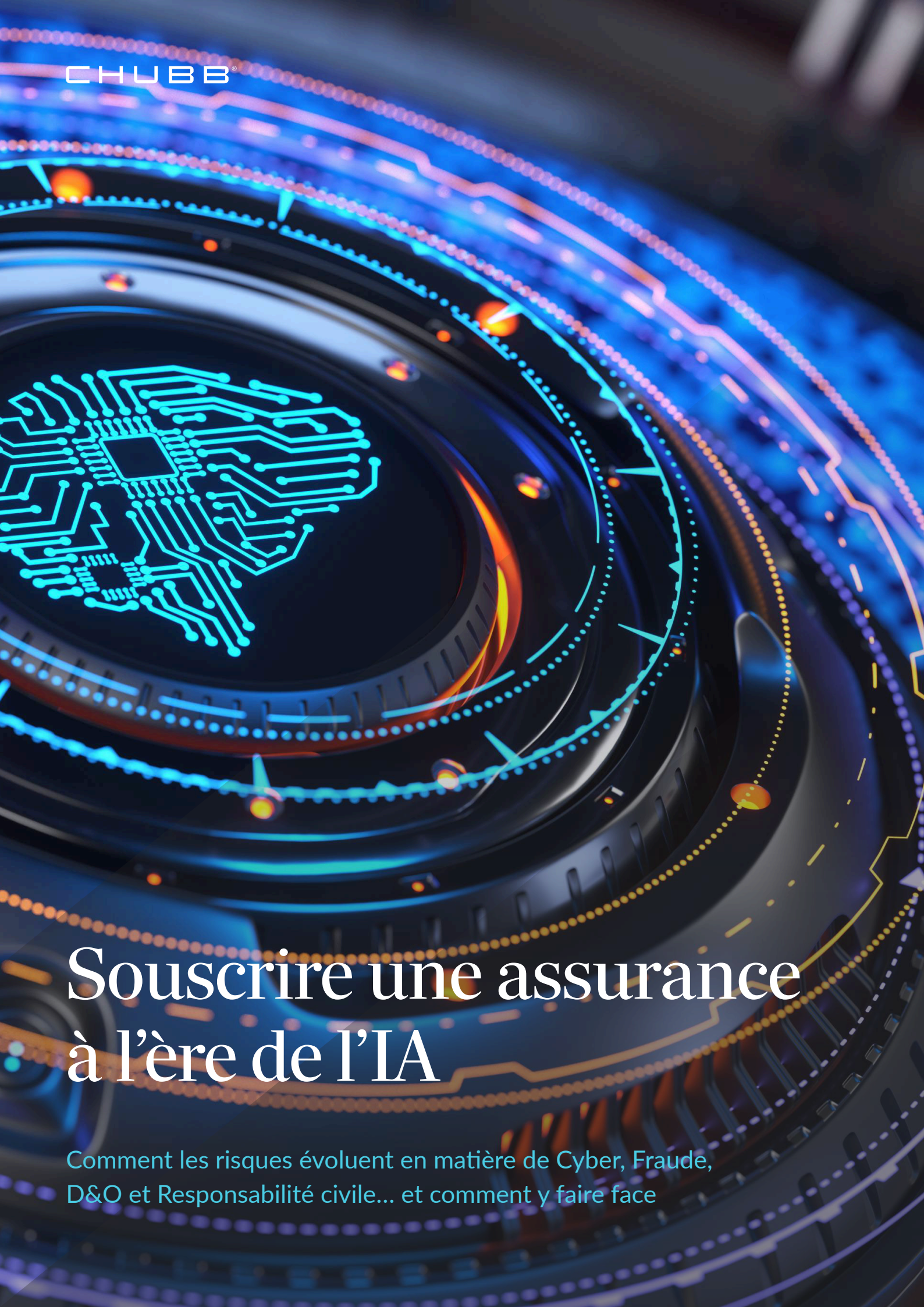
CHUBB®



Souscrire une assurance à l'ère de l'IA

Comment les risques évoluent en matière de Cyber, Fraude, D&O et Responsabilité civile… et comment y faire face

Résumé exécutif

L'intelligence artificielle (IA) s'invite de plus en plus dans le quotidien et dans la quasi-totalité des processus métier.
Elle est de plus en plus intégrée aux activités opérationnelles, qu'il s'agisse du service client, de la finance, des ressources humaines, de la sécurité, du marketing ou encore des processus décisionnels. Elle est également directement embarquée dans les produits et services.

Pour les assurés, cette évolution est majeure : l'IA ne crée pas simplement une nouvelle catégorie de risques. Elle transforme en profondeur les risques déjà couverts par les assurances, en particulier dans les domaines de la cybersécurité, de la fraude, de la responsabilité des dirigeants (D&O) et de la responsabilité civile (Liability / E&O).

L'IA modifie l'issue des sinistres en combinant la vitesse (les incidents évoluent plus vite que la réponse), l'échelle (les erreurs se répliquent d'une transaction à l'autre), l'opacité (il devient plus difficile d'expliquer pourquoi les systèmes ont agi ainsi) et la dépendance (une reliance accrue aux chaînes d'approvisionnement des prestataires). Il en résulte un environnement où les pertes peuvent être davantage corrélées et systémiques, où les frais de défense peuvent augmenter du fait de la complexité des preuves, et où les récits de responsabilité mettent de plus en plus l'accent sur la gouvernance, la supervision et la responsabilité de l'organisation.

En pratique, pour les Risk Managers, de nombreux incidents liés à l'IA se présenteront sous la forme de sinistres déjà connus (fraude, atteinte à la vie privée, négligence, diffamation, discrimination ou dommages corporels), plutôt que comme des « sinistres IA» à part entière. Cela accroît à la fois la gravité des risques et la complexité des programmes d'assurance.

Pour anticiper efficacement le renouvellement des contrats, les assurés devraient :

- Documenter la gouvernance de l'IA et définir clairement les responsabilités.
- Renforcer les contrôles de diligence et les exigences contractuelles vis-à-vis des fournisseurs.
- Moderniser les dispositifs de lutte contre la fraude afin de faire face aux menaces liées aux deepfakes.
- Tester des scénarios de gestion des sinistres impliquant plusieurs polices d'assurance.
- Vérifier les clauses des contrats afin d'identifier d'éventuelles lacunes de couverture ou des évolutions des exclusions.

Pourquoi l'IA est un enjeu d'assurance (et non un simple débat informatique)

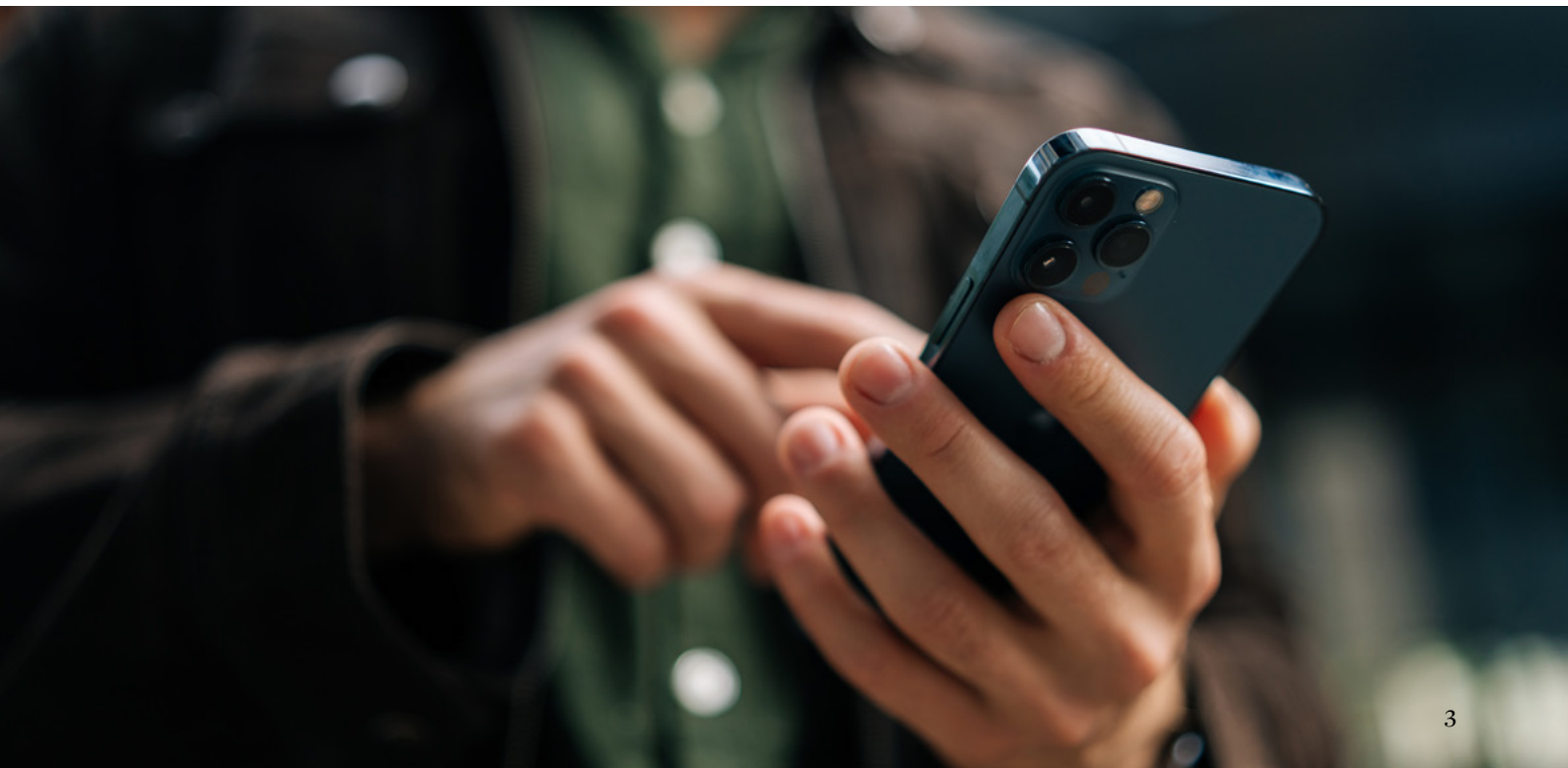
Les systèmes d'IA sont de plus en plus utilisés pour formuler des recommandations, traiter des dossiers, valider des transactions, échanger avec les clients et produire des informations sur lesquelles les humains s'appuient ensuite. À mesure que l'IA s'intègre dans les processus de travail quotidiens, elle influence directement les risques assurés et les sinistres, avec des conséquences concrètes pour les assurés, les courtiers et les souscripteurs

Le point essentiel est que la plupart des risques liés à l'IA ne se traduisent pas par une nouvelle catégorie de « sinistres IA». En réalité, l'IA transforme la manière dont les sinistres traditionnels surviennent. Elle les accélère, en amplifie les effets et les rend plus complexes à investiguer. Par exemple, une fraude à la paie rendue possible par une voix générée par deepfake reste un sinistre relevant de la fraude.

De la même manière, un chatbot qui divulgue des informations personnelles constitue toujours un incident cyber ou une atteinte à la vie privée. Un modèle d'IA qui fournit des conseils erronés peut toujours donner lieu à un sinistre en responsabilité professionnelle (E&O). En revanche, l'IA modifie les circonstances qui sous-tendent chacun de ces sinistres et influence ainsi à la fois la responsabilité et la réponse de l'assurance.

C'est pourquoi l'IA doit être considérée comme un multiplicateur des risques assurés existants, plutôt que comme un risque distinct. Le véritable défi, lors de la souscription d'une assurance, consiste à comprendre comment les mécanismes des sinistres et les exigences en matière de preuve ont évolué, ainsi que les conséquences pour la conception des programmes d'assurance et le processus de souscription.

> « L'IA doit être considérée comme un multiplicateur des risques assurés existants, plutôt que comme un risque distinct.»



Comment l'IA transforme les sinistres assurés : six mécanismes

L'IA modifie les scénarios de sinistres assurés de manière récurrente et prévisible. Ces mécanismes sont utiles car ils s'appliquent aux risques liés à la cybercriminalité, à la fraude, à la responsabilité civile et à la gouvernance. Ils constituent également un cadre pratique pour les discussions lors du renouvellement des contrats d'assurance.

1

Mécanisme 1 – Vitesse les incidents se développent plus rapidement que les cycles de réponse

L'IA peut agir en quelques millisecondes et à très grande échelle. Cela signifie que les erreurs, les exploitations malveillantes et les résultats nuisibles peuvent se propager avant même qu'une organisation ne détecte le problème, n'enquête ou ne mette en place un mécanisme d'arrêt. Cette rapidité réduit le temps disponible pour réagir et augmente la probabilité que les pertes s'aggravent avant d'être maîtrisées.

2

Mécanisme 2 – Échelle : une seule erreur est reproduite dans un grand nombre de décisions

Les systèmes d'IA sont conçus pour reproduire un comportement à grande échelle. Si un système est erroné, biaisé ou compromis, il peut répéter la même erreur sur des centaines ou des milliers de transactions, de clients ou de décisions opérationnelles. Cela accroît la probabilité de sinistres de grande ampleur, plutôt que de réclamations isolées.

3

Mécanisme 3 – Opacité : des comportements difficiles à expliquer augmentent les coûts de défense

De nombreux modèles d'IA ne fournissent pas de raisonnement clair et compréhensible par l'humain. Même lorsqu'il est possible de tester les résultats, il peut être difficile d'expliquer précisément pourquoi un système est parvenu à une décision, ou si un résultat différent aurait été obtenu dans des conditions légèrement modifiées. Cette incertitude augmente les difficultés probatoires et peut faire grimper les coûts juridiques, en particulier lorsqu'une réclamation repose sur la démonstration d'un défaut, d'une négligence ou d'un manquement au devoir de diligence raisonnable.

4

Mécanisme 4 – Dépendance : l'IA introduit un risque lié à la chaîne de fournisseurs

Contrairement aux systèmes traditionnels, développés et maintenus en interne, les systèmes d'IA dépendent souvent de nombreux tiers : fournisseurs de modèles, jeux de données, plateformes cloud, intégrateurs et mises à jour continues. Une défaillance ou une compromission peut provenir de n'importe quel maillon de cette chaîne, bien au-delà du contrôle direct de l'entreprise utilisatrice. Cela complique l'attribution des responsabilités et crée une exposition aux risques qui s'étend à l'ensemble des relations avec les fournisseurs.

5

Mécanisme 5 – Manipulation : des attaquants peuvent fausser ce sur quoi l'IA s'appuie

Les systèmes d'IA peuvent être compromis non seulement par des attaques informatiques classiques, mais aussi par la manipulation des informations sur lesquelles ils s'appuient : données d'entrée, prompts, documents, sources de récupération d'informations ou données d'entraînement. En pratique, cela peut amener le modèle à se comporter comme si de fausses informations étaient vraies, générant ainsi des résultats erronés avec un haut niveau de confiance. Cela élargit les possibilités de fraude et crée de nouveaux vecteurs de préjudice pour les consommateurs ainsi que de dysfonctionnements opérationnels

6

Mécanisme 6 – Délégation : les résultats de l'IA sont perçus comme émanant d'un représentant de confiance

À mesure que les systèmes d'IA formulent des recommandations, rédigent des communications, approuvent des actions ou orientent la prise de décision, ils agissent de plus en plus comme s'ils étaient un collaborateur ou un agent auquel des responsabilités ont été déléguées.
Dans le cadre de sinistres, par exemple, une organisation peut être tenue responsable de résultats préjudiciables parce que le système d'IA était considéré comme faisant autorité et a été utilisé dans le processus de décision, même si le fournisseur de la solution d'IA a également contribué à la défaillance.

Pris ensemble, ces mécanismes augmentent la gravité, la corrélation et l'incertitude des risques.
Trois facteurs qui modifient sensiblement les résultats assurantiels et mettent à l'épreuve la conception des polices d'assurance.

Le défi majeur lors de l'achat d'une assurance : le « risque IA silencieux » et les lacunes de couverture

L'IA doit avant tout être considérée comme un facteur d'amplification des risques. Dans la plupart des cas, elle intervient au sein de sinistres déjà connus. C'est un point essentiel lors du choix d'une assurance : les problématiques de couverture sont rarement présentées comme des « risques liés à l'IA ». Elles se traduisent plutôt par des interrogations sur la police d'assurance qui doit intervenir et sur la conformité du sinistre aux définitions prévues par le contrat.

De nombreux incidents impliquant l'IA peuvent déclencher simultanément plusieurs polices d'assurance, notamment :

- **Cyber (**atteinte à la vie privée, incident de sécurité du réseau)
- **Fraude** (Crime) (instruction frauduleuse / usurpation d'identité)
- **Responsabilité professionnelle / Erreurs & Omissions (Tech E&O / PI)** (conseil négligent, préjudice lié à la confiance accordée)
- **Médias** (diffamation)
- **Responsabilité des dirigeants (D&O)** (défaillance de gouvernance, obligations de divulgation, « AI washing », enquêtes réglementaires)
- **Responsabilité civile générale / préjudice** causé aux consommateurs

À travers le marché, les libellés des contrats d'assurance varient considérablement dans la manière dont ils traitent les scénarios de pertes liés à l'IA. Cela peut s'expliquer par des niveaux d'expérience différents selon les assureurs ainsi que par la rapidité avec laquelle les clauses de souscription ont évolué pour suivre les risques liés à l'IA.

Les assurés doivent porter une attention particulière aux points suivants :

- L'étendue d'une « défaillance de sécurité » couverte lorsque l'IA y contribue
- Le fait qu'une erreur générée par l'IA entre dans la définition des « services professionnels »
- Le fait qu'une production synthétique ou générée par l'IA constitue une « instruction » au sens des garanties fraude
- La manière dont s'appliquent les exclusions (par exemple, exclusions algorithmiques, exclusions liées aux services professionnels)
- Le fait qu'une défaillance d'un prestataire tiers soit traitée comme un « risque lié à un prestataire externalisé »

En conséquence, les Risk Managers doivent partir du principe que l'IA est susceptible de créer certaines ambiguïtés de couverture et prendre des mesures proactives lors de la conception et de l'achat de leur programme d'assurance

Cartographie des couvertures en cas d'incident IA : où se rangent les scénarios courants selon les polices

Le tableau ci-dessous montre comment les incidents typiques liés à l'IA sont susceptibles d'être pris en charge selon les polices d'assurance. Il s'agit d'une indication uniquement : les résultats réels dépendent de la rédaction, des définitions, des exclusions et des sous-limites. De nombreuses pertes liées à l'IA mobilisent plusieurs garanties en même temps.

Scénario d'incident / de perte lié à l'IA	Principal type de perte	Réponse la plus probable de la police principale	Police secondaire / chevauchement fréquent	Principales zones de tension / point de litiges
Un salarié saisit des données personnelles ou confidentielles dans un outil d'IA public, entraînant une fuite de données.	Atteinte à la vie privée + risque réglementaire	Cyber (protection des données, gestion de crise, défense réglementaire)	Tech E&O (si préjudice client), D&O (si gouvernance)	L'assuré a-t-il manqué à ses obligations de traitement des données ? La fuite constitue-t-elle une violation des réglementation sur la protection des données ?
Une attaque par prompte injection conduit un chatbot à divulguer des informations sensibles sur des clients	Atteinte à la vie privée + incident de sécurité	Cyber	RC Pro Tech (E&O)	La police couvre-t-elle les "actes malveillants informatiques" et prévoit-elle une garantie de responsabilité liée à la vie privée ?
Le système d'IA « hallucine » et fournit des consignes erronées, entraînant une perte financière pour le client	Faute professionnelle / erreur de conseil	RC Pro Tech (E&O) / Responsabilité civile professionnelle	RC Générale (rare), Médias	Déterminer si l'exclusion « services professionnels » s'applique ; preuve du lien de causalité et de la confiance accordée
Un chatbot d'IA diffame une personne ou génère un contenu discriminatoire	Responsabilité liée aux contenus diffusés à des tiers	Responsabilité médias (ou RC Pro Tech/E&O si incluse)	RC générale (parfois), EPL (si contexte salarié)	Déclencheurs publication/diffamation, exclusions liées à l'intention, exclusions de contenu en E&O
Marketing généré par l'IA comporte des affirmations trompeuses (performances, prix, « résultats garantis »)	Protection des consommateurs / pratiques commerciales trompeuses	RC Pro Tech (E&O) / Médias	D&O (si impact sur les investisseurs)	Information trompeuse vs tromperie délibérée ; exclusions pour faute intentionnelle
L'IA génère un contenu protégé par le droit d'auteur (ou très proche) et le titulaire des droits engage une action	Défense/frais liés à une atteinte aux droits de PI	Responsabilité médias (le plus adapté), parfois Tech E&O	D&O (en cas de publication par une société cotée), Cyber (rare)	Les exclusions PI varient fortement (droit d'auteur vs marque vs brevet) ; des sous-limites s'appliquent souvent
Une IA est entraînée sur des secrets d'affaires/données prétendument dérobés	PI + secrets d'affaires	Tech E&O (si la rédaction est suffisamment large)	D&O	Les polices excluent souvent les réclamations PI/secrets d'affaires, sauf négociation
Un modèle d'IA utilisé en RH génère des décisions d'embauche discriminatoires	Discrimination au travail	EPL (Responsabilité des Pratiques d'Emploi)	D&O (supervision), Tech E&O (risque fournisseur)	Si la décision automatisée enfreint la loi ; la couverture des actions réglementaires varie
Crédit/souscription/ tarification par IA: résultats injustes ou discriminatoires	Action réglementaire + recours collectifs	Tech E&O / RC générale (selon les cas), parfois D&O	D&O	Certaines polices excluent les décisions de tarification; les régulateurs peuvent viser des sanctions non assurables

Scénario d'incident / de perte lié à l'IA	Principal type de sinistre	Réponse la plus probable de la police principale	Police secondaire / chevauchement fréquent	Principales zones de tension / point de litiges
Refus ou tri automatisé de sinistres ou de prestations entraînant un préjudice systémique	Préjudice opérationnel + action collective de consommateurs	Tech E&O / Responsabilité civile professionnelle	D&O	Négligence, pratiques déloyales, défaut de supervision ; les coûts de défense peuvent fortement augmenter.
Usurpation d'identité par deepfake entraînant un virement frauduleux	Perte financière	Fraude (ingénierie sociale / fraude au virement de fonds)	Cyber (en cas d'intrusion du système), D&O	Vérifier si la notion d'« instruction » couvre la voix ou la vidéo, ainsi que les contrôles d'authentification.
Fraude à la facturation ou au paiement par IA utilisant de fausses coordonnées fournisseurs	Perte financière	Fraude	Cybersécurité	Litiges sur l'application de la garantie « fraude informatique » et les sous-limites liées à l'ingénierie sociale.
Outil d'IA générant automatiquement un paiement au mauvais bénéficiaire	Erreur opérationnelle	Fraude (selon les circonstances) ou RC professionnelle (E&O)	D&O	Déterminer s'il s'agit d'une fraude ou d'une erreur; de nombreuses polices Criminalité ne couvrent pas les erreurs pures.
Extorsion par rançongiciel facilitée par une reconnaissance préalable réalisée grâce à l'IA	Cyber-extorsion	Cyber	Crime (rare)	Exclusions liées aux risques systémiques et litiges impliquant les fournisseurs.
Vulnérabilité d'un outil d'IA fourni par un prestataire entraînant un incident de sécurité	Cyber + responsabilité fournisseur	Cyber	Tech E&O	Défaillance d'un tiers et déclenchement des garanties liées à l'interruption d'activité dépendante.
Dérive d'un modèle d'IA produisant des résultats erronés causant un préjudice aux clients	Sinistre Tech E&O	Tech E&O	RCMS (D&O)	Vérifier si la surveillance du modèle était raisonnable ; risque de contentieux sur la gouvernance
Incident lié à l'IA déclenchant une enquête réglementaire	Frais d'enquête	D&O (la couverture des enquêtes varie)	Cyber (en cas d'atteinte à la vie privée / à la sécurité)	Déterminer si l'enquête constitue un « sinistre » et si les sanctions sont assurables.
Chute du cours de bourse d'une société cotée après une controverse liée à l'IA	Action collective d'actionnaires	D&O	–	Communication financière, caractère significatif des informations, confiance accordée aux déclarations et responsabilité des dirigeants.
Un prestataire certifie un modèle d'IA qui cause ensuite un dommage	Négligence fondée sur la confiance accordée	RC professionnelle du testeur / E&O Tech (police du fournisseur)	Tech E&O de l'acheteur / D&O	Limites contractuelles de responsabilité et recours contre les tiers.
Panne d'un fournisseur d'IA perturbant les opérations	Interruption d'activité	Cyber (si une garantie « panne technologique » existe)	Dommages aux biens / Perte d'exploitation (rarement) / Supply Chain	Vérifier si les défaillances du fournisseur et des systèmes sont bien couvertes.

Conseil d'action pour l'assuré : demandez à votre courtier de fournir une « vue de réponse multi-polices pour un incident unique » pour au moins trois scénarios liés à l'IA. De nombreux litiges ne naissent pas d'un manque d'assurance, mais d'une incertitude sur la police qui est prioritaire.

Gestion pratique des risques par branche d'assurance

Les recommandations ci-dessous montrent comment les six principaux mécanismes de risque liés à l'IA se traduisent en risques spécifiques à chaque branche d'assurance et en actions concrètes. Les responsables des risques peuvent s'appuyer sur cette liste de contrôle opérationnelle en complément de leur processus de renouvellement.

Cyber : l'IA étend la surface d'attaque au-delà de l'IT

L'IA crée de nouveaux risques de fuite de données (salariés saisissant des informations sensibles dans des outils d'IA), de nouvelles techniques d'exploitation (injection de prompts) et de nouveaux risques de contenus préjudiciables côté client. Son adoption accroît aussi la dépendance à des plateformes d'IA tierces et à des services cloud, ce qui peut complexifier l'attribution des responsabilités et le reporting en cas d'incident.

Ce que les responsables des risques devraient faire :

- Mettre en place une liste d'outils d'IA autorisés et des contrôles de prévention des pertes de données (DLP)
- Journaliser et surveiller, lorsque cela est possible, l'usage des outils d'IA et leurs résultats
- Mener une due diligence fournisseurs sur les éditeurs de modèles, l'hébergement et les sous-traitants
- Vérifier que la police d'assurance couvre les incidents de confidentialité impliquant des services d'IA.

D&O : la supervision, la transparence et la gouvernance deviennent essentielles

À mesure que l'IA devient déterminante pour les opérations, échecs et controverses se transforment en sujets de gouvernance. L'exposition peut découler d'allégations de supervision insuffisante, de communications trompeuses, de préjudices pour les consommateurs, de résultats discriminatoires ou de déclarations inexactes sur les capacités de l'IA et la conformité.

Ce que les responsables des risques devraient faire :

- Considérer la documentation de gouvernance comme un véritable outil de protection
- Veiller à une parfaite clarté sur les enquêtes, les demandes des régulateurs et les déclencheurs de sinistre
- Tester la robustesse de l'adéquation de la Side A et de la couverture de l'entité
- Vérifier les communications publiques afin de limiter les accusations d'« AI washing ».

Criminalité : la fraude par usurpation d'identité devient massive et crédible

Les deepfakes audio/vidéo et l'imitation linguistique de très haut niveau rendent l'intuition humaine moins fiable pour détecter les fraudes. L'usurpation d'identité assistée par l'IA peut faciliter les validations de paiement frauduleuses, le détournement de factures fournisseurs et l'ingénierie sociale à grande échelle.

Ce que les responsables des risques devraient faire :

- Ne plus fonder l'authentification uniquement sur la voix ou la vidéo
- Renforcer la vérification via un canal distinct pour les validations sensibles
- Vérifier si la formulation instruction frauduleuse couvre bien les scénarios d'usurpation synthétique
- S'assurer que les contrôles opérationnels correspondent à la position attendue de l'assureur

Responsabilité civile/Tech E&O/Médias : préjudices liés à la dépendance, résultats erronés, propriété intellectuelle et atteinte à la réputation

Les contenus générés par l'IA peuvent entraîner des pertes en cascade lorsqu'ils sont utilisés comme base par des clients, des équipes internes ou des contreparties. Cela inclut des recommandations « hallucinées », des décisions de triage inexactes, des atteintes à la réputation, de la diffamation et des litiges en propriété intellectuelle.

Ce que les responsables des risques devraient faire :

- Mettre en place des contrôles sur les sorties IA destinées aux clients
- Clarifier les chevauchements et exclusions entre E&O et médias
- Encadrer contractuellement les indemnités fournisseurs ainsi que la répartition des responsabilités.
- Définir clairement les responsabilités, les engagements et les mécanismes d'indemnisation liés aux projets d'IA.
- S'assurer que les tests et les responsabilités des développeurs sont clairement définis entre le fournisseur technologique et le client

Questions clés pour les courtiers et les souscripteurs sur l'IA

Les questions ci-dessous visent à obtenir des positions de souscription claires et à mettre au jour les angles morts. Les Risk Managers devraient les inscrire comme point structuré à l'ordre du jour lors du renouvellement.

Structure du programme et exposition IA implicite

- Où les pertes les plus importantes liées à l'IA sont-elles censées être couvertes : Cyber, Criminalité, D&O, EPL, Tech E&O, Médias ou Responsabilité Civile
- Certaines polices de notre programme comportent-elles des exclusions ou limitations visant l'IA, les algorithmes ou les modèles ? Si oui, merci de les préciser et d'en expliquer les conséquences.
- Des sous-limites de garantie sont-elles susceptibles de s'appliquer aux sinistres liés à l'IA (ingénierie sociale, réglementation sur la protection des données, médias/propriété intellectuelle, erreurs technologiques, etc.)

D&O / gouvernance

- La police D&O couvre-t-elle les enquêtes réglementaires préalables à toute réclamation liées à la gouvernance de l'IA (utilisation des données, discrimination, sécurité de l'IA, etc.) ? Quels sont les événements déclencheurs de cette garantie ?
- L'assureur considère-t-il l'IA comme un risque critique en matière de gouvernance ? Quels éléments de gouvernance au niveau du conseil d'administration permettraient d'améliorer les conditions d'assurance ?
- L'assureur a-t-il défini une position concernant les risques d'AI washing ? Attend-il des informations spécifiques relatives à l'IA dans les facteurs de risque communiqués par l'entreprise ?

Spécifique cyber

- Notre police Cyber couvre-t-elle les fuites d'informations via des prompts d'IA ou les attaques par injection de prompts sur des chatbots ? Sur quelles dispositions contractuelles cette couverture repose-t-elle ?
- La police couvre-t-elle les incidents liés à la protection des données résultant de l'utilisation par les collaborateurs d'outils d'IA tiers (copilotes, plateformes LLM, etc.) ?
- Une interruption de service d'un fournisseur d'IA est-elle couverte au titre des garanties Perte d'exploitation ou Interruption d'activité dépendante ?

Responsabilité civile / E&O / Médias

- Quelle police couvre les hallucinations de l'IA ou les conseils erronés générés par l'IA ayant causé un préjudice à un client : Tech E&O, Responsabilité Civile Professionnelle (PI) ou Responsabilité Civile Générale (GL) ? Existe-t-il des zones non couvertes ?
- Comment sont traitées les réclamations liées à la propriété intellectuelle lorsque le dommage résulte d'un contenu généré par l'IA (droit d'auteur, marque, brevet) ? Les frais de défense sont-ils couverts ? Des sous-limites s'appliquent-elles ?
- Les polices excluent-elles les réclamations résultant d'algorithmes ou de décisions automatisées, même lorsque l'IA n'est qu'un facteur contributif parmi d'autres ?

Criminalité et ingénierie sociale

- La notion d'« instruction frauduleuse » inclut-elle explicitement l'usurpation via deepfake audio/vidéo, ou uniquement les instructions écrites / par e-mail ?
- Existe-t-il des exclusions (remise volontaire, instruction autorisée, échec d'authentification) susceptibles d'écarter des sinistres liés aux deepfakes ?
- Quels dispositifs de contrôle l'assureur attend-il que nous mettions en place (rappel téléphonique, double validation, vérification via un canal distinct) et seront-ils érigés en garanties contractuelles ?

Conclusion

L'IA transforme profondément la nature des sinistres assurables en augmentant leur rapidité d'apparition, leur ampleur, les dépendances entre les risques et l'incertitude quant aux éléments de preuve.
Pour les assurés, le principal défi ne réside pas uniquement dans une probabilité accrue de sinistres mais également dans leur gravité, leur interdépendance et les incertitudes liées à la coordination des garanties entre les différentes polices du programme d'assurance.
La réponse la plus efficace repose sur une approche pragmatique fondée sur une gouvernance solide : documenter les usages significatifs de l'IA, renforcer la due diligence des fournisseurs, moderniser les dispositifs de lutte contre la fraude, cartographier les couvertures à partir de scénarios concrets et clarifier les clauses contractuelles avant que les exclusions et la jurisprudence ne se durcissent.

Le contexte réglementaire ajoute une dimension supplémentaire qui nécessitera une vigilance constante et deviendra probablement de plus en plus déterminant pour les assurés. Au sein de l'Union européenne, les obligations de gouvernance prévues par l'AI Act sont déjà en vigueur pour certains usages à haut risque, tandis que les régimes de responsabilité du fait des produits évoluent afin d'intégrer les logiciels et fonctionnalités reposant sur l'IA.

Aux États-Unis, la coexistence des recommandations du National Institute of Standards and Technology (NIST), des réglementations sectorielles, des législations propres à chaque État et d'une responsabilité largement façonnée par les contentieux crée un environnement en constante évolution. Un constat s'impose toutefois dans toutes les juridictions : la capacité à se défendre repose avant tout sur la démonstration d'une gouvernance et d'une supervision raisonnables, davantage que sur la seule sophistication technique.

Au-delà de l'Union européenne et des États-Unis, les pays d'Asie-Pacifique, du Moyen-Orient et d'Amérique latine développent également, à des rythmes différents, leurs propres cadres réglementaires, recommandations sectorielles et règles de responsabilité spécifiques à l'IA.

La configuration du risque réglementaire lié à l'IA sur ces marchés et ses implications pour la conception de programmes multinationaux fera l'objet d'analyses complémentaires à mesure que ce paysage se consolide.

C'est un sujet qui appelle une attention étroite et continue de la part des Risk Managers et de leurs courtiers, au fil de l'évolution des discussions de renouvellement.

CHUBB®

9184-HS 04/26