L'intelligence artificielle dans la conformité et la surveillance

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Surveillance des transactions et criminalité financière

La conformité est l'un des domaines les plus prometteurs, mais aussi les plus délicats, pour l'intelligence artificielle. Les systèmes traditionnels de surveillance des transactions génèrent un grand nombre d'alertes, dont la plupart se révèlent infondées après examen manuel. Les modèles d'apprentissage automatique peuvent classer les alertes selon leur probabilité d'être fondées, détecter des schémas récurrents entre plusieurs comptes et analyser des informations non structurées telles que des articles de presse. La MAS (Monetary Authority of Singapore, l'autorité monétaire et de surveillance financière) a constaté que les banques utilisent couramment de tels modèles dans leurs systèmes de lutte contre le blanchiment d'argent et de détection de la fraude. Le danger réglementaire est symétrique. Un modèle qui supprime des alertes fondées expose la banque à des violations des règles de lutte contre le blanchiment d'argent examinées dans la partie H. Un modèle incapable d'expliquer son résultat est difficile à défendre devant une autorité de surveillance ou un tribunal. La MAS range le risque réglementaire parmi les principaux risques de l'intelligence artificielle et cite l'exemple des mauvaises performances d'un modèle utilisé pour soutenir la lutte contre le blanchiment.[1]

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Les données dont dépendent ces modèles ont, elles aussi, évolué. Depuis le 1er avril 2024, six grandes banques commerciales peuvent partager des informations sur les clients présentant plusieurs signaux d'alerte au moyen de COSMIC, une plateforme numérique que la MAS a lancée avec elles en vertu du Financial Services and Markets (Amendment) Act 2023. Elle se concentre dans un premier temps sur l'utilisation abusive de personnes morales, le détournement du financement du commerce international et le financement de la prolifération.[2] Une plateforme de ce type fournit des signaux structurés que les modèles analytiques peuvent exploiter. Son cadre juridique et sa portée pour la lutte contre le blanchiment d'argent sont examinés dans la partie H.

Modèles de tiers et concentration

La plupart des établissements achètent leurs modèles génératifs auprès d'un petit nombre de fournisseurs mondiaux. La MAS en a déduit trois risques : des biais inconnus issus des données de pré-entraînement, des préoccupations en matière de protection des données et un risque de concentration, lorsque de nombreux établissements dépendent des mêmes modèles sous-jacents. Les banques ont réagi par des tests compensatoires, des plans de continuité et des contrats révisés prévoyant des garanties de performance, la protection des données, des droits d'audit et une notification lorsqu'un fournisseur introduit l'intelligence artificielle dans un service existant.[3]

Les lignes directrices définitives tranchent la question de principe. Un établissement peut ne pas être en mesure d'imposer à un fournisseur tiers des pratiques rigoureuses de gestion des risques. Il demeure néanmoins responsable de la manière dont l'IA de tiers est utilisée au sein de son organisation et de ses effets possibles sur les clients et les autres parties prenantes.[4] Les règles relatives à l'externalisation et à la gestion des risques technologiques, examinées au chapitre E.I, s'appliquent en parallèle.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Incidents, surveillance et continuité

Les lignes directrices définissent les incidents d'IA comme des incidents impliquant une défaillance, un dysfonctionnement ou des performances insuffisantes du système ou du modèle sous-jacent. La MAS a renoncé à instaurer pour eux un régime de déclaration distinct. Les établissements doivent continuer à déclarer les incidents selon les exigences existantes en matière de risques technologiques et de continuité d'activité, quelle qu'en soit la cause profonde. Des plans de continuité sont exigés pour les cas d'usage présentant une importance de risque élevée. Les modèles qui se mettent à jour automatiquement, comme les systèmes d'apprentissage par renforcement, appellent une surveillance plus stricte, car leur comportement peut évoluer en cours de fonctionnement sans intervention humaine.[5]

Pour les systèmes agentiques, la surveillance doit s'étendre aux flux d'informations et aux chemins de décision au sein des processus, y compris les raisonnements, les actions accomplies et les outils utilisés. Une telle surveillance permet à un établissement de reconstituer chaque action le long de chaînes d'agents et de localiser l'origine d'une défaillance. La MAS a également suggéré que l'étendue de l'accès aux outils et aux systèmes puisse servir de critère supplémentaire pour apprécier l'importance du risque, car des agents dotés de larges autorisations peuvent aggraver le risque de compromission des données.[6]

L'utilisation des données par l'autorité de surveillance elle-même

La MAS applique l'analyse de données à ses propres travaux depuis la création du poste de Chief Data Officer, qu'occupait David Hardoon lors de la publication des FEAT Principles. Les superviseurs utilisent des outils analytiques pour traiter les déclarations réglementaires, pour trier les déclarations de transactions suspectes et pour détecter des schémas d'abus de marché.[7] Ces outils ne modifient pas la relation de surveillance elle-même. Ils aident l'autorité à sélectionner les établissements et les transactions qui méritent son attention, tandis que l'appréciation reste un jugement humain exercé dans le cadre des lois décrites au chapitre E.I.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Notes

1. MAS, Information Paper, décembre 2024, para. 2.1 : les modèles de ML fondés sur des arbres de décision sont « commonly used in anti-money laundering (AML) systems to detect suspicious transactions, and in fraud detection systems » – MAS, Information Paper, décembre 2024, para. 2.2 : « Regulatory risks, e.g., poor performance of AI used to support AML efforts could lead to non-compliance with regulations. » ↩
2. MAS, « COSMIC » (mas.gov.sg, consulté en novembre 2026) : lancée le 1er avril 2024 ; participants DBS, OCBC, UOB, SCB, Citibank et HSBC ; base légale dans le Financial Services and Markets (Amendment) Act 2023 et les Financial Services and Markets (Information Sharing Scheme for Prescribed Financial Institutions) Regulations 2024 ; trois domaines de risque. ↩
3. MAS, Information Paper, décembre 2024, para. 7.2.1 : les risques liés à l'IA de tiers comprennent « unknown biases from pre-training data, data protection concerns, as well as concentration risks due to increased interdependencies » – MAS, Information Paper, décembre 2024, para. 7.2.2(a)–(d) : tests compensatoires, plans de continuité, accords juridiques comportant des clauses sur « performance guarantees, data protection, the right to audit, and notification when AI is introduced », et actions de sensibilisation. ↩
4. MAS, Response to Feedback, 7 octobre 2026, paras. 9.3–9.4 : l'établissement « remains accountable for how third-party AI is used within its organisation » ; « the onus is on the FI to ensure that risks arising from its use of third-party AI are appropriately managed ». ↩
5. MAS, Response to Feedback, 7 octobre 2026, para. 10.69 : définition des « AI incidents » ; « MAS does not intend to introduce AI-specific incident reporting requirements at this juncture » – MAS, Response to Feedback, 7 octobre 2026, paras. 10.67 et 10.70. ↩
6. MAS, Response to Feedback, 7 octobre 2026, para. 12.8 – MAS, Response to Feedback, 7 octobre 2026, para. 7.7 : un établissement peut considérer « the

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

extent of access to tools and systems granted as an additional dimension for AI risk materiality assessments of agentic AI ». ↩

7. Sur l'utilisation par la MAS de l'analyse de données et de l'apprentissage automatique dans la surveillance et dans l'analyse des déclarations de transactions suspectes, voir les rapports annuels de la MAS à partir de 2018/19 ainsi que les discours de responsables de la MAS sur les technologies de surveillance. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com