baw businessatwork | Part of Mantu

FRAUDE PUBLIQUE EN RÉSEAU

De la donnée isolée à la détection de communautés de fraudeurs en 3 étapes

1 LA DONNÉE ISOLÉE
avant l'approche graph

Vision dossier par dossier → taux de détection limité

- Données en silos : RIB, adresses, IP, flux financiers non croisés
- Vision fragmentée et cloisonnée
- Taux de détection limité

RÉSULTAT : fraudes en réseau organisé non détectées

2 LA MODÉLISATION GRAPH
la transformation

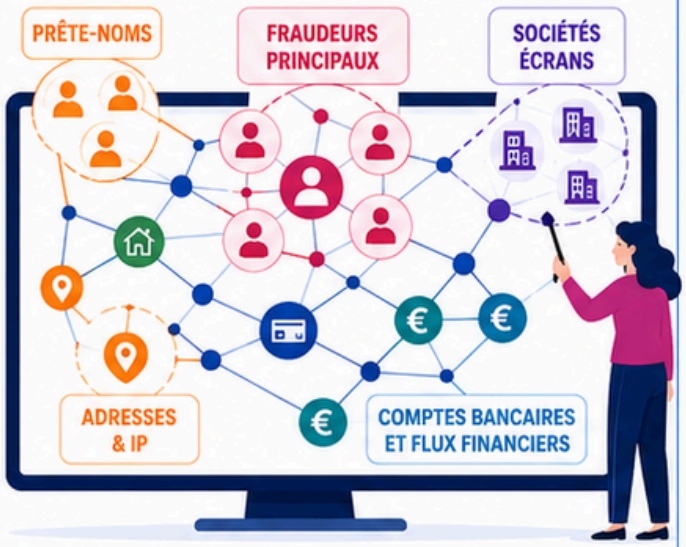
On relie les données, on révèle les liens cachés

- **Résolution d'entités** : création des liens entre personnes, foyers, entreprises, comptes
- **Algorithmes de communautés** : détection automatique de groupes de fraudeurs
- **Métriques de centralité** : priorisation des dossiers à fort enjeu
- **Pseudonymisation des données** : conformité RGPD & CNIL

RGPD CNIL

3 LA DÉTECTION EN RÉSEAU
après l'approche graph

Vision réseau : fraudeurs, prête-noms, sociétés écrans identifiés



- **Listes de contrôle hiérarchisées** : brigades de vérification focalisées sur les cas à fort enjeu
- **Décisions justifiables** : chaîne de décision traçable de la donnée brute à la sanction
- **Extension automatique du périmètre** : marquage "à risque" des entités connexes

VOIR LA DÉMONSTRATION NEO4J EN CONTEXTE FRAUDE PUBLIQUE →

PLANIFIER UN ÉCHANGE AVEC UN EXPERT BAW