Considérations pour les assureurs et les experts

À l'instar du cyber il y a quelques années, l'IA s'impose progressivement comme un enjeu majeur, encore mal appréhendé par les assureurs. Si aucune assurance dédiée à l'IA n'existe à ce jour, les sinistres liés à son utilisation pourraient néanmoins être couverts par des polices classiques, souvent de manière implicite. Ce flou juridique et technique, combiné à l'arrivée de nouvelles réglementations européennes comme l'AI Act et la directive sur les produits défectueux, appelle à une réflexion approfondie sur la manière dont les acteurs du marché doivent adapter leurs pratiques.

Avant 2020, plusieurs études sur l'assurance cyber avaient pointé les freins et difficultés du marché. Les couvertures silencieuses en faisaient partie et les assureurs et réassureurs compris avaient du mal à évaluer leur exposition.

Cinq ans plus tard, bien qu'il n'existe pas d'assurance dédiée IA (il ne faut présager de rien), les couvertures silencieuses font reparler d'elles. En cas de sinistre lié à une IA (attaque, défaillance, arrêt du service, etc.), certaines conséquences peuvent alors être couvertes par des polices d'assurance dommages ou RC classiques, qui incluent ou excluent – de manière parfois implicite ou ambiguë – les risques liés à l'IA.

À ce jour, les assureurs ne semblent pas avoir encore intégré ce risque et nous n'avons pas constaté de sous-limites IA ou d'exclusions dans les contrats. Quoi qu'il en soit, les polices Tous Sauf des grands groupes pourraient faire l'objet d'une refonte avec l'essor des IA et leur arrivée dans les entreprises.

Autre considération que nous évoquions en début de dossier, c'est la conformité et le respect des obligations qui découlent de l'AI Act, le règlement européen sur l'intelligence artificielle (premier du genre). Aussi bien chez les assureurs (en souscription) que chez les experts qui souhaitent appréhender l'IA et son cadre réglementaire, il est recommandé d'en prendre connaissance (ne serait-ce qu'avec un haut niveau de lecture) pour comprendre les risques et les obligations liés aux IA.

En complément, la directive sur la responsabilité des produits défectueux, directive EU 2024/2853 qui remplace la précédente (datant de 1985) est aussi une lecture recommandable à l'expert spécialisé. En effet, cette directive a considérablement élargi la définition des produits défectueux. Elle couvre, désormais, les logiciels et s'appliquera donc par voie de conséquence aux systèmes d'IA.

D'un point de vue « expertal », l'IA qui est de plus en plus évoquée en souscription cyber semble, en dépit des défis techniques qui jalonnent sa mise en œuvre, représenter un risque avant tout RC pour l'entreprise. Disons qu'elle cherche encore sa place, comme le cyber il y a quelques années… Le volet cyber est certes important, mais ce risque est adressable et intégrable avec les outils d'analyse existants comme NIST *(National Institute of Standards and Technology)* ou la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité). À ce titre, une des questions qui pourrait être posée à un assuré déployant un système d'IA serait de savoir dans quelle mesure sa PSSI (Politique de sécurité du système d'information) a été mise à jour, pour y intégrer l'IA, et sinon pourquoi.

QUESTION DE LA PREUVE

Enfin, reste la délicate question de la preuve en cas de sinistre. L'expertise cyber représentait déjà un défi en soi tant par la volatilité, la qualité de

Frank Boston – généré à l'aide de l'IA /Adobestock

Un sinistre impliquant un système d'IA atteindra certainement des niveaux de complexité non égalés tant le mille-feuille des responsabilités peut être disparate.

la preuve ou encore parfois la non-volonté de la manifester. On peut présager qu'un sinistre impliquant un système d'IA atteindra des niveaux de complexité non égalés encore tant le mille-feuille des responsabilités peut être disparate en fonction des tâches et du cycle de vie.

Nous pouvons citer l'exemple de cette entreprise de production. Une IA chargée du contrôle de processus dans une ligne d'assemblage en sous-traitance ne stoppe pas une production de pièces dont les intervalles de tolérance sont dépassés sur une partie des lots. La production livrée doit être recommencée. La mise en place d'une IA sur les process de contrôle avait conduit l'entreprise à diminuer les contrôles manuels économisant de la masse salariale. Les mesures sont effectuées par laser à chaque pièce produite et comparées avec les tables d'ajustements récupérées par l'IA dans les données d'entraînement.

Il apparaît qu'une partie de la référence, la clé de tête de la pièce, a été modifiée par le fournisseur des plans et que l'IA avait interprété cette partie de la référence comme fixe et traitée comme un masque de champ. En conséquence, l'IA n'a pas vu la nouvelle référence ni intégré les nouveaux intervalles de tolérance.

Le sous-traitant se défend d'une erreur dans ses processus et indique avoir suivi le cahier des charges de son client en déployant son modèle IA pour effectuer les contrôles.

La société qui a développé le modèle d'IA indique ne pas avoir reçu pour information qu'une pièce pouvait partiellement changer de référence. En revanche, elle avait bien intégré le remplacement complet d'une référence. Une variation de la clé de tête n'était pas détectée, car le reste de la référence correcte avec la désignation et le code du bureau de dessin n'avait pas de raison de soulever une alerte.

Nattapat- généré à l'aide de l'IA /Adobestock

Une législation contraignante devrait voir le jour d'ici quelques années pour définir les obligations contractuelles des acteurs impliqués dans un système d'IA, notamment en matière de traçabilité, d'historisation et de durée de rétention.

De son côté, le prestataire qui a entraîné le modèle d'IA n'avait pas jugé nécessaire de mettre en place des contrôles de cohérence entre les références, la désignation des pièces et une évolution des écarts de tolérance (ce qui aurait pu détecter les anomalies en phase de production).

Enfin, pour pimenter le tout, les représentants du personnel se saisissent de l'affaire, dénoncent la suppression des contrôles qu'ils avaient signalée quelques mois plus tôt et menacent la direction d'un arrêt de la production.

Comme on peut le voir sur un court exemple issu d'une expérience de pensée, le mille-feuille des responsabilités peut rapidement exploser sur un cas simple et nous, expert, devrons garder l'esprit de synthèse et la compétence technique pour dessiner au mieux les arbres des causes que ces futurs sinistres nous réservent.

D'où vraisemblablement une normalisation à venir, voire une législation contraignante d'ici quelques années pour définir les obligations contractuelles des acteurs impliqués dans un système d'IA, notamment en matière de traçabilité, d'historisation et de durée de rétention.

Normalisation qui, nous l'espérons, clarifiera également qui aura la charge de la preuve et prévoira un régime de sanction pour les tiers qui ne prendront pas les dispositions liées à leur conservation. À ce sujet, le triptyque mis en place par le RGPD, confidentialité, disponibilité et intégrité, est de plus en plus complété par le terme traçabilité. En tant qu'experts, nous ne pouvons que nous en féliciter, mais sans contrainte cela pourrait rester un vœu pieux.

À ce point, ajoutons l'uniformisation, ou la normalisation du niveau d'information. Nous ne pouvons pas exclure qu'à un certain horizon l'analyse des données techniques liées à un sinistre impliquant une IA et plusieurs tiers nécessite de la part des assureurs et de leurs experts des capacités à stocker et traiter de larges volumes de données techniques.

Déjà sur quelques sinistres cyber majeurs, les assureurs demandent aux assurés de conserver les journaux d'événements. Parfois, ils ont été utilisés pour des analyses complémentaires ou à titre de vérification des enquêtes numériques, c'est-à-dire pour les besoins d'une contre-expertise.

À ce jour, le flou domine et déterminer une ou des responsabilités en l'absence de preuves reste une gageure. Sauf à ce que l'IA soit intégralement internalisée (y compris le modèle d'IA) en cas de

sinistre et de recours, déterminer les responsabilités et leur partage relève aujourd'hui du nœud gordien.

LES ACTES HOSTILES DEPUIS L'ÉTRANGER

Pour terminer sur les défis qui nous attendent avec l'arrivée de l'IA, notons qu'à l'instar du cyber, la guerre étrangère ou les actes de guerre hostiles rentrent dans le champ des exclusions et des limitations.

La France a récemment attribué pour la première fois des attaques cyber à un groupe affilié à un État (la Russie), APT28, son mode opératoire étant identifiable.

Concrètement, les systèmes d'IA et leur potentiel de manipulation et d'exfiltration des données vont représenter une cible de choix croissante pour les groupes cyber y compris ceux affiliés aux États dans les années à venir. Les effets domino et les réactions en chaîne qui peuvent découler de ces attaques mettront à l'épreuve la résilience des entreprises, voire d'un pan important de l'économie.

Un système d'IA défaillant ou indisponible pourra affecter des milliers d'entreprises clientes et les services qui en découlent. L'attribution d'une attaque sur un système d'IA à un tel groupe désigné par la France, un État européen ou encore Interpol pourrait avoir de sérieuses conséquences pour l'indemnisation d'un sinistre IA dans la mesure où elle pourrait constituer une exclusion. L'attribution peut donc être catastrophique au niveau macroéconomique.

CONCLUSION

Nous, expert, nous devons rester vigilants, nous documenter et suivre avec intérêt l'arrivée de l'IA. Cette spécialité, tout comme le cyber il y a quelques années, est en train de prendre forme, suivons son évolution. Ne l'évitons pas, car elle représente une rupture technologique majeure qui va impacter nos sociétés dans leur globalité. Le monde de l'assurance se dote d'IA et ses répercussions se feront sentir y compris dans notre manière de travailler et dans notre métier d'expert.