NEOLI

Lutte contre la fraude à l'assurance : état des lieux, impact de l'IA & solutions innovantes

Edition 2026

Introduction

La fraude à l'assurance est un phénomène ancien et répandu, qui affecte l'ensemble des branches d'assurances (dommages, épargne, santé). Elle se manifeste par des actes intentionnels visant à **obtenir indûment un bénéfice d'un contrat d'assurance,** par exemple en simulant un sinistre, en falsifiant des documents ou en mentant sur les circonstances pour toucher une indemnisation injustifiée. Si elle est difficile à quantifier précisément, les experts estiment que la fraude représente une part significative du coût des sinistres pour les assureurs. En Europe, ce coût est évalué à environ **10 % du montant total des sinistres** réglés. Il est supérieur dans certaines branches ou pays moins contrôlés. En France, l'Agence de Lutte contre la Fraude à l'Assurance (ALFA) indique que les enjeux financiers liés à la fraude peuvent aller **jusqu'à 20 % du coût des sinistres** dans certains portefeuilles[1].

Au-delà des coûts engendrés, la fraude à l'assurance soulève des **enjeux multiples** : augmentation des primes pour les assurés honnêtes, érosion de la confiance dans le système assurantiel et même risques d'entraînement d'autres fraudeurs si le phénomène se banalise. Face à ces défis, le secteur de l'assurance intensifie la lutte antifraude. Depuis quelques années, les avancées en **intelligence artificielle (IA)** offrent de nouvelles armes pour détecter plus efficacement les tentatives de fraude, mais posent aussi de nouveaux défis techniques, juridiques et éthiques. Les fraudeurs eux-mêmes s'emparent de ces technologies (génération de faux documents par IA, deepfakes, etc.) dans une véritable course technologique.

Dans ce dossier, nous proposons un **état des lieux** de la fraude à l'assurance et les **perspectives** offertes par l'intelligence artificielle pour la combattre. Après avoir défini le phénomène et son contexte (partie I), nous verrons comment l'IA transforme les méthodes de détection et de gestion de la fraude (II), puis nous passerons en revue quelques **solutions du marché** et exemples d'outils disponibles (III). La partie IV sera dédiée à des **retours d'expérience** concrets d'assureurs, et enfin nous aborderons les **limites, enjeux éthiques et perspectives** autour de l'IA antifraude (V). Chaque section se conclut par un encadré « À retenir » résumant les points clés.

L'objectif est de fournir aux acteurs du secteur un panorama clair et documenté des enjeux actuels et à venir, en démontrant l'expertise disponible pour les accompagner dans ces transformations.

Bonne lecture.

[1] Rapport annuel ALFA 2024

Sommaire

I.

Contexte : comprendre les enjeux de la fraude en assurance

- 01.Définition et typologies des fraudes
- 02. Données chiffrées et tendances
- 03. Conséquences pour les assureurs, les assurés et la société

01. Définition et typologie des fraudes

Définition

En l'absence de définition légale stricte, les professionnels s'accordent pour définir la fraude à l'assurance comme « un acte intentionnel, réalisé par une personne morale ou physique, afin d'obtenir indûment un profit du contrat d'assurance ».

Autrement dit, le fraudeur cherche à tirer un avantage illégitime d'une police d'assurance, en contradiction avec le principe de l'aléa et de la bonne foi.

Les tendances

Il existe **plusieurs formes de fraudes** : d'une part selon **le moment où elles interviennent**, et d'autre part selon **leur degré de sophistication ou d'organisation**.

- **Fraude à la souscription** : elle a lieu **lors de la déclaration du risque**, c'est-à-dire à la souscription du contrat. L'assuré fournit sciemment de fausses informations ou omet des éléments importants dans le questionnaire (sur son état de santé, l'usage d'un véhicule, la valeur des biens, etc.) afin de payer une prime plus basse ou d'obtenir une couverture qu'il n'aurait pas eue honnêtement. Par exemple, mentir sur l'adresse de parking d'une voiture pour réduire la prime, ou souscrire l'assurance alors que le sinistre est déjà survenu. La sanction en cas de fausse déclaration intentionnelle à la souscription est la **nullité du contrat**[2], avec obligation pour le souscripteur de rembourser les indemnités éventuellement perçues et pour l'assureur de conserver les cotisations payées.

- **Fraude à l'indemnisation (au sinistre)** : elle intervient **lors d'un sinistre**. L'assuré va profiter de la réalisation (ou de la prétendue réalisation) d'un dommage pour tromper l'assureur sur la réalité des faits, afin d'être indemnisé indûment. Cela prend la forme de **fausses déclarations** (inventer un sinistre, falsifier les circonstances ou la date), de **sinistres provoqués intentionnellement** (par ex. incendie volontaire d'un bien, simulation d'un vol), ou encore de **surévaluation des pertes** par ajout de dommages antérieurs ou inexistants. Dans ces cas, si l'intention frauduleuse est prouvée, l'assureur refusera la prise en charge en invoquant la clause de déchéance pour fausse déclaration[3] et pourra réclamer le remboursement des sommes indûment versées. La fraude au sinistre est la plus courante dans les portefeuilles dommages, car l'occasion du sinistre réel fournit un prétexte facile à l'exagération, c'est la **fraude opportuniste** typique.

[2]Article L113-8 du Code des assurances
[3]Article L113-1 du Code des Assurances

01. Définition et typologie des fraudes

- **Fraude opportuniste vs fraude organisée** : en effet, on classe souvent les fraudes selon qu'elles sont **isolées et opportunistes** ou **structurées et organisées**. La **fraude opportuniste** est le fait d'un assuré lambda qui, sans préméditation de longue date, **profite d'une occasion** pour tirer un gain indu. Par exemple, après un accident automobile mineur, faire passer d'anciennes rayures pour des dégâts du sinistre afin de se les faire rembourser, ou gonfler le montant d'une facture de réparation. Ce type de fraude est fréquent et diffus, souvent difficile à détecter car le dossier paraît légitime à la base. À l'inverse, la **fraude préméditée/organisée** implique une **planification en amont** et souvent la collusion de plusieurs individus (on parle de **réseaux**). Il peut s'agir de véritables **bandes organisées** qui montent de faux sinistres de toutes pièces (par ex. accidents de voiture « mis en scène » avec complicités, réseaux de vol de véhicules ensuite maquillés en sinistres). Ces réseaux peuvent inclure des **complices internes ou professionnels** (ex. garagistes malveillants, médecins complaisants, faux témoins, voire employés corrompus) afin de donner du réalisme à la fraude. La fraude organisée, plus rare en nombre, cause en revanche des préjudices financiers très lourds et nécessite des investigations approfondies.

- **Fraude interne ou externe** : la fraude **interne** implique un salarié de l'assureur ou un intermédiaire complice, par exemple un agent qui détournerait des fonds ou validerait de fausses factures. La fraude **externe** est commise par des assurés ou tiers sans complicité interne.

Sanctions encourues

Au civil :

Sur le plan **civil**[4], comme mentionné précédemment, la fausse déclaration intentionnelle à la souscription entraîne la nullité du contrat et la perte de tout droit à garantie. En cas de fraude lors d'un sinistre, l'assureur est délié de toute obligation d'indemnisation pour ce sinistre et peut réclamer les indemnités payées indûment. Les contrats prévoient généralement la déchéance de garantie pour toute tentative de fraude avérée.

[4]Articles 1131 et 1127 du Code civil et L113, L121 et L324 du Code des assurances

01. Définition et typologie des fraudes

Au pénal :

Sur le plan **pénal**, il n'existe pas d'infraction spécifique « fraude à l'assurance », mais les faits relèvent le plus souvent de l'**escroquerie**[5]. Ainsi, obtenir le versement d'une somme indue par des manœuvres frauduleuses est puni de **5 ans d'emprisonnement et 375 000 € d'amende**. Le **faux et usage de faux** (par ex. fournir une fausse facture, un faux constat) constituent également un délit pénal pouvant être retenu. En pratique cependant, beaucoup de fraudes à l'assurance sont traitées à l'amiable (refus d'indemnisation, radiation du contrat) et seuls les cas graves aboutissent à des poursuites pénales.

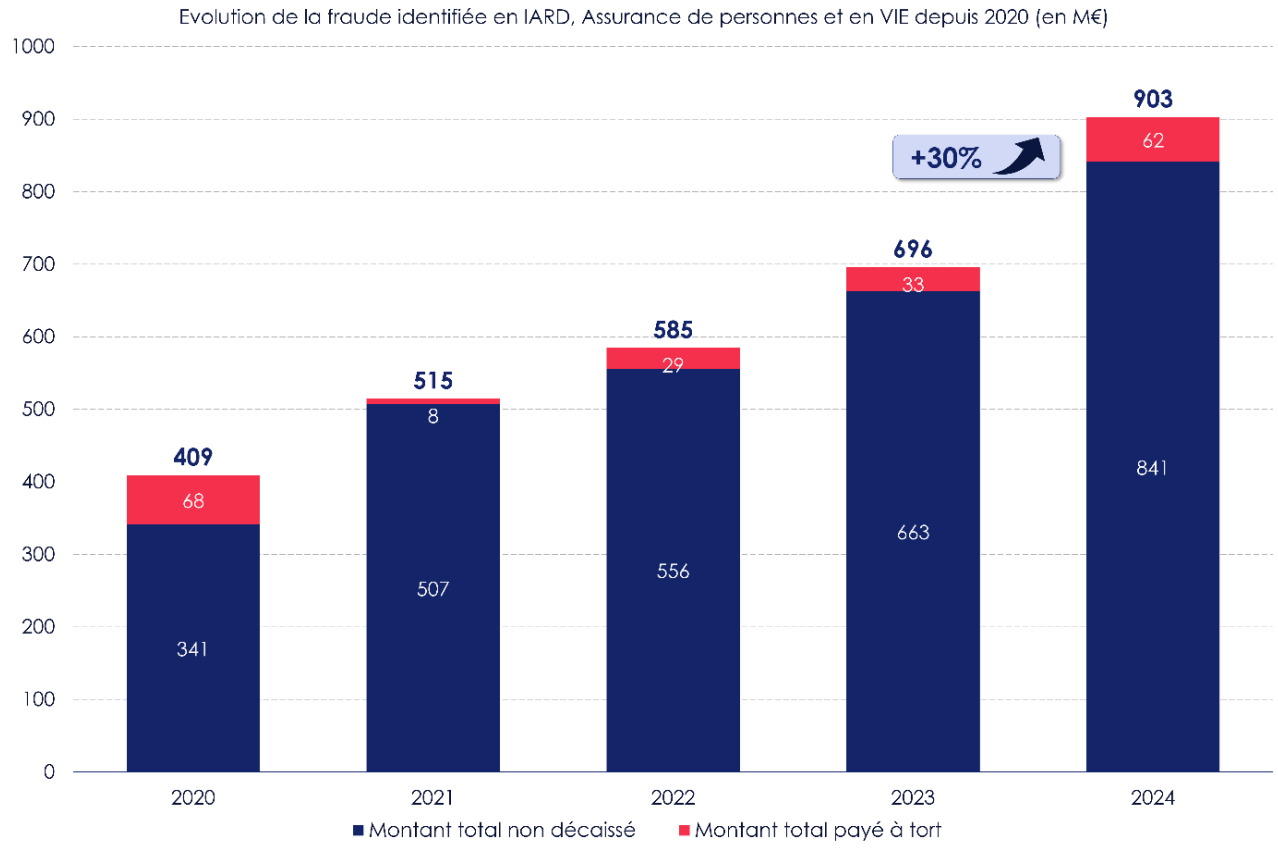
Ce qu'il faut retenir

→ La fraude à l'assurance est un acte intentionnel pour tirer un profit illégitime d'un contrat. Elle peut survenir **à la souscription** (fausse déclaration initiale) ou **à l'indemnisation** d'un sinistre (fausse déclaration, sinistre provoqué, exagération des dommages). On distingue la **fraude opportuniste**, isolée et liée à une occasion (ex. gonfler un sinistre réel), de la **fraude organisée**, préméditée en réseau (ex. faux accidents montés de toutes pièces). Toutes les branches sont concernées. Les fraudeurs risquent la nullité de leur contrat, la perte des indemnités, et potentiellement des **sanctions pénales** (escroquerie punie de 5 ans de prison). Les assureurs ont développé un arsenal de contrôle pour traquer ces pratiques.

[5]Article 313-1 du Code pénal

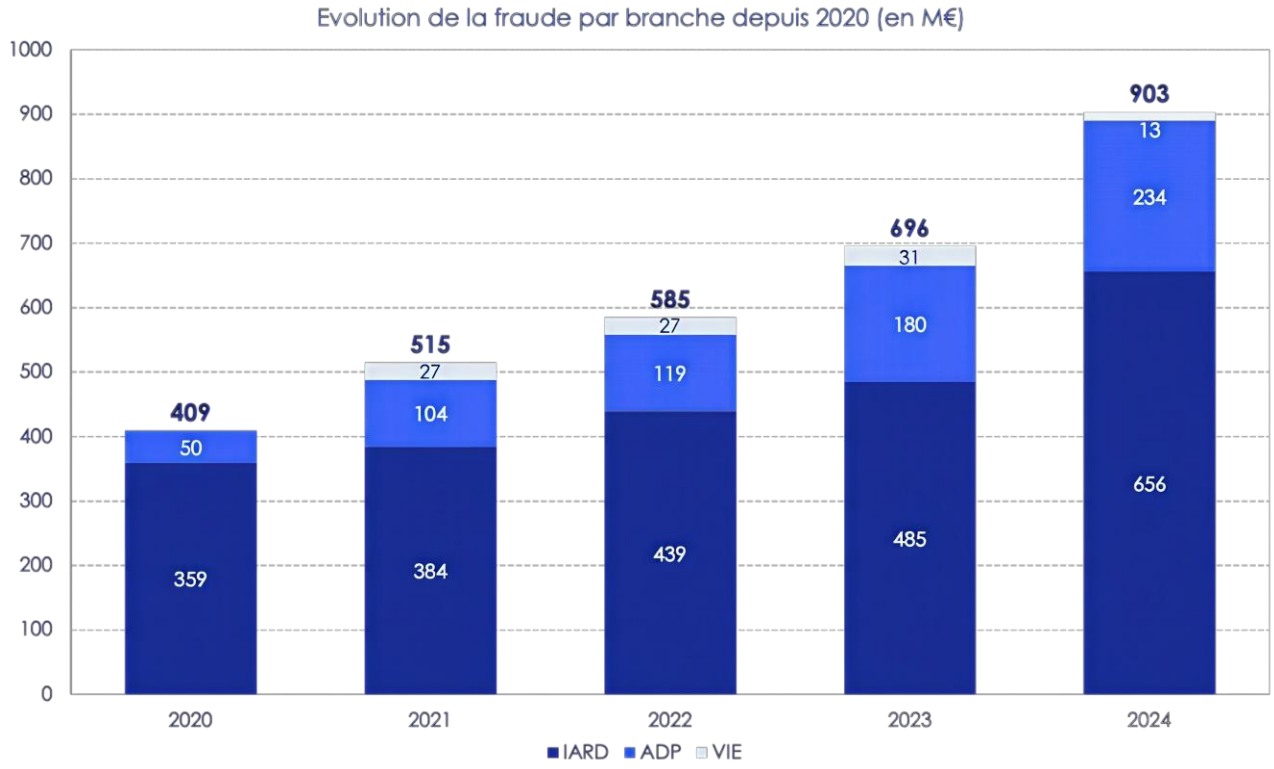
02. Données chiffrées et tendances

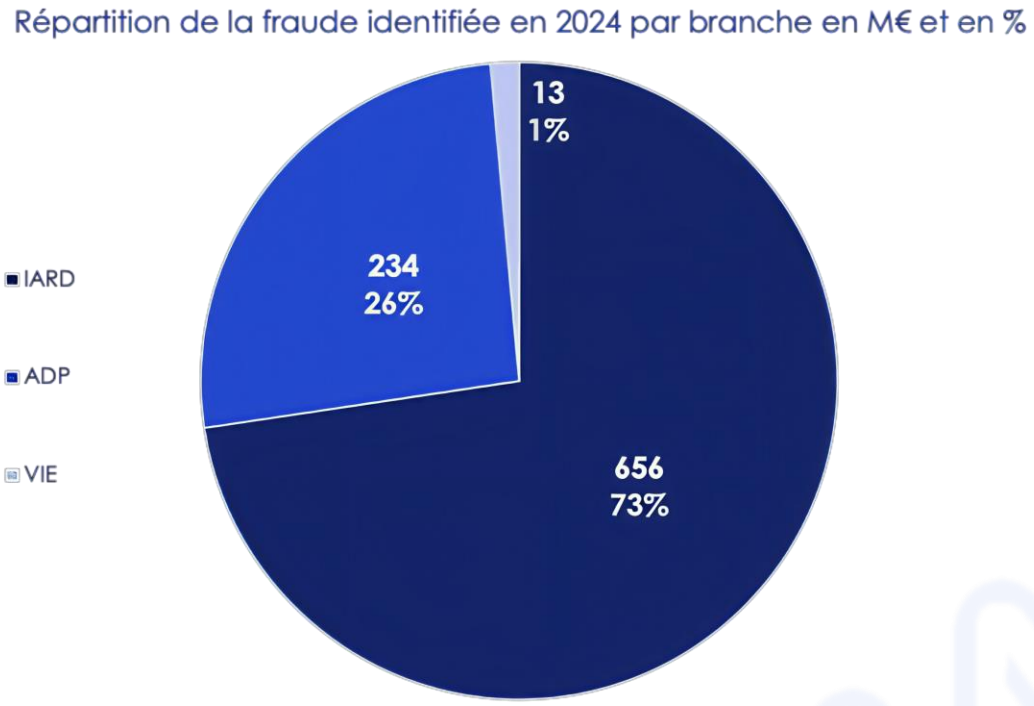
La fraude représente un enjeu financier majeur pour le secteur assurantiel. En **France**, les compagnies d'assurance détectent chaque année des centaines de millions d'euros de fraudes. Selon le dernier rapport de l'ALFA, le montant total des fraudes **identifiées** par les assureurs français en 2024 a atteint **903 millions d'euros**, en hausse de +30 % par rapport à 2023. Ce chiffre est en progression constante : il était d'environ 696 millions d'euros en 2023 et a plus que doublé depuis 2020, une évolution notable que certains associent en partie aux effets post-Covid et à la digitalisation accrue des échanges.



02. Données chiffrées et tendances

Sur ces 903 M€ de fraudes détectées en 2024, la branche des **assurances de dommages (IARD)** concentre la majeure partie avec **656 M€** (environ 2/3 du total). Les **assurances de personnes** représentent **234 M€**, et les assurances sur la **vie** environ **13 M€**[6].





[6]Rapport annuel ALFA 2024

02. Données chiffrées et tendances

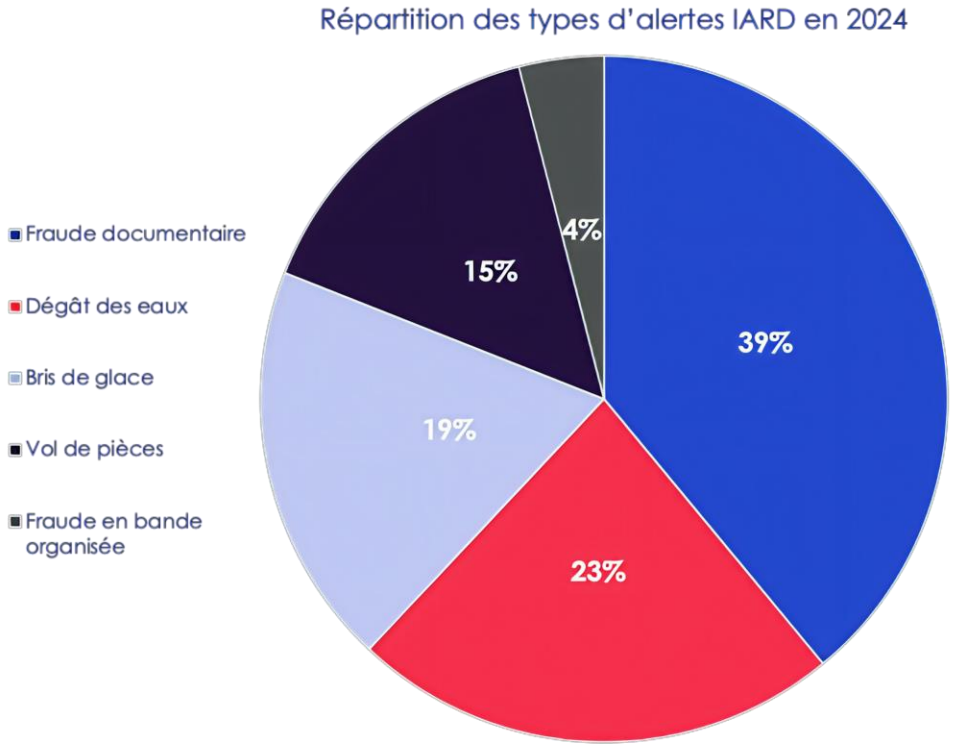
Ces montants correspondent aux fraudes *identifiées et stoppées* par les assureurs (sinistres non versés ou récupérés). Ils demeurent inférieurs à la fraude réelle, qui inclut une part non détectée.

2.5 Mds €

Ce que la fraude coûte aux assureurs en France

D'après France Assureurs, la fraude à l'assurance *coûterait* en réalité plus de **2,5 milliards d'euros par an en France** (estimation 2024), soit environ quatre fois le montant de la fraude effectivement prouvée. Ce manque à gagner considérable équivaut à plusieurs points de ratio combiné pour les assureurs, et justifie les efforts accrus en matière de détection. Le nombre de dossiers suspects signalés augmente chaque année, porté notamment par l'amélioration des outils de détection. Par exemple, dans le secteur de l'**automobile,** qui est historiquement l'un des plus sujets à fraude, on a constaté en 2024 une forte hausse du nombre de sinistres frauduleux avérés, couplée à une baisse du montant moyen de la fraude : signe que davantage de petites fraudes sont détectées en amont. L'automobile représente à elle seule plus de 50 % des cas de fraudes détectées en IARD.

Une **infographie** de l'ALFA (voir ci-dessous) montre la prépondérance des faux documents et des tentatives de **fraude sur le périmètre** IARD.



02. Données chiffrées et tendances

Du point de vue des **tendances récentes**, plusieurs phénomènes sont à signaler :

- **Professionnalisation et industrialisation de la fraude** : les fraudeurs opportunistes demeurent nombreux, mais on observe une montée de fraudes plus organisées et **sophistiquées**. Le directeur général d'ALFA souligne *« l'essor de la fraude documentaire et la professionnalisation des fraudeurs sur les réseaux sociaux »*. Des groupes criminels proposent désormais des « kits » prêts à l'emploi vendus en ligne (par ex. pour simuler un bris de glace ou monter un faux sinistre clé en main). Sur les réseaux sociaux, on voit fleurir des annonces pour fournir de fausses factures ou recruter des comparses. Cette **industrialisation via le digital** rend la fraude plus accessible et plus difficile à tracer, d'où la nécessité pour les assureurs de coopérer et d'investir dans des moyens technologiques équivalents.

- **Impact de la crise Covid et du contexte économique** : après un creux en 2020 (les confinements ayant réduit l'exposition aux sinistres, et donc les fraudes opportunistes), la fraude est repartie nettement à la hausse. La période post-Covid, marquée par des tensions économiques (inflation, baisse du pouvoir d'achat), a pu inciter davantage de personnes en difficulté à *« tenter le coup »* pour obtenir indûment de l'argent de l'assureur. Une enquête a montré que **68 %** des sondés estiment que les fraudeurs pensent pouvoir s'en tirer, notamment s'ils ont des besoins financiers ponctuels ou estiment payer des primes trop chères. La tentation de frauder augmente donc en période de crise. Par ailleurs, la **digitalisation des processus** (souscription en ligne, déclaration de sinistre par appli, etc.) peut ouvrir de nouvelles brèches à exploiter pour les fraudeurs. En 2024, les assureurs constatent ainsi une hausse des fraudes liées aux comptes en ligne : des fraudeurs parviennent à pirater ou usurper les identités numériques de clients pour détourner des indemnités ou souscrire des contrats à des fins frauduleuses.

- **Fraude documentaire et faux documents** : l'avènement d'outils numériques a aussi fait exploser la **fraude aux documents**. En France, on estime que la fraude documentaire (faux RIB, fausses factures, faux certificats) a doublé en 2021. Désormais, avec des logiciels courants et même des IA génératives, il est très facile de fabriquer de toutes pièces un document d'apparence authentique.

Par exemple, un faux relevé d'identité bancaire pour détourner un remboursement, ou de fausses factures de réparation à joindre à un dossier de sinistre. ALFA relève que dans les alertes qu'elle reçoit en assurance dommages, **73 % des cas impliquent des faux documents** à un stade ou un autre.

73 %
des alertes impliquent de faux documents

Cette tendance oblige les assureurs à renforcer les contrôles documentaires (via des outils spécialisés dont on parlera en partie II et III).

02. Données chiffrées et tendances

En résumé, la fraude à l'assurance est à la fois un **phénomène persistant et en mutation**. Le **coût direct** pour les assureurs se chiffre en centaines de millions d'euros par an rien qu'en France (et plusieurs milliards en coût indirect), avec une nette croissance ces dernières années. Cette progression s'explique en partie par une **meilleure détection** (effet positif des investissements antifraude) mais aussi par une réelle **augmentation des tentatives** dans un contexte de digitalisation et de tensions économiques. La fraude tend à se **professionnaliser**, utilisant des méthodes toujours plus élaborées. Face à cela, la filière assurance intensifie la lutte, notamment via des **approches basées sur les données et l'intelligence artificielle** que nous détaillerons plus loin.

Ce qu'il faut retenir

→ En France, près de **900 M€** de fraudes ont été détectées par les assureurs en 2024, mais le **coût réel** de la fraude est estimé autour de **2 à 3 milliards d'euros par an**. La branche IARD concentre le plus gros des fraudes (automobile en tête). Le nombre de cas détectés est en forte hausse grâce à de meilleurs outils, mais aussi parce que la **fraude explose** après la crise Covid (+100 % depuis 2020). Les fraudeurs profitent de la digitalisation (faux documents faciles à produire, usurpations d'identités en ligne) et se professionnalisent (réseaux organisés sur les réseaux sociaux, vente de kits de fraude). La **fraude documentaire** représente désormais la majorité des tentatives repérées. Ces tendances obligent les assureurs à innover pour contrer un phénomène en pleine mutation.

03. Conséquences pour les assureurs, les assurés et la société

La fraude à l'assurance a des conséquences multiples et néfastes qui s'étendent bien au-delà du simple montant financier détourné. Elle affecte à la fois les **compagnies d'assurance**, l'ensemble des **assurés** (clients) et plus généralement la **société** en alimentant un cercle vicieux de méfiance.

- **Impact économique pour les assureurs** : chaque euro indûment versé à un fraudeur est une charge supplémentaire dans le ratio de sinistralité de l'assureur et pèse sur sa rentabilité. En outre, la lutte contre la fraude engendre des coûts opérationnels (services d'enquête interne, outils spécialisés, actions en justice). Selon une étude de LexisNexis, en France chaque euro de fraude peut coûter **3,64 € aux compagnies** si l'on intègre les coûts de détection et de gestion associés. Au-delà du préjudice financier direct, la **viabilité de certains produits** peut être remise en question en cas de fraude massive. Par exemple, si une niche d'assurance (comme l'assurance construction obligatoire) devient une cible privilégiée de fraudeurs, l'assureur peut se retirer du marché ou augmenter drastiquement ses tarifs, compromettant l'assurabilité. Dans certains pays ou segments (ex. complémentaire santé dans des zones à forte fraude), la situation devient peu attractive pour les assureurs. Enfin, la fraude consomme du temps et des ressources qui pourraient être dédiés à un meilleur service client ou à l'indemnisation des vrais sinistres.

- **Répercussion sur les assurés honnêtes** : l'assurance fonctionne sur le principe de la mutualisation des risques, les primes de la communauté payent pour les sinistres de quelques-uns. La fraude vient fausser ce principe en introduisant des *coûts artificiels*. En conséquence, les assureurs compensent les pertes liées aux fraudes en augmentant progressivement les **primes d'assurance** pour l'ensemble de leur portefeuille.

  + 50 € / contrat

  Le surcoût minimum qu'induit la fraude aux assurés français

  Autrement dit, ce sont les assurés honnêtes qui *« paient la facture »*. À titre d'exemple, en Grande-Bretagne la fraude représente 2,5 milliards USD par an, ce qui induit un surcoût d'environ 50 £ par contrat et par an pour les assurés britanniques. En France, le même calcul avoisinerait 50 à 100 € par an, par assuré si l'on rapporte les 2,5 Mds € de fraude au nombre de contrats. **L'image de l'assurance** en pâtit également : la prolifération des fraudes entretient un **climat de défiance**. Cela peut démotiver les « assureurs honnêtes » à respecter strictement les règles. C'est le risque d'**effet domino** ou de banalisation.

03. Conséquences pour les assureurs, les assurés et la société

- **Atteinte au lien de confiance et au contrat social** : la **confiance** est une pierre angulaire du secteur assurantiel ; on paye une prime en confiance que l'assureur tiendra sa promesse en cas de sinistre. La fraude mine cette confiance de plusieurs façons. D'une part, les assureurs tendent à multiplier les contrôles et la suspicion pour se protéger, ce qui peut alourdir les démarches pour tous les clients et dégrader l'expérience (par exemple, devoir justifier de tout, subir des enquêtes, etc.). D'autre part, les assurés peuvent perdre confiance en l'équité du système en prenant conscience qu'ils payent pour les fraudeurs. Ce cynisme peut conduire à une **tolérance accrue** vis-à-vis de la fraude voire à une augmentation des fraudes opportunistes. Ainsi, la fraude détruit la mutualisation solidaire et remplace la confiance par la méfiance.

Enfin, on peut souligner que la fraude, surtout lorsqu'elle est liée à des réseaux criminels, peut alimenter des **circuits de blanchiment d'argent** ou de financement d'activités illégales plus larges. C'est pourquoi les organismes comme TRACFIN intègrent le secteur assurance dans leur périmètre de vigilance anti-blanchiment. La fraude à l'assurance ne constitue pas un délit sans victimes : **tout le monde y perd**, soit financièrement, soit en qualité de service, soit en confiance dans l'écosystème. En réaction, la lutte contre la fraude est devenue un **enjeu stratégique majeur** pour les assureurs. Non seulement elle permet de préserver le ratio technique (chaque euro de fraude évité améliore le ratio combiné, avec un potentiel gain de 1 à 3 % des indemnisations), mais elle contribue à maintenir une tarification juste pour les clients et à sauvegarder la réputation du secteur. *« Lutter contre ce fléau permet de préserver les assurés intègres, d'abaisser le montant moyen des sinistres et de renforcer la rentabilité »*, résume un article spécialisé. De plus, une politique antifraude visible a un **effet dissuasif** : savoir que l'assureur est vigilant peut décourager certains candidats à la fraude.

Ce qu'il faut retenir

→ La fraude détériore l'équilibre du système assurantiel. **Pour les assureurs**, ce sont des pertes financières directes et des coûts de contrôle accrus, qui remettent en cause la rentabilité de certains produits. **Pour les assurés**, la fraude se traduit par des **primes plus élevées** (5 à 10 % de la prime sert à compenser la fraude), et une expérience client dégradée (contrôles renforcés, suspicion généralisée). Au niveau **sociétal**, la fraude mine la **confiance** mutuelle pourtant au cœur de l'assurance et peut encourager une banalisation du mensonge (effet d'entraînement). Elle profite souvent à des réseaux criminels organisés, ce qui en fait l'affaire de tous de la combattre. En somme, **tout assuré honnête paie pour la fraude**, d'où l'importance d'une lutte antifraude efficace pour rétablir l'équité et la confiance.

II.

Comment l'IA transforme la lutte contre la fraude

01. L'IA au service de la détection

L'intelligence artificielle (IA) est en train de **refaçonner les pratiques de détection et de prévention** de la fraude dans le secteur de l'assurance. Traditionnellement, la lutte antifraude reposait sur des contrôles manuels, l'expertise humaine des gestionnaires, et quelques **règles métier** prédéfinies telles que des indicateurs déclenchant une alerte. Ces approches, bien qu'utiles, montraient leurs limites face à l'explosion du volume de données et à l'ingéniosité croissante des fraudeurs. Les technologies d'IA, en particulier le **machine learning** et l'analyse des données massives, offrent de nouvelles capacités : identification de « signaux faibles », traitement automatisé en temps réel, reconnaissance de schémas complexes, etc. Dans cette partie, nous examinons comment l'IA est utilisée au service de la détection de fraude (II.A), les gains d'efficacité obtenus (II.B), ainsi que le **revers de la médaille** : l'utilisation de l'IA par les fraudeurs eux-mêmes et la course en avant technologique (II.C). Les assureurs ont commencé à intégrer des **modules d'IA** dans leurs dispositifs antifraude pour améliorer la détection des anomalies et automatiser le filtrage des dossiers suspects. Concrètement, on peut distinguer plusieurs types d'outils IA déployés dans la lutte antifraude :

Détection d'anomalies et scoring prédictifs :

L'IA est particulièrement performante pour analyser de grands volumes de données et détecter des **schémas inhabituels**. Par exemple, des algorithmes d'**apprentissage automatique** (machine learning) peuvent passer au crible des milliers de sinistres et établir un **score de risque** de fraude pour chacun, en se basant sur de multiples variables (profil de l'assuré, caractéristiques du sinistre, historique, etc.). Ces modèles apprennent à partir de données historiques de fraudes avérées et de sinistres légitimes. Ils parviennent ainsi à **révéler des motifs cachés** ou des corrélations subtiles que des règles manuelles ne détecteraient pas. Par exemple, un croisement inhabituel entre la localisation du sinistre, l'heure déclarée et le type de dommage pourrait échapper à un œil humain, mais être identifié comme statistiquement anormal par le modèle. Les solutions comme **Shift Technology** ou **FRISS** (cf. III) revendiquent une capacité à identifier non seulement les fraudes connues, mais aussi des **nouveaux scénarios** émergents via ces analyses prédictives. L'IA peut aussi mettre en évidence des **réseaux de fraude** (liens entre dossiers) en indiquant par exemple qu'un même *tiers* intervient dans de nombreux sinistres ou que plusieurs sinistres apparemment sans lien partagent des éléments communs troublants. Ces détections automatiques orientent ensuite le travail des enquêteurs humains.

01. L'IA au service de la détection

Règles d'alerte « intelligentes » :

Historiquement, les assureurs utilisaient déjà des **règles métier** (scénarios de fraude connus) pour générer des alertes, par ex. « sinistre corporel déclaré juste après souscription », « plusieurs sinistres de vol déclarés par le même client en peu de temps », etc. L'IA permet de rendre ces règles plus **puissantes et adaptatives**. D'une part, les plateformes modernes combinent **moteur de règles** et **moteur d'IA** pour une approche hybride : l'IA peut prioriser ou pondérer les alertes en fonction de sa prédiction. D'autre part, certaines solutions proposent des **bibliothèques de scénarios pré-entraînés** (*« sur étagère »*) issues de l'expérience de nombreux assureurs. Par exemple, Shift Technology a développé dès 2016 un catalogue de scénarios de fraude fréquents intégrés à son logiciel, qui ont fait leurs preuves et peuvent être déployés rapidement chez un nouvel assureur. Ces scénarios évoluent en continu grâce au retour des données : on parle d'IA « apprenante » qui ajuste ses modèles à mesure que de nouveaux cas sont résolus. Ainsi, on bénéficie du meilleur des deux mondes : la **connaissance experte** codifiée (règles) et la **découverte automatisée** (machine learning).

Analyse automatisée des documents :

Une part importante des fraudes implique des **documents falsifiés** (factures, devis, cartes grises, documents d'identité, relevés bancaires, etc.). L'IA, couplée à la vision par ordinateur, révolutionne ce domaine en permettant de **vérifier l'authenticité des documents de manière automatique**. Des solutions spécialisées, comme la start-up française **Finovox**, utilisent des algorithmes d'IA pour analyser la composition d'un document numérique : elles examinent les **polices de caractères, les alignements, les couleurs, la structure du fichier**… afin de détecter des incohérences révélatrices d'une altération ou d'un faux. Par exemple, une facture falsifiée peut présenter de légères différences de typographie ou un total incohérent avec la somme des lignes ; de faux bulletins de salaire peuvent être composés d'éléments assemblés de sources diverses. Couplée à de l'OCR (lecture optique) et à des bases de documents de référence, l'IA peut aussi **vérifier le contenu** : s'assurer que le numéro de TVA d'une entreprise sur une facture existe, que le total correspond aux lignes, que la date n'est pas incohérente, etc. De plus, ces systèmes peuvent fonctionner **en temps réel** sur de gros volumes : l'API de Finovox permet de contrôler jusqu'à des millions de documents par mois automatiquement. Les bénéfices sont considérables : plus besoin d'une vérification manuelle chronophage de chaque document, l'IA signale directement ceux qui semblent suspects. Certaines fraudes qui échappaient totalement aux radars (par exemple de faux relevés bancaires dans des dossiers emprunteur) peuvent ainsi être détectées.

01. L'IA au service de la détection

Surveillance des comportements numériques :

l'IA peut aussi analyser les **données de navigation** ou de saisie des utilisateurs lors de processus en ligne pour repérer des fraudes. Par exemple, en assurance emprunteur, un fraudeur qui remplit un formulaire de santé de façon incohérente ou trop rapide pourrait être détecté via des algorithmes de détection d'anomalie sur le *web journey*. De même, certaines compagnies utilisent l'IA pour analyser les interactions sur les espaces client en ligne et repérer des tentatives de **piratage de compte** ou d'**usurpation d'identité** (détection d'accès suspects, de changements inhabituels d'adresse ou de coordonnées bancaires, etc.).

En s'appuyant sur ces différents outils, l'IA permet aux assureurs de **passer d'un mode réactif à un mode proactif**. Plutôt que d'enquêter a posteriori sur des fraudes avérées, on peut filtrer et noter *dès la déclaration* du sinistre (voire à la souscription) pour identifier en amont les dossiers douteux. En effet, l'IA peut donner une **"feuille de route" en temps réel** au gestionnaire : tel sinistre a un score de 95/100 de probabilité de fraude, vérifier impérativement ce point ; tel autre a 5/100, on peut payer sans attendre. **L'intégration dans le parcours client** est donc un atout : certaines compagnies parviennent à traiter instantanément les demandes de remboursement jugées honnêtes tout en isolant les dossiers à risque pour inspection manuelle. Ainsi, FRISS indique que grâce à son IA, jusqu'à **90 % des demandes** peuvent être traitées sans frictions et payées plus vite, en se concentrant sur les 10 % potentiellement problématiques.

Un exemple illustratif est celui d'une grande assurance IARD ayant déployé la solution Shift : l'IA de Shift détecte la fraude en **temps réel** avec un taux de pertinence 3 fois supérieur aux anciens processus. Cela signifie moins de "faux positifs" (dossiers innocents injustement suspectés) et une capacité à repérer davantage de vrais cas de fraude.

Ce qu'il faut retenir

→ L'IA **améliore nettement le taux de détection** et la précocité des alertes, tout en limitant les fausses alarmes. Grâce au **machine learning**, on peut scorer chaque sinistre et **déceler des anomalies subtiles** ou des liens cachés que l'humain ne verrait pas. Les moteurs combinent **scénarios pré-paramétrés** et apprentissage pour repérer aussi bien les fraudes classiques que les schémas émergents. En parallèle, des IA de **vision artificielle** traquent les **faux documents** (factures, pièces justificatives) en repérant la moindre incohérence visuelle ou textuelle. L'ensemble de ces outils permet de traiter de gros volumes en temps réel et de **prioriser le travail d'enquête** sur les dossiers vraiment suspects. On passe d'une logique « loupe et intuition » à une logique « **big data** et signaux faibles ». L'IA ne remplace pas l'expert fraude, mais l'accompagne en **filtrant et en analysant** des données massives 24h/24.

02. L'IA au service de l'efficacité

Le recours à l'intelligence artificielle dans la lutte contre la fraude apporte des **gains d'efficacité significatifs**. Ceux-ci se mesurent tant en termes quantitatifs (taux de détection, économies réalisées, temps de traitement réduit) qu'en termes qualitatifs (meilleure orientation des enquêtes, expérience client améliorée). Voici les principaux bénéfices constatés :

- **Amélioration du taux de détection** : les assureurs équipés d'IA constatent généralement une hausse du nombre de fraudes identifiées, y compris des cas qui auparavant passaient inaperçus. Par exemple, Generali France a témoigné avoir obtenu **20 millions d'euros de gains annuels** supplémentaires grâce à l'IA de Shift Technology. L'IA permet de **détecter plus finement** (y compris de petites fraudes opportunistes qui, agrégées, pèsent lourd) et d'**élargir le filet** de contrôle sans augmenter exponentiellement les effectifs. Une banque-assurance ayant implémenté l'IA Bleckwen a pu éliminer 80 % de la fraude résiduelle qui échappait encore à ses anciens outils.

  20 millions
  de gains annuels grâce à Shift Technology

  Dans le secteur automobile, un assureur a vu le montant des sinistres frauduleux non-payés passer de 173 M€ à 223 M€ en un an après renforcement des dispositifs, signe d'une détection plus efficace évitant des indemnisations indues. En réduisant aussi les **faux négatifs** (fraudes loupées), l'IA améliore le **"taux de capture"** et donc les économies réalisées sur sinistres.

- **Accélération des traitements** : l'IA travaille à la vitesse de la machine. Un algorithme peut analyser en quelques secondes un dossier que l'humain mettrait des heures à éplucher. Ainsi, les délais pour trier et vérifier les demandes s'en trouvent drastiquement réduits. FRISS annonce par exemple une réduction de **66 % du temps de traitement** des sinistres grâce à son logiciel IA. Concrètement, cela signifie que de nombreux dossiers peuvent être clos quasi instantanément s'ils ne présentent pas de signaux de fraude. Le gestionnaire n'a plus besoin de tout revoir manuellement : il se concentre sur les cas à risque, pendant que l'IA valide automatiquement les cas simples. **Le gain pour les clients honnêtes est considérable** : leurs indemnisations sont payées plus vite. On évite aussi de les importuner inutilement avec des demandes de justificatifs superflus. L'IA permet ainsi d'**accélérer l'indemnisation** des assurés légitimes, améliorant la satisfaction client, tout en réservant l'attention humaine aux dossiers suspects. Cette capacité de **tri intelligent** des flux fait aujourd'hui partie intégrante des parcours clients digitalisés. Par exemple, certaines néo-assurances comme Luko ont intégré un outil de fraude documentaire qui filtre en amont les justificatifs suspects : le client ayant déposé des documents corrects bénéficie d'un remboursement quasi immédiat, tandis qu'un faux document déclenchera un contrôle approfondi.

02. L'IA au service de l'efficacité

- **Automatisation du tri des dossiers suspects** : au-delà de la rapidité, l'IA apporte une **automatisation robuste** qui soulage les équipes antifraudes. Avant la montée en puissance des outils, un analyste devait évaluer manuellement une grande partie des sinistres pour décider s'il y avait lieu d'enquêter. Avec l'aide de l'IA, les modèles affectent un **score** à chaque sinistre et **priorisent** les dossiers. Par exemple, chez un grand assureur canadien, l'IA réduit de 75 % le nombre de **faux positifs** (alertes injustifiées) par rapport aux systèmes de règles antérieurs. Cette **efficience opérationnelle** se traduit souvent par un ROI rapide sur les investissements IA.

  En guise d'exemple, Carrefour Assurance a estimé que l'IA de Bleckwen lui a fait gagner l'équivalent de **1,5 ETP (équivalent temps plein)** en charge de travail évitée, grâce à l'automatisation du repérage des dossiers douteux. Les collaborateurs peuvent consacrer leur expertise aux enquêtes complexes plutôt qu'au tri fastidieux.

  -75 %
  de faux positifs chez un assureur canadien

- **Intégration dans le parcours client (décisions en temps réel)** : un avantage clé de l'IA est de pouvoir fonctionner **en temps réel**, notamment via des API reliées aux systèmes de gestion. Ainsi, lors de la déclaration d'un sinistre en ligne, le système peut immédiatement calculer un score de risque. Si le score est faible, le sinistre est orienté vers une voie rapide (ex. indemnisation automatique ou accélérée) ; s'il est élevé, il passe en revue manuelle ou en demande de justificatifs supplémentaires. Tout cela se fait de manière **transparente** pour le client. L'intégration de ces mécanismes IA dans les systèmes de gestion de sinistres ou de souscription est facilitée par les solutions du marché, qui offrent des connecteurs vers les progiciels majeurs (Guidewire, DuckCreek, Salesforce, etc.). Cela engendre un *« tunnel antifraude »* invisible tout au long du parcours client. L'IA joue alors un rôle de contrôle. Plus concrètement, lorsqu'un prospect demande un devis en ligne, un score peut indiquer s'il présente un profil à risque (histoire de fraudes passées, incohérences dans les données fournies) et adapter la réponse (par ex. exiger une visite de risque, ou refuser la souscription en ligne). De même, lors du règlement d'un sinistre, l'IA peut recommander d'orienter le client vers un **parcours spécial** si suspicion (par ex. lui proposer un entretien téléphonique avec un expert, plutôt que le laisser en auto-déclaration). Globalement, cela permet de **sécuriser chaque étape** sans alourdir le parcours pour la majorité des clients.

En synthèse, l'IA accroît l'**efficacité opérationnelle** de la lutte anti-fraude de plusieurs ordres de grandeur. Cette évolution technologique permet des gains d'efficience pouvant atteindre plusieurs jours selon les actes de gestion. Nous assistons donc à une **montée en gamme** générale du dispositif antifraude.

02. L'IA au service de l'efficacité

Ces gains d'efficacité se réalisent **sans nécessairement déshumaniser** complètement le processus. Au contraire, ils libèrent du temps aux équipes pour se concentrer sur les enquêtes complexes nécessitant du **jugement humain**. L'automatisation intelligente prend en charge le répétitif et l'analyse brute, l'humain garde la main sur les décisions finales notamment lorsque la situation est ambiguë.

Enfin, notons que cette efficacité profite aussi aux pouvoirs publics : plus de fraudes détectées signifie plus de signalements à la justice ou à TRACFIN pour les cas graves, et in fine une **dissuasion accrue**. Un fraudeur qui sait que l'assureur utilise une IA sophistiquée pour le traquer réfléchira à deux fois.

Ce qu'il faut retenir

→ L'adoption de l'IA se traduit par des **résultats tangibles** dans la lutte anti-fraude. Les assureurs constatent une **hausse du nombre de fraudes détectées** et des **économies significatives** (ex. +20 M€/an pour Generali avec l'IA, 80 % de fraude en moins chez un bancassureur). La **vitesse de traitement** s'améliore drastiquement : l'IA analyse un dossier en quelques secondes, réduisant les délais d'indemnisation pour les clients honnêtes (jusqu'à 90 % des demandes payées sans délai grâce au filtrage IA).

→ Les équipes antifraudes gagnent en efficience : moins de faux positifs (–75 % annoncés), tri automatisé des cas, ce qui permet aux enquêteurs de se concentrer sur les vrais dossiers suspects. L'intégration **temps réel** dans les processus rend le parcours client à la fois plus fluide pour la majorité et plus sécurisé contre les fraudeurs. En somme, l'IA permet de **détecter plus, plus vite, et mieux**, tout en améliorant l'équité du traitement.

03. L'IA, alliée des fraudeurs ?

Si l'intelligence artificielle est un formidable outil pour les assureurs, elle peut tout autant être exploitée par les fraudeurs eux-mêmes. L'IA est en effet une technologie à double tranchant : accessible à tous, elle donne aux individus malveillants de nouvelles **armes pour tromper** les dispositifs de contrôle. On assiste ainsi à une sorte de **course technologique** entre fraudeurs et assureurs, chacun essayant de prendre une longueur d'avance. Voici quelques-unes des façons dont l'IA peut devenir l'alliée des fraudeurs en assurance :

Génération de faux documents et images :

Là où il fallait autrefois être graphiste ou faussaire professionnel pour créer de faux papiers, aujourd'hui des outils d'IA générative permettent de produire en un clic des contenus **extrêmement réalistes**. Des modèles comme *DALL·E* ou *MidJourney* peuvent générer des images de sinistres fictifs plus vraies que nature. Par exemple, un fraudeur peut fabriquer une photo d'une voiture accidentée qui est en réalité un montage d'IA. La scène de l'accident n'a jamais existé, mais l'image est convaincante. De même, on voit émerger des **fausses factures générées automatiquement** : l'IA peut apprendre le style de factures d'un vrai garagiste et en produire une fausse avec en-tête, logo, TVA… parfaitement crédible. Ces documents passaient jusqu'ici relativement bien les contrôles humains, surtout si l'assureur n'avait pas de base de comparaison. L'IA générative abaisse le coût et la difficulté de produire des **faux de haute qualité**, rendant la fraude documentaire plus aisée. Un exemple concret cité est la génération de **photos de dégâts** : un assuré pourrait soumettre au dossier une photo d'objets endommagés totalement fabriquée par IA (ex. une télé cassée) pour appuyer sa déclaration de sinistre, très difficile à discerner si on ne dispose pas d'outils spécialisés. De plus, ces IA peuvent fonctionner sur smartphone, de façon décentralisée, ce qui les rend plus accessibles et difficiles à tracer.

03. L'IA, alliée des fraudeurs ?

Deepfakes et faux témoignages :

L'IA permet aussi de manipuler l'audio et la vidéo. Les **deepfakes,** ces vidéos truquées qui imitent le visage et la voix de quelqu'un, représentent un danger émergent en assurance. Les cas d'usage suivants pourraient voir le jour : **fausse vidéo de témoin** attestant un sinistre. De même, des enregistrements audios falsifiés pourraient servir de "preuves". Ces contenus **difficiles à distinguer du réel** peuvent berner les enquêteurs si ces derniers ne disposent pas d'outils d'authentification avancés. Les deepfakes peuvent également servir à l'**usurpation d'identité** : un fraudeur pourrait se faire passer pour un client au téléphone via un synthétiseur vocal imitant la voix de celui-ci (après l'avoir obtenue sur une vidéo en ligne par ex.). Cela pourrait lui servir à duper un conseiller et changer les coordonnées de virement pour toucher l'indemnisation sur son compte, etc. Ce type de scénario, encore rare, est pris très au sérieux par les acteurs de l'assurance, car il **compromet la fiabilité** de nombreuses procédures.

Automatisation des récits frauduleux :

Outre les images, les textes générés par IA représentent une menace. Avec des modèles de langage comme *ChatGPT*, un fraudeur peut **rédiger un récit de sinistre cohérent et détaillé** en quelques secondes, même s'il n'a pas une grande imagination. Par exemple, fournir une description très réaliste d'un vol de téléphone ou d'un accident domestique. Bien sûr, les enquêteurs chevronnés savent repérer les incohérences, mais l'IA aide les fraudeurs à ne pas en laisser, et le ton peut être paramétré pour brouiller les pistes. Demain, un assuré pourrait même interagir avec un chatbot qui lui *dicte* les réponses crédibles à apporter à l'assureur. On voit aussi apparaître des **bots capables de remplir automatiquement des formulaires de sinistre en masse** avec des données fictives mais plausibles. Des réseaux pourraient ainsi tenter de noyer les assureurs sous de multiples petites demandes frauduleuses (phénomène de fraude à la "mouche", plein de petits sinistres pour passer sous les radars). L'IA rend possible la **scalabilité** de la fraude : un même individu peut tenter des dizaines de fraudes simultanément, assisté d'outils qui personnalisent chaque dossier pour qu'il paraisse unique.

03. L'IA, alliée des fraudeurs ?

Usurpation d'identité numérique :

Les fraudeurs ont recours à des techniques de phishing et de hacking pour voler des identifiants de clients, et l'IA peut les y aider. Par exemple, des outils d'IA peuvent générer des emails d'hameçonnage extrêmement convaincants (ex. un faux email de la compagnie d'assurance demandant à l'assuré de "vérifier son compte"), avec un texte personnalisé. En récupérant les accès, les fraudeurs peuvent ensuite se connecter à l'espace client et faire des **actes frauduleux** : modifier l'IBAN du client (pour que les remboursements aillent sur leur compte), déclarer un faux sinistre au nom du client, ou recueillir des informations personnelles pour de futures fraudes. L'ALFA signale que certains fraudeurs **multicartes** utilisent le phishing pour obtenir des infos puis s'introduire dans les portails clients d'assurance vie, par exemple. Ces attaques combinées (social engineering assisté par IA + exploitation des données volées) complexifient la tâche des assureurs car elles brouillent la frontière entre le vrai client et le fraudeur.

Face à ces menaces, les assureurs ne restent pas inactifs et développent aussi des parades technologiques. On assiste à une **escalade technologique permanente**. Les assureurs développent des **IA adversariales** capables de repérer la "patte" d'un générateur d'images (certains artefacts mathématiques dans le fichier, etc.). Face aux deepfakes, des startups proposent des solutions de détection d'altérations vidéo. Les assureurs renforcent l'authentification (double facteur, etc.) pour contrer l'usurpation. Néanmoins, il est clair que l'IA a abaissé la barrière d'entrée pour les fraudeurs occasionnels en leur donnant des outils autrefois réservés aux cybercriminels experts.

Nous sommes entrés dans l'ère de la **fraude 2.0**, où les fraudeurs utilisent l'IA comme "*booster*". Cette évolution demande aux assureurs d'être encore plus réactifs et innovants. ALFA parle d'ailleurs d'**« industrialisation de la fraude sur les réseaux sociaux »** et de fraudeurs très technophiles, parfois basés à l'étranger et s'appuyant sur des complices locaux pour récupérer les fonds. Chaque avancée du côté assureur (ex. adoption d'une IA de détection) finit par entraîner une adaptation côté fraudeur (ex. trouver comment tromper cette IA). Cela souligne l'importance pour les assureurs de **collaborer** et de partager informations et retours d'expérience, afin de ne pas lutter en ordre dispersé face à des fraudeurs organisés globalement.

03. L'IA, alliée des fraudeurs ?

Un autre aspect inquiétant est la **démocratisation** de ces outils de fraude : un assuré lambda peut aujourd'hui trouver en ligne, via des forums ou des prestataires douteux, de l'aide pour monter sa fraude. Il existe des *« coachs en fraude »* proposant leurs services, et l'IA risque d'amplifier ce phénomène en rendant la fraude "clé en main". En 2025, on a même vu apparaître des offres illégales de bots proposant de déclarer un sinistre fictif à votre place pour quelques dizaines d'euros, promettant un remboursement substantiel. Les assureurs doivent donc conjuguer **technologie et pédagogie** pour renforcer les systèmes de détection, et en parallèle sensibiliser les clients sur les risques (juridiques et moraux) de la fraude, pour éviter cette banalisation.

Ce qu'il faut retenir

→ L'IA n'est pas l'apanage des assureurs : les **fraudeurs aussi l'adoptent**. Elle leur permet de créer des **faux documents, images et vidéos** hyperréalistes (ex. photos de sinistres générées, deepfakes de témoins), de **rédiger des faux récits** très convaincants et même d'automatiser l'envoi de demandes frauduleuses en masse. Les techniques d'**usurpation d'identité** sont amplifiées par l'IA (phishing sophistiqué, imitation de voix, etc.).

→ On assiste à une **course technologique** entre assureurs et fraudeurs : chaque avancée de l'un entraine l'autre à s'adapter. La fraude tend à **s'industrialiser** via les outils numériques, ce qui oblige les compagnies à investir dans des contre-mesures IA (détection de deepfake, vérification de documents, sécurisation des accès…). En somme, l'IA est un **formidable levier** aussi bien pour améliorer la détection que pour monter de nouvelles fraudes : le secteur doit en être conscient et se préparer à cette lutte de plus en plus technique.

III.

Panorama des outils et solutions de marché

- 01. Start-up et insurtech spécialisées
- 02. Intégration avec d'autres systèmes

01. Start-up et insurtech spécialisées dans la lutte anti-fraude

Face à la montée des enjeux, un écosystème de **solutions technologiques** s'est développé pour aider les assureurs dans la lutte contre la fraude. Des startups spécialisées (*insurtechs*) proposent des logiciels prêts à l'emploi basés sur l'IA, tandis que les grands éditeurs intègrent des modules antifraudes dans leurs offres. Cette partie dresse un panorama non exhaustif des principaux outils du marché et de leur intégration dans le SI des assureurs. On distinguera (III.01) quelques **acteurs spécialisés** marquants et (III.02) l'**intégration de ces solutions** dans l'écosystème assurantiel (core systems, collaborations externes, etc.).

Plusieurs jeunes pousses se sont fait un nom ces dernières années en offrant aux assureurs des solutions innovantes pour détecter et gérer la fraude. En voici quelques-unes des plus en vue :

Shift Technology :

SHIFT

Cocorico, Shift est une start-up française (fondée en 2014) devenue une référence mondiale de l'IA anti-fraude en assurance. Devenue licorne en 2021, elle compte plus de 100 assureurs clients dans le monde. Sa solution phare **Shift Claims Fraud Detection** est un logiciel SaaS qui analyse les déclarations de sinistres en temps réel et signale les cas potentiellement frauduleux. Shift combine des **modèles prédictifs** entraînés sur des millions de sinistres avec une base de **scénarios prêts à l'emploi** issus de son expérience. Elle revendique un taux de précision bien supérieur aux approches traditionnelles : *« une pertinence trois fois plus élevée que celle des processus manuels ou à base de règles »*. Generali, MACIF, CNA, MS&AD font partie de ses clients affichés. Shift met aussi l'accent sur l'**explicabilité** des résultats (fournir les raisons de l'alerte) et propose un module d'enquête intégré pour suivre le traitement des suspicions. Outre la fraude, Shift a étendu sa plate-forme à d'autres usages (détection de sinistres graves, optimisation de processus), mais la fraude reste son cœur de métier. En termes de résultats, Generali France a communiqué sur 20 M€ d'économies annuelles grâce à Shift, et d'autres assureurs saluent la **réduction drastique des faux positifs** obtenue. Shift a su convaincre autant en assurance de dommages qu'en assurance de personnes (des projets sont en cours sur les périmètres prévoyance, santé, etc. avec adaptation des modèles).

01. Start-up et insurtech spécialisées dans la lutte anti-fraude

FRISS :

Originaire des Pays-Bas (fondée en 2006), FRISS est un pionnier des solutions antifraude pour l'assurance P&C. Sa suite logicielle couvre la **détection à la souscription, en gestion de sinistres, et le monitoring des portefeuilles**. FRISS utilise l'IA et l'analyse de données pour fournir un *score FRISS* sur chaque dossier, en s'intégrant directement aux systèmes de l'assureur (via des connecteurs à Guidewire, Sapiens, etc.). La plateforme FRISS est enrichie de nombreuses **données externes** (listes de véhicules volés, bases de données publiques, réseaux sociaux quand c'est possible, etc.) afin d'alimenter ses algorithmes. Elle excelle dans la **détection en temps réel** et l'automatisation : *« notre logiciel alimenté par l'IA détecte automatiquement les demandes suspectes, révèle les réseaux et découvre des modèles cachés »*. FRISS insiste aussi sur l'amélioration de l'expérience client honnête : réduction de 75 % des faux positifs et traitement rapide de 90 % des demandes légitimes. Présente en Europe, Amérique du Nord et Latam, FRISS a plus de 300 implémentations dans 45 pays. Elle apporte une dimension intéressante de **vision "confiance"** : son leitmotiv est de restaurer la confiance dans l'assurance en empêchant les fraudeurs de faire payer plus cher les honnêtes. Certains de ses clients témoignent d'économies importantes (21 M$ sur 2 ans pour l'un d'eux). FRISS se positionne comme une **solution clé en main** antifraude, facile à déployer et avec gouvernance des règles par le métier.

01. Start-up et insurtech spécialisées dans la lutte anti-fraude

Bleckwen :

Startup française fondée en 2016, Bleckwen est spécialisée dans la **détection de fraudes financières en temps réel**. Initialement centrée sur la fraude bancaire (notamment la fraude aux paiements et au crédit), elle a élargi son spectre aux acteurs de l'assurance et de la bancassurance. Bleckwen se distingue par son approche de **« Managed AI »** : elle fournit des modèles de machine learning sur mesure pour chaque client, tout en permettant aux équipes métier de garder le contrôle via des scores et des seuils ajustables. Sa force réside dans la **détection des fraudes organisées et complexes**, grâce à une analyse comportementale poussée et une adaptation continue des modèles. Par exemple, pour Carrefour Assurance (banque & assurance du groupe Carrefour), Bleckwen a déployé un modèle détectant les demandes de crédit frauduleuses, ce qui a réduit de 80 % la fraude résiduelle et de 30 % les tentatives de fraude en quelques mois. De même, chez Mobilize Financial Services (RCI Bank, groupe Renault), Bleckwen a permis de réduire les pertes nettes dues à la fraude de 50 à 80 % selon les segments, avec un taux de faux positifs excellent (moins de 3 pour 1 fraude avérée). Ces résultats montrent la **précision** de ses algorithmes. Bleckwen met en avant la **collaboration humain-IA** : leurs scores sont expliqués et l'équipe accompagne dans le recalibrage régulier des modèles. Pour l'assurance, Bleckwen s'applique par exemple à la fraude à l'assurance emprunteur, aux fausses souscriptions, ou aux sinistres complexes impliquant possiblement des réseaux (fraudes au carrousel TVA , etc.). C'est un acteur à la frontière de l'assurance et de la finance, qui illustre la **convergence Insurtech/Fintech** sur le sujet de la fraude.

01. Start-up et insurtech spécialisées dans la lutte anti-fraude

Finovox :

Finovox

Jeune pousse française (2019) dédiée à la **fraude documentaire**. Finovox a développé un logiciel capable d'**analyser 100 % des documents** reçus par un assureur pour en détecter les falsifications, grâce à du **deep learning**. Sa promesse : *« divisez par 6 la fraude documentaire »* en attrapant tous les faux docs qui auparavant passaient à travers. La solution s'intègre aux processus de souscription ou sinistre via API : dès qu'un client charge un document (facture, pièce d'identité, RIB…), Finovox l'analyse et retourne une alerte s'il est suspect. Techniquement, Finovox combine de la **vision par ordinateur** (détecter les altérations visuelles) et des règles métier (vérifier les données présentes). Elle est agnostique au format et à la langue, ce qui est utile pour des assureurs traitant des documents variés. Luko, assureur habitation digital, a adopté Finovox fin 2022 : en quelques mois, **18 % des fraudes avérées** chez Luko comportaient un faux document détecté grâce à Finovox. Surtout, Finovox a permis de **doubler les économies de fraude** réalisées par Luko, en attrapant des escroqueries qui leur échappaient auparavant. Finovox vise tant l'assurance (sinistres auto, MRH, santé où prolifèrent de fausses factures de soin) que la banque (fausses fiches de paie, etc.). Avec la flambée de la fraude documentaire, ce type d'outil devient presque indispensable en complément d'un détecteur de fraude global.

01. Start-up et insurtech spécialisées dans la lutte anti-fraude

Doc vérif :

Doc vérif est un dispositif public français de vérification documentaire, développé et opéré par l'État dans le cadre de la lutte contre la fraude à l'identité. Mis en place par le ministère de l'Intérieur et opéré par l'Agence nationale des titres sécurisés (ANTS), Doc Vérif permet de **contrôler l'authenticité et la validité des titres officiels** (cartes nationales d'identité, passeports, titres de séjour) en les comparant aux bases de données de l'État. Sa promesse : **fiabiliser les contrôles d'identité** et réduire les risques de fraude documentaire dans les parcours sensibles. Le dispositif est accessible, sous conditions et habilitations spécifiques, à des acteurs publics et privés (administrations, forces de l'ordre, établissements bancaires ou assurantiels) via une intégration aux systèmes existants. Concrètement, dès qu'un document d'identité est présenté, Doc Vérif permet de vérifier son existence, sa validité et sa cohérence avec les données de référence. Techniquement, la solution repose sur des mécanismes de consultation sécurisée de bases régaliennes, combinés à des règles de contrôle strictement encadrées par la réglementation. Contrairement aux solutions privées de détection de fraude basées sur l'IA ou l'analyse visuelle, Doc Vérif s'inscrit dans une **logique institutionnelle de contrôle à la source**, garantissant un haut niveau de fiabilité juridique. Dans un contexte de renforcement des obligations KYC et de montée de la fraude à l'identité, Doc Vérif constitue un socle public de référence, souvent utilisé en complément d'outils privés de lutte globale contre la fraude.

- **Autres acteurs notables** : parmi les grands noms internationaux, citons **SAS** (éditeur historique d'analytics, qui propose une solution de détection de fraudes à l'assurance combinant règles et machine learning), **BAE Systems (NetReveal),** utilisé par certains bancassureurs pour déceler fraudes et blanchiment, ou encore **IBM** avec sa suite **Counter Fraud Management.** En assurance santé, des solutions spécifiques existent pour repérer les fraudes à l'Assurance Maladie ou aux complémentaires (ex. des algorithmes développés par l'Assurance Maladie elle-même qui ont permis de repérer 9,1 Mds € de fraudes en 2024, record lié en partie à l'IA). Enfin, de nombreuses insurtechs se positionnent sur des niches : par ex. **DetektIA** (mentionnée par Mieux Assuré) spécialisée aussi en fraude assurance, **ou Snapsheet** (USA, détection de fraudes auto via analyse photo), etc. L'offre est donc riche et en croissance, car les investisseurs ont bien compris que les assureurs sont prêts à investir pour gagner cette bataille.

01. Start-up et insurtechs spécialisées dans la lutte anti-fraude

En choisissant une solution antifraude, les assureurs regardent plusieurs critères : **efficacité prédictive** (prouver qu'on attrape plus de fraudes), **intégration SI** (doit s'imbriquer sans tout bouleverser), **explicabilité et conformité RGPD**, **coût et ROI**, et souvent la capacité à couvrir **plusieurs branches** (multi-lignes, multi-types de fraude). La **réputation** compte aussi : des acteurs comme Shift ou FRISS, forts de dizaines de projets, inspirent confiance. Parfois, des assureurs développent aussi en interne leurs propres modèles maison (notamment les plus gros, qui disposent de data scientists). La majorité des acteurs se tourne cependant vers ces partenaires spécialisés pour aller plus vite et profiter de leur expérience mutualisée.

Ce qu'il faut retenir

→ Le marché propose désormais des **solutions antifraude clé en main**. Parmi les stars : **Shift Technology** dont l'IA de détection de sinistres frauduleux est utilisée par des assureurs du monde entier, **FRISS** qui offre une plateforme complète de scoring en temps réel et se targue de réduire fortement faux positifs et délais, **Bleckwen** (Fraude comportementale en temps réel, ROI important avec - 80 % de fraude résiduelle chez certains clients), **Finovox** (spécialiste français de la **fraude documentaire**, adopté par Luko pour stopper les faux papiers). Toutes ces solutions exploitent le machine learning et s'intègrent aux systèmes existants.

→ D'autres acteurs (SAS, BAE NetReveal, IBM, etc.) sont également présents. Le choix se fait selon la **taille et besoins** de l'assureur : un grand groupe multi-lignes privilégiera peut-être une solution globale (Shift/Friss), là où une mutuelle santé pourra s'équiper d'un outil ciblé (ex : anti-fraude aux soins). L'essor de ces insurtechs témoigne en tout cas d'un secteur en ébullition, où l'innovation est mise au service d'un enjeu concret : déjouer les fraudeurs.

02. Intégration avec d'autres systèmes

La mise en place d'outils de détection de fraude ne se fait pas en silo : ces solutions doivent s'intégrer de manière cohérente au sein du **système d'information** de l'assureur et s'articuler avec divers processus existants, ainsi qu'avec les acteurs externes (partenaires, autorités). Plusieurs dimensions d'intégration méritent d'être soulignées :

Couplage aux systèmes cœur (CRM, gestion de sinistres, etc.)

Les logiciels antifraudes sont d'autant plus efficaces qu'ils sont **étroitement connectés** aux flux de données de l'assureur. Ainsi, l'intégration à l'outil de **gestion de sinistres** est cruciale : typiquement, la solution d'IA s'interface via API au moment de la déclaration de sinistre ou pendant son instruction, pour analyser les données et renvoyer un score/une alerte. Des connecteurs existent pour les principaux outils du marché (Guidewire ClaimCenter, Salesforce Industries, etc.).

De même, l'outil antifraude peut être branché au système de **souscription** (pour filtrer dès l'entrée en portefeuille). L'intégration au **CRM** permet de consolider toutes les informations client : par exemple, si un client a été détecté frauduleux sur un contrat auto, l'information pourrait remonter lors d'une nouvelle souscription habitation pour vigilance. Certains assureurs vont jusqu'à créer une **vision 360° anti-fraude** dans leur datawarehouse, alimentée par les outils IA, consultable par les gestionnaires. Par ailleurs, les alertes fraude doivent souvent être gérées dans un **outil de case management** (souvent fourni avec la solution ou via un module SI interne) pour tracer les investigations, les décisions (paiement refusé, etc.) et éventuellement les suites (dépôt de plainte, récupération de fonds). Une intégration réussie permet au gestionnaire de visualiser la criticité de ses dossiers selon un code couleur (vert, orange, rouge). Selon le risque de fraude associé, l'outil propose un plan d'action au gestionnaire. En arrière-plan, cela suppose un **partage de données fluide** entre les systèmes : les algorithmes ont besoin d'accéder aux données clients, historiques de sinistres, etc., ce qui peut soulever des enjeux de droits d'accès, de performance (gérer la latence en temps réel). La plupart des projets réussis passent par une phase de **connectivité SI** assez lourde mais indispensable.

02. Intégration avec d'autres systèmes

Interaction avec les outils d'enquête et services juridiques

Une fois une fraude détectée ou suspectée, elle doit être traitée par des humains (analystes fraude, agents d'investigation) qui vont approfondir. Ces équipes peuvent avoir des **outils dédiés** (par ex. accès à des bases externes comme les fichiers des immatriculations, outils de OSINT, recherche sur internet, etc.). L'intégration ici est plus de l'ordre de la **procédure** : souvent, l'alerte générée par l'IA sera transmise au *service lutte contre la fraude* via une plateforme qui permet d'ajouter des notes, de collecter des preuves (photos, rapports d'experts) et de décider de la suite. Certaines solutions (Shift, SAS) incluent un **module de workflow enquête** où l'on peut affecter un dossier à un enquêteur, planifier des actions, historiser les résultats (par ex. "07/09 : appel au client, aveu de fausse déclaration"). Ces informations peuvent ensuite rétroalimenter le système (les gestionnaires précisent s'il s'agit d'une alerte à raison ou à tort afin d'améliorer les modèles d'IA). L'intégration avec le **service juridique** est également importante. Si une fraude avérée justifie une action en justice (plainte pour escroquerie), le dossier constitué doit être transmis au juridique/contentieux. On veille alors à ce que les éléments recueillis par l'IA soient utilisables en justice (cf. partie V.B sur la preuve). Par exemple, conserver les logs, copies d'écran, etc. L'outil antifraude peut parfois générer un rapport synthétique du cas. Sur un plan organisationnel, nombre d'assureurs ont mis en place des **comités internes** réunissant les départements Indemnisation, Conformité, Juridique et Anti-fraude pour gérer les dossiers sensibles. L'IA facilite cette collaboration en apportant une **vue objective** (score) et en centralisant l'info.

02. Intégration avec d'autres systèmes

Interopérabilité entre assureurs et acteurs publics

La fraude à grande échelle étant souvent **transverse**, la coopération externe est cruciale. En France, l'ALFA joue ce rôle de plateforme de partage entre assureurs. Les membres d'ALFA peuvent déclarer des *« alertes »* sur des sinistres suspects dans une base commune, ce qui permet de voir si le même sinistre a été déclaré chez un concurrent, ou si un individu est signalé multiple fois. ALFA facilite la **coordination d'affaires** entre organismes d'assurance. L'IA vient en support : par exemple, certains assureurs intègrent directement dans leur outil une requête vers la base ALFA lors du traitement d'un dossier (recherche de similitudes, etc.). De plus, ALFA collecte chaque année les chiffres et tendances pour l'ensemble du marché, ce qui aide chacun à se comparer aux standards de marché. Au-delà des assureurs entre eux, il y a la relation avec les autorités publiques : d'une part les autorités de contrôle (ACPR en France), d'autre part les autorités anti-fraude de l'État (TRACFIN, police, justice). Sur le volet **réglementaire**, l'ACPR encourage les assureurs à renforcer leurs dispositifs anti-fraude et peut demander des comptes. A ce titre, elle a besoin de données, ex : nombre de fraudes détectées, montants, etc. Les outils antifraudes peuvent produire ces statistiques plus facilement. Concernant **TRACFIN** (la cellule anti-blanchiment), les assureurs ont l'obligation légale de déclarer toute opération suspecte qui pourrait relever du blanchiment ou d'une infraction financière. Or, certaines fraudes à l'assurance peuvent s'inscrire dans des schémas de blanchiment (par ex. multiplier de faux sinistres pour blanchir des fonds). Les systèmes IA peuvent aider à **identifier ces cas complexes** et alerter le référent TRACFIN de l'entreprise. S'en suit la **déclaration de soupçon** via la plateforme ERMES. Une bonne pratique est de paramétrer l'outil de détection pour qu'il remonte aussi des signaux liés à des typologies de blanchiment (ex. un assuré qui multiplie les petits sinistres indemnisés sur son compte puis résilie ; ou une collusion entre un client et un fournisseur pour surfacturer). Ainsi, l'outil peut contribuer à la **LCB-FT** (lutte contre blanchiment, financement du terrorisme) en plus de la fraude "classique".

02. Intégration avec d'autres systèmes

Interopérabilité entre assureurs et acteurs publics

Notons que **les assureurs ne peuvent opposer le secret professionnel à TRACFIN** : si ce dernier requiert des informations sur un dossier, l'assureur doit fournir toutes les pièces. D'où l'intérêt d'avoir bien centralisé et documenté les investigations. D'autre part, les assureurs santé souhaitent pouvoir échanger davantage avec la Sécurité sociale pour repérer ensemble les professionnels de santé fraudeurs ; cela implique un cadre légal. En 2025, dans le PLFSS, les assureurs réclamaient une base légale renforcée pour l'échange d'infos entre régime obligatoire et complémentaires. L'évolution des lois pourrait rendre possible une **interconnexion** de certaines bases, et l'IA serait alors utilisée pour exploiter ce volume accru de données multi-sources. Enfin, en cas de fraude de grande ampleur, l'assureur travaille avec les services de police spécialisés (Brigades de répression de la délinquance astucieuse, etc.). Les rapports générés par les systèmes antifraude peuvent servir de base à leurs enquêtes. Une bonne intégration consiste parfois à **standardiser les rapports** pour qu'ils soient exploitables par les enquêteurs externes.

Partage d'informations au niveau international

La fraude étant globale (des réseaux opèrent entre pays), il existe des échanges via des forums internationaux d'assureurs, ou par le biais de **réassureurs** qui centralisent certaines infos. Par exemple, la réassurance peut exiger de ses cédantes un reporting sur la fraude, car cela impacte la sinistralité. Certaines sociétés proposent des **bases mondiales** (Insurance Fraud Bureau etc. dans certains pays) pour recouper les données. L'intégration passe alors par la capacité de l'outil à consulter ces bases externes. FRISS, par exemple, intègre nativement des *watchlists* internationales et des données agrégées de différentes sources, ce qui aide à repérer un fraudeur qui changerait de pays.

02. Intégration avec d'autres systèmes

En somme, l'efficacité d'une solution antifraude repose beaucoup sur sa **connectivité** : connectivité interne (SI de l'assureur) et externe (partenaires, organismes). Les projets antifraudes sont souvent transverses, impliquant DSI, Métier Indemnisation, Conformité, Juridique. Au-delà de l'outil technique, la **gouvernance** pour s'assurer que toutes les alertes sont bien traitées a une place centrale dans le dispositif.

Heureusement, les assureurs sont de plus en plus enclins au **partage d'informations** dans ce domaine, car ils comprennent que c'est mutuellement bénéfique. Par exemple, via ALFA ils partagent des *modi operandi* et des profils de fraudeurs. Certains réfléchissent même à des plateformes **blockchain** pour tracer certains types de sinistres et éviter les multi-déclarations (en auto notamment). L'IA pourrait tirer parti de telles initiatives en ayant accès à encore plus de données.

Ce qu'il faut retenir

→ Les solutions antifraudes doivent **s'imbriquer** dans l'écosystème de l'assurance. Elles sont **connectées aux outils de gestion** (sinistres, contrats, CRM) pour analyser les données clients en temps réel et renvoyer des alertes directement aux gestionnaires. Elles s'intègrent aussi aux **workflows d'enquête** internes : assignation des cas aux analystes, enrichissement avec des infos externes, puis transmission au **juridique** si nécessaire. Sur le plan externe, l'IA anti-fraude s'insère dans une chaîne plus large : coopération via **ALFA** entre assureurs (plateforme de partage d'alertes), déclarations de soupçon à **TRACFIN** (lorsque la fraude cache du blanchiment), échange potentiel avec la Sécurité sociale, etc.

→ **L'interopérabilité** est un enjeu clé : les outils doivent pouvoir ingérer et échanger des données multiples. C'est en brisant les silos entre services internes et entre acteurs du marché qu'on parvient à **déjouer les fraudes organisées**. Les assureurs plaident d'ailleurs pour un cadre légal facilitant ces échanges (par ex. en santé). En résumé, la lutte anti-fraude pilotée par l'IA n'est efficace que si elle est **bien intégrée** : intégrée au SI de l'assureur et intégrée dans la **stratégie collective** du secteur.

IV.

En pratique : retours d'expérience

- 01. Axa
- 02. SwissLife
- 03. Shift Technology
- 04. France Titres

Xuan Nguyen, Data leader Fraude IARD – AXA France

Neoli : quelle est la stratégie d'AXA France en matière de lutte contre la fraude ?

Xuan : « La détection de la fraude s'appuie historiquement sur des scénarios de détection internes, utilisant la data pour générer des alertes de suspicion, qui sont ensuite investiguées manuellement. Deux systèmes principaux sont utilisés : le système applicatif interne (Solaris) et la solution externe Shift, permettant le croisement de données et l'enrichissement des scénarios de détection. »

Neoli : concrètement, comment sont gérés les cas de faux positifs ?

Xuan : « Il y a une méfiance vis-à-vis des assureurs. L'équipe travaille à enrichir les données utilisées pour la détection, notamment en exploitant des données clients et des données d'impayés, afin d'améliorer la précision des alertes et de réduire les faux positifs. L'accent est mis sur la qualité des données et l'utilisation de moteurs intelligents pour affiner la détection. »

Neoli : la qualité des données serait alors un facteur clé de succès ?

Xuan : « Oui. L'enjeu réside autour de la qualité de donnée et de l'optimisation via la technologie, comme l'IA Générative. Mais d'abord, nous devons travailler sur la qualité de notre donnée, et l'enrichir pour espérer réduire drastiquement les cas de faux positifs. »

Neoli : nous observons que la tendance est également à l'anticipation et non plus uniquement à la réaction ?

Xuan : « En effet, en plus de la détection au moment du sinistre, AXA France a mis en place une surveillance à la souscription via le programme Nadia, qui mutualise les données entre différentes branches (santé, épargne, prévoyance) pour identifier des comportements frauduleux en amont, notamment par le partage d'informations sur des clients ou coordonnées suspectes. »

Neoli : d'autant que les fraudeurs sont de plus en plus difficiles à contrer ?

Xuan : « Nous ne faisons plus face uniquement à des bandes organisées mais parfois même à des réseaux de conseils diffusés via des canaux comme Snapchat. L'équipe doit donc s'adapter à des fraudes de plus en plus sophistiquées et massives, facilitées par la technologie et la dématérialisation. »

Neoli : vous nous le disiez, Agilité et Indépendance Technologique sont alors les maitres mots ?

Xuan : « L'enjeu pour AXA France est de gagner en agilité pour s'adapter rapidement aux nouveaux modes opératoires des fraudeurs, en cherchant à limiter la dépendance à des prestataires externes comme Shift et à renforcer la capacité d'action interne, tout en maintenant une veille sur les évolutions technologiques. »

Neoli : nous l'avons compris, avant d'intégrer l'IA, la priorité est à la qualité de donnée. Cependant, comme vous avez commencé à l'évoquer, l'IA Générative joue un rôle central dans la lutte contre la fraude ?

Xuan : « En effet, les équipes travaillent avec Shift pour développer des outils capables de détecter si un document ou une photo a été généré par une IA, en analysant notamment les pixels, les métadonnées et la ressemblance avec des images existantes. L'objectif est d'identifier les incohérences et les manipulations dans les justificatifs fournis par les clients.

Même si l'IA générative peut détecter des anomalies invisibles à l'œil nu, la validation finale de la fraude repose toujours sur l'expertise humaine, notamment pour constituer un dossier probant et présenter les preuves au client ou en justice si nécessaire. »

Neoli : AXA France choisit-elle d'externaliser ou internaliser les ressources pour intégrer l'IA ?

Xuan : « À date, AXA France privilégie l'externalisation des compétences en IA générative auprès de start-ups spécialisées. L'investissement interne serait trop coûteux et les prestataires externes sont souvent mieux placés pour suivre l'évolution rapide des technologies. »

Neoli : pouvez-vous nous partager des exemples concrets d'actions permettant de lutter contre la fraude à l'assurance ?

Xuan : « La base MDDA (mise à disposition des données automobiles) permet à AXA France et à d'autres assureurs de mutualiser leurs données pour détecter des réseaux de fraude, couvrant environ 60% du marché français. Des scénarios de détection sont appliqués sur l'ensemble de ces données pour identifier des comportements suspects. »

Neoli : à quelle typologie de fraude faites-vous essentiellement face ?

Xuan : « La majorité des tentatives de fraude sont opportunistes (petits montants, sinistres exagérés), tandis que les réseaux organisés visent parfois des sinistres plus importants mais restent minoritaires en volume. La surveillance est adaptée en fonction du canal (agence ou en ligne), les assureurs en ligne étant plus exposés à la fraude dématérialisée. »

Neoli : comment vous organisez-vous pour les contrer ?

Xuan : « Les équipes sont formées à la gestion de la relation client, à la communication sur les contrôles antifraude et à la gestion du stress, afin de maintenir une expérience client satisfaisante même lors de vérifications renforcées. La posture client est travaillée pour expliquer la nécessité des contrôles sans stigmatiser les clients honnêtes.

Aussi, la détection de la fraude permet d'identifier les défaillances dans les parcours clients et les systèmes applicatifs, ce qui alimente une démarche d'amélioration continue des contrôles et de la qualité des parcours, en automatisant autant que possible les vérifications pour limiter les interventions humaines et les risques d'erreur.

Il est primordial de trouver un équilibre entre la sécurité des parcours (pour éviter la fraude) et la fluidité de l'expérience client, en évitant de rendre les démarches trop contraignantes pour les clients. »

Elodie Hasbrouck, Manager Pôle Accompagnement Conformité Santé & Prévoyance - SwissLife

Neoli : pouvez-vous décrire la stratégie de votre entreprise en matière de lutte contre la fraude ?

Elodie : « La stratégie de lutte contre la fraude repose sur une organisation différenciée selon les métiers, en particulier entre la santé et la prévoyance. En prévoyance, le dispositif s'appuie sur des référents fraude intégrés dans les équipes opérationnelles, avec un ou deux référents par équipe, surtout en prestation, qui conservent avant tout une expertise métier et traitent la fraude en complément de leurs missions principales. En santé, une évolution récente a été engagée avec la création d'une équipe dédiée à la fraude depuis le 1er janvier, dotée d'un management identifié, afin d'harmoniser les pratiques et de mieux piloter les actions. »

Neoli : quels outils technologiques ou solutions utilisez-vous pour détecter et prévenir la fraude ?

Elodie : « Le dispositif repose sur plusieurs briques complémentaires : des alertes inter-assureurs via Alfa, des moniteurs internes qui génèrent des alertes chaque nuit selon certains critères, des signalements internes et des tableaux de bord data permettant d'identifier des comportements atypiques. Ces outils constituent avant tout des aides à la détection et à la priorisation, et non des systèmes de décision autonomes. »

Neoli : depuis la mise en place de ces dispositifs, quelles améliorations avez-vous constatées ?

Elodie : « Les principales améliorations portent sur l'enrichissement progressif de la donnée disponible dans les systèmes. De nouvelles informations sont désormais saisies, comme les numéros de dent, de finess ou de prescripteur, ce qui permet de commencer à disposer de bases pour faire des croisements plus utiles. La donnée est identifiée comme un levier central, la data étant vraiment l'essence même du dispositif. »

Neoli : comment s'articule la collaboration interne dans la lutte anti-fraude ?

Elodie : « La lutte contre la fraude repose sur une collaboration étroite entre les équipes de gestion, les référents fraude, le pôle conformité, et une cellule fraude transverse. Cette cellule joue principalement un rôle de pilotage et de coordination transverse. Cette organisation permet de conjuguer cohérence d'ensemble et expertise métier. »

Neoli : selon vous, quels sont les facteurs clés qui permettent d'améliorer efficacement la détection de fraude ?

Elodie : « Plusieurs leviers apparaissent déterminants : la qualité de l'expertise métier, la montée en puissance des équipes data, l'existence d'un budget projet dédié à la fraude et le recours à des experts conseils. La donnée constitue la base du dispositif, mais l'expertise humaine reste indispensable, et le fait de disposer d'un budget projet dédié à la fraude piloté en interne est un point structurant. »

Neoli : quels sont aujourd'hui les principaux défis ou obstacles rencontrés ?

Elodie : « Les défis portent principalement sur la volumétrie élevée de signalements, le retard historique sur certaines données non saisies, la difficulté à industrialiser certains processus et les contraintes réglementaires fortes. Même avec des renforts, l'ensemble des signalements ne pourra pas être traité rapidement, et les contraintes sur l'utilisation des données structurent fortement les dispositifs. »

Neoli : comment équilibrez-vous l'automatisation et l'intervention humaine ?

Elodie : « Les outils automatisés sont utilisés comme des aides à la détection et à la priorisation, mais la décision finale reste toujours humaine, en particulier pour les dossiers sensibles. Les outils ressortent des doutes mais jamais des certitudes, et le collaborateur reste toujours indispensable pour instruire le dossier. »

Neoli : avez-vous observé une évolution des méthodes de fraude en réaction à vos pratiques de détection ?

Elodie : « Il est difficile de distinguer entre une augmentation réelle de la fraude et une amélioration des capacités de détection. La question de savoir s'il y en a plus ou si l'on détecte simplement mieux reste ouverte, certaines fraudes organisées existant de longue date et restant complexes à caractériser. »

Neoli : quels sont vos projets ou besoins futurs pour renforcer la lutte contre la fraude ?

Elodie : « Les priorités portent sur la poursuite de l'enrichissement de la donnée, la structuration des processus, le renforcement de l'expertise métier et l'utilisation de l'IA comme outil d'aide à la lecture et à la priorisation. Avant d'automatiser davantage, il est jugé nécessaire de consolider d'abord l'organisation et la donnée. »

Neoli : quelle a été la perception de l'arrivée de l'IA par vos gestionnaires ?

Elodie : « L'arrivée des outils d'aide à la détection est perçue comme un soutien au travail des gestionnaires plutôt que comme une remise en cause de leur rôle. L'IA est vue comme un outil d'assistance qui ne remplacera jamais le collaborateur mais vient compléter son analyse. »

Neoli : en prévoyance, quels sont aujourd'hui les principaux freins techniques à une détection plus automatisée ?

Elodie : « En prévoyance, la détection repose encore largement sur l'expertise des collaborateurs et les signalements externes, faute de données structurées dans les systèmes. Historiquement, en dehors de l'expertise humaine et d'Alfa, il n'existait quasiment aucun moyen de détection automatisée. »

Neoli : avant l'automatisation, quels chantiers d'industrialisation des processus vous paraissent prioritaires ?

Elodie : « Avant d'aller plus loin dans l'automatisation, un important travail de standardisation des pratiques est nécessaire, notamment sur les demandes de pièces et les courriers. Aujourd'hui, il n'existe pas de demande de pièce type, chacun produisant encore ses propres modèles, et certaines demandes de pièces médicales sont encore faites par mail, ce qui doit être corrigé. »

Neoli : avez-vous mis en place des dispositifs spécifiques dès la souscription pour prévenir certains risques ?

Elodie : « Un dispositif spécifique a été mis en place sur certaines souscriptions, notamment celles issues de néobanques, afin de sécuriser les flux et limiter les risques d'impayés et de fraude. Dès qu'une souscription provient d'une néobanque, le dossier est mis en attente et des justificatifs renforcés sont demandés, avec parfois la demande d'un autre RIB qu'un RIB de néobanque. »

Neoli : comment gérez-vous les situations où la lutte contre la fraude croise des enjeux internes sensibles ?

Elodie : « Certaines situations internes ont conduit à faire évoluer l'organisation, notamment sur la gestion de certains contrats spécifiques, afin de limiter les risques organisationnels et préserver la confidentialité des données. Le fait que des personnes aient connaissance des pathologies et des salaires de leurs collègues n'était pas satisfaisant, et la meilleure solution a été de ne plus gérer directement ces contrats. »

Eric Sibony, CSO & Co-fondateur – Shift Technology

Neoli : sur quel constat fort s'est construit la proposition de valeur initiale de Shift Technology ?

Eric : « Elle s'est construite à partir d'un constat terrain : le principal problème rencontré par les assureurs dans la lutte contre la fraude n'était pas uniquement la capacité à détecter des cas suspects, mais la difficulté des équipes d'investigation à comprendre pourquoi un dossier était suspect et comment agir concrètement. Les solutions existantes permettaient d'identifier des anomalies, mais apportaient peu d'éléments réellement exploitables pour les gestionnaires fraude, ce qui limitait leur capacité à maximiser les économies liées à la fraude. »

Neoli : dans vos déploiements, quelle est aujourd'hui la principale limite à la création de valeur : la technologie, la donnée ou l'organisation des assureurs ?

Eric : « Les échanges montrent que la principale limite à la création de valeur ne vient pas prioritairement de la technologie. L'organisation des équipes antifraude et la structuration des dispositifs internes jouent un rôle déterminant dans la performance des solutions. Les meilleurs résultats sont observés lorsque les équipes fraude sont centralisées, expérimentées et organisées de manière cohérente, ce qui leur permet de tirer pleinement parti des informations produites par les outils.

Ce constat rejoint également les analyses de Neoli, qui identifie l'organisation et la qualité des données comme deux enjeux structurants de la performance des dispositifs antifraude. »

Neoli : selon vous, en quoi la qualité des données côté assureur est-elle un prérequis important dans le succès de l'implémentation d'une solution IA ?

Eric : « La qualité des données est un prérequis important, mais Shift a fait le choix d'investir fortement sur ce sujet afin de ne pas dépendre exclusivement du niveau de maturité data des assureurs. L'entreprise a consacré des moyens significatifs au nettoyage, à la structuration et à l'exploitation de données de qualité variable, y compris sur des tâches moins valorisées comme la récupération de documents issus de systèmes de GED hétérogènes.

Shift n'a jamais rencontré de situation où les données étaient totalement inutilisables, même si l'absence de certaines données fournies par les assureurs peut limiter la performance des modèles. Dans cette logique, Shift propose de restituer aux assureurs les données enrichies et nettoyées, généralement via des exports par batch, même si peu d'acteurs mettent aujourd'hui en place les intégrations nécessaires pour les réinjecter pleinement dans leur système d'information. »

Neoli : quelles grandes tendances observez-vous aujourd'hui dans l'évolution de la fraude à l'assurance côté fraudeur, notamment avec l'essor des nouvelles technologies ?

Eric : « Deux grandes tendances se dégagent clairement dans l'évolution récente de la fraude à l'assurance. La première concerne l'utilisation croissante de l'IA par les fraudeurs pour générer de faux documents ou de fausses images, ce qui facilite la production de justificatifs frauduleux à grande échelle.

La seconde tendance est une professionnalisation accrue de la fraude, avec l'émergence de réseaux structurés impliquant des acteurs professionnels, comme certains réparateurs ou professionnels de santé. Ces pratiques existaient déjà, mais elles deviennent plus organisées, plus industrielles et plus difficiles à détecter lorsqu'on se limite à l'analyse d'un sinistre isolé. »

Neoli : face à ces évolutions, comment adaptez-vous vos modèles et votre produit pour répondre à ces nouvelles formes de fraude ?

Eric : « Pour faire face à ces nouvelles formes de fraude, Shift développe des modèles spécifiques dédiés à la détection de contenus frauduleux, notamment les faux documents ou images générés par IA. Ces modèles sont régulièrement évalués et benchmarkés afin de maintenir leur efficacité dans un contexte où les techniques de fraude évoluent rapidement.

La détection ne repose plus uniquement sur l'analyse d'un document pris individuellement, mais sur une approche élargie intégrant davantage de contexte, de relations entre acteurs et de schémas de comportement, ce qui permet de mieux identifier des réseaux ou des pratiques frauduleuses organisées. »

Neoli : quel impact l'IA a-t-elle eu jusqu'à présent sur les capacités de détection de la fraude ?

Eric : « L'IA a permis d'améliorer les résultats en matière de détection de la fraude. Shift a commencé par utiliser l'IA sur des périmètres ciblés, comme le nettoyage et la structuration des données, avant de progresser vers des usages plus avancés sur certaines étapes du traitement. Les avancées récentes en IA générative ont permis un saut qualitatif important, tout en nécessitant un travail de calibration pour garantir la fiabilité et la robustesse des résultats. »

Neoli : selon vous, à quoi pourrait ressembler la lutte contre la fraude à l'assurance dans cinq ans ?

Eric : « À horizon cinq ans, la lutte contre la fraude pourrait évoluer vers un environnement où assureurs et assurés utiliseraient chacun des agents IA. Cette perspective pose la question de la manière dont ces agents interagiront, voire s'opposeront, dans un contexte où la fraude et sa détection seront de plus en plus automatisées.

Cette évolution hypothétique soulève des enjeux majeurs en matière de gouvernance, de régulation et de place de l'intervention humaine dans les dispositifs antifraude. »

Thomas Puydoyeux, Chef de projets Data – Doc Vérif

Neoli : sur quel besoin initial s'est construit la solution DocVerif ?

Thomas : « DocVerif a été développé pour répondre principalement à la fraude sur les titres d'identité, notamment les cartes nationales d'identité, passeports et titres de séjour. L'outil a été mis en production dès 2016, puis enrichi en 2023 avec une fonctionnalité supplémentaire permettant de vérifier la concordance entre le nom et le premier prénom. L'objectif dès l'origine était de permettre aux organisations de vérifier l'authenticité d'un titre directement à la source, via la base souveraine des titres électroniques sécurisés de l'État, avec des données à jour en temps réel. »

Neoli : comment fonctionne concrètement DocVerif et à qui s'adresse-t-il ?

Thomas : « DocVerif est structuré en deux environnements distincts. Le premier est réservé aux forces de l'ordre, qui peuvent interroger directement la base nationale pour obtenir les informations d'un titre et son statut de validité. Le second est destiné aux acteurs privés et publics comme les banques, assurances ou administrations. Sur les six plus grandes banques françaises, cinq utilisent déjà DocVerif, et l'outil est également utilisé via des dispositifs interprofessionnels comme ALFA. Certains partenaires dépassent un million d'interrogations par an, ce qui montre que la solution est conçue pour fonctionner sur de très fortes volumétries. »

Neoli : comment DocVerif s'intègre-t-il dans les parcours clients des organisations ?

Thomas : « Historiquement, l'outil a d'abord été utilisé par des équipes fraude de second niveau, puis, une fois maîtrisé, il est progressivement intégré dans des processus automatisés. Techniquement, l'API DocVerif est simple à utiliser ; la complexité se situe surtout côté partenaire, dans l'intégration au système d'information et dans la manière dont les réponses sont exploitées pour déclencher des décisions, comme accepter, bloquer ou renforcer un contrôle. »

Neoli : quelles informations sont nécessaires pour interroger DocVerif et quels types de réponses sont renvoyés ?

Thomas : « Pour interroger le service, il faut renseigner le type de titre, son numéro et sa date de délivrance. Cette exigence garantit que l'acteur dispose bien du document complet et évite les cas où seul le recto circulerait. Le système renvoie ensuite différents statuts : valide si le titre est valable, invalide s'il ne l'est plus, ou inconnu si le titre n'existe pas dans la base ou ne correspond à aucun enregistrement. Ce statut inconnu n'indique pas automatiquement une fraude, mais constitue un signal fort. Une vérification supplémentaire peut aussi être faite sur la concordance nom / prénom, avec un retour conforme ou non conforme. »

Neoli : quels gains concrets ont été observés chez les organisations utilisatrices ?

Thomas : « Certains partenaires bancaires ont observé un changement très significatif après l'intégration de DocVerif, passant d'environ trois fraudes détectées par jour à environ trente. La valeur dépend toutefois fortement de la capacité des équipes à interpréter correctement les résultats. L'analyse repose sur des combinaisons de statuts, par exemple un titre valide mais avec une identité non conforme crée une suspicion, tandis qu'un titre invalide et non conforme constitue une alerte maximale. La formation à la lecture de ces statuts est donc un facteur clé d'efficacité. »

Neoli : quelle est la nature institutionnelle du dispositif DocVerif ?

Thomas : « DocVerif s'inscrit dans un cadre fortement institutionnel. La convention d'utilisation est tripartite entre le ministère de l'Intérieur, France Titres et l'organisation partenaire. Le service est directement connecté à la base nationale des titres d'identité, ce qui garantit un niveau de fiabilité élevé puisque les informations proviennent de la source officielle. »

Neoli : quel rôle joue l'IA par rapport à une solution comme DocVerif ?

Thomas : « DocVerif n'est pas une solution d'analyse d'image mais une solution de vérification à la source. Là où l'IA peut analyser un document en étudiant son apparence, ses métadonnées ou ses zones lisibles, DocVerif fournit une réponse référente car elle interroge directement la base maître de l'État. Dans ce sens, l'outil peut être complémentaire aux solutions d'IA, voire rendre certaines briques d'analyse moins nécessaires pour la vérification de titres officiels. »

Neoli : quels freins à l'adoption observez-vous chez les organisations ?

Thomas : « Le principal frein n'est pas la qualité de la donnée, qui constitue justement la force du dispositif. Les obstacles peuvent être d'ordre organisationnel ou économique. Certains acteurs peuvent ne pas avoir toujours intérêt à lutter contre la fraude au maximum lorsqu'ils privilégient des logiques de volume. L'argument du coût est parfois évoqué, même si la rentabilité est généralement rapide : une fraude bancaire moyenne représentant environ douze mille euros, un déploiement peut être amorti rapidement au regard des gains. »

Neoli : constatez-vous une évolution récente de la fraude documentaire liée aux nouvelles technologies ?

Thomas : « Oui, une évolution nette est observée avec l'arrivée de documents falsifiés générés par intelligence artificielle, très crédibles visuellement. Toutefois, ces faux documents ne passent pas les contrôles DocVerif, car ils ne correspondent pas à des titres existant réellement dans la base officielle. Dans la pratique, ce sont souvent les établissements bancaires eux-mêmes qui partagent des exemples de fraudes que l'outil a permis d'éviter. »

Neoli : quel rôle joue le 2D-Doc dans la lutte contre la fraude documentaire ?

Thomas : « Le 2D-Doc constitue un levier complémentaire important. Il s'agit d'un QR code contenant les informations d'un document et signé électroniquement. Toute modification du contenu invalide la signature, ce qui rend la falsification impossible. Lors d'un contrôle, il suffit de lire le code et de comparer les données avec celles affichées sur le document. Cette technologie est déjà utilisée pour certains documents comme les avis d'impôt, et elle est appelée à s'étendre à d'autres justificatifs, avec à terme plusieurs dizaines de formats compatibles. »

Neoli : selon vous, quelles seront les grandes tendances de la lutte contre la fraude documentaire dans les prochaines années ?

Thomas : « L'avenir devrait s'appuyer de plus en plus sur les wallets numériques et les attributs d'identité certifiés comme preuves authentiques. Toutefois, leur adoption sera progressive et ne concernera pas immédiatement l'ensemble de la population. Dans ce contexte, les solutions existantes comme DocVerif ou 2D-Doc devraient rester durablement pertinentes. L'évolution reste difficile à anticiper précisément, car les fraudeurs innovent très rapidement et les nouvelles technologies, notamment l'IA, ne devraient pas simplifier la situation. »

V.

Limites, enjeux éthiques et perspectives

Si l'intelligence artificielle offre indéniablement des gains pour la lutte anti-fraude, elle soulève également des questions et des limites qu'il convient d'anticiper. L'algorithme n'est pas infaillible ni neutre par essence. De plus, le cadre légal et éthique doit être respecté scrupuleusement pour que ces nouveaux outils s'inscrivent dans une démarche responsable et acceptée de tous. Enfin, l'évolution vers une fraude "augmentée à l'IA" pose la question de la place de l'humain et de la gouvernance à adopter. Dans cette partie, nous abordons successivement : (01) les risques de biais algorithmiques et d'atteinte à l'équité, (02) les enjeux juridiques et réglementaires (RGPD, preuve, etc.), et (03) la nécessité d'une gouvernance responsable de l'IA antifraude, conciliant efficacité et respect des droits.

01. Limites, enjeux éthiques et perspectives

Un algorithme d'IA n'est pas magique : il apprend des données du passé, avec leurs qualités et leurs défauts. Il y a donc un risque que les modèles de détection de fraude introduisent des biais et aboutissent à des décisions injustes ou discriminatoires envers certains assurés, de manière involontaire. Ce point est crucial, car il touche à l'équité de traitement et peut entraîner des conséquences éthiques et juridiques.

- **Sources de biais possibles :** les biais peuvent provenir des données d'entraînement ou de la conception du modèle. Par exemple, si historiquement on a détecté plus de fraudes dans telle population (disons, les jeunes conducteurs de certaines zones urbaines), l'algorithme pourrait en conclure que ces caractéristiques sont hautement prédictives de fraude et sur-scorer négativement ces profils. Même si l'âge ou le code postal ne sont pas explicitement mis comme facteurs (ce qui serait illégal si cela conduit à de la discrimination arbitraire), ils peuvent être corrélés à d'autres variables utilisées. On parle de biais proxy. **Un autre biais classique est le manque de représentativité** : si le modèle n'a pas assez vu de cas de sinistres provenant d'une minorité donnée, il pourrait mal juger ces dossiers (erreurs plus fréquentes). Dans d'autres secteurs, on a vu des IA de reconnaissance faciale moins fiables pour les personnes de couleur faute de données diversifiées. En assurance, il faut veiller à ce que l'IA ne pénalise pas indûment des profils socio-économiques vulnérables, par exemple.

01. Limites, enjeux éthiques et perspectives

- **Exemple de dérive :** un cas emblématique hors assurance est celui d'un algorithme déployé par la ville de Rotterdam pour détecter la fraude aux aides sociales. Il scorait les allocataires selon un risque de fraude. Il s'est avéré qu'il classait "à risque élevé" de nombreuses femmes issues de minorités ethniques, en partie du fait de critères biaisés, ce qui a mené à des contrôles intrusifs injustifiés sur ces populations. Face au tollé, le système a été suspendu. Transposé à l'assurance, on pourrait imaginer un modèle qui, par inadvertance, suspecterait plus souvent tel type d'assuré (par ex. résidant dans tel quartier défavorisé) parce que les données historiques liaient fraude et précarité alors que bien sûr, la majorité des gens précaires ne fraudent pas. **Il est illégal et moralement inacceptable de discriminer sur des critères protégés** (origine, genre, etc.), même indirectement. Or, un algorithme mal encadré pourrait le faire de facto.

- **Transparence et explicabilité :** pour prévenir ces écueils, il est important que les assureurs exigent de leurs solutions IA une certaine **transparence**. Cela signifie pouvoir expliquer pourquoi un dossier a été marqué suspect. Par exemple, être capable de dire "ce sinistre a été noté à risque car le montant réclamé est très élevé par rapport à la moyenne pour ce type de dommage, et car le même appareil a déjà fait l'objet d'un sinistre récemment". Si jamais la raison était "parce que la personne habite tel quartier + profil X", cela devrait alerter. Des efforts sont faits par les éditeurs pour fournir des **explications compréhensibles** à leurs modèles (on parle de XAI, eXplainable AI). FRISS, par exemple, travaille sur l'amélioration des explications fournies par son IA en partenariat avec Microsoft. **L'explicabilité** est non seulement une exigence réglementaire (le RGPD prône le droit à une explication pour les décisions automatisées significatives), mais aussi un outil de détection des biais. Si une explication met en avant un critère problématique, on peut ajuster le modèle.

- **Éviter les critères prohibés :** évidemment, un modèle antifraude ne devrait jamais utiliser directement des critères comme l'ethnie, la religion, etc. (d'ailleurs l'assureur ne les connaît pas officiellement). Mais il doit aussi éviter d'en faire des **substituts**. Par exemple en assurance auto, on sait que le Code des assurances n'autorise pas la tarification selon l'origine ou l'ethnie, de même pour la détection de fraude, on ne saurait tolérer des modèles qui cibleraient en pratique certains groupes protégés. Il y a un travail de **test de biais** à effectuer sur les algorithmes : simuler des cas et voir s'il y a un traitement différentiel non justifié. Des organismes comme le Défenseur des droits en France soulignent que les **données historiques** peuvent encapsuler des discriminations passées, et qu'il faut donc être vigilant pour ne pas les reproduire via l'IA.

01. Limites, enjeux éthiques et perspectives

- **Équité vs efficacité :** il existe parfois des cas où améliorer l'efficacité de détection semble entrer en conflit avec l'équité. Par exemple, si statistiquement un type de contrat présente 10 fois plus de fraudes, le modèle va fortement pondérer ce facteur. Mais cela veut dire aussi potentiellement suspecter 10 fois plus les clients de ce type, dont une majorité sont innocents. L'assureur doit ajuster sa stratégie de profiling. Il s'agit d'un débat éthique. L'enjeu réside en **l'identification d'un maximum de fraude** sans discriminer de population spécifique.

  L'approche recommandée est de mitiger ces biais : par exemple, imposer dans le modèle une forme de normalisation **pour ne pas trop impacter un groupe particulier**, ou ajouter des variables de contexte pour affiner (peut-être que dans ce groupe, la fraude était surtout le fait d'un segment particulier, etc.).

- **Surveillance humaine :** ces biais mettent en exergue l'importance de garder un humain "dans la boucle" qui puisse avoir du recul critique. Un algorithme antifraude doit être vu comme un assistant, pas un oracle incontestable. La compagnie doit mettre en place un suivi des performances du modèle, non seulement en % de fraude détectée, mais aussi en vérifiant qu'il ne génère pas de traitements inéquitables.

Ce qu'il faut retenir

→ Les algorithmes anti-fraude doivent impérativement être maîtrisés pour éviter les biais. Un modèle d'IA apprend des données historiques, qui peuvent refléter des biais (corrélations entre fraude et certains profils). **Sans garde-fous, on risquerait de cibler injustement certains assurés** (par ex. selon l'âge, le revenu, la localisation) sur la base de stéréotypes data. Cela serait contraire à la loi et à l'éthique. Il faut donc tester et rendre explicables les décisions pour détecter tout effet indésirable.

→ Les assureurs mettent en place des **chartes éthiques** et **des contrôles** pour s'assurer que l'IA demeure impartiale et ne reproduit pas de discrimination. La transparence envers le client (explications en cas de suspicion) est aussi un moyen de s'assurer qu'on peut **justifier proprement les alertes**. En somme, "efficacité" ne doit pas rimer avec "injustice" : l'IA antifraude de confiance est celle qui attrape les tricheurs sur leurs actes, sans biais cognitifs.

02. Problématiques juridiques et réglementaires

L'utilisation de l'IA dans la lutte contre la fraude s'insère dans un cadre légal qu'il convient de respecter scrupuleusement, sous peine de voir sa démarche invalidée, voire de s'exposer à des sanctions. Plusieurs volets du droit sont à considérer : **la protection des données personnelles (RGPD)**, les règles sectorielles (Code des assurances, obligations TRACFIN), le droit de la preuve et les libertés individuelles (droit à l'explication, à l'erreur). Passons en revue les principaux enjeux juridiques :

- **Protection des données (RGPD) :** les assureurs manipulent des quantités de données clients, parfois sensibles (santé, etc.). Le RGPD impose que tout traitement (y compris par IA) ait une base légale, une finalité déterminée et proportionnée. La lutte contre la fraude est reconnue comme un **intérêt légitime** de l'entreprise, qui peut justifier la collecte et le traitement de données à cette fin. Cependant, les principes de **minimisation et de proportionnalité** s'appliquent : on ne peut exploiter que les données pertinentes et nécessaires. Par exemple, aller fouiller sans discernement les réseaux sociaux d'un client serait excessif si on n'a pas de suspicion fondée.

  De plus, le RGPD encadre les **décisions automatisées** ayant un effet juridique ou significatif sur les individus (article 2255). Bloquer ou résilier un contrat sur la seule base d'un score algorithmique de fraude pourrait être contesté si aucune intervention humaine n'a eu lieu. En pratique, les assureurs veillent à conserver une **revue humaine** pour les décisions négatives importantes (refus d'indemnisation pour fraude par ex.), ce qui les sort du champ de l'article 22 strict. Néanmoins, ils doivent informer les personnes de l'existence de ces traitements antifraude. Il n'est pas rare de voir dans les notices RGPD des assureurs une mention du type « des traitements automatisés peuvent être utilisés pour évaluer le risque de fraude lors de la souscription ou du sinistre ».

  Le RGPD confère aussi **un droit d'accès et de rectification aux personnes**. Un assuré peut s'interroger sur les données et règles qui ont conduit à le suspecter. Dans ce cas, l'assureur doit être en mesure de fournir une réponse compréhensible, sans révéler ses secrets industriels mais en apportant les facteurs généraux (par ex. "votre déclaration présentait des incohérences factuelles qui ont entraîné un examen approfondi"). C'est un équilibre délicat entre transparence et confidentialité des critères.

  Enfin, toute donnée utilisée doit être conservée selon des durées conformes. Les données des fraudeurs présumés ne peuvent être conservées éternellement, sauf à les anonymiser dans des statistiques globales. La CNIL en France encourage ainsi les acteurs à documenter leurs traitements IA, à faire des **analyses d'impact** (AIPD) lorsque c'est nécessaire, et à mettre en place des mesures pour contrôler les dérives.

02. Problématiques juridiques et réglementaires

- **Droit à l'erreur et traitement des faux positifs :** un concept apparu en 2018 dans le droit français (Loi « pour un État au service d'une société de confiance ») est **le droit à l'erreur** pour les administrés dans leurs déclarations, sans sanction immédiate s'ils régularisent de bonne foi. Les outils d'IA peuvent parfois signaler un dossier "suspect" alors qu'il s'agit d'une confusion ou omission non volontaire de l'assuré (ex : un assuré déclare un ancien dommage en pensant qu'il est couvert, sans intention de frauder). Les assureurs ont intérêt à traiter ces faux positifs avec discernement, en donnant la possibilité au client de s'expliquer et de corriger. Cela rejoint l'idée du **droit à l'explication** : si un client est dans le collimateur, on doit pouvoir lui demander des justifications complémentaires, et le disculper s'il clarifie la situation. Par exemple, un sinistre auto tardivement déclaré peut être perçu comme suspect (car fraude fréquente), mais si le client prouve qu'il était hospitalisé et n'a pu déclarer avant, on doit le considérer. L'IA ne connaît pas ce contexte, **d'où l'importance de l'appréciation humaine** pour laisser place à l'erreur de bonne foi. Sur le plan juridique, si l'assureur refusait indûment une indemnisation sur base d'un soupçon non avéré, il pourrait se voir condamné pour non-respect du contrat. Donc, il faut bien calibrer son processus : **suspicion => enquête => décision avec preuves.**

- **Admissibilité des preuves et procédures :** si un assureur découvre une fraude via l'IA, par ex. l'algorithme détecte que le document fourni est faux, cela reste **une présomption** technique. Pour refuser d'indemniser, l'assureur s'appuiera sur une clause contractuelle (fausse déclaration) et devra idéalement **constituer une preuve recevable**. Un rapport technique de l'outil (ex. Finovox) peut être un élément de preuve, mais souvent on cherchera à le corroborer (par ex. en contactant l'émetteur supposé du document pour confirmer qu'il est faux). En cas de contentieux, le juge appréciera la validité de ces éléments. Un juge pourrait refuser une preuve obtenue de manière déloyale ou non transparente pour l'assuré. Par exemple, si l'assureur utilisait en secret des données privées du client (comme des photos Facebook non publiques obtenues en se faisant passer pour un ami), ce moyen pourrait être jugé illicite et la preuve écartée. En revanche, une analyse algorithmique interne bien documentée, non intrusive, peut être tout à fait acceptée comme indice. Il n'y a **pas de jurisprudence massive** encore sur l'IA antifraude, mais par analogie avec d'autres domaines, les tribunaux exigent de plus en plus de pouvoir **comprendre le raisonnement** qui a mené à une décision. L'assureur devra présenter les faits concrets mis en évidence (ex : incohérences, multi-déclarations, etc.). Aussi, **la formation du personnel est importante** : un gestionnaire ne peut pas justifier la fraude en mettant en avant le scoring auprès du fraudeur. Sur le plan pénal, si un dossier est amené en justice (ex. l'assureur porte plainte), les preuves doivent être recueillies légalement pour être recevables. Par exemple, enregistrer à l'insu du client un aveu serait illicite. En somme, l'IA sert à orienter les recherches de preuve, mais ne peut être la seule preuve.

02. Problématiques juridiques et réglementaires

- **Cadre européen (AI Act) :** le Règlement (UE) 2024/1689 « **AI Act** » est en vigueur depuis le **1er août 2024**. Il instaure une approche fondée sur les risques avec des obligations graduées et un calendrier d'application échelonné : interdictions depuis février 2025, obligations pour les modèles GPAI (d'IA à usage général) en août 2025, et majorité des obligations (dont la plupart des usages haut risque) en août 2026, avec un délai jusqu'à août 2027 pour certains systèmes intégrés à des produits régulés. Pour l'assurance, l'évaluation du risque et la tarification en vie/santé relèvent du haut risque (Annexe III), alors que la détection de fraude financière bénéficie d'une exception dans le périmètre "solvabilité/crédit". Les superviseurs (ex. ACPR) insistent déjà sur une **gouvernance robuste de l'IA** (traçabilité, supervision, explicabilité), ce qui plaide pour **anticiper** conformité et contrôles dès maintenant.

Ce qu'il faut retenir

→ Le déploiement de l'IA antifraude doit se faire dans le strict respect du cadre légal. Du côté données personnelles, l'assureur doit veiller au RGPD : utiliser les données de manière légitime et proportionnée, informer les clients, et garder un contrôle humain sur les décisions importantes (un refus d'indemnisation ne doit pas être purement algorithmique). Le droit à l'explication implique de pouvoir justifier les décisions : on ne peut se retrancher derrière une "boîte noire". Les soupçons détectés par l'IA doivent être confirmés par des preuves recevables avant sanction : **l'IA sert d'outil d'orientation, pas de juge final**.

→ Il faut aussi laisser une place à l'erreur de bonne foi : distinguer le fraudeur intentionnel du client négligent, et offrir des recours/explications. Les interactions avec TRACFIN et les autorités doivent être gérées en suivant les procédures légales (secret, etc.). En somme, l'IA doit s'insérer dans un processus conforme aux droits des assurés : transparence, non-discrimination, possibilité de contestation. Les régulateurs y veillent de près, et un assureur aurait tout à perdre à outrepasser ces lignes rouges (risque de sanctions CNIL, de perte de confiance, etc.). La confiance dans l'IA se bâtit aussi ainsi : en montrant qu'elle est utilisée de façon responsable et encadrée, non comme une autorité arbitraire.

03. Vers une gouvernance responsable de l'IA antifraude

Au vu de tout ce qui précède, il apparaît que le succès d'une démarche d'IA antifraude ne repose pas uniquement sur la technologie, mais aussi sur l'humain, l'organisation et l'éthique autour. Il s'agit d'instaurer une gouvernance responsable de ces nouveaux outils. Voici les axes à considérer pour y parvenir :

- **Encadrement éthique et principes directeurs :** comme évoqué, de plus en plus d'assureurs formalisent des chartes éthiques de l'IA. CNP Assurances, par exemple, a nommé un "Responsable éthique de l'IA" et créé un comité pluridisciplinaire sur le sujet. Ils se sont dotés de **5 principes de conduite pour l'IA** : transparence, équité, usage responsable (fiabilité, contrôle des impacts), protection des données, et humain au cœur. Ces principes guident tous les projets, dont celui de la fraude. Ce genre d'instance de gouvernance, impliquant conformité, direction des risques, DSI, direction métier, est indispensable pour arbitrer les dilemmes. Par exemple, décider du seuil de score à partir duquel on bloque un paiement est autant une question de risque que de relation client : une gouvernance collective permet de trouver l'équilibre. L'éthique doit aussi être communiquée aux équipes opérationnelles : **la fin** (attraper des fraudeurs) **ne justifie pas n'importe quel moyen**. Un enquêteur ne peut scruter la vie privée d'un assuré sur Facebook sans cadre légal. La culture d'entreprise doit intégrer ces limites.

- **Place de l'humain dans le dispositif :** l'humain est au cœur des dispositifs antifraude. Ainsi, il convient de définir les moments de parcours pour lesquels l'intervention humaine est obligatoire. Concrètement et pour exemple, une alerte rouge d'IA doit être revue par un analyste avant décision finale. L'humain doit décider de dénoncer un assuré pour tentative de fraude. Cela permet de garder du discernement et de gérer les cas particuliers. **L'humain reste le lien privilégié** avec le client. Ainsi, il peut être amené à s'entretenir avec le client soupçonné de fraude et à évaluer, selon son ressenti, la bonne foi de celui-ci. Ce travail a fortiori humain, ne peut être assuré par une machine. L'IA sert d'assistant et non de remplaçant. Elle tend à montrer une complémentarité : **l'IA fait le tri et la pré-analyse, ce qui libère du temps aux gestionnaires pour des tâches à plus forte valeur ajoutée** (enquêtes terrain, entretiens, montage de dossiers juridiques…).

- **Transparence vis-à-vis des clients :** une gouvernance responsable implique également de traiter les clients avec respect et transparence. Cela ne veut pas dire révéler tous les secrets de nos algorithmes (au risque de les rendre inefficaces). Mais ça peut passer par de la pédagogie sur le fait que l'assureur lutte activement contre la fraude pour préserver l'équité. Par exemple, certains assureurs communiquent dans leurs rapports publics le montant de fraude détecté, les moyens mis en œuvre, etc., ce qui envoie un **signal de dissuasion aux fraudeurs** et de rassurance aux honnêtes (on protège la mutualité). En cas de litige individuel, être transparent veut dire expliquer au client suspecté quels éléments posent problème, et l'écouter. Cette transparence s'arrête là où commence la confidentialité nécessaire.

03. Vers une gouvernance responsable de l'IA antifraude

- **Mesure et suivi des performances :** une bonne gouvernance, c'est mesurer ce qu'on fait. Il faut donc suivre des **KPIs** non seulement de succès de l'IA (taux de fraude détectée, ratio faux positifs, économies…) mais aussi des **KPIs de qualité** (par ex. taux de réclamations clients sur soupçons infondés, délais induits par les contrôles, etc.). Le dispositif antifraude ne doit pas alourdir de façon significative les parcours et processus en place. La gouvernance implique donc un **pilotage fin** : trouver le bon calibrage entre laxisme (laisser filer de la fraude) et excès de zèle (voir de la fraude partout).

- **Collaboration sectorielle et retours d'expérience :** une approche responsable implique un effort collectif. Des **lignes directrices communes** au secteur assurantiel sur l'usage de l'IA en assurance, notamment antifraude, pourraient permettre aux acteurs de s'accorder. Ainsi, nous pourrions imaginer un document intégrant les fondamentaux exprimés à travers cette étude : vérifier les biais, conserver du contrôle humain, etc. Ces lignes directrices s'inscriraient dans une logique d'homogénéisation des pratiques et pourraient limiter les risques réputationnels en cas de dérives de certains acteurs. Les régulateurs pourraient également réfléchir à la mise en place de **label** ou d'**audit externe** des algorithmes anti-fraude, en s'assurant qu'ils respectent bien les critères de conformité et d'éthique. Cette transparence sectorielle serait un gage de confiance pour les assurés. Déjà, l'ACPR publie des travaux sur l'IA dans la finance, concluant qu'il faut *"veiller à des modèles transparents, impartiaux et éthiques"*[63], ce qui rejoint notre propos.

- **Équilibre efficacité/droits :** enfin, tout se résume à ce mot **équilibre**. Il faut gagner en efficacité sans sacrifier les droits. Trouver le point d'**optimisation global** où la fraude est la plus basse possible tout en maintenant un niveau de service et de respect des clients très élevé. Cela suppose parfois de **renoncer** à certaines pratiques pour des raisons éthiques. La confiance assuré/assureur est un prérequis à l'établissement d'une relation d'affaire saine et pérenne.

- **Pour conclure sur les perspectives :** l'IA va continuer à se perfectionner (IA génétique, systèmes auto-apprenants, etc.), la fraude va muter aussi, mais si les acteurs mettent en place cette gouvernance solide, ils pourront naviguer dans ce paysage mouvant en gardant le cap éthique. On peut imaginer demain des **IA explicables by design, des modèles "certifiés" sans biais**, et une coopération encore plus forte entre assureurs et autorités grâce à l'IA (par ex. détection proactive de fraudes en réseau entre plusieurs compagnies simultanément). Tout cela ne sera acceptable qu'avec un encadrement strict et l'adhésion de tous les acteurs, y compris des assurés. D'où l'importance d'impliquer l'humain à chaque étape, que ce soit l'expert assurance, le juriste, le data scientist et même, dans une certaine mesure, le client (via l'information et la pédagogie).

03. Vers une gouvernance responsable de l'IA antifraude

Ce qu'il faut retenir

→ L'utilisation de l'IA contre la fraude doit s'inscrire dans une gouvernance responsable. Cela implique de définir **des principes éthiques clairs** (transparence, équité, respect de la vie privée, primauté de l'humain) et de créer des instances internes pour surveiller les algorithmes (comité éthique IA, référent conformité…). L'humain doit rester au centre : **l'IA assiste mais ne décide pas seule**, et les experts fraudes voient leur rôle évoluer vers plus d'analyse qualitative plutôt que du tri quantitatif. Il faut aussi être transparent envers les assurés, expliquer la démarche et permettre la contestation/rectification en cas d'erreur.

→ Une telle gouvernance permet de trouver le **bon équilibre entre efficacité opérationnelle et respect des droits**. C'est ce qui conditionne l'acceptabilité sur le long terme de l'IA dans l'assurance. En agissant de la sorte avec rigueur, éthique et collaboration les assureurs pourront tirer le meilleur de l'IA pour combattre la fraude, tout en renforçant la confiance de leurs clients et partenaires.

VI.

Conclusion de l'étude

Conclusion

→ L'intelligence artificielle n'est plus une promesse : elle est devenue un levier stratégique dans la lutte contre la fraude à l'assurance. Face à un phénomène massif, mouvant et de plus en plus technologique, elle permet de détecter plus tôt, plus finement et à grande échelle les comportements frauduleux, tout en fluidifiant le traitement des dossiers pour les assurés honnêtes.

→ Mais cette puissance appelle une responsabilité. Car les fraudeurs s'arment eux aussi d'IA, et parce qu'un algorithme mal gouverné peut fragiliser la confiance qu'il cherche à protéger. L'efficacité ne peut donc se dissocier d'une gouvernance exigeante : transparence, équité, maîtrise des biais, respect du cadre réglementaire et maintien de l'humain dans la décision.

→ Bien encadrée, l'IA ne remplace pas l'expertise ; elle l'augmente. Elle renforce la justice du modèle mutualiste en protégeant les ressources communes et en limitant les hausses de primes injustifiées. La bataille contre la fraude reste évolutive, mais le rapport de force change. L'enjeu des prochaines années sera clair : conjuguer performance technologique et responsabilité éthique pour faire de l'IA un pilier durable de la confiance assurantielle.

À mesure que l'IA s'impose des deux côtés du miroir, chez les assureurs comme chez les fraudeurs, une question demeure : quels seront les schémas de fraude de demain, et serons-nous prêts à les anticiper ?

VII.

Qui sommes-nous ?

01. NEOLI en quelques mots

Neoli est un cabinet de **conseil en transformation et mise en conformité & gestion de risque.**

Neoli est animé par l'envie de créer des liens de confiance avec ses clients et partenaires. Pour ce faire, nos consultants sont sélectionnés pour leur **engagement, leur fiabilité, leur expertise et leur proactivité.**

"Le lien entre vos ambitions et notre engagement"

Nos domaines d'intervention :

ACCOMPAGNEMENT DE PROJETS DIGITAUX, SI, MÉTIERS

- ✓ Schéma directeur et aide au choix de solution
- ✓ Pilotage de projets et programmes (agiles ou traditionnels)
- ✓ Stratégie et évolutions produit (PO/PM)
- ✓ Modélisation de processus et efficacité opérationnelle
- ✓ Accompagnement au changement

MISE EN CONFORMITÉ ET GESTION DE RISQUES

- ✓ Pilotage de projet de conformité
- ✓ Management de transition
- ✓ Audit
- ✓ Plan de continuité d'activité (PCI/PCA)
- ✓ Expertises spécifiques (LCB-FT, DORA, pratiques commerciales, RGPD…)
- ✓ Refonte et optimisation de process et procédures internes

NEOLI

Nous contacter

Julien SIMON

06 73 76 21 52
julien.simon@neoli.eu.com

Nathan PAPIN

06 31 61 77 11
nathan.papin@neoli.eu.com