À l'heure actuelle, les institutions financières utilisent principalement la juricomptabilité post-analyse pour enquêter sur les crimes économiques. Bien que cette approche permette de découvrir des preuves d'actes répréhensibles et puisse entraîner des poursuites judiciaires, elle n'empêche pas que des événements similaires se reproduisent à l'avenir. De plus, de nombreuses fraudes ne sont pas détectées, et même les fraudes étudiées peuvent prendre des années à être résolues, ce qui entraîne des pertes financières importantes. Par conséquent, il est urgent de disposer de nouveaux outils capables d'examiner les données transactionnelles à l'avance et de fournir des suggestions sur l'orientation des ressources d'enquête pour atténuer le risque de criminalité financière.

Références:

[1] J. West, M. Bhattacharya et R. Islam, « Pratiques intelligentes de détection de la fraude financière : une enquête », 2015. [PDF] (en anglais)

[2] S. Rabiul Islam, W. Eberle et S. Khaled Ghafoor, « Credit Default Mining Using Combined Machine Learning and Heuristic Approach », 2018. [PDF] (en anglais)

[3] C. Chimonaki, S. Papadakis, K. Vergos et A. Shahgholian, « Identification de la fraude aux états financiers en Grèce à l'aide de techniques d'intelligence computationnelle », 1970. [PDF] (en anglais)

[4] T. DeLise, « Détection d'anomalies semi-supervisée approfondie pour la détection de fraude sur le marché à terme », 2023. [PDF] (en anglais)

[5] J. Danielsson et A. Uthemann, « Sur l'utilisation de l'intelligence artificielle dans la réglementation financière et l'impact sur la stabilité financière », 2023. [PDF] (en anglais)

[6] C. Liu, Y. Chan, S. Hasnain Alam Kazmi et H. Fu, « Modèle de détection de la fraude financière basé sur une forêt aléatoire », 2015. [PDF] (en anglais)

[7] J. West et M. Bhattacharya, « Mining Financial Statement Fraud : An Analysis of Some Experimental Issues », 2015. [PDF] (en anglais)

[8] S. Chen, « Détection des états financiers frauduleux à l'aide de l'approche hybride d'exploration de données », 2016. ncbi.nlm.nih.gov

[9] G. Starke, A. D'Imperio et M. Ienca, « Hors de leurs esprits ? « Externalist challenges for using AI in forensic psychiatry », 2023. ncbi.nlm.nih.gov

[10] Y. Zheng, Z. Wu, Y. Yuan, T. Chen et al., « PCAL : Un cadre intelligent de modélisation du risque de crédit préservant la confidentialité basé sur l'apprentissage contradictoire », 2020. [PDF] (en anglais)

[11] I. Perez, J. Wong, P. Skalski, S. Burrell et al., « Modèles d'intégration privés localement différentiellement dans les systèmes de prévention de la fraude distribués », 2024. [PDF] (en anglais)

[12] J. Pombal, A. F. Cruz, J. Bravo, P. Saleiro et al., « Comprendre l'injustice dans la détection des fraudes grâce aux interactions de biais de modèle et de données », 2022. [PDF] (en anglais)

[13] M. Lokanan, « Les déterminants de la fraude à l'investissement : une approche d'apprentissage automatique et d'intelligence artificielle », 2022. ncbi.nlm.nih.gov