

Intelligence artificielle et fraude ou le poison et l'antidote

Les technologies d'intelligence artificielle générative, et en particulier les grands modèles de langage (LLM), ont bouleversé la lutte contre la fraude. D'un côté, elles permettent de renforcer la prévention et la détection grâce à des capacités inédites d'analyse, de génération de données synthétiques et de détection d'anomalies comportementales. D'un autre côté, elles offrent aux fraudeurs des outils puissants pour élaborer des attaques plus crédibles et plus difficiles à détecter.

■ IA générative : accélérateur de fraude

Les fraudeurs utilisent l'IA générative pour déjouer les dispositifs de sécurité traditionnels (notamment en générant de fausses identités ou en imitant des comportements utilisateurs crédibles) et rendre leurs attaques plus convaincantes :

- **Phishing avancé**

L'IA permet de générer des emails et messages parfaitement rédigés, personnalisés et crédibles, rendant les attaques de phishing beaucoup plus difficiles à détecter.

- **Deepfakes et usurpation d'identité**

Le clonage vocal et la manipulation vidéo facilitent des attaques d'ingénierie sociale sophistiquées, où l'identité de personnes de confiance est usurpée pour tromper les collaborateurs, tiers, ...

- **Fraude automatisée à grande échelle**

Les outils IA permettent aux fraudeurs d'orchestrer des attaques simultanées sur de nombreuses cibles, augmentant ainsi le taux de succès potentiel et la rapidité d'exécution.

L'IA rend la fraude plus rapide, mieux réalisé mais les scénarios restent les mêmes (fraude au faux virements, fraude au président, ...)

■ L'IA au service de la lutte contre la fraude

Les équipes de sécurité exploitent aussi l'IA générative pour renforcer la prévention, la détection et le traitement de la fraude.

- **Meilleure détection d'anomalies**

Les modèles génératifs établissent des profils de comportement normal, ce qui facilite l'identification des écarts susceptibles d'indiquer une fraude.

- **Génération de données synthétiques**

L'IA peut créer des ensembles de données réalistes pour entraîner les modèles de détection de fraude, notamment pour les cas rares.

- **Analyse assistée par IA**

Les assistants IA aident les analystes fraude à traiter de grands volumes de données et à repérer les schémas pertinents plus rapidement.

- **Systèmes de défense adaptatifs**

L'IA permet aux systèmes de sécurité d'apprendre et d'évoluer en continu, pour anticiper les nouvelles tactiques de fraude

Quelques exemples de solutions utilisant l'IA :

- Détection de faux documents, score de confiance tiers, anticipation des problèmes de solvabilité (Meelo)
- Détection de fraude basée sur l'analyse comportementale des historiques de paiements (Datalog Finance)
- Continuité des processus financiers (Astran)

■ Les limites des outils et les facteurs humains

Les outils sont très utiles, mais ils ne font pas tout loin de là. Qu'est qui va faire qu'une fraude va rester au stade de tentative ?

La réponse tient en 2 points :

• **Vigilance individuelle**

La technologie ne suffit pas. La vigilance, l'esprit critique et la capacité à poser des questions en cas de doute restent essentiels pour empêcher la fraude de passer du stade de tentative à celui de fraude avérée

• **Un contrôle interne fort**

- ✓ Ségrégation des tâches : plus il y a d'intervenants dans un processus, plus la fraude est compliquée.
- ✓ Des procédures auxquelles on pourra se référer, notamment pour les opérations exceptionnelles
- ✓ Des contrôles périodiques sur la correcte application des procédures métiers et sécurité

■ Bonnes pratiques et recommandations

• **Collaboration**

La coopération entre banques, entreprises est le vrai pare-feu contre la fraude.

• **Approche hybride**

Combiner les contrôles traditionnels (procédures, audits, supervision humaine) et les solutions IA pour une stratégie robuste et adaptative.

• **Formation continue**

Sensibiliser et former régulièrement les équipes aux nouveaux risques et aux bonnes pratiques.

Pour en savoir plus sur la formation en lien avec cette thématique, flashez le QRCode



MODÉRATEURS



Isabelle CATUSSE
présidente de la commission AFTE
« lutte contre la fraude financière »



Sylvie SOUNDARAVELOU
TotalEnergies

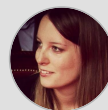
INTERVENANTS



Philippe GOMES
Meelo



Benoît MERQUIOL
TotalEnergies



Mathilde PLACEND
Natixis CIB