

# risques

n°137  
mars  
2024



SOCIÉTÉ  
**Entretien avec  
Philippe Wahl**

ANALYSES & DÉFIS  
**Les risques  
géostratégiques**

RISQUES & SOLUTIONS  
**Numérique  
et assurance**

ÉTUDES & DÉBATS  
**La hausse des prix  
dans l'assurance  
est-elle une fatalité ?**

# Éditorial



**JEAN-HERVÉ  
LORENZI**  
Directeur de la rédaction

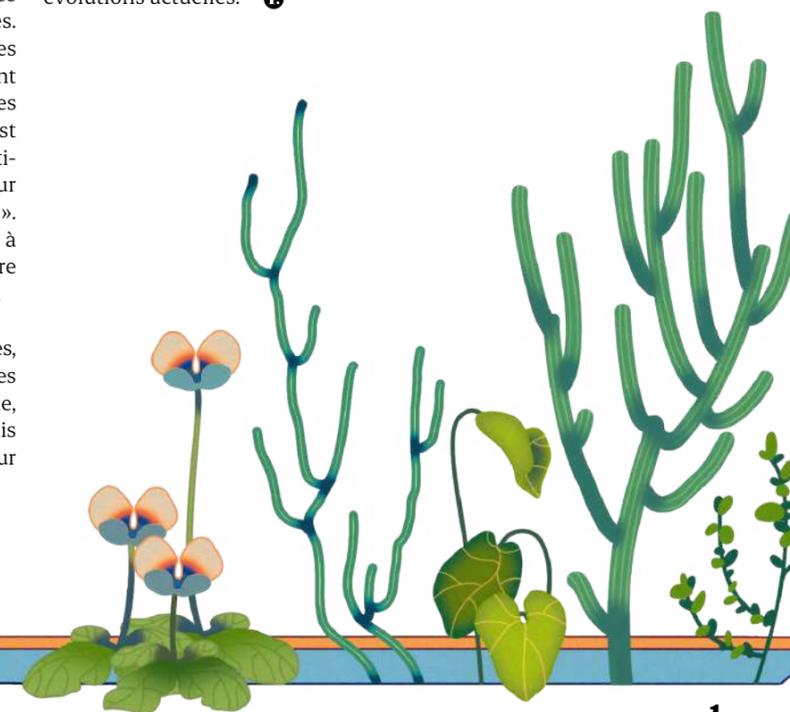
Décidément, *Risques* aborde toujours les thèmes qui s'imposeront dans les débats des mois à venir. Il est évident que nous ne savons pas comment traiter les trois transitions auxquelles nous sommes confrontés, climatique, numérique, démographique ; et cela, ni sur le plan financier, ni sur le plan technologique.

Jusqu'à présent, peu de choses ont été dites sur ces deux sujets. Sur le premier, on constate à l'envi que l'on ne dispose pas aujourd'hui des montants et des canaux de financements suffisants pour investir dans ces trois ruptures essentielles. Sur l'autre, on en est encore au stade des spéculations et des grandes interrogations sur l'impact de l'intelligence artificielle sur l'emploi. Et puis ajoutons les crises géostratégiques, ce qu'elles impliquent en matière d'augmentation des dépenses militaires. Enfin, les risques encourus et les moyens que l'assurance offre pour les prendre en charge n'ont été que peu abordés. C'est particulièrement dommageable, car chacun sait que l'assurance crée la confiance des acteurs économiques et que la confiance crée la croissance. C'est d'ailleurs ce que nous dit Philippe Wahl, dans son interview très stimulante en présentant La Poste comme un acteur désormais majeur de l'assurance lorsqu'il la décrit comme un « réassureur du lien social ». Quelle superbe ambition pour le plus beau réseau de France de traiter à la fois des problèmes de solitude, de santé et pour tout dire de bien-être de toutes les populations sur notre territoire, y compris les plus isolées.

Bien entendu, en poursuivant notre démarche d'anticipation des risques, nous avons tenté de cerner le rôle que pouvait jouer les technologies les plus avancées, et évidemment en premier lieu l'intelligence artificielle, sur les modes de fonctionnement des entreprises de l'assurance, mais également ce risque si souvent évoqué, celui de la cybersécurité, pour lequel les solutions assurantielles sont encore à trouver.

Second thème abordé, celui de la géostratégie. En effet, les assureurs se trouvent comme bien d'autres secteurs d'activité confrontés à un risque encore plus important, la guerre. Tout cela était inimaginable il y a quelques mois encore, mais, comme toujours, l'histoire est un éternel recommencement. L'impact de ces conflits armés qui n'ont jamais été prévus, car ils ne concernaient jusqu'alors que des zones très éloignées, et pour lequel peu de solutions ont été anticipées, est d'une ampleur inconnue jusqu'alors. Dans cette partie « Analyses & défis », il s'agit plus de déterminer les problèmes posés, qu'il s'agisse de la permanence des chaînes d'approvisionnement ou des chocs énergétiques. Mais là, comme précédemment, ce sont des problèmes radicalement nouveaux qu'il nous faut évoquer avec méthode, clarté et souci d'amorcer des solutions.

Une conclusion s'impose, tout cela peut rendre les produits d'assurance plus onéreux, même si les évolutions technologiques, au contraire, peuvent avoir un effet baissier. C'est cette question de l'évolution des prix de l'assurance que nous nous sommes posée dans un débat très vivant, car traitant autant des risques de dommages que de personnes. Sans surprise, il n'y a pas de réponse évidente, car les impacts de ces chocs et de ces transitions sont multiples. Notre objectif est de présenter les enjeux pour l'assurance de ces évolutions si brutales. À nous tous, désormais, de faire des propositions aussi nouvelles que les évolutions actuelles. 



## Ours

Directeur de la rédaction  
**Jean-Hervé Lorenzi**

Directeur de la publication  
**Franck Le Vallois**

**Courriel :**  
risques@franceassureurs.fr

**Éditeur**  
SARL Seddita  
26, boulevard Haussmann  
75009 Paris

**Prix de l'abonnement**  
(4 numéros)  
• France : 164 €  
• Étranger : 184 €

**Prix au numéro**  
• France : 48 €  
• Étranger : 56 €

www.revue-risques.fr

**Direction artistique  
& coordination éditoriale**  
Enderby

**Illustration de couverture**  
Jee-ook Choi

**Crédit photographique**  
Romuald Meigneux

**Impression**  
STIPA



Créée en 1990 avec le soutien de la Fédération Française de l'Assurance, la revue *Risques* apporte des éléments d'analyse et de réflexion sur les grands débats de société et constitue une référence sur les questions de risque et d'assurance. Lieu de débat et de réflexion, cette revue à caractère scientifique réunit un comité composé d'universitaires de toutes les disciplines du risque et de praticiens de l'assurance.



**PHILIPPE WAHL**  
Président-directeur  
général du Groupe  
La Poste

p°8

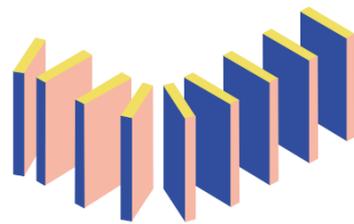
SOCIÉTÉ

# La Poste, acteur de la gestion des risques face aux transitions

p°46

ANALYSES & DÉFIS

# Les risques géostratégiques



p°14

RISQUES & SOLUTIONS

# Numérique et assurance

+

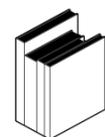
Débat avec  
**Olivier Gayraud,**  
**Bertrand Labilloy,**  
**Séverine Salgado,**  
**Catherine Touvrey**

p°84

ÉTUDES & DÉBATS

# La hausse des prix dans l'assurance est-elle une fatalité ?

p°92



**Livres**

## Sommaire détaillé <sup>+</sup>

### • SOCIÉTÉ •

p°8 La Poste, acteur de la gestion des risques face aux transitions  
**PHILIPPE WAHL**

### • RISQUES & SOLUTIONS • Numérique et assurance

p°16 Introduction  
**GILLES BÉNÉPLANC**

p°18 L'IA, un levier stratégique pour les assureurs  
**JÉRÔME BALMES**

p°22 Éthique de l'IA dans l'assurance : entre innovation et responsabilité  
**DAVID DORN, RICHARD EUDES**

p°26 Comment redessiner l'assurance avec l'IA générative ? Avec esprit critique et co-intelligence.  
**NICOLAS MARESCAUX, FLORENCE PICARD, PIERRE VALADE**

p°30 Menace cyber et assurance : où en sommes-nous ?  
**SÉBASTIEN HÉON, DIDIER PARSOIRE**

p°38 Anticiper les évolutions du risque cyber : un chemin vers son assurabilité  
**CAROLINE HILLAIRET, OLIVIER LOPEZ**

p°42 Ratio combiné : combler l'écart entre le coût des sinistres et les primes grâce à l'IA  
**JEREMY JAWISH**

### • ANALYSES & DÉFIS • Les risques géostratégiques

p°48 Introduction  
**DANIEL ZAJDENWEBER**

p°50 Des risques géopolitiques enchevêtrés, aggravés par le jeu des anticipations  
**GILLES ANDRÉANI**

p°54 Les assureurs face au risque géopolitique dans un monde en polycrise  
**FRANÇOISE GILLES, PAUL-LOUIS MORACCHINI**

p°58 Assurance et conflit : Protéger la continuité de la chaîne logistique  
**JEAN-ÉTIENNE QUINTIN**

p°62 Après le choc, quel nouveau paysage pétrolier ?  
**PATRICE GEOFFRON**

p°66 Sanctions économiques : Quel coût pour le secteur de l'assurance ?  
**PIERRE-CHARLES PRADIER**

### • ÉTUDES & DÉBATS •

p°72 Partage des données, à qui profite le crime ?  
**LAURENCE BARRY, ARTHUR CHARPENTIER**

p°76 Le risque géostratégique : l'éternel retour ?  
**PIERRE MARTIN**

p°82 Secteur à la loupe : La presse écrite à l'épreuve des plateformes  
**DOMINIQUE SEUX**

p°84 Les Débats de *Risques* : La hausse des prix dans l'assurance est-elle une fatalité ?  
**OLIVIER GAYRAUD, BERTRAND LABILLOY, SÉVERINE SALGADO, CATHERINE TOUVREY**

p°90 Pourquoi le secteur européen de l'assurance-vie doit-il innover ?  
**ACTUALITÉS DE LA FONDATION DU RISQUE- INSTITUT LOUIS BACHELIER**

### • LIVRES •

p°92 Henry Farrell, Abraham Newman, *Underground Empire: How America Weaponized the World Economy*, Henry Holt.  
**PIERRE-CHARLES PRADIER**

p°93 Cedomir Nestorovic, *Geopolitics and Business – Relevance and Resonance*, Springer, 2023.  
**PIERRE-CHARLES PRADIER**

## Comité éditorial <sup>+</sup>

**JEAN-HERVÉ LORENZI**  
Directeur de la rédaction

**FRANCK LE VALLOIS**  
Directeur de la publication

### • SOCIÉTÉ •

**EMMANUELLE CALES  
BERTRAND LABILLOY  
MATHILDE VIENNOT**

### • RISQUES & SOLUTIONS •

**GILLES BÉNÉPLANC  
CORINNE CAPIÈRE  
DANIEL ZAJDENWEBER**

### • ANALYSES & DÉFIS •

**SANDRINE LEMERY  
ECATERINA NISIPASU  
PHILIPPE TRAINAR**

### • ÉTUDES & DÉBATS •

**PIERRE BOLLON  
ARNAUD CHNEIWEISS  
PIERRE-CHARLES PRADIER**

—  
**ÉMILIE NETTER  
MARIANNE ESTRANGIN**

## Comité <sup>+</sup> scientifique

Luc Arrondel, Philippe Askenazy, José Bardaji, Didier Bazzocchi, Jean Berthon, Jean-François Boulter, Brigitte Bouquot, François Bucchini, Gilbert Canameras, Corinne Capière, Brigitte Dormont, Patrice Duran, Louis Eeckhoudt, François Ewald, Didier Folus, Pierre-Yves Geoffard, Claude Gilbert, Frédéric Gonand, Rémi Grenier, Vincent Gros, Marc Guillaume, Dominique Henriet, Vincent Heuzé, Meglena Jeleva, Gilles Johanet, Elyès Jouini, Jérôme Kullmann, Dominique de La Garanderie, Patrice-Michel Langlumé, Régis de Larouillère, Robert Leblanc, François Lusson, Florence Lustman, Olivier Mareuse, Pierre Martin, André Masson, Luc Mayaux, Erwann Michel-Kerjan, Marie-Christine Monsallier-Saint-Mleux, Laurent Montador, Bertrand Munier, Carlos Pardo, Jacques Pelletan, Pierre Pestieau, Pierre Petauton, Pierre Picard, Manuel Plisson, Jean-Claude Prager, André Renaudin, Angelo Riva, Geoffroy de Saint-Amand, Christian Schmidt, Côme Segretain, Jean-Charles Simon, Kadidja Sinz, Olivier Sorba, Lucie Taleyson, Patrick Thourot, Alain Trognon, François de Varenne, Oliver Wild, Jean-Luc Wybo

## Contributeurs <sup>+</sup>



**GILLES ANDRÉANI**  
Président de chambre à la Cour des comptes et Président de la Commission du secret de la Défense nationale (CCSDN)



**JÉRÔME BALMES**  
Direction Pilotage d'activité & Technologie, France Assureurs



**LAURENCE BARRY**  
Co-titulaire de la chaire PARI



**ARTHUR CHARPENTIER**  
Professeur à l'UQAM, Université du Québec à Montréal

# Contributeurs <sup>+</sup>



**DAVID DORN**

Partner, Deloitte Insurance



**RICHARD EUDES**

Managing Director,  
Risk Advisory, Deloitte



**OLIVIER GAYRAUD**

Juriste, Association Consommation,  
Logement et Cadre de vie (CLCV)



**PAUL-LOUIS MORACCHINI**

Responsable des risques émergents, Groupe AXA



**DIDIER PARSOIRE**

Directeur Cyber Solutions,  
SCOR



**FLORENCE PICARD**

Actuaire certifiée, membre du Directoire,  
Fondation du risque



**PATRICE GEOFFRON**

Professeur d'économie,  
Université Paris-Dauphine-PSL



**FRANCOISE GILLES**

Directrice des risques,  
Groupe AXA



**SÉBASTIEN HÉON**

Directeur adjoint  
Cyber Solutions, SCOR



**PIERRE-CHARLES PRADIER**

Économiste



**JEAN-ÉTIENNE QUINTIN**

Membre de l'Académie de marine,  
Directeur de clientèle Département Transports  
et Spécialités, DIOT SIACI



**SÉVERINE SALGADO**

Directrice générale,  
Mutualité française (FNMF)



**CAROLINE HILLAIRET**

Professeure,  
CREST & ENSAE IP Paris



**JEREMY JAWISH**

CEO et co-fondateur,  
Shift Technology



**BERTRAND LABILLOY**

Directeur général, CCR Re



**DOMINIQUE SEUX**

Directeur délégué, *Les Échos*  
et éditorialiste, France Inter



**CATHERINE TOUVREY**

Directrice générale,  
Harmonie Mutuelle



**PIERRE VALADE**

Actuaire certifié, membre de la commission  
ERM, Institut des actuaires



**OLIVIER LOPEZ**

Professeur,  
CREST & ENSAE IP Paris



**NICOLAS MARESCAUX**

Actuaire certifié, membre de la commission  
ERM, Institut des actuaires



**PIERRE MARTIN**

Historien



**PHILIPPE WAHL**

Président-directeur général,  
Groupe La Poste

SOCIÉTÉ

# La Poste, acteur de la gestion des risques face aux transitions

**PHILIPPE WAHL**

Président-directeur général du groupe La Poste



Entretien réalisé par Jean-Hervé Lorenzi, Pierre Bollon, Pierre-Charles Pradier, Daniel Zajdenweber.

## Risques

Quelle est votre perception des risques en 2024 ?

### Philippe Wahl

Au regard du contexte actuel, j'identifie principalement deux sources majeures de risques.

D'une part, le risque géopolitique. Nous traversons en effet un moment de basculement du monde au sens braudélien du terme, ponctué par de nombreuses crises géopolitiques. Ukraine, Proche-Orient, Afghanistan... L'heure est à la multiplication et à l'exacerbation des conflits et donc des risques.

D'autre part, notre époque se caractérise par la convergence d'une multitude de transitions, nos sociétés évoluant en profondeur sur plusieurs plans. Prenons l'exemple de la question démographique. Le vieillissement du monde touche bon nombre de nos sociétés, notamment dans les pays développés, et nous n'en sommes qu'au début de la prise de conscience de cette transition et de ses conséquences. Un autre exemple de transition marquante concerne l'environnement, avec comme

scénario possible celui d'un monde irrespirable. Une perspective que le film de Denis Villeneuve, *Blade Runner 2049*, sorti en salles en 2017, donne à voir avec force. Cette transition climatique est une source de risques encore inconnus.

Citons également la numérisation progressive de nos sociétés. Mutation encore plus importante qu'Internet, l'IA modifie nos modes de fonctionnement et nos cadres de pensée.

Enfin, nous sommes également très sensibles au basculement territorial, c'est-à-dire à la polarisation entre le local et le global.

La convergence de ces quatre transitions sociétales, en parallèle de la crise géopolitique, génère de l'aléatoire, du dangereux, de l'imprévisible. Cet accroissement significatif des risques entraîne de facto une hausse de la demande de protection qu'exprime la population.

## Risques

La Poste a toujours cultivé une proximité forte avec les Français. Comment cela se traduit-il dans un monde en transition ?

### Philippe Wahl

Notre mission est d'aider le grand public à affronter les transitions. Nous sommes un réassureur de risques dans la mesure où nous accompagnons les Français dans leur vie quotidienne.

Cette démarche est au cœur de notre histoire et de notre mémoire collective. Par exemple, lorsque l'instruction publique s'est démocratisée à la fin du XIX<sup>e</sup> siècle, La Poste a joué un rôle clé dans l'extension de l'écriture et de la lecture grâce à leurs pratiques de masse ; et, face à l'irruption de l'économie de la connaissance, dans la gestion de cette transition par la société.

L'autre exemple marquant qui me vient à l'esprit remonte à 1919. Au cours de cette année, nous avons lancé les comptes chèques postaux pour tous. Avant cela, ce moyen de paiement était l'apanage des hommes d'affaires. Nous avons été à l'origine de sa démocratisation.



**“Notre époque se caractérise par la convergence d'une multitude de transitions, nos sociétés évoluant en profondeur sur plusieurs plans.”**

## Risques

Aujourd’hui, face à la transition démographique et à l’isolement des populations, comment entretenez-vous cette proximité ?

### Philippe Wahl

Dès le lancement de notre plan stratégique, « La Poste 2020 : conquérir l’avenir », nous avons dressé le constat suivant : le vieillissement fragilise une partie de la population. Couplé à la numérisation, cela mène à un éloignement des êtres humains les uns des autres. Dans ce contexte, la préservation du lien social devient essentielle. Notre métier, au sens profond du terme, n’est pas seulement d’assurer la

circulation du courrier, mais de permettre au lien social de perdurer et à l’échange économique de se développer. Cette proximité, nous l’entretenons aussi en acheminant des repas au domicile des personnes âgées et fragiles. Nous accompagnons ce vieillissement en étant, une fois encore, des réassureurs de ce risque de rupture du lien social et en donnant confiance dans le futur.

## Risques

Quel regard portez-vous sur le numérique ?

### Philippe Wahl

Comme vous le savez, nous sommes fortement impactés par le numérique. Les SMS et les mails ont supplanté les lettres. Le colis s’est fortement démocratisé. Pour autant, en France, il ne compense pas la perte de revenus liée au déclin du courrier traditionnel.

Fondamentalement, une partie significative de la population se trouve exclue du numérique. Les jeunes générations n’échappent pas à ce phénomène malgré leur aisance manifeste dans l’utilisation des réseaux sociaux. Le numérique ne se limite pas aux réseaux sociaux. Il s’agit d’un parcours, il faut maîtriser son usage dans sa complexité et dans l’ensemble

de ses fonctionnalités. Nous considérons que c’est notre rôle de contribuer à la lutte contre la fracture numérique. Nous aidons ainsi ceux qui en ont besoin à effectuer leurs démarches administratives en ligne dans les bureaux de poste France services. Nous accompagnons également les seniors dans l’appropriation des usages numériques avec la tablette Ardoiz. Nous en avons commercialisé plus de 100 000. Nous avons aussi permis l’ouverture de cinq millions d’identités numériques. C’est un exemple parlant de réassurance numérique, nous diminuons les risques car nous sommes moteurs de proximité et d’accompagnement du plus grand nombre.



“Notre métier, au sens profond du terme, n’est pas seulement d’assurer la circulation du courrier, mais de permettre au lien social de perdurer et à l’échange économique de se développer.”



“Nous considérons que c’est notre rôle de contribuer à la lutte contre la fracture numérique.”

## Risques

Le numérique est source d’opportunités mais aussi de risques. La cybersécurité est-elle un enjeu important pour vous ?

### Philippe Wahl

La lutte contre les cyberattaques est une priorité pour nous et pour nos clients. Nous avons d’excellents spécialistes du sujet en interne. Je songe notamment à Guillaume Poupard, ancien directeur général de l’Agence nationale de la sécurité des systèmes d’information (ANSSI). Nous mettons tout en œuvre pour nous assurer un haut niveau de protection contre les attaques informatiques. C’est un travail de vigilance permanente.

Et il serait inexact et imprudent d’affirmer que nous pouvons résister à tout. Nous vendons par ailleurs des produits liés à l’assurance cyber. Sur le sujet, nous associons la capacité assurantielle de CNP Assurances à l’offre complète de cybersécurité pour les PME et les collectivités que Docaposte, notre filiale numérique, vient de lancer. C’est une solution qui va permettre aux organisations de taille moyenne de mieux se protéger face au risque cyber.

## Risques

Quel est le rôle de l’assurance dans le dispositif de La Poste ?

### Philippe Wahl

En 2020, nous avons construit un modèle complet de « bancassurance ». L’opération Mandarine, menée avec Éric Lombard sous l’égide de Bruno Le Maire, a permis le rapprochement du Groupe La Poste et de la Caisse des Dépôts d’une part et le rapprochement de La Banque Postale et de CNP Assurances d’autre part. Il a donc permis à La Banque Postale de se doter d’un modèle d’« assurbanque ». J’utilise cette expression à dessein car le bilan assurantiel pèse aujourd’hui plus lourd que le volet purement bancaire de La Banque Postale.

Nous avons construit un modèle stratégique qui fait ses preuves. Standard & Poor’s a d’ailleurs amélioré notre note de manière spontanée en octobre 2023, jugeant que cette orientation stratégique était un vecteur d’accroissement de notre capacité de solvabilité.

CNP Assurances, qui était un *monoline* d’assurance-vie, s’est vu doter de la capacité de devenir une compagnie d’assurance complète (habitat, voiture, prévoyance, santé, etc.) grâce à l’apport des activités non-vie de La Banque Postale. Cela conforte et diversifie le modèle de CNP Assurances et diminue sa consommation de capital.

Il y a quelques semaines nous avons annoncé la prise de contrôle des activités prévoyance et santé de La Mutuelle Générale par CNP Assurances. Aussi, cette

opération va faire de nous un acteur de ce marché qui, compte tenu du vieillissement de notre population, est appelé à prendre de l’importance.

Ce nouveau modèle sera un levier de croissance en France, en Europe mais également à l’international. Nous sommes par exemple l’un des principaux assureurs au Brésil grâce à notre partenariat avec la Caixa Econômica Federal, grande banque publique brésilienne.

Nous cherchons aussi à suivre l’évolution des risques numériques dans le champ des assurances. Réputation numérique, risques numériques spécifiques, cyberattaques, etc. Comment construire le modèle d’une assurance numérique ?

Pour finir sur ce sujet de l’assurance, nous souhaitons être le leader du développement durable dans ce domaine. Cela procède de notre attachement profond au service public. Nous estimons que La Banque Postale, banque citoyenne, qui a été la première au monde à s’engager à la sortie du financement des énergies fossiles d’ici à 2030 doit également être exemplaire en matière d’assurance responsable. C’est d’ailleurs tout le sens de l’annonce faite par CNP très récemment sur le retrait des surprimes et la fin de l’exclusion en matière d’assurance emprunteur, pour les personnes ayant surmonté un cancer du sein.

## Risques

L'an dernier, des tests de résistance menés par l'autorité bancaire européenne ont mis en lumière les fragilités de La Banque Postale. Quelle analyse dressez-vous de ces résultats ?

### Philippe Wahl

C'est une question importante pour nous. Il est bon de rappeler que ce sont des tests de résistance aux risques. Au niveau méthodologique, je tiens à dire qu'ils ont été menés selon les normes IFRS 4, alors que nous avons changé de modèle de référence. S'ils avaient été menés selon les normes actuelles, IFRS 17, les résultats auraient été différents.

La dégradation du résultat de ces tests par rapport à ceux réalisés en 2021 est liée à l'injection d'hypothèses très défavorables à La Banque Postale, notamment en raison de notre grande liquidité.

Si l'on s'intéresse à notre entropie du risque, on ne peut que constater notre solidité par rapport aux autres acteurs.

Caractérisons notre structure de risques. Nous avons, du côté de la banque, des crédits immobiliers accordés aux particuliers. Là-dessus, le risque est faible. Bon nombre de nos encours liés à des personnes morales proviennent des collectivités locales. Nous sommes les leaders du financement commercial de ces collectivités. Ce qui, là encore, présente un risque faible.

## Risques

Qu'en est-il des postes européennes ? Ont-elles amorcé une diversification semblable à la vôtre ?

### Philippe Wahl

Les Allemands ont diversifié leur poste bien avant nous, mais de manière très différente. Ils ont abandonné la banque et n'ont pas mis l'accent sur le volet service humain de proximité. En revanche, ils ont fait de leur poste un leader mondial de la logistique, derrière UPS et FedEx.

Les Italiens, qui ont une poste puissante également, se sont diversifiés en développant la banque et l'assurance mais en étant moins présents dans les activités logistiques.

Mais finalement, rares sont les postes aussi diversifiées que la nôtre.

L'attrition du courrier est un réel danger de court-moyen terme pour les postes qui n'auront pas engagé la diversification de leurs activités. Il suffit de regarder plusieurs pays dans lesquels la poste est fragilisée.

Si vous ne diversifiez pas un métier cœur qui est en difficulté, cela met en péril votre modèle stratégique. Évidemment,

diversifier c'est sortir de notre zone de confort. Nous ne pouvions pas mener les transformations que nous avons réalisées sans prendre des risques.

Nous sommes un cas emblématique d'entreprise schumpétérienne : quand des métiers disparaissent, d'autres apparaissent. Le courrier traditionnel ne représente plus que 16% de notre chiffre d'affaires. Le fait que la filiale numérique de La Poste, Docaposte, approche du milliard d'euros de chiffre d'affaires est une preuve de ce renouvellement. De même, nos services de proximité humaine, du fait des changements démographiques que nous connaissons, seront demain un élément clé de notre stratégie de lien social avec tous.

Notre responsabilité de dirigeant, c'est de pousser l'horizon stratégique le plus loin possible en mettant l'accent sur la transformation des métiers. 



**“Nous sommes un cas emblématique d'entreprise schumpétérienne : quand des métiers disparaissent, d'autres apparaissent.”**



**“Notre responsabilité de dirigeant est de pousser l'horizon stratégique le plus loin possible en mettant l'accent sur la transformation des métiers.”**





RISQUES & SOLUTIONS

# Numérique & assurance

La technologie nous a habitués à des croissances extraordinaires - au plein sens du terme - de toutes ses dimensions : performance des processeurs, capacité de stockage, nombre d'utilisateurs, investissements.

Pour autant, l'évolution récente de l'intelligence artificielle générative dépasse tout ce que nous avons connu jusqu'alors. Il a fallu à CHAT GPT cinq jours pour compter 1 million d'utilisateurs, puis deux mois pour atteindre le cap des 100 millions, alors que Netflix avait atteint le cap du million d'utilisateurs en 1 278 jours et celui des 100 millions en trois ans et demi. →



**GILLES BENEPLANC**  
Comité éditorial, Risques

•••

→ Aussi, la rubrique «Risques & Solutions» de votre revue a choisi de contribuer à la nécessaire réflexion sur l'intelligence artificielle et son impact dans les domaines de l'assurance et de la gestion des risques. Pour ne pas se perdre dans ce sujet d'une rare complexité, le questionnement doit se faire selon plusieurs angles différents.

En premier lieu, la profession doit participer au débat général sur l'intelligence artificielle et sur les transformations que son développement va engendrer pour nos sociétés. Si un premier volet est d'identifier les cas d'usages et leurs conséquences, la question fondamentale reste celle de la gouvernance, à la fois pour maîtriser les évolutions techniques de l'IA, mais également son utilisation. Il faut avancer sur la protection du droit des personnes et des entreprises et plus généralement du bien commun, sans bloquer les innovations positives. Ce débat, qui est à la fois éthique et technique, questionne le principe de précaution.

Le deuxième sujet est opérationnel. Comment les acteurs du marché peuvent-ils améliorer leur performance grâce aux possibilités offertes par l'intelligence artificielle? Tous les marchés d'assurance se caractérisent par une concurrence intense, de telle sorte que la procrastination n'est pas une option viable. Cela est d'autant plus vrai que nous ne sommes qu'aux prémices des utilisations de l'IA et que les domaines d'amélioration sont nombreux. Le premier axe de progrès qui vient à l'esprit est celui de l'efficacité opérationnelle, tout particulièrement dans la gestion administrative, mais l'IA va également transformer le cœur des métiers de l'assurance: développement commercial et marketing, souscription, indemnisation, lutte contre la fraude. Ainsi, dans un scénario optimiste, l'intelligence artificielle va faire émerger des assureurs augmentés, plus performants et plus compétents.

Dans une économie qui devient chaque jour plus digitale, le risque de cybersécurité est devenu l'un des risques majeurs auxquels tous

les acteurs économiques sont exposés. La couverture de ce risque complexe pose problème parce qu'il produit des sinistres à la fois fréquents, de haute intensité et corrélés entre eux. Pourtant, malgré ces difficultés techniques, les assureurs et les réassureurs jouent un rôle central dans la gestion et l'assurance de ces risques et il est probable que cette branche nouvelle devienne l'une des plus importantes de l'assurance de biens et responsabilités. Avec le développement de l'intelligence artificielle, les assureurs doivent analyser comment elle va déformer l'univers des risques mais aussi comment son usage peut contribuer à une meilleure analyse des risques ou à la prévention des sinistres.

Les auteurs de cette rubrique vont approfondir ces questions et contribuer ainsi à ce débat aussi passionnant que fondamental.



## EN UN COUP D'ŒIL



### BILAN DE L'ÉDITION 2024 DU CES

Grand-messe des technologies «grand public», le Consumer Electronics Show (CES) a encore connu un franc succès cette année avec 4 000 exposants et 130 000 visiteurs. Au programme, des objets connectés, des véhicules volants, smart home, exosquelettes. Certaines de ces nouvelles technologies intéressent directement les assureurs, notamment lorsqu'elles préviennent des pathologies.

### CARTOGRAPHIE PROSPECTIVE 2024 des risques de la profession de l'assurance et de la réassurance France Assureurs

Le risque de cyberattaques se maintient, de peu, en tête du classement des risques pour les entreprises d'assurance et de réassurance. Ce risque occupe cette position depuis la toute première édition de la cartographie et son score évolue peu depuis.

On constate une forte augmentation des attaques par rançongiciel (un tiers des incidents) en début d'année 2023 dans l'Union européenne, avec comme principales cibles le secteur public et en particulier les collectivités locales et les hôpitaux, dont les systèmes d'information sont insuffisamment sécurisés, avec des conséquences potentiellement très graves.

Les entreprises poursuivent la mise en application de mesures et de protocoles de sécurité, mais la sévérité des attaques pourrait s'accroître du fait du contexte géopolitique et de l'émergence de nouvelles techniques liées à l'intelligence artificielle.



### Quelques principes pour une IA éthique



- Une prise de décision humaine *in fine*
- Transparence et explicabilité
- Intégrité des données
  - Auditabilité
  - Recherche du bien commun
  - Responsabilité
  - Impartialité



### Le chiffre à retenir

# 10 trillions \$

montant estimé des dommages liés au cybercrime en 2025

# L'IA, un levier stratégique pour les assureurs

## Retour sur l'édition 2024 du Consumer Electronics Show

Le CES est l'un des plus importants rassemblements annuels consacrés aux technologies « grand public ». Avec plus de 4 000 exposants et 130 000 visiteurs, le CES 2024 a renoué avec la fréquentation d'avant-Covid. Jérôme Balmes, directeur pilotage d'activité et technologie de France Assureurs, a participé à la délégation MEDEF qui s'est rendue sur place du 8 au 12 janvier dernier.



**JÉRÔME BALMES**  
Directeur pilotage d'activité et technologie, France Assureurs

**A**vec 5,4 milliards de personnes connectées à travers la planète, soit deux tiers de la population en moyenne (40 % pour l'Afrique, 46 % pour l'Inde, 73 % pour la Chine, 87 % pour l'Europe, 92 % pour les États-Unis) et un milliard de personnes de plus qui seront connectées d'ici à 2027, la technologie a fait le tour de la planète : nous sommes une civilisation de la connectivité et de la donnée.

Cette connectivité est sans cesse plus étendue et performante avec la 5G, les objets connectés (IoT et Edge computing) et le Wifi qui sera complété sous peu par le « LiFi » : utilisation de la lumière pour l'accès à Internet. Les

infrastructures digitales ont atteint un degré de maturité très élevé et c'est la connectivité couplée au stockage (cloud) et à l'exploitation des données (IA) qui permettent de déployer logiciels et plateformes intelligents, jumeaux numériques et robotique avancée.

### Omniprésence de l'IA

« Rien de grand ne s'est accompli dans le monde sans passion » disait le philosophe... et rien de significatif ne se déploiera sans IA (la « classique » et la « générative ») dans l'univers technologique, nous dit le CES 2024. Le secteur de l'assurance est bien évidemment concerné

au premier chef par l'essor de l'IA, dont il sera à la fois utilisateur pour sa chaîne de valeur et assureur pour les usages d'autres entreprises.

Les assureurs devront continuer de s'inspirer de l'expérience client fluide et interactive déployée par les géants du e-commerce : par exemple, le suivi en temps réel sur une application mobile de sa demande d'indemnisation à la suite d'un sinistre, à l'instar de la traçabilité des livraisons jusqu'à son réfrigérateur que propose Walmart, géant américain de la grande distribution. Ils devront proposer des chatbots 24h/24 et 365 jours par an, capables d'un niveau de conversation et d'assistance égalant celui d'un service opéré par des humains – qui se concentreront sur les dossiers les plus complexes, nécessitant expertise et empathie.

Cette omniprésence de l'IA résulte de l'interaction croissante et parfois irréversible entre la notion de « produit » et celle de « logiciel ». Depuis les objets du quotidien jusqu'aux robots et machines industrielles, les capacités de ces outils sont démultipliées par les logiciels qu'ils embarquent. Ces logiciels embarqués, à partir de capteurs de plus en plus nombreux, précis, miniaturisés (caméras, sonars, radars, lidars...), permettent de conférer des degrés de sophistication et d'autonomie sans cesse plus impressionnants aux produits technologiques.

La fusion progressive entre « logiciels » et « produits » donnant naissance à des objets connectés et robots, plus ou moins automatisés, tous connectés, transforme notre environnement et représente un enjeu à double titre pour le secteur de l'assurance.

Un enjeu de résilience cyber tout d'abord avec une montée des risques autour de ce qui se passe « en ligne » mais qui peut également se passer dans le monde réel puisque des objets connectés et robots seront de plus en plus dotés de capacités d'action dans le monde physique. L'interconnectivité d'objets et de systèmes constitue un défi, du fait de l'émergence de risques « cyber-systémiques » qu'il sera parfois complexe d'appréhender pour les assureurs.

Un deuxième enjeu pour le secteur sera d'accorder une vigilance toute particulière en Europe à la révision de la *product liability directive*. Nous devons collectivement veiller à éviter deux écueils : la tentation de faire porter le risque d'innovation et le risque cyber en intégralité par les assureurs à travers des mécanismes

**Fort heureusement, nombre d'innovations technologiques s'appuyant sur l'IA constituent des leviers d'optimisation de productivité ou d'augmentation des capacités humaines – « Augmenter et non remplacer ».**

comment l'IA s'intègre progressivement au sein de l'ensemble de sa gamme, pour personnaliser ses offres de soins de la peau ou ses parfums à personnaliser.

L'autre démonstration qui a impressionné les participants fut celle de Walmart, avec une approche systématique et intégrée de la technologie et de l'IA pour l'ensemble de sa chaîne de valeur : depuis l'assistance aux collaborateurs en passant par la logistique (camions autonomes de réapprovisionnement de ses hypermarchés) et jusqu'au dernier kilomètre (livraison par drones, livraison personnalisée jusqu'au sein de son réfrigérateur – intégrant une IA passant commande automatiquement).

Une IA omniprésente ainsi que des outils et robots de plus en plus efficaces et automatisés viennent couvrir des besoins sensiblement équivalents à travers la planète :

- difficulté à recruter et à fidéliser sur des métiers pénibles (logistique des entrepôts par exemple) ;
- pénurie de salariés qui ne sont plus revenus dans certains secteurs à la suite du Covid (transport routier...);
- vieillissement de la population et difficultés de recrutement dans le secteur de la santé.

Fort heureusement, nombre d'innovations technologiques s'appuyant sur l'IA constituent des leviers d'optimisation de productivité ou d'augmentation des capacités humaines (exosquelettes pour soulager les personnes manipulant les malades par exemple) – « augmenter et non remplacer ».

d'assurance obligatoire et la tentation de tout judiciaireiser. L'établissement des responsabilités devra en effet rester fluide et souple pour préserver une assurabilité à des coûts raisonnables.

Ces systèmes d'IA et logiciels ont besoin d'une puissance de calcul de plus en plus importante pour exploiter les données fournies par les différents capteurs, afin d'en tirer des « enseignements » et aboutir à des « prises de décision » : la définition même de l'intelligence artificielle.

Il est donc logique de constater que la plupart des secteurs sont désormais concernés par les progrès technologiques en lien avec l'intelligence artificielle. Une des présentations les plus réussies au cours de cette édition 2024 du CES, car inattendue, fut celle de L'Oréal, démontrant

Néanmoins se dessine aussi en creux un univers technologique très abouti, avec des robots qui pourraient devenir omniprésents, pour nous simplifier la vie, servir de compagnons éducatifs à nos enfants, améliorer prévention et santé au quotidien, nous apporter assistance en situation de handicap, de dépendance ou de grand âge... mais un univers qui serait de plus en plus dépourvu d'humains. États-Unis, Europe, Japon, Corée du Sud illustrent la tendance de certaines sociétés à vouloir se refermer sur elles-mêmes, tout en pariant sur l'IA et les robots.

### Mobilité connectée et automatisée, livraisons, véhicules volants

Automatisation, connectivité et électrification continuent d'être les trois axes majeurs de

transformation du monde automobile – avec l'IA comme «chef d'orchestre» des technologies mises en œuvre.

Des robotaxis sillonnent ainsi les rues de Phoenix, 24h/24 et 365 jours par an (plan à damier, météo très clémente toute l'année...) mais aussi désormais de San Francisco (géographie urbaine plus complexe) et de Las Vegas (avec un réseau de tunnels conçu par Tesla, prévu pour desservir aéroport, stade et une trentaine d'hôtels) même si les autorisations d'opérer sans chauffeur «de secours» sont parfois retirées temporairement, dans le cadre d'enquêtes à la suite d'accidents.

De son côté, Walmart utilise une flotte de camions d'approvisionnement autonomes depuis ses entrepôts vers les hypermarchés du groupe, en empruntant des parcours précis, pour faire face à la pénurie de chauffeurs routiers depuis la fin de la crise sanitaire. Le géant de la grande distribution a aussi déployé des drones autonomes de livraison de petits colis et médicaments, desservant 200 000 logements dans une sorte de bêta-test géant.

Mais c'est en dehors des voies publiques, à faible vitesse et sur des domaines d'emploi circonscrits et plus sécurisés (absence d'autres véhicules, piétons, cyclistes...) que les véhicules autonomes sont désormais arrivés à maturité avec les engins agricoles et de chantier autonomes, depuis les mini-pelleteuses pour environnement urbain aux bulldozers et camions géants de transport de gravats dans des sites miniers.

Au-delà de ces cas d'usage terrestres, la volonté de développer des véhicules volants à décollage et atterrissage vertical – «VTOL» – persiste et fait face sur le papier à moins de complexité, au moins en phase de vol (possibilité de créer des couloirs virtuels, pas de cyclistes ou de piétons...). Ces véhicules volants, électrifiés, très silencieux et beaucoup moins polluants que les hélicoptères traditionnels (sous réserve de disposer d'électricité décarbonée) se heurtent néanmoins à des réticences des autorités de régulation (les Asiatiques étant les plus permissifs, les Nord-Américains plus souples et les Européens les plus rigides...). Ces nouveaux aéronefs au design souvent sublime devraient donc demeurer au stade expérimental, au moins encore jusqu'à la fin de la décennie.

### Smart Home

Le grand enjeu des *Smart Homes* est le «contrôle» via une enceinte connectée, son smartphone... ou son téléviseur: tous les constructeurs cherchent à déployer une ou plusieurs interfaces simples et intuitives permettant d'allumer / éteindre à distance des appareils (lave-linge, volets roulants, éclairage), d'optimiser sa consommation d'électricité ou d'eau ou de vérifier à distance le contenu de son frigo (quand ce n'est pas le frigo intelligent lui-même qui commande un réapprovisionnement en fonction de son analyse de la consommation hebdomadaire...). On notera aussi l'émergence de robots domestiques de plus en plus «multi-tâches» (au-delà du simple aspirateur autonome): gestion de visiteurs et de l'animal domestique, robot de compagnie pour les personnes âgées (avec rappel des heures de prise de médicament, dispositifs de veille anti-chute), robot-compagnon éducatif pour les enfants...

Les progrès de la robotique sont nourris par les progrès de l'intelligence artificielle: ce sont les IA qui permettent à une même enveloppe «physico-mécanique» de passer des doigts gourds et maladroits d'il y a quelques années au robot Tesla, capable de saisir un œuf et de le manipuler sans le casser. Et si l'on ajoute au mix les capacités de conversation de l'IA générative, conjuguées à des apparences de plus en plus humanoïdes, nous nous rapprochons à grands pas d'un monde au sein duquel humains et robots cohabiteront et «échangeront» au quotidien.

### Santé et inclusivité

En matière de santé, l'IA confère désormais une très grande fluidité et précision dans la gestion de mouvements des exosquelettes: une entreprise coréenne a ainsi dévoilé une petite ceinture dotée de deux bras articulés que l'on vient accrocher à hauteur des genoux. Ce dispositif très léger (2,5 kg) permet pendant trois ou quatre heures à une personne à mobilité réduite, en rééducation ou souffrant de certaines maladies (Parkinson) de soulager jusqu'à 20 % du poids du corps, tout en veillant à la stabilité de la marche, par un mécanisme de compensation de la force appliquée à une jambe par rapport à une autre. C'est probablement dans les pavillons dédiés à la santé de

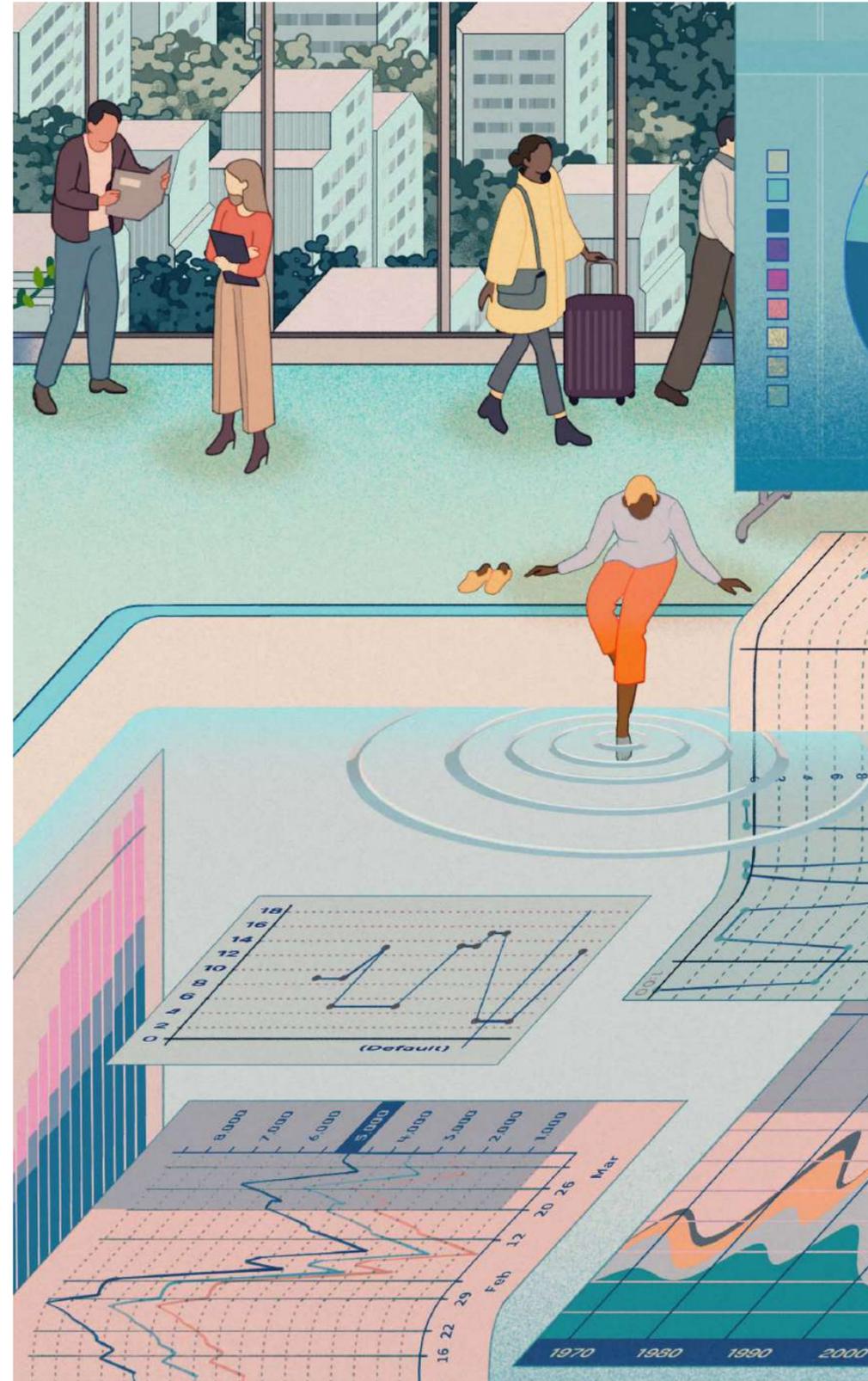
demain et à l'inclusivité que l'on constate à quel point la technologie peut être mise au service d'enjeux majeurs pour des pans entiers de la population mondiale.

Siemens a ainsi dévoilé des prothèses en 3D et pilotées par IA, permettant à un enfant de réaliser l'apprentissage de l'utilisation de son nouveau bras artificiel en quinze minutes au lieu de six mois à un an. Le coût de fabrication est par ailleurs abaissé à moins de 10 000 euros vs 100 000 euros grâce à l'impression 3D. D'autres acteurs ont exposé des dispositifs permettant d'assister les personnes à mobilité réduite, souffrant d'un handicap (vision, ouïe) ou de soulager les personnels médicaux (fauteuils autonomes de transfert de malade d'un service à un autre).

L'utilisation combinée de capteurs miniaturisés et d'IA permet également de déployer des «wearables» (objets connectés que l'on porte sur soi) de plus en plus performants, pour réaliser toute une gamme de mesures allant du bien-être à la prévention et jusqu'au champ médical. De nombreux cas d'usage sont visés autour de la qualité du sommeil, la mesure du taux d'oxygène dans le sang ou du rythme cardiaque. Le «Gaal ultime» en matière d'objets connectés demeure la mesure non-invasive (sans piqûre) du taux de glycémie pour les personnes prédiabétiques ou diabétiques – à l'aide d'un capteur suffisamment miniaturisé pour pouvoir être intégré un jour dans une montre connectée.

De nombreuses start-ups et entreprises cherchent aussi à enrichir les possibilités d'exams à distance et en téléconsultation, pour faire face à la pénurie de personnels médicaux qui touche de nombreuses zones géographiques: Withings a ainsi présenté un dispositif de «check-up» complet que l'on peut réaliser soi-même avant envoi à un médecin à distance (température, rythme cardiaque, saturation en oxygène, stéthoscope digital). Une autre entreprise a présenté un robot doté d'une caméra articulée permettant de réaliser un bilan dermatologique sur l'ensemble de son corps dans une cabine d'examen.

L'impressionnante dynamique des technologies autour du bien-être, de la santé ou dans le champ médical est elle aussi riche de promesses pour les assureurs. Il devient envisageable – sous réserve du consentement



préalable des personnes concernées – de déployer des stratégies à grande échelle de prévention avec mesure d'efficacité comparée et de rechercher des parcours de soin ou de rééducation optimisés.

Le déploiement d'exosquelettes en logistique ou sur des chantiers pourrait ainsi être encouragé pour prévenir les troubles musculo-squelettiques. Les montres connectées pourraient faire l'objet de subventions à des fins de prévention de certaines pathologies cardiovasculaires (fibrillation atriale ou arythmies). Pour permettre le maintien à domicile de personnes âgées et dépendantes, il existe désormais de nombreux types de détecteurs de chute à domicile (très protecteurs pour la vie privée car reposant sur des radars plutôt que des caméras). Enfin, afin d'encourager l'observance et de limiter les dépenses de transport, de nombreuses solutions de rééducation à domicile sont désormais disponibles.

Toutes les parties prenantes – dont les assureurs – auraient à gagner à évaluer collectivement et à déployer certaines de ces solutions lorsqu'elles sont suffisamment éprouvées – la prévention demeurant le parent pauvre de notre système de santé.

Au terme de cette «déambulation virtuelle» et de cette petite sélection loin de viser à l'exhaustivité, on notera enfin que les enjeux de durabilité ont semblé être mis en avant de manière plus prononcée que les années précédentes. La technologie constitue en effet un levier particulièrement prometteur pour faire face à la transition climatique. L'investisseur emblématique de la Silicon Valley, Marc Andreessen, fait même de ce levier l'alpha et l'oméga de toute stratégie pour préserver l'humanité dans le futur, à travers son *Techno-Optimist Manifesto*. Entre appels à la décroissance d'un côté et projets «techno-solutionnistes» de l'autre, la préservation de notre planète passera vraisemblablement par un chemin de crête entre ces deux extrêmes. 📌

# Éthique de l'IA dans l'assurance : entre innovation et responsabilité

2023 a semblé marquer l'avènement de l'IA générative : ses modèles, qui s'appuient sur des fondations comme GPT-4 d'OpenAI, ont été entraînés sur des ensembles massifs de données. Ils ont ainsi acquis la capacité à reconnaître des modèles de langage naturel, ce qui leur permet de générer du texte, des images ou de la musique de manière convaincante. De nombreux assureurs commencent à explorer le potentiel des grands modèles de langage (LLM) en gestion des risques et doivent relever le défi de fournir à leurs clients un accès simple et compréhensible à des données, des modèles et des outils complexes. Ces innovations ouvrent un débat éthique autour de l'intelligence artificielle, à tel point que les risques liés à celle-ci inquiètent et font leur entrée fracassante dans le top 5 des grands risques auxquels nos sociétés doivent faire face ! 2024 sera-t-elle l'année de l'IA responsable ?

## Trois grands principes éthiques pour bâtir une intelligence artificielle responsable<sup>1</sup>

Si l'IA révolutionne le secteur de l'assurance, elle ouvre un débat sur la nécessité de sa mise en œuvre éthique pour éviter de créer de l'antisélection ou de la discrimination. Pour ce faire, les acteurs du marché devront faire preuve de vigilance sur les usages et travailler de concert avec des spécialistes de l'éthique.

L'éthique dans l'intelligence artificielle (IA) repose sur trois grands principes orientant nos actions, distinguant le bien du mal dans nos sociétés. Cette distinction devient primordiale dans le secteur de l'assurance, où les décisions algorithmiques influent de manière significative sur les vies et les biens. En encadrant l'IA autour du bien commun, du respect de

l'autonomie individuelle et de la promotion de l'équité et de la justice, l'éthique en IA aspire à diriger l'emploi de ces technologies vers des applications bénéfiques pour tous.

• **Bienfaisance** : L'IA en assurance doit viser à améliorer le bien-être des individus. Un défi éthique majeur se présente lorsque les systèmes d'IA aboutissent involontairement à exclure certains groupes vulnérables en raison de biais dans les données d'entraînement. Par exemple, dans le processus d'évaluation des risques, l'usage d'algorithmes doit



**DAVID DORN**  
Partner, Deloitte Insurance



**RICHARD EUDES**  
Managing Director, Risk Advisory, Deloitte

s'accompagner d'une vigilance constante pour éviter les biais qui pourraient mener à des décisions préjudiciables. La bienfaisance se manifeste également dans le développement de systèmes d'IA qui facilitent une indemnisation rapide et juste des sinistres, améliorant ainsi l'expérience client.

• **Justice** : Une distribution équitable des avantages et des charges est cruciale. L'IA doit traiter chaque individu de manière équitable, sans discrimination. Les assureurs doivent s'engager dans une démarche transparente d'audit et de correction des algorithmes pour garantir une équité réelle dans la tarification et l'offre de services. Cela implique une analyse rigoureuse et une correction des biais potentiels dans les données d'entraînement des algorithmes.

• **Autonomie** : La transparence des systèmes d'IA en assurance encourage l'autonomie des utilisateurs en leur permettant de comprendre comment les décisions sont prises. Cela peut inclure des explications sur la manière dont les primes sont calculées ou les réclamations évaluées et traitées. Favoriser l'autonomie signifie également garantir le contrôle des individus sur leurs données personnelles, conformément aux principes de consentement éclairé et de respect de la vie privée. Par exemple, dans le contexte de l'assurance santé, l'utilisation des données de santé pour personnaliser les offres doit être conditionnée par un consentement explicite des clients, garantissant ainsi leur autonomie dans la décision.

En mettant en avant ces principes éthiques et en s'engageant activement dans leur application, le secteur de l'assurance pourra évoluer à l'ère de l'IA avec intégrité, en construisant une relation de confiance durable avec ses clients.

## IA et relation client : entre satisfaction accrue et enjeux éthiques majeurs

L'adoption croissante de l'IA transforme la relation avec les assurés et améliore leur satisfaction ; elle soulève également des défis éthiques significatifs auxquels le secteur s'adapte.<sup>2</sup>

• **Biais et discrimination**. Un rapport de la CNIL<sup>3</sup> a souligné la nécessité d'une vigilance

renforcée contre les discriminations potentielles introduites par les algorithmes d'IA. En réponse, certaines compagnies d'assurance ont commencé à implémenter des outils d'audit algorithmique pour détecter et corriger les biais dans leurs systèmes d'évaluation des risques et de tarification. Par exemple, un assureur a ajouté des sauvegardes intégrées aux algorithmes d'IA pour éviter la discrimination dès la conception. Par ailleurs, l'équipe de recherche de cet assureur a développé une « boussole de l'équité » qui s'attaque à la surabondance d'informations empêchant les professionnels de sélectionner la mesure d'équité la plus appropriée.

• **Manque de transparence**. L'Autorité européenne des assurances et des pensions professionnelles (EIOPA)<sup>4</sup> a publié des lignes directrices soulignant l'importance de la transparence et de l'explicabilité des décisions algorithmiques. En réponse à ces recommandations, les assureurs entreprennent de plus en plus d'actions pour renforcer la transparence, en clarifiant les méthodes et les raisons qui président à certaines décisions de souscription ou de tarification, améliorant ainsi la confiance et la compréhension des assurés vis-à-vis de l'utilisation de l'IA.

• **Érosion de la vie privée**. Le règlement général sur la protection des données (RGPD)<sup>5</sup> en Europe a établi un cadre rigoureux pour la gestion des données personnelles. Un acteur du monde de l'assurance a adapté ses pratiques de collecte et de protection de données pour se conformer au RGPD, en fournissant une information détaillée sur leurs traitements et leur finalité, tout en garantissant le consentement explicite des clients avant l'utilisation de leurs données personnelles dans ses modèles d'IA.

• **Responsabilité insuffisante**. Certaines juridictions élaborent des cadres législatifs pour clarifier la responsabilité en cas de dommages causés par des systèmes d'IA. Dans ce contexte, la Commission européenne est intervenue en 2022 afin d'introduire des règles spécifiques aux dommages causés par un système d'IA, protéger les victimes et leur garantir une réparation.

Ces exemples illustrent les efforts déployés par les compagnies d'assurance et les régulateurs pour aborder les défis éthiques posés par l'IA. En adoptant une approche proactive pour garantir l'équité, la transparence, la protection

de la vie privée et la responsabilité, le secteur de l'assurance pourra appréhender le panorama complexe de l'IA, tout en préservant la confiance et l'intégrité du marché.

## Les enjeux de la réglementation de l'IA dans le secteur de l'assurance

Face aux défis éthiques imposés par le développement de l'IA, les réglementations se multiplient et évoluent rapidement. Imposant des normes strictes pour l'utilisation des données et l'application des technologies d'IA, elles deviennent à leur tour un défi majeur pour le secteur de l'assurance. Pour autant, se conformer à ces règles est crucial, non seulement pour protéger les assurés, mais parce qu'en définissant des attentes claires en termes de justice, de transparence et de contrôle humain, elles encouragent l'innovation responsable.

Pour aligner leurs opérations sur ces exigences réglementaires, les assureurs devront adopter une stratégie proactive<sup>6</sup>, impliquant :

1. **L'intégration de valeurs éthiques** : ancrer chaque initiative IA dans les valeurs fondamentales de l'entreprise pour garantir une congruence avec sa mission globale.
2. **La diversité des équipes** : former des groupes de travail hétérogènes pour créer des solutions IA inclusives, répondant aux divers besoins des clients.
3. **La gouvernance des données** : établir des politiques rigoureuses pour assurer la fiabilité et la traçabilité des données traitées par l'IA.
4. **La spécificité des systèmes d'IA** : veiller à ce que les applications d'IA soient précisément conçues pour des tâches définies, avec des mécanismes de validation et de vérification pour en garantir la robustesse et la fiabilité.

Ainsi, pour anticiper efficacement ces changements réglementaires, il est conseillé aux assureurs :

- **D'évaluer les systèmes d'IA existants** en réalisant un audit pour mesurer l'impact des nouvelles réglementations sur les opérations.
- **D'identifier les besoins de conformité** en analysant les écarts entre les pratiques en place et les exigences pour les systèmes à haut risque.

# 4 Cas d'usage réussis de l'IA éthique en assurance :

Déjà déployés par certaines entreprises d'assurance, les exemples ci-dessous démontrent l'impact positif que l'IA éthique peut avoir sur le secteur, offrant des avantages tangibles tant pour les entreprises que pour les consommateurs :



**Recours à l'IA pour l'analyse des images satellite et drone afin d'accélérer l'évaluation des sinistres. C'est une illustration parfaite d'utilisation de l'IA pour améliorer l'efficacité tout en adhérant à des normes élevées de gouvernance numérique et de protection de la vie privée.**



**Engagement en faveur d'une IA basée sur l'équité, l'éthique, la transparence et la supervision humaine. Cette stratégie souligne l'importance de développer des technologies à la pointe et alignées sur des principes éthiques solides.**



**Mise en avant de l'importance de l'adhésion au consentement pour une utilisation éthique des données et d'IA, améliorant ainsi la relation client et optimisant la gestion interne.**



**Institution d'une gouvernance d'IA mettant l'accent sur l'humain et l'éthique, avec un comité dédié au développement d'outils d'IA transparents, justes et respectueux.**

En adoptant une approche centrée sur l'éthique, les compagnies d'assurance peuvent ainsi naviguer avec succès dans les défis posés par l'IA, tout en renforçant la confiance et l'engagement envers leurs clients.

- **De développer des stratégies d'adaptation** en mettant en œuvre un cadre de gouvernance adapté aux spécificités de l'IA.
- **De renforcer les compétences des collaborateurs** en investissant dans la formation des équipes pour leur permettre de s'approprier ces nouveaux contextes réglementaires.

que ces systèmes sont développés et utilisés de manière responsable. Deloitte a conçu son propre cadre «Trustworthy AI™»<sup>7</sup> pour aider les entreprises à préserver l'éthique à chaque étape du cycle de vie de l'IA. Il met en avant six dimensions clés d'une IA digne de confiance : la transparence, l'équité, la robustesse, la protection de la vie privée, la sécurité et la responsabilité.

Les Directives de l'EIOPA de 2021<sup>8</sup> fournissent également un exemple concret de gouvernance solide pour l'IA. Elles sont conçues pour assurer que les systèmes d'IA dans l'assurance sont développés et utilisés de manière à respecter pleinement les droits et la dignité des individus.

Pour ancrer l'éthique au cœur des initiatives d'IA, les compagnies d'assurance doivent aller au-delà de la conformité réglementaire et

adopter une démarche proactive vis-à-vis des enjeux éthiques. « Développer des codes de conduite et des programmes de formation pour sensibiliser à l'éthique de l'IA est essentiel », suggère le Deloitte AI Institute<sup>9</sup>. Cela implique un engagement de toutes les parties prenantes, y compris les dirigeants, les collaborateurs et les clients, dans le développement et l'utilisation responsable de l'IA.

Ainsi, la gouvernance éthique de l'IA n'est pas seulement une question de conformité légale ; c'est un engagement envers une innovation qui respecte les droits et la dignité de tous. En plaçant l'éthique au premier plan, les compagnies d'assurance peuvent suivre l'évolution technologique, tout en construisant une base solide pour un avenir durable et équitable.

## Stratégies concrètes pour une intégration éthique de l'IA en assurance

L'intégration éthique de l'IA dans le secteur de l'assurance exige donc une combinaison de conscience, de responsabilité et d'approches innovantes. Voici quelques axes stratégiques concrets pour atteindre cet objectif :

**Responsabilité et conscience.** « La première étape vers une IA éthique est la reconnaissance de sa puissance et de ses limites », souligne un rapport de DreamQuark sur l'éthique de l'IA dans le secteur financier<sup>10</sup>. La responsabilité doit être partagée à tous les niveaux de l'organisation, des développeurs d'IA aux dirigeants.

**Diversité des équipes.** La pluridisciplinarité des équipes de conception et de développement d'IA est cruciale pour comprendre et incorporer les nuances éthiques, sociales et techniques. « Intégrer une variété de perspectives et d'expertises peut réduire les risques de biais et promouvoir une IA plus inclusive, » affirme un rapport de l'EIOPA.

**Contrôle continu.** Des protocoles de révision régulière et d'évaluation sont nécessaires pour identifier et corriger rapidement tout écart par rapport aux principes éthiques.

**Assurance d'une IA équitable.** Pour garantir l'équité de l'IA, les compagnies d'assurance doivent adopter des outils et des méthodes d'évaluation et de rectification des biais algorithmiques.

## Check-list pour une IA équitable pour tous :

📌 **conseil sans décision :** L'IA devrait servir de support pour offrir des conseils et des recommandations, laissant toujours la décision finale à l'humain.

📌 **transparence et explicabilité :** Les mécanismes décisionnels de l'IA doivent être accessibles et compréhensibles, permettant aux clients et aux professionnels de l'assurance de suivre et comprendre les raisonnements à l'origine de chaque décision.

📌 **intégrité des données :** Les données doivent être exemptes de toute manipulation ou falsification, assurant l'authenticité et la fiabilité des informations produites par l'IA.

📌 **bien commun :** Les applications de l'IA doivent être évaluées sur leur capacité à servir l'intérêt général, mettant en évidence son importance pour le progrès social et économique.

📌 **auditabilité :** Les systèmes d'IA doivent permettre une surveillance efficace pour détecter et corriger les erreurs, avec une intervention humaine possible en cas de nécessité.

📌 **responsabilité et gouvernance :** Les choix de gouvernance autour de l'IA doivent refléter une responsabilité éthique, se questionnant sur l'usage de la technologie pour compléter l'humain plutôt que de le remplacer, et sur son utilité ultime pour la société.

📌 **impartialité :** Il est crucial que l'IA soit développée pour prendre des décisions objectives, évitant tout biais discriminatoire et garantissant une égalité de traitement pour tous les clients.

**Qualité et diversité des données.** L'engagement pour une collecte de données éthique et transparente est un pilier pour une IA équitable. « Assurer une collecte de données exhaustive et représentative est essentiel pour développer des systèmes d'IA justes », note un rapport de l'AI Act de l'UE.

**Cybersécurité.** La mise en œuvre de mesures de sécurité avancées est essentielle pour protéger les données sensibles des assurés contre les violations, permettant de maintenir la confiance des clients et la conformité réglementaire.

**Ethics by design.** L'intégration de principes éthiques dès la conception des systèmes d'IA est fondamentale pour maximiser le bien-être, réduire les inégalités et soutenir l'autonomie. Des procédures de développement et de surveillance proactive sont indispensables pour identifier et corriger rapidement toute défaillance, garantissant ainsi une application éthique de l'IA à travers son cycle de vie.

En adoptant ces stratégies, les compagnies d'assurance peuvent garantir une utilisation avancée d'IA sur le plan technologique et alignée sur des principes éthiques rigoureux. Cela soutient les initiatives d'IA responsables et bénéfiques pour la société, renforçant la confiance et la durabilité dans le secteur de l'assurance.

## Perspectives sur l'évolution de l'IA dans l'assurance et son impact éthique

Pour instaurer une IA éthique, les compagnies d'assurance devront en premier lieu définir un cadre éthique robuste. Avant tout déploiement à grande échelle, il est crucial d'établir des fondations éthiques solides qui guideront l'utilisation de l'IA. Ce cadre doit être évolutif pour s'adapter aux changements technologiques et réglementaires et créé en collaboration avec des experts en éthique de l'IA. Dans un deuxième temps, une réflexion approfondie sur les objectifs et les valeurs que l'entreprise cherche à promouvoir est nécessaire. Ceci déterminera les domaines où l'humain doit rester prépondérant et ceux où l'IA peut apporter une valeur ajoutée, en prenant en compte le point de vue des clients pour renforcer leur confiance.



### Notes

<sup>1</sup> Designing an AI ethics framework | Deloitte Insights

<sup>2</sup> Balancing AI ethics and bias | Deloitte Insights

<sup>3</sup> Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle (CNIL)

<sup>4</sup> Artificial Intelligence and the Insurance Industry | Deloitte UK. Ethics Guidelines for AI. European Insurance and Occupational Pensions Authority (EIOPA)

<sup>5</sup> Règlement général sur la protection des données - RGPD (CNIL)

<sup>6</sup> Trustworthy AI Governance in Practice | Deloitte US

<sup>7</sup> Trustworthy AI (deloitte.com). State of AI in the Enterprise, 2<sup>nd</sup> Edition, Loucks, Davenport, and Schatsky | Deloitte Insights

<sup>8</sup> Guidelines - European Union (europa.eu). Artificial Intelligence governance principles: towards ethical and trustworthy Artificial Intelligence in the European insurance sector

<sup>9</sup> Deloitte AI Institute - AI Insights | Deloitte US

<sup>10</sup> How is responsible AI changing the banking and insurance industries - Dreamquark

L'IA révolutionne le secteur de l'assurance, promettant d'améliorer l'efficacité et l'accessibilité des services. Toutefois, une mise en œuvre éthique est cruciale pour éviter les écueils potentiels comme l'antisélection ou la discrimination. Une démarche proactive, en collaboration avec des spécialistes de l'éthique, et une vigilance constante sur les pratiques de développement et d'utilisation de l'IA, est essentielle pour maintenir la confiance et assurer une évolution positive et équitable du secteur. 📌

# Comment redessiner l'assurance avec l'IA générative ?

Avec esprit critique et co-intelligence

Comment l'intelligence artificielle générative redessine-t-elle l'assurance ? Décryptons son impact, confrontons les défis éthiques et sociaux et naviguons entre la co-intelligence et la décision humaine, pour esquisser un secteur plus résilient.



**NICOLAS MARESCAUX**  
Actuaire certifié, membre de la commission ERM, Institut des actuaires



**FLORENCE PICARD**  
Actuaire certifiée, membre du Directoire, Fondation du risque



**PIERRE VALADE**  
Actuaire certifié, membre de la commission ERM, Institut des actuaires

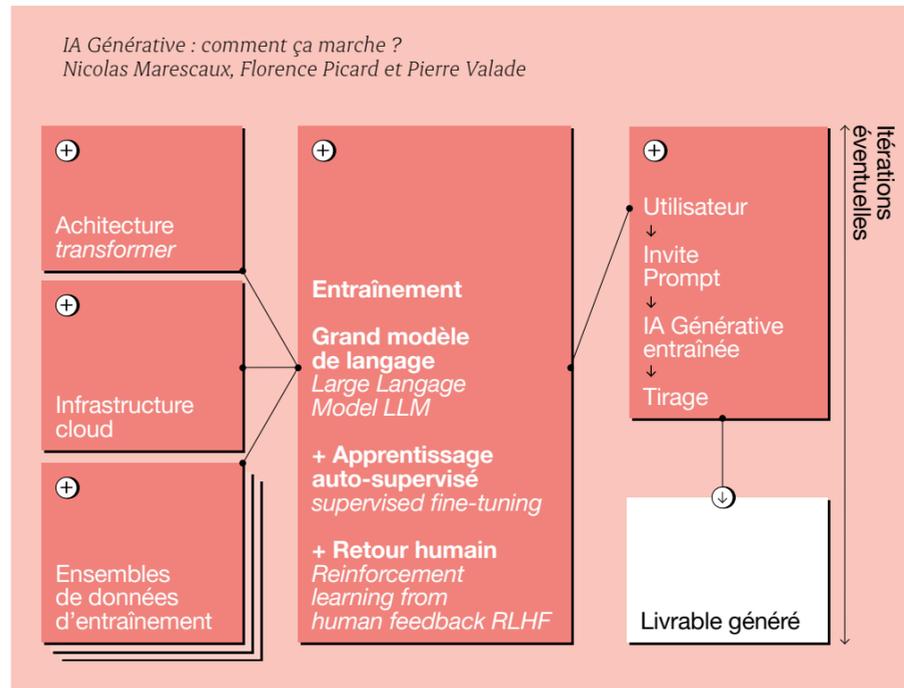
## Appliquons le levier de transformation cognitive de l'IA générative à l'assurance

**Une utilisation réussie de l'intelligence artificielle dans le secteur de l'assurance suppose une vigilance et un esprit critique fort face aux complexités des algorithmes et de rechercher à renforcer la performance humaine par le développement d'une forme de co-intelligence.**

Dans l'enceinte de l'Université Paris-Dauphine, l'amphithéâtre Raymond-Aron, là où les échos du Conseil de l'Otan résonnaient avec gravité, accueille le Printemps de l'assurance. Sous la maxime latine *Animus in consulendo liber* (« délibérer l'esprit libre ») – la communauté assurantielle confronte l'intelligence artificielle générative (GenAI) à l'épreuve du partage

des risques, soulignant l'importance de l'esprit critique et de la co-intelligence.

L'intelligence artificielle, c'est « ce qu'un ordinateur ne peut pas encore faire ». Nous avons inventé la roue, qui augmente nos capacités physiques, les tableurs, qui automatisent des tâches complexes et maintenant GenAI, capable d'émuler les productions créatives humaines, sur la base des créations passées. La puissance de GenAI repose sur un travail statistique massif, le volume des données, la puissance des processeurs, le nombre de paramètres et



l'efficacité des algorithmes, même si GenAI n'a pas encore démontré sa capacité à produire du désir, une intention ou un objectif, qui restent les prémisses de toutes ces productions. Les technologies cognitives d'application générale telles que l'écriture, l'alphabet, l'imprimerie et GenAI ont un impact sur notre perception et interaction avec le monde. Pour reprendre Marshall McLuhan, les nouveaux outils sont d'abord conçus pour s'adapter aux flux de travail existants mais, au fil du temps, les flux de travail changent pour s'adapter aux outils.

GenAI s'est démocratisée grâce à son interface, son adaptabilité et ses gains d'efficacité. Un algorithme de tirage stochastique va choisir les mots de la réponse. Pour l'améliorer, fournissez du contexte dans votre prompt afin d'orienter l'IA vers un volet plus pertinent de ses connaissances. Les grands modèles de langage s'inspirent ainsi d'une structure fondamentale des sociétés humaines : chacune de nos actions est au croisement de notre passé incorporé, sous la forme de dispositions à agir, sentir, penser, ou de compétences, et des propriétés du contexte dans lequel nous agissons. Bernard Lahire l'énonce ainsi : *Dispositions (passé incorporé) + Contexte (présent) = Pratiques*.

Quels impacts sur l'assurance, qui touche tous les domaines de la vie ? L'assurance fonctionne selon un cycle de production inversé, où

l'assureur fixe un prix de vente avant de connaître son prix de revient. L'IA peut améliorer le repérage et la mesure du risque et favoriser les mesures de prévention. Elle fluidifie l'aiguillage et la gestion de flux irréguliers et volumineux. Elle aide à détecter les fraudes, dont la résolution profite à l'ensemble des assurés. Elle appuie les conseillers pour expliquer le contenu d'un contrat de manière simple. De la connaissance des personnes et des biens à la gestion des contrats et des sinistres, elle renforce l'efficacité, la précision et la personnalisation. En acquisition, elle produit du contenu optimisé pour les moteurs de recherche. En relation client, elle trie les mails, prépare des réponses, remplit un formulaire. En souscription, elle comprend les besoins spécifiques des clients et propose des contrats adaptés. En cas de sinistres, elle fournit les règles de gestion à appliquer. En analyse de données, elle aide à structurer le travail, contrôler la qualité, nettoyer, analyser de grands volumes de données non structurées. En programmation, elle génère du code, traduit un langage, accélère le développement de modèles plus avancés. En documentation, elle analyse et résume rapidement des documents ou appels d'offres et produit des rapports automatisés. Par exemple, Antoine Heranval, qui pour sa thèse avec la Mission des Risques Naturels, a appliqué des méthodes d'apprentissage statistique pour évaluer la nature et le

coût des dommages, indique qu'aujourd'hui GenAI l'aiderait à mieux analyser les données textuelles des rapports d'expertise pour étudier la sinistralité à l'échelle fine du bâti.

Mais GenAI, comme l'art et toutes les technologies, produit du faux ou altère notre perception de la réalité.

## Confrontons les limites des algorithmes sournois

L'intégration de GenAI dans la société soulève des interrogations : manque de gouvernance, perte de confiance, érosion des valeurs, évolution des compétences requises, impact environnemental, utilisation abusive avec le cyber-piratage, la contrefaçon, ou la désinformation qui, comme le souligne Pierre-Marie Lledo, peut miner le tissu même de notre société démocratique. Alors que 2024 est la plus grande année électorale de l'histoire de l'humanité, la géopolitique de l'IA révèle des tensions entre la vision stratégique des États-Unis, l'approche centralisée de la Chine et les défis réglementaires européens. L'AI Act a été approuvé par le Parlement européen le 13 mars 2024. Le débat sur la responsabilité civile de l'IA est en cours.

Luc de Brabandere, mathématicien, accole l'adjectif « sournois » aux algorithmes qui restent en partie cachés et incompréhensibles. GenAI peut reproduire des bruits ou cristalliser des biais existants dans les données d'apprentissage. Des problèmes techniques peuvent interrompre la continuité des opérations. Des brèches peuvent exposer des données sensibles. GenAI peut produire des résultats incohérents, inattendus, opaques. Par exemple, la génération de code informatique fonctionne comme un langage sans notion mathématique. L'interprète de code aide à traiter des données rapidement et de manière accessible. Il permet à toute personne d'agir en analyste de données sans en avoir les compétences. Faute d'une connaissance approfondie des méthodes analytiques, l'outil pourrait contribuer à propager des informations erronées.

« Toute technique suffisamment avancée est indiscernable de la magie », rappelait Arthur C. Clarke. Flaubert, dans son *Dictionnaire des idées reçues*, ajouterait une nouvelle entrée autour de la prédictibilité. Si avec l'IA,

L'assureur peut mieux prédire, certains profils ne pourront plus être protégés? L'IA n'apporte pas plus à la connaissance du risque que ne pourraient le faire des statistiques très fines. Elle calcule vite mais ne peut pas prédire qui aura l'aile gauche avant de son véhicule embouti par un camion entre 15 heures et 15 h 30 demain place de l'Étoile ou votre date de décès. Le remède réside dans un choix de société sur la nature du contrat social: quels aléas font l'objet d'une mutualisation et lesquels d'un tarif individualisé?

Selon Universcience, une part significative de la population aborde l'IA avec prudence: 31% des sondés la perçoivent comme un risque pour l'emploi, alors que 34% considèrent qu'elle offre autant de risques que d'avantages. Ces inquiétudes peuvent être modérées par deux paradoxes. Hans Moravec, expert en robotique, stipule que «ce qui est facile pour l'homme est souvent difficile pour la machine»: les compétences humaines uniques, telles que l'empathie et la créativité, ne peuvent être facilement remplacées. Michael Polanyi, philosophe, souligne que «nous en savons plus que ce que nous pouvons exprimer»: de nombreuses tâches ne peuvent pas être verbalisées ou codées. GenAI peut automatiser certaines tâches mais ne peut pas remplacer complètement les travailleurs humains. Elle peut aider à gérer les réclamations, à affiner les tarifs ou à anticiper les sinistres, mais reste moins performante que nous pour comprendre les subtilités de chaque situation ou développer une relation client de qualité et de proximité.

Avons-nous la capacité de comprendre et de juger, pour mesurer, analyser et circonscrire ces changements?

### Musclons notre cerveau et la co-intelligence pour embrasser la complexité et mieux décider

L'IA soulage les équipes de tâches répétitives et à faible valeur ajoutée et leur permet de se concentrer sur des activités plus qualitatives, telles que les échanges avec les clients et les partenaires. Familiarisons les collaborateurs aux outils et données de l'IA générative, pour un usage raisonné, loin des discours alarmistes mais de façon non naïve, embrassant les dimensions normatives, réglementaires,



N. Marescaux, ChatGPT & Dall-E: «Créez une illustration de la collaboration stratégique entre un centaure et un cyborg...»

environnementales, sociétales, et de compétences, évitant de lui attribuer des traits humains. Le contrôle humain doit rester prépondérant, particulièrement en ce qui concerne la qualité des données entrantes, la précision des demandes faites aux outils d'IA (Ekimetrics utilise deux injonctions à GenAI: «Tu n'inventes pas et, si tu ne sais pas, tu ne réponds pas»), et la vérification des résultats produits. Informons les assurés quand ils ont affaire à une IA et donnons-leur la possibilité de quitter le traitement mécanique pour passer à un traitement humain. Identifier les processus dont découle une décision de l'IA pour éviter les biais et les bruits. Pour préserver la confidentialité des données, les assureurs, soumis à une large législation, sont rompus à l'exercice.

Une démarche structurée aide à évaluer les bénéfices et les risques associés à l'IA. Créez une liste de cas d'usage potentiels, accompagnés d'une analyse détaillée: qualité des données, caractéristiques des résultats attendus, investissement, valeur générée. Interrogez vos fournisseurs sur leurs projets en matière d'IA. Fluidifiez les processus avant d'ajouter GenAI, ou ce sera un cautère sur une jambe de bois. Guidez le déploiement avec une démarche éthique, pour que les technologies adoptées soient en harmonie avec les valeurs et principes de l'organisation. Pour réduire l'empreinte environnementale, l'IA frugale vise à réduire les temps de calcul et à produire des modèles plus petits. L'IA permet aussi de gagner en efficacité

énergétique et d'améliorer les cycles de maintenance. Une charte d'usage claire et opérationnelle interdit les pratiques inacceptables tout en favorisant les activités à valeur ajoutée. L'IA explicable peut renforcer la transparence et la confiance, en offrant des points de repères clairs sur le fonctionnement des algorithmes et leur prise de décision.

L'intelligence collective peut s'appliquer entre machines. Avec la «sagesse des foules», la moyenne des estimations d'un groupe de personnes est souvent plus précise que les prédictions individuelles. Les études récentes de Philipp Schoenegger, spécialiste du comportement, et de ses co-auteurs montrent que la performance collective de 12 grands modèles de langage égale celle d'une foule humaine, faisant de la «foule de silicium» une nouvelle arme pour les prévisions. L'intelligence collective entre humains et machines peut être illustrée par les modèles Centaure et Cyborg. Le modèle Centaure repose sur une collaboration stratégique entre l'humain et la machine, avec une répartition des tâches selon leurs forces respectives. Cela permet aux humains de déléguer les tâches répétitives ou analytiques à l'IA et de se concentrer sur les aspects plus créatifs ou relationnels du travail. Le modèle Cyborg, quant à lui, cherche une fusion des capacités humaines et de l'IA, exploitant l'intelligence pour améliorer le potentiel créatif et décisionnel humain. Ces modèles soulignent l'intérêt d'une approche

hybride et adaptable pour tirer le meilleur parti des capacités de l'IA tout en respectant et en amplifiant les compétences humaines. Pour bien utiliser l'IA, opposons un doute rationnel à ses données, méthodes et résultats. L'esprit critique est la posture interrogative qui met à distance les affirmations qui nous sont soumises. Pour Jean Piaget, psychologue de l'enfant, le développement de l'enfant passe par quatre stades: sensorimoteur chez le bébé, prélogique intuitif entre 2 et 7 ans, logique-concret entre 7 et 12 ans et enfin rationnel et abstrait à partir de l'adolescence. Mais Daniel Kahneman, psychologue et économiste qui vient de nous quitter, montre que les humains sont plutôt irrationnels dans leur jugement. Nous utilisons plus souvent le système 1, l'intuition, une stratégie automatique très rapide, que le système 2, la logique, plus lent et analytique. Comment résoudre ce paradoxe Kahneman-Piaget? Pour Olivier Houdé, psychologue, nous avons un troisième système de pensée dans notre cerveau, la capacité d'inhibition, qui permet d'éviter de tomber dans le piège de la seule intuition et d'activer la logique. Renforçons le système 3, le doute, le regret de s'être trompé, la curiosité des systèmes complexes et de savoir comment trouver la solution.

Dans cette interface entre l'humain et la machine naissent des désaccords féconds, qui poussent à la réflexion critique et à réinventer les services, à améliorer la gestion des risques et à renforcer la relation avec les assurés. Raphaël Gaillard, psychiatre, nous invite à «lire, affûté et d'aplomb pour grandir, s'armer et chevaucher vers bien d'autres hybridations». Suivons son conseil et embrassons l'intelligence artificielle sans perdre notre identité, apprenons d'elle sans être induits en erreur, et canalisons nos dons pour créer un meilleur avenir humain. L'IA a 73 ans. GenAI a 2 ans. Ses capacités émergentes, son ampleur, son volume, et la variété des générations possibles vont évoluer. Il restera toujours une part d'incertitude. GenAI, comme la science, nous donne des possibilités mais son application est notre décision et notre responsabilité. En cette année de Jeux olympiques et paralympiques Paris 2024, «musclons notre cerveau» et embrassons la complexité, pour développer une assurance plus performante et résiliente, au service d'un avenir plus sûr pour tous.



### Bibliographie

Luc de Brabandere, *Petite philosophie des algorithmes sournois*, Eyrolles, 2023.

Arthur Charpentier, Nicolas Marescaux, «L'incertitude empêche-t-elle de prendre des décisions?», revue *Risques* n° 135, septembre 2023.

Commission de l'intelligence artificielle, «IA: notre ambition pour la France», 13 mars 2024.

David Cortés, «L'explicabilité des langageurs: des pistes via le *topic modeling*?», *Alvidence*, juillet 2023.

Charles. Efferson et al. *Super-additive cooperation*. *Nature* 626, 1034–1041, 2024, <https://doi.org/10.1038/s41586-024-07077-w>.

Giuliano Da Empoli, *Les ingénieurs du chaos*, Folio, 2023.

Fabrizio Dell'acqua et al., *Navigating the Jagged Technological Frontier*, Harvard Business School, Working Paper 24-013, Sep 2023.

France Assureurs, «Cartographie prospective 2024 des risques», février 2024.

Raphaël Gaillard, *L'homme augmenté*, Grasset, 2024.

Antoine Heranval, «Application de méthodes d'analyse textuelle aux données d'expertise d'assurance pour améliorer la connaissance des dommages occasionnés par des événements naturels», Conférence Printemps de l'assurance, 21 mars 2024.

Olivier Houdé, «Comment raisonne notre cerveau», PUF, coll. La bibliothèque des QSJ, 2023.

Daniel Kahneman et al., «Noise: Pourquoi nous faisons des erreurs de jugement et comment les éviter», Odile Jacob, 2021.

Bernard Lahire, *Les structures fondamentales des sociétés humaines*, La Découverte, 2023.

Pierre-Marie Lledo, «Musclons notre cerveau contre la désinformation», *Les Échos*, 3 novembre 2023.

Nicolas Marescaux, Selma Mehyaoui, Florence Picard et Pierre Valade, «IA Générative, pratique et esprit critique», Institut des Actuaire, Journée 100% Actuaire & Data Science, 21 novembre 2023.

Ethan Mollick, *Co-Intelligence: Living and Working with AI*, Portfolio, April 2024.

Gabriel Olympie, Natalia de la Calzada et Jean Lelong, «Climate Q&A: l'IA générative au service du climat», Ekimetrics, Retour d'expérience Datacraft, mai 2023.

Florence Picard, Olivier Fliche, Nicolas Marescaux, Françoise Soulie-Fogelman, Olivia Tambou, «La place de l'IA générative en assurance», Table ronde Printemps de l'assurance, 21 mars 2024.

Hugues Ribière, «Union européenne, acteurs et fonctionnement: exemple de l'IA Act», webinaire de l'Institut des Actuaire, 26 mars 2024.

Philipp Schoenegger et al., *Wisdom of the Silicon Crowd: LLM Ensemble Prediction Capabilities Rival Human Crowd Accuracy*, 6 March 2024, <https://arxiv.org/abs/2402.19379>.

Françoise Soulie-Fogelman, «Small is beautiful. Les grands modèles de langage vont-ils continuer à grandir?», ActuaIA 13, octobre 2023.

Universcience, Opinionway, «Baromètre de l'esprit critique 2024», mars 2024.

Victor Storchan, «10 points sur la géopolitique de l'IA générative», Grand Continent, 8 septembre 2023.

# Menace cyber et assurance : où en sommes-nous ?

Développement technologique effréné et dépendance croissante aux outils et services numériques transforment nos modes de vie et notre appréhension du réel. À côté des bénéfices immédiats dans l'efficacité de nos tâches ou la globalisation des savoirs, apparaissent des vulnérabilités, exploitées par la cybercriminalité ou contribuant à la polarisation des sociétés et aux désordres internationaux. Le risque cyber est la résultante de ces forces. Un équilibre dynamique, sujet à des dérives et des chocs, mais qui obéit à la rationalité d'intérêts bien compris. Le jeu n'est malheureusement pas à somme nulle et les attaques coûtent chaque année des milliers de milliards de dollars à l'économie mondiale. Une rupture de cet équilibre est-elle possible ? Comme avec toute arme de dissuasion, il nous faut l'envisager. Les lignes qui suivent tentent de décrire l'état actuel de la menace cyber et comment le marché de l'assurance et de la réassurance y répond à force de transformations.



**SÉBASTIEN HÉON**  
Directeur adjoint Cyber Solutions,  
SCOR



**DIDIER PARSOIRE**  
Directeur Cyber Solutions,  
SCOR

## Des attaques cyber de plus en plus nombreuses et variées

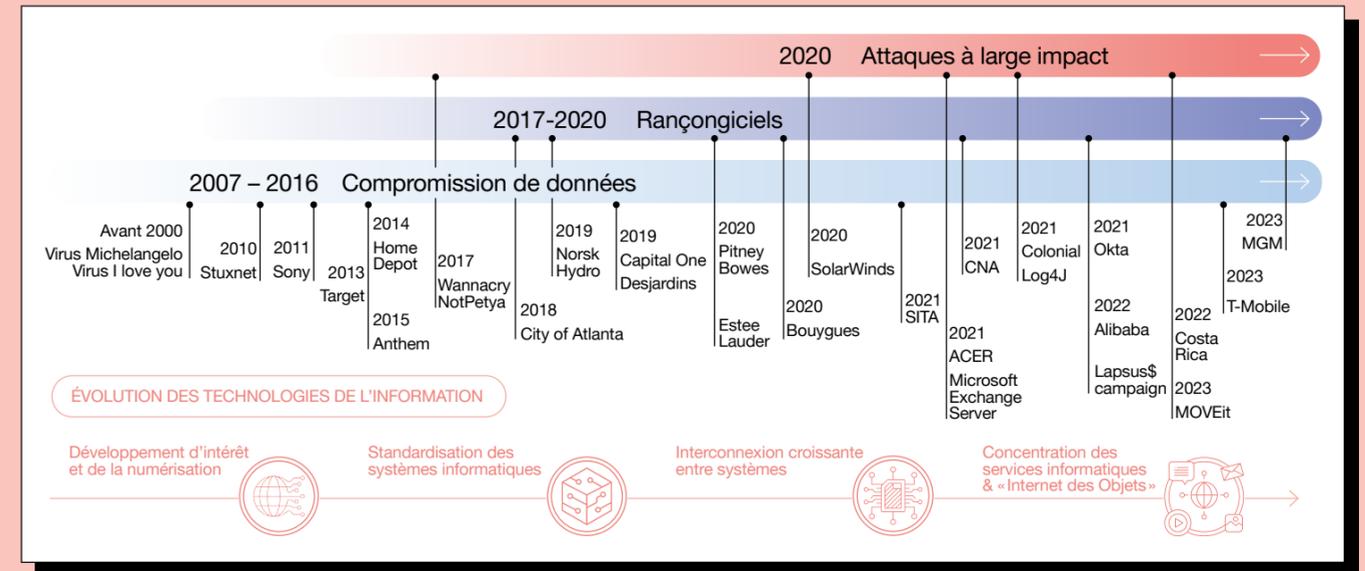
À l'origine, Internet a été développé sans sécurité. Quelques années après, le réseau s'était largement étendu, si bien qu'un programmeur eut envie de compter combien d'ordinateurs étaient interconnectés. Pour cela, il créa un programme qui se propageait d'ordinateur en ordinateur jusqu'à revenir à lui en ayant compté le nombre de sauts effectués. Le premier virus informatique était né.

Depuis, les acteurs malveillants ont développé des outils de plus en plus sophistiqués pour exploiter les failles informatiques des systèmes d'information, des systèmes industriels, et des objets connectés. La figure 1 montre une vue simplifiée de l'évolution des attaques informatiques au fil des innovations technologiques.

Malgré des tactiques toujours plus variées et sophistiquées, les attaques cyber ont des impacts assez stables dans le temps. Un vol de données va engendrer des coûts pour l'entreprise touchée : réparer les systèmes attaqués, prévenir les autorités et les victimes dont les

Malgré la difficulté intrinsèque à analyser le risque cyber et anticiper ses évolutions, l'assurance et la réassurance ont su s'adapter pour aujourd'hui contribuer fortement à la résilience numérique en assurant les risques mais également en prodiguant des conseils de prévention et de l'assistance à ses clients.

Fig. 1 Évolution des attaques cyber dans le temps



source: SCOR

### LE SCHÉMA NOUS MONTRE PLUSIEURS PHÉNOMÈNES :

- **Les vols de données** (qui ne sont pas des vols à proprement parler puisque le propriétaire légitime des données les possède encore après l'attaque) sont apparus à l'aube des années 2010 aux États-Unis (Sony, Home Depot, Target par exemple) et n'ont jamais cessé depuis. Un des plus récents est le vol de 15 millions de données des utilisateurs de la plateforme de gestion de projets Trello en janvier 2024.
- À ces vols s'ajoutent des attaques par **ransomware**, ou « **rançongiciels** ». Ce sont des programmes malveillants introduits par des attaquants dans les systèmes informatiques des victimes et qui chiffrent toutes les informations qui s'y trouvent. L'attaquant demande alors une rançon à la victime en échange d'une clé de déchiffrement qui, en théorie, devrait lui rendre le contrôle de ses systèmes. Les attaques par **ransomware** ont connu un pic en 2019-2020, tant en nombre d'attaques qu'en montant de rançon.
- Pour optimiser leur impact et mieux rentabiliser leurs investissements, les attaquants ont ajouté une nouvelle tactique à leur catalogue, en complément du vol de données et des **ransomwares**. Ils pénètrent les réseaux informatiques ou corrompent les logiciels de **prestataires informatiques**, ce qui leur permet d'accéder en parallèle aux clients de ces prestataires. L'exemple de l'éditeur informatique SolarWinds en 2020 montre bien l'efficacité et la sophistication de cette technique : les attaquants ont pénétré le réseau informatique de SolarWinds et ont introduit un programme malveillant dans la mise à jour de leur produit phare, Orion. Les clients de SolarWinds, en installant la mise à jour, ont activé le logiciel malveillant permettant ainsi aux attaquants d'accéder à leur réseau.

Toutes ces techniques d'attaques exploitent les évolutions technologiques. Par exemple, l'attaque « par prestataires » s'appuie sur l'interconnexion massive des entreprises avec leurs clients, partenaires et prestataires, rendant possible des effets de contagion importants. De même, les technologies de l'information et de la communication se sont fortement concentrées autour de quelques acteurs majeurs : les GAFAM pour le logiciel et le cloud et quelques constructeurs de matériel (Ericsson, Huawei, Cisco...) Ces effets d'interconnexion et de concentration révèlent la forte dépendance de notre société à quelques entreprises nécessaires au fonctionnement numérique. Que se passerait-il, en effet, si tous les ordinateurs sous Windows cessaient de fonctionner simultanément dans le monde entier ?

données ont été volées, faire face à de possibles actions de groupe (« class actions ») de la part de ces victimes ou à des enquêtes administratives. Un rançongiciel aura, lui, comme principal effet une perte d'exploitation due au blocage des systèmes contaminés, à laquelle s'ajoutera le coût de remise en état des réseaux informatiques. L'assurance cyber s'est progressivement structurée autour de ces postes de coût comme on le verra plus loin.

—  
**La tension continue entre attaquants et défenseurs crée un état d'équilibre**

Face à la pression des attaquants, les défenses s'améliorent elles aussi de manière continue. Nos antivirus sont devenus des HIPS puis des EDR et des XDR; les SOC sont apparus pour exploiter des SIEM. Autant d'acronymes pour désigner les boucliers mis en œuvre par les professionnels de la cybersécurité. En renfort des solutions techniques de sécurité, des standards ont été développés pour expliquer comment organiser les défenses et gouverner la cybersécurité des organisations. Au fil des ans, l'écosystème de la défense s'est considérablement développé, passant d'une matière de *geeks* à de véritables axes stratégiques des entreprises. On estime que le budget mondial consacré à la cybersécurité en 2023 s'élève à environ 224 milliards de dollars, en hausse de 13% par rapport à 2022<sup>1</sup>.

Ainsi est né un équilibre entre des attaquants et des défenseurs, déterminés et engagés dans une bataille qu'on imagine sans fin.

**Le risque cyber dans une situation d'équilibre soumise à de nombreux stimuli**

Un état d'équilibre des forces s'est établi entre les capacités des attaquants, le glaive, et celles des défenseurs, le bouclier. Il peut s'observer à travers plusieurs focales : à l'échelle micro d'une entreprise ou d'un système informatique particulier qui doit se défendre contre des attaques constantes, ou à l'échelle mondiale, entre les gangs d'attaquants, très organisés, et les forces de l'ordre qui les poursuivent. L'équilibre attaque/défense contient lui-même d'autres équilibres au sein de chaque camp : pour les défenseurs, la cybersécurité doit être dosée

correctement pour apporter une défense efficace sans bloquer les processus métiers ou gêner le travail des utilisateurs (ah les dizaines de mots de passe!). De même, certains attaquants doivent composer entre leur appétit d'attaques et la tolérance envers leurs actions criminelles de la part des autorités qui les abritent, parfois avec bienveillance.

Les attaquants, comme les défenseurs et le milieu dans lequel ils évoluent, sont en perpétuelle évolution : attaques quotidiennes, nouveau patch de sécurité venant corriger une vulnérabilité logicielle dangereuse, nouveaux objets connectés utilisés en masse. La cybersécurité est finalement en perpétuelle oscillation autour de l'équilibre. L'assurance cyber contribue d'ailleurs à cet équilibre en compensant dans une certaine mesure les écarts provoqués par des attaquants.

**Des déséquilibres pluriels**

—  
**Des déséquilibres endogènes dus aux évolutions technologiques**

L'arrivée d'une nouvelle technologie perturbe forcément l'équilibre des forces. L'IA en est une illustration particulièrement intéressante : les attaquants utilisent l'IA générative pour forger des messages de *phishing* très réalistes, et on peut imaginer que l'utilisation de *deep fakes* viendra crédibiliser les attaques au président dans un avenir proche. À l'inverse, le *machine learning* est un outil très précieux pour les défenseurs qui peuvent améliorer considérablement leur capacité de détection d'attaques en « apprenant » à identifier le comportement des attaquants.

En cybersécurité, les nouvelles technologies sont donc surtout affaire de contexte. Quand la crise du Covid s'est déclenchée, le recours massif au télétravail s'est fait dans l'urgence, avec la continuité opérationnelle comme priorité absolue. La sécurité des connexions ainsi que la sensibilisation des salariés aux risques cyber furent secondaires et parfois négligées, ce dont les attaquants ont profité pour intensifier les attaques. Selon Deloitte<sup>2</sup>, les attaques sur les systèmes de visio-conférence ont touché plus d'un demi-million de personnes entre février et mai 2020. La pandémie a donc créé un choc technologique qui a modifié l'équilibre antérieur entre attaquants et défenseurs.

Au-delà de ce cas concret, il existe des chocs

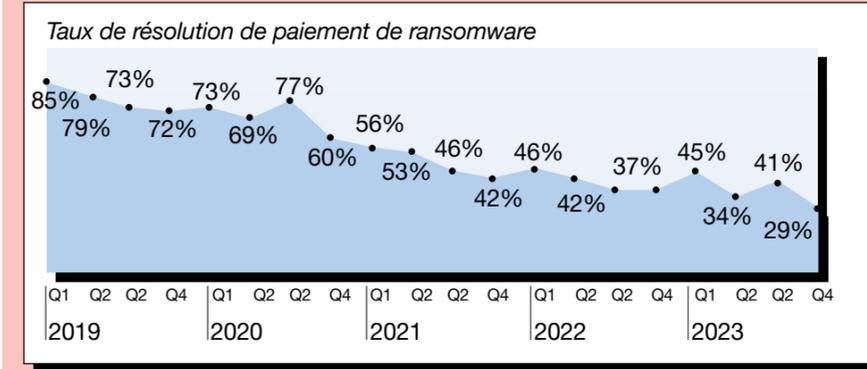
latents dont les effets peuvent se déclencher de manière subite. L'ensemble des logiciels, codes intégrés dans des objets connectés et hardware recèle des vulnérabilités non encore découvertes et qui pourraient devenir le terreau de futures attaques. Toutes ne donneront pas lieu à des attaques cyber de grande ampleur ou ne seront même jamais découvertes. Mais cette accumulation de vulnérabilités constitue une dette de sécurité que les utilisateurs, les (ré) assureurs et la société devront compenser quand elle se matérialisera. Ce sont autant de chocs que l'équilibre des forces pourrait subir, en fonction de la gravité des vulnérabilités découvertes.

Sur un autre plan, il est intéressant de remarquer que la dette de sécurité est assumée par la société alors que les profits des logiciels reviennent aux entreprises qui les développent...

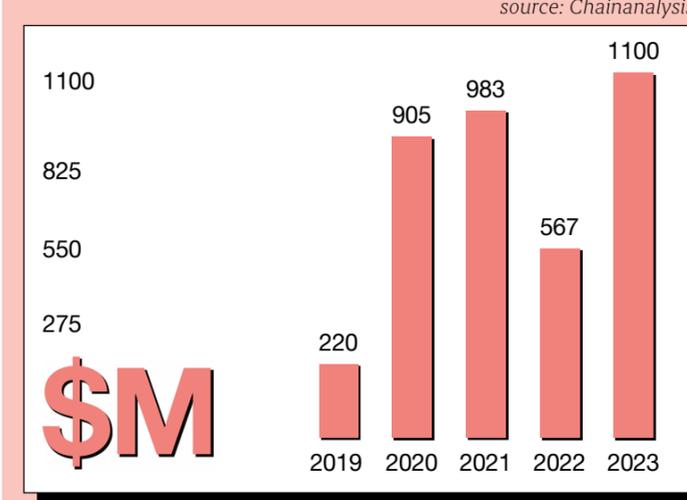
Outre la dette de sécurité logicielle, les services numériques continuent de se développer : une majorité d'entreprises a maintenant recours aux services de *cloud computing*, les CDN<sup>3</sup> assurent la disponibilité de nos contenus numériques partout et sans latence, les véhicules autonomes commencent à se déployer. Ces services porteurs de progrès et d'efficacité opérationnelle sont, à l'instar des logiciels, également porteurs de chocs latents. Les prestataires de ces services, très concentrés (AWS possède une part de marché de 31% de l'infrastructure *cloud* dans le monde au quatrième trimestre 2023<sup>4</sup>), sont des points d'accumulation au sens où le défaut d'un de ces prestataires touchera un très large ensemble d'utilisateurs, simultanément et où qu'ils se trouvent, avec des impacts financiers importants. Les réassureurs étudient ces types de scénarios à l'aide de modèles stochastiques spécifiques qui ont vu le jour à la fin des années 2010 et qui ne cessent de se développer.

Un autre changement d'équilibre, positif celui-là : la proportion des victimes de rançongiciels qui paient finalement la rançon diminue tendanciellement depuis 2019. Selon Coveware<sup>5</sup>, ce pourcentage serait passé de 85% au début de l'année 2019 à 29% à la fin de l'année 2023. On peut expliquer cette évolution positive par une meilleure préparation des organisations au risque, notamment grâce à l'amélioration des sauvegardes des systèmes et des données, permettant de restaurer des systèmes bloqués par un rançongiciel quasiment sans perte.

**Fig. 2** Selon Coveware, la proportion des victimes de rançongiciels qui paient une rançon dans l'espoir de récupérer leur système d'information et/ou leurs données diminue au fil du temps. *source: Coveware*



**Fig. 3** Montant des rançons payées entre 2019 et 2023 en \$M. *source: Chainanalysis*



Mais, face à des victimes plus résistantes, les attaquants cherchent à maintenir leurs gains financiers par d'autres moyens. Le phénomène de double extorsion consiste ainsi à voler le plus de données possible avant de déclencher le rançongiciel. L'attaquant demande alors une rançon pour débloquer le système et une autre pour ne pas diffuser publiquement les informations volées.

Malgré la bataille gagnée par les défenseurs grâce à de meilleures protections, les gains des gangs de rançongiciel ont atteint la somme record de 1,1 milliard de dollars en 2023, après une baisse notable en 2022, selon la plate-forme Chainanalysis<sup>6</sup>.

—  
**Les tensions géopolitiques, vecteurs de déséquilibres exogènes**

Les tensions géopolitiques ont un fort impact sur la cybersécurité, en agissant sur les deux camps de manière symétrique. Certains attaquants vont se mobiliser pour accompagner des idéologies, des prises de positions politiques ou de grandes causes, humanitaires par exemple. Ce faisant, ils concentreront leurs attaques sur un pays ou une industrie qu'ils jugent opposés à leurs opinions. Par exemple, certains attaquants proches du Hamas revendiquent la recherche de vulnérabilités dans des logiciels israéliens pour mener des campagnes d'attaque contre les clients de ces outils.

Plus frappant encore, la guerre en Ukraine a mis en évidence une dynamique dans laquelle des hackers russes, d'ordinaire motivés par les gains financiers des attaques à rançon, se sont « engagés » dans le conflit pour soutenir l'action militaire de leur pays. On ne saura probablement pas s'ils l'ont fait par pur patriotisme ou s'ils ont été incités à s'engager en échange d'une tolérance des autorités russes pour leurs activités criminelles habituelles. Néanmoins, certaines attaques cyber ont été menées dans le cadre du conflit. La plus importante est sans doute celle qui a interrompu le réseau mobile de l'opérateur ukrainien Kyivstar pendant plusieurs jours en décembre 2023. Cette attaque, complexe techniquement et difficile à planifier, a bloqué les communications mobiles, certains systèmes d'alerte aérienne, des distributeurs de billets dans tout le pays. L'impact de l'attaque aurait pu être bien plus important si elle avait été menée juste avant et coordonnée avec l'invasion de l'Ukraine, et non près de deux ans après.

Notons enfin le rapport « Portal Kombat » de VIGINUM<sup>7</sup> publié en février 2024 qui met en lumière un important dispositif de relais et d'amplification de la propagande prorusse à destination d'audiences internationales dont l'objectif principal semble être de couvrir le conflit russo-ukrainien en présentant positivement « l'opération militaire spéciale » et en dénigrant l'Ukraine et ses dirigeants.

Il est donc possible que la guerre en Ukraine fasse progressivement aboutir le concept de guerre cyber qui reste pour l'instant une composante militaire difficile à intégrer dans la doctrine d'emploi des forces.

Symétriquement, quand la pression des attaques cyber devient trop forte, les gouvernements peuvent réagir, soit sous l'angle politique et diplomatique, soit en intensifiant la répression contre les attaquants.

Depuis longtemps, les États-Unis sont particulièrement actifs dans la diplomatie du cyberspace et savent signifier à leurs adversaires les limites que des attaques cyber ne doivent pas franchir. En 2015, à la veille d'une rencontre avec le dirigeant chinois Xi Jinping, le président des États-Unis Barack Obama a ainsi mis en garde très clairement le gouvernement chinois accusé de diriger des attaques cyber contre les États-Unis<sup>8</sup>. Antérieurement, en 2011, un rapport au Congrès américain

mentionnatit des attaques cyber de grande ampleur contre les États-Unis<sup>9</sup>, déclaration réitérée en 2015 par le Deputy Secretary of Defense de l'époque, Robert O. Work, indiquant que les États-Unis « se réservent le droit de répondre à une cyberactivité malveillante au moment, au lieu et de la manière de leur choix. »

Plus récemment, en 2021, des hackers ont attaqué l'entreprise Colonial Pipeline qui exploite un des plus grands pipelines de carburant entre le Texas et la côte Est des États-Unis. À la suite de cette attaque majeure, l'entreprise avait dû fermer le pipeline par précaution, craignant que les pirates informatiques n'aient pu obtenir des informations leur permettant de mener de nouvelles attaques sur des parties vulnérables du pipeline. L'interruption a créé des pénuries de carburant frappant par exemple l'aéroport de Charlotte. Le président des États-Unis Joe Biden a déclaré l'état d'urgence et déclenché un plan de crise important pour acheminer le carburant par camions. Un mois après l'attaque rapidement attribuée au groupe de hackers DarkSide, le FBI a récupéré 2,3 millions de dollars (63,7 bitcoins) de la rançon payée par Colonial Pipeline et a démantelé l'infrastructure informatique des hackers. Le message des autorités fédérales américaines a été clair : en attaquant une infrastructure critique américaine, une ligne rouge a été franchie par les hackers, qui s'exposent alors à des représailles d'ampleur.

Les forces de l'ordre ont d'ailleurs une action de fond contre les cyberattaquants qui aboutit régulièrement à des mises hors d'état de nuire de groupes de hackers. En février 2024, notamment, le puissant groupe Lockbit a été démantelé et son infrastructure informatique saisie, comme cela avait été le cas pour le groupe Hive en janvier 2023, et BlackCat/ALHPV en décembre 2023.

Finalement, la géopolitique est un élément fondamental à l'équilibre des forces, parfois en amplifiant les attaques, parfois en les amortissant.

## Des points de rupture

Certains acteurs pourraient avoir intérêt à briser le système. On pense en premier à des cyberterroristes dont l'objectif serait de déstabiliser le monde en détruisant des

infrastructures numériques. Il faudrait qu'ils atteignent un degré de sophistication et d'organisation de très haut niveau, surpassant celui des hackers traditionnels, pour arriver à mener des actions à grande échelle.

L'intensification non-contrôlée d'actions militaires cyber en appui d'un conflit classique est un autre risque de déstabilisation. Mais les militaires savent que ces frappes sont risquées à cause d'effets en cascade qui pourraient finalement se retourner comme un boomerang vers ceux qui les ont lancées.

Reste la panne, simple et implacable. Le monde s'était enflammé pour « le bug de l'an 2000 » qui n'avait finalement pas eu de conséquences désastreuses, peut-être grâce aux mesures prises alors. Avons-nous aujourd'hui une si grande confiance en nos logiciels qu'une telle panne nous paraît impossible ? D'autant que la part de l'économie dépendant du numérique a considérablement augmenté en vingt-cinq ans.

## Le marché de la cyberassurance : l'âge de raison

Les auteurs ont relu avec intérêt l'article qu'ils avaient publié dans cette même revue et sur ce même sujet en 2015<sup>10</sup>. Force est de constater que le marché de l'assurance cyber s'est entièrement renouvelé depuis, même si les questions soulevées à l'époque restent pleinement d'actualité. Il est tout aussi intéressant d'observer que le marché actuel s'est façonné au gré des déséquilibres et des chocs que nous venons de décrire. Voyons comment ils ont transformé sa physionomie.

### 2017 : NotPetya, l'an 1 du marché

La genèse du marché cyber tel que nous le connaissons aujourd'hui se trouve dans le choc produit par cette attaque survenue en juin 2017. NotPetya désigne un logiciel malveillant qui détruit les données (un « wiper ») bien qu'il apparaisse sous la forme d'un rançongiciel. Il exploite une faille de sécurité du système d'exploitation Windows déjà à l'origine de l'attaque massive WannaCry un mois plus tôt et se propage sur l'ensemble du réseau de l'entreprise à partir d'une machine infectée. La première infection a eu lieu à la suite de la mise à jour d'un logiciel de comptabilité ukrainien (l'Ukraine,

déjà !) très utilisé par les entreprises implantées dans le pays ; attaque vraisemblablement pétrée par un groupe d'attaquants russes. Cela explique sa viralité : en quelques heures, des centaines de milliers d'ordinateurs sont affectés dans le monde entier, conduisant à des arrêts de production et des pertes d'exploitation importantes. On estime son coût économique à environ 10 milliards de dollars. Le coût pour l'assurance est estimé à 3 milliards de dollars, essentiellement concentré sur quelques grandes entreprises avec le géant pharmaceutique Merck au premier rang mais aussi des sociétés comme Saint-Gobain, Mondelez ou Reckitt Benckiser. Fait notable, l'essentiel du sinistre est porté par des polices dommages et les polices cyber ne paieront que 10 % environ du montant total. La raison en est la faible pénétration à cette époque du marché cyber chez les entreprises industrielles et le fait que les polices dommages comportent encore des clauses ambiguës sur la définition du dommage matériel ou l'exclusion du péril cyber.

### Le marché de l'assurance va très vite en tirer quelques conclusions :

#### • La nécessité de clarifier les couvertures d'assurance cyber

Le marché voit l'urgence de clarifier l'exposition au risque cyber des polices « non-cyber » : dommage, responsabilité civile et autres spécialités. Le régulateur britannique, PRA, est le premier à s'émouvoir des incertitudes liées aux expositions dites « silencieuses » ou « non-affirmatives » en 2019, relayé par des instructions du Lloyd's auprès de ses syndicats qui s'étageront entre 2020 et 2021 selon les branches d'assurance avec une priorité sur la branche dommage, vue comme la plus exposée à l'aune de l'expérience NotPetya. Aujourd'hui, le travail est fait pour l'essentiel sur cette branche, excluant les pertes de données et autres dommages immatériels et précisant la couverture des dommages matériels consécutifs à un événement cyber. Ainsi se fortifie la distinction entre le péril cyber et le produit cyber, renforçant l'identité du marché de la cyberassurance.

#### • L'extension du produit d'assurance cyber

Autre enseignement de NotPetya : la nécessité de couvrir la perte d'exploitation sans dommage. On assiste très vite à une convergence des

polices d'assurance entre les États-Unis et l'Europe. Les couvertures de responsabilité pour compromission des données ou de la sécurité des systèmes informatiques se conjuguent aux garanties de restauration des données et systèmes et de pertes d'exploitation. L'assurance des rançons demandées en cas de chiffrage des données devient aussi un standard. La police d'assurance cyber devient ce qu'elle est aujourd'hui : un produit complet de dommage et de responsabilité avec des déclencheurs multiples : découverte de l'attaque, survenance du dommage, réclamation de tiers ...

#### • L'expansion du marché

NotPetya joue aussi le rôle de signal d'alerte face à la menace et conduit plus d'entreprises à s'assurer, en particulier dans le secteur industriel qui se croyait plutôt prémuni avant l'avènement des rançongiciels. On assiste à un rééquilibrage face aux acheteurs traditionnels plutôt concernés par les fuites de données (entreprises de technologies et de services).

#### • La modélisation du risque de catastrophe

NotPetya est l'un des premiers et, encore aujourd'hui, l'un des seuls événements catastrophe qu'ait connu le marché. Il révèle le caractère global des catastrophes cyber et la nécessité de mieux quantifier cette exposition. À partir de 2018, les modèles stochastiques se développent aux cotés des scénarios déterministes utilisés jusqu'alors. Ils deviennent plus sophistiqués au fil du temps, affinant les scénarios, les vecteurs de propagation (technologies, fournisseurs de services) et les paramètres d'exposition et de vulnérabilité des entreprises. Plusieurs agences de modélisation se créent ou se développent sur ce segment (Cyence/Guidewire, CyberCube, AIR, RMS, Kovrr, etc.) avec des fortunes diverses au vu des investissements nécessaires en matière de technologie et de compétence.

### 2018-2021 : Industrialisation et sophistication des attaques

Cette période voit se développer les attaques à rançongiciel et le système « Ransomware as a Service (RaaS) », une spécialisation des services entre développeurs de logiciels malveillants, groupes d'attaquants et assistance pour le paiement des rançons. Cette industrialisation

**L'adversité pousse les acteurs à améliorer leurs opérations, par une montée en compétence des équipes et l'amélioration des processus de souscription.**

des attaques agit comme un rouleau compresseur avec une forte augmentation de la fréquence de celles-ci. Entre 2018 et 2021, le nombre d'attaques de type *ransomware* répertoriées dans le monde passe de 206 millions à 623 millions, soit une multiplication par trois ! En parallèle, les attaques se font aussi plus ciblées avec une hausse sensible des demandes de rançon et plus dévastatrices avec la chasse au gros, « *big game hunting* » en anglais, qui cible de grandes entreprises en fonction de leur capacité et de leur probabilité à payer les rançons.

Conjugué avec l'extension des garanties offertes par les assureurs, cela génère une envolée des sinistres en fréquence et en sévérité et une dégradation forte des résultats sur les exercices 2020 et 2021. Le ratio sinistre à prime aux États-Unis passe ainsi de 34 % en 2018 à 73 % en 2020 et 67 % en 2021 pour les polices cyber autonomes, selon les chiffres du NAIC<sup>11</sup>.

### Là encore, le marché va montrer une adaptation rapide à ces changements :

#### • Renforcement de la discipline de souscription :

Les attaques à rançongiciel se manifestent par des sinistres à développement court, ce qui permet au marché d'observer rapidement la dégradation des résultats et de prendre dès 2021 des mesures correctives. La capacité du marché va se réduire sur les grands risques : les acteurs qui offraient jusqu'à 25 millions de dollars se limitent à 10 millions de dollars pour la plupart. Les taux remontent drastiquement : sur 2021 et 2022, les taux de prime vont subir

une hausse cumulée de plus de 200 %. Les conditions d'assurances deviennent plus restrictives : doublement des rétentions et franchises, sous-limitation des garanties pour les attaques à rançongiciel. Au même moment, la question de l'assurabilité des rançons devient aiguë, particulièrement en France. Certains acteurs renoncent à offrir la garantie. Le débat sur l'incitation de l'assurance à payer les rançons n'a pas vraiment été tranché, mais le caractère global de la menace décourage les initiatives nationales en matière d'interdiction. En France, le législateur ne franchira pas le pas et préférera, à travers la loi LOPMI<sup>12</sup> de 2023, imposer le dépôt de plainte pour toute réclamation d'assurance liée à une attaque cyber, gage d'une meilleure visibilité sur la menace. Quoi qu'il en soit, la tendance baissière des paiements de rançon soulignée dans la partie précédente semble être plutôt le reflet d'une meilleure cybersécurité des entreprises, véritable dissuasion contre l'extorsion.

#### • Professionnalisation du marché :

L'adversité pousse aussi les acteurs à améliorer leurs opérations, par une montée en compétence des équipes et par l'amélioration des processus de souscription. L'expertise technique est de plus en plus internalisée ; les souscripteurs mieux formés à la cybersécurité. Les assureurs renforcent aussi la sélection et l'évaluation des risques : les questionnaires de sécurité deviennent plus pertinents et systématisés ; les outils de *scanning* qui recueillent sur Internet les indicateurs de vulnérabilité ou de mauvaises pratiques des assurés se généralisent et s'intègrent à la décision de souscription.

#### • Nouveaux acteurs, nouveaux produits :

Cette période voit aussi l'irruption des « assuretech » dans le marché avec l'apparition de plusieurs agences de souscription, principalement aux États-Unis (At Bay, Coalition, Corvus, Resilience, etc.), qui allient la technologie, l'expertise en cybersécurité et l'analyse de données pour renouveler l'offre d'assurance, principalement vers les PME. La distribution et le processus de souscription via des plateformes digitales se trouve simplifiés. Certaines agences internalisent dans leur offre d'assurance des prestations comme la gestion active du risque (préconisations sur la gestion du risque, détection de vulnérabilités) tout au long du contrat ou une assistance de

bout en bout en cas de sinistre. Ces agences ont connu une forte progression de leurs chiffres d'affaires sur la période et dans une logique d'expansion, elles étendent leur offre aux ETI voire aux grands risques et prennent maintenant pied en Europe. En France aussi, des agences comme Stoik ou Dattak suivent ce modèle pour stimuler l'offre vers les PME et les ETI. On peut également mentionner l'initiative de l'agence française Descartes Underwriting qui propose un produit d'assurance paramétrique pour couvrir les pertes d'exploitation. La cherté et la raréfaction de la capacité pour les grands risques en 2021 et 2022 ont aussi conduit 12 entreprises européennes à créer la première mutuelle cyber par capitalisation, Miris<sup>13</sup>, offrant dès le 1<sup>er</sup> janvier 2023, 25 millions de dollars de capacité à chacun de ses membres.

### 2022 à aujourd'hui : La géopolitique du risque cyber

#### Appréhender le risque systémique

La guerre en Ukraine et plus récemment le conflit au Moyen-Orient ont soulevé avec plus d'acuité la question de l'exposition à la cyberguerre. Comme indiqué dans la partie précédente, il n'y a pas aujourd'hui de doctrine établie sur l'usage de l'arme cyber dans le contexte de la guerre. Pour autant, l'exposition potentielle à ce risque a conduit les assureurs à clarifier et actualiser les exclusions du risque de guerre, dont certaines datent d'avant la Seconde Guerre mondiale ! Là encore, le Lloyd's a donné l'impulsion et plusieurs clauses de marché ont vu le jour pour exclure

le risque de cyberguerre ou d'opérations cyber menées par des États et qui auraient un caractère systémique. L'articulation des concepts n'est pas aisée et a donné lieu à de multiples discussions de marché. L'attribution des attaques en particulier reste un sujet difficile. On assiste néanmoins à une diffusion progressive de ces clauses, en particulier sous l'impulsion des réassureurs. En France, leur pleine adoption nécessitera une révision de la définition de la guerre inscrite dans le code des assurances.

#### La quête de la capacité

Le marché de l'assurance cyber a connu une forte progression depuis NotPetya passant de 4 milliards de dollars de prime en 2017 à environ 15 milliards en 2023. Pourtant, son taux de pénétration reste encore relativement faible chez les PME et les ETI et il couvre une portion minime des coûts de la cybercriminalité. Il est donc promis à une forte croissance dans les années à venir, pour autant que la capacité soit disponible pour l'accompagner.

Le marché de la réassurance a joué son rôle de partenaire en offrant une capacité essentiellement proportionnelle sur la période écoulée, avec une cession de prime de l'ordre de 50%. Cependant, avec la croissance des expositions, la gestion du risque catastrophe devient plus aigüe. Dans le même temps, les bons résultats du marché augmentent l'appétit des assureurs et les conduisent à rechercher des formes plus optimales de réassurance pour se prémunir précisément contre le risque extrême. Le marché de la réassurance commence à proposer des couvertures par événement et l'on assiste à un intérêt naissant du marché des capitaux avec les premières obligations catastrophes cyber émises en 2023. Les freins à l'émergence des couvertures catastrophes sont connus. Ils tiennent d'une part à la définition même de l'événement qui peut prendre des formes diverses dans sa temporalité, son empreinte géographique et ses impacts : propagation de virus, interruption de service d'un opérateur critique (services «cloud», par exemple), exploitation d'une vulnérabilité critique au sein d'une technologie largement diffusée, etc.; et d'autre part à sa modélisation. Sur ce dernier point, les modèles ont progressé et les distributions de perte s'affinent mais des efforts restent encore à accomplir, avec la

gagueuse que constitue l'exercice de quantifier des événements sans expérience significative. Enfin, le risque systémique décrit plus haut doit aussi être clairement bordé, car il est par essence inassurable.

#### Perspectives

On le voit, le marché de l'assurance a su s'adapter à la fluidité du risque cyber. Il a fait preuve de réactivité et s'est emparé en un laps de temps très court des outils développés sur des décennies pour des risques bien plus matures. On peut même dire qu'il questionne de façon proactive des sujets laissés de côté par les branches traditionnelles comme la clarification de la couverture par les polices dommage de la perte d'exploitation sans dommage matériel (et ce avant la crise du Covid!) ou encore la redéfinition du risque de guerre. En ce sens, on peut dire que la cyberassurance a atteint l'âge de raison.

#### Et après ?

Le produit poursuit son adaptation : certains poussent pour une dissociation entre garanties de dommage et de responsabilité ou encore pour des produits plus spécialisés par péril (type d'attaque, risque de guerre), ceci afin de faciliter l'accès à la capacité de réassurance. A contrario, on pourrait assister à l'émergence de polices plus globales pour couvrir les conséquences matérielles et immatérielles du péril cyber. Tout reste ouvert.

Les acteurs aussi évoluent : les assurtech se rapprochent des assureurs traditionnels, d'une part parce que la hausse des taux d'intérêts depuis 2022 a mis un frein sur les investissements, ce qui rend problématique le financement de ces start-up, d'autre part parce que les assureurs traditionnels voient dans ces agences le moyen de développer leur offre PME. Récemment, l'assureur américain Travelers a, par exemple, acquis l'agence Corvus.

Enfin, la mesure du risque s'améliore. En cyber, les données sont à la fois le problème et la solution. Ce qui est visible par l'attaquant peut l'être aussi par l'assureur. Les traces numériques laissées par les entreprises sur le réseau Internet et leur corrélation à l'exposition et à la vulnérabilité aux attaques est de mieux en

mieux appréhendée par les outils d'analyse de risque, aidés par les techniques d'intelligence artificielle et de *data science*. La souscription aspire à devenir plus prédictive, moins rétrospective. Après avoir adopté les bonnes pratiques de ses aînés, la cyberassurance pourrait bien devenir le modèle à suivre.

### L'assurance, acteur de la résilience numérique

Certains risques comme le changement climatique évoluent avec une certaine prévisibilité dans une direction donnée. À l'inverse, le risque cyber est en situation d'équilibre, soumis à d'importantes forces contradictoires. Cet « équilibre de sumos » où les forces appliquées sont titanesques sans que les protagonistes semblent bouger, peut-il être déstabilisé au point de changer d'état ? Et dans ce cas, le secteur de la (ré)assurance privée peut-il suffire à compenser le choc ?

On l'a vu, les attaquants et les défenseurs obéissent à des logiques opposées mais rationnelles qui assurent un équilibre au système. Bien sûr, de nombreuses perturbations internes et externes créent des oscillations permanentes et parfois quelques dérives (la vague de *ransomware* en 2019-2020 par exemple), mais pas au point de déstabiliser la situation. L'équilibre semble plus stable qu'on le penserait initialement.

L'assurance cyber a évolué très rapidement vers l'âge de raison. Sa capacité d'adaptation et son attitude proactive face à un risque évolutif lui permettent aujourd'hui de jouer un rôle fondamental. En sensibilisant ses clients au risque, en apportant de l'assistance en cas de sinistre, en soutenant l'application des réglementations, l'assureur est maintenant un agent régulateur important du risque cyber. En cela, il agit positivement sur la résilience numérique et contribue fortement à l'équilibre du marché.

#### Mais les forces en présence peuvent-elles échapper à la rationalité ?

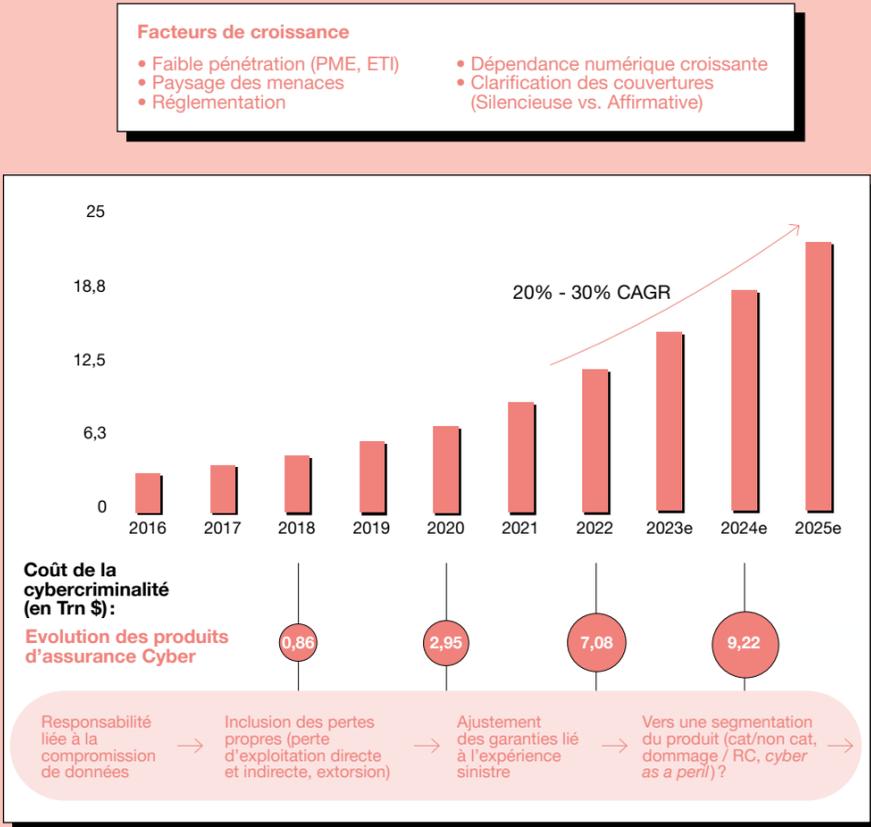
Qu'il émane de cyber terroristes, d'opérations de guerre cyber incontrôlées ou d'une panne majeure, le chaos numérique, s'il devait se matérialiser, déborderait les capacités



### Notes

- Les dépenses mondiales en cybersécurité vont augmenter de 13,2 % en 2023 selon Canalys - ChannelNews
- Impact of Covid on Cybersecurity (deloitte.com)
- Content Delivery Networks
- Chart: Amazon Maintains Cloud Lead as Microsoft Edges Closer | Statista
- New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying (coveware.com)
- Ransomware Hit \$1 Billion in 2023 (chainalysis.com)
- Portal Kombat : un réseau structuré et coordonné de propagande prorusse | SGDSN
- Obama: China cyber attacks 'unacceptable' - BBC News
- U.S. reserves right to meet cyber attack with force | Reuters
- « Cyberassurance : Offres et Solutions » - Didier Parsoire - *Risques* N°101
- National Association of Insurance Commissioners
- LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur
- Mutual Insurance and Reinsurance for Information Systems

Fig. 4 L'évolution du marché de la cyberassurance et ses facteurs de croissance (SCOR).



Sources : SCOR (composition), Munich RE, S&P Global, Statista

# Anticiper les évolutions du risque cyber: un chemin vers son assurabilité

Face au déploiement massif de systèmes connectés et à la digitalisation croissante de nos sociétés, le risque d'une défaillance cyber est une préoccupation grandissante des entreprises et institutions du secteur public comme privé. Anticiper les conséquences d'un événement cyber majeur peut accélérer le développement d'une offre d'assurance robuste répondant aux besoins des acteurs économiques.



**CAROLINE HILLAIRET**  
Professeur,  
CREST & ENSAE IP Paris



**OLIVIER LOPEZ**  
Professeur,  
CREST & ENSAE IP Paris

**La digitalisation galopante de la société et l'interconnexion entre les systèmes font du risque cyber une préoccupation majeure de acteurs économiques. À l'instar de ce qui a été fait pour d'autres risques systémiques, il faut, pour améliorer son assurabilité, s'engager dans une approche statistique rigoureuse basée sur les scénarios de sinistres tout en renforçant les démarches de prévention.**

D'après Jerome Powell, Président de la Réserve fédérale des États-Unis, les cyberattaques constituent désormais la principale menace pour le système financier mondial<sup>1</sup>, alors que l'ampleur des pertes liées au risque cyber est en forte croissance. Les dommages liés au cybercrime, estimés<sup>2</sup> à un trillion de dollars en 2021 (1 % du PIB mondial), pourraient s'élever<sup>3</sup> à 10 trillions de dollars en 2025. À titre illustratif, les paiements des rançons ont atteint en 2023 le chiffre record du milliard de dollars. Les défaillances cyber sont complexes et multiformes (hacking, rançongiciels, attaques par déni de service DDoS

qui visent à rendre un système indisponible par l'envoi de requêtes multiples...), aux conséquences variées, telles que la corruption et/ou la perte de données (par exemple, la cyberattaque de janvier 2023 ayant entraîné le vol de données de plus de 33 millions d'assurés en France), ou bien des ruptures d'activités avec des conséquences potentiellement importantes sur la *supply chain*. Ainsi, le risque cyber peut entraîner une défaillance de l'économie, causée par des attaques massives à grande échelle frappant un grand nombre de victimes ou bien des événements cyber plus ciblés mais fragilisant un réseau

d'interdépendances industrielles. L'assurance cyber apparaît dès lors comme un élément important pour contribuer à la résilience du tissu économique et industriel. Néanmoins, pour voir émerger une protection financière à large échelle économiquement viable et permettant une mutualisation efficace des pertes en cas de sinistre majeur, l'assurance cyber doit surmonter les défis inhérents aux spécificités de ce risque émergent.

## Une mutualisation en péril

Le mécanisme de l'assurance étant basé sur l'anticipation des coûts futurs et leur mutualisation solidaire, l'enjeu est de modéliser et quantifier les dommages causés par le risque à partir des données historiques disponibles. Or, la quantification, et donc l'anticipation, des impacts du risque cyber est rendue difficile par la nature même de ce risque émergent, en rapide évolution et très dépendant de l'évolution des comportements de l'écosystème (hackers, usagers, acteurs de la protection). De plus, le caractère volatile et hétérogène du risque entraîne une forte variance dans les estimations, à laquelle s'ajoute la variance statistique due au manque de données historiques fiables pour calibrer les modèles.

Face à cette incertitude, la structuration et la tarification des contrats d'assurance cyber est dès lors plus délicate, dans l'objectif de proposer des contrats adaptés aux expositions cyber des assurés et des tarifs équitables et supportables par les entreprises, afin d'élargir la base de mutualisation. Les rapports LUCY<sup>4</sup> (LUMière sur la CYberassurance) réalisés par l'Association pour le management des risques et des assurances de l'entreprise (AMRAE) depuis 2021, illustrent ce tâtonnement de l'assurance cyber en France. Il s'agit donc pour les acteurs de proposer des méthodes quantitatives innovantes permettant d'effectuer un suivi fin et continu de ce risque très évolutif, tout en prenant en compte l'hétérogénéité du risque et des effets de dépendance complexes. Pour étudier la composante fréquence du risque, les modèles dynamiques et adaptatifs, tels que les processus de Hawkes<sup>5,6</sup>, sont une alternative intéressante aux modèles stationnaires traditionnellement utilisés en assurance (tels que les processus de Poisson). Les sinistres cyber n'arrivent pas indépendamment les uns des

autres, contrairement à d'autres risques plus classiques, ces modèles alternatifs, dits « auto-excités », ont la capacité d'appréhender les effets boule de neige des cyber-événements ainsi que leurs interactions. Leurs versions multidimensionnelles, auxquelles peuvent s'ajouter des chocs exogènes (tels que la divulgation de vulnérabilités), permettent de capter les interactions des cyberévénements en fonction de leurs caractéristiques, tout en bénéficiant d'une représentation paramétrique interprétable et parcimonieuse. Une autre préoccupation majeure est le caractère systémique du risque cyber. Or cette dimension systémique est elle aussi difficile à quantifier. Un événement majeur, ou « cyberpandémie », peut découler de la survenance concomitante d'un nombre important de sinistres mineurs, entraînant la défaillance simultanée de nombreux assurés et mettant ainsi en péril la mutualisation. La construction de scénarios stochastiques de crise<sup>7,8</sup> permet de disposer d'un spectre très large de *stress tests* afin d'étudier l'impact potentiel d'un événement cyber massif et d'estimer la capacité de l'entité (assureur/réassureur/grandes entreprises) à absorber un choc d'ampleur significative. Au-delà de l'appréhension d'éventuelles pertes de mutualisation causées par un événement cyber massif, ces scénarios stochastiques, qui intègrent des modules de protection, permettent également de souligner l'importance de la préparation à une crise et de la capacité de réaction quand elle survient. En effet, la réactivité des acteurs et leur comportement est un élément essentiel de la réduction des pertes, permettant de limiter les coûts des sinistres liés à ces scénarios d'accumulation. En ce sens, l'assurance cyber est également un outil de cyberdéfense, puisque la protection financière fournie par l'assurance est souvent couplée (dans de nombreux contrats) de mesures d'accompagnement (mise en place de bonnes pratiques, assistance en cas de crise...), qui s'ajoutent aux contre-mesures déployées face aux incidents cyber.

## Anticiper l'inédit

Le caractère explosif du risque cyber pose donc la question de son éventuelle inassurabilité. S'il est acquis que le marché de l'assurance privée ne peut absorber les conséquences d'une cyberguerre massive, les situations de conflits géopolitiques (qui sont au cœur de la

**Le risque cyber en quelques chiffres**



**1<sup>T</sup> \$**

montant estimé des dommages liés au cybercrime en 2021



**33<sup>M</sup>**

nombre d'assurés Français dont les données ont été volées en janvier 2023



**10<sup>Md</sup> \$**

montant des dommages causés par NotPetya



**1<sup>Md</sup> \$**

montant du paiement des rançons en 2023

stratégie d'exclusion des Lloyd's<sup>9</sup>) ne sont pas les seules qui peuvent conduire à des pertes astronomiques. Définir les frontières de l'assurabilité est affaire d'anticipation: si l'on parvient à prévoir les montants en jeu, on est capable de définir ce qui peut être couvert. Une approche fréquence (nombre de sinistres attendus) - sévérité (montant moyen de ceux-ci) ne peut suffire, car une catastrophe peut rendre caduc le scénario central qu'est censée refléter la prime d'assurance. Il faut donc définir les contours de cette catastrophe potentielle et rassurer sur la capacité du secteur à absorber un tel choc.

L'une des particularités du risque cyber est que son potentiel catastrophique est essentiellement en devenir. D'autres menaces tutoient bien entendu les frontières de l'inassurabilité. Mais on peut se faire une représentation assez claire d'un désastre naturel et le Covid a remis à jour nos connaissances sur les conséquences d'une crise épidémiologique. Dans ces deux domaines, de nombreuses questions se posent sur la fréquence de répétition des phénomènes extrêmes ainsi que sur l'évolution de leur sévérité. On dispose néanmoins d'une représentation assez claire des conséquences de l'événement redouté. Ainsi, lorsque la Caisse centrale de réassurance s'interroge sur les conséquences d'une crue de la Seine équivalente à celle de 1910<sup>10</sup>, les conditions de l'étude sont clairement établies. Si les projections des impacts financiers sont très incertaines, on sait définir l'événement qui les suscite: huit à neuf mètres au niveau du pont d'Austerlitz.

Pour le cyber, il faut faire preuve de beaucoup plus d'imagination, car dans ce domaine, il n'existe pas dans l'histoire de catastrophe à laquelle on puisse se référer. Cette assertion peut paraître de prime abord provocatrice. L'actualité nous apporte régulièrement de nouveaux incidents spectaculaires. Les cyberpandémies WannaCry et NotPetya en 2017 sont souvent citées comme des catastrophes fondatrices d'une prise de conscience. Mais force est de constater que ni les 4 milliards de dollars de dommages générés par WannaCry, ni les 10 milliards de NotPetya, ni même les pertes attribuées au « Lovebug » en 2001 lorsqu'Internet n'était encore qu'adolescent, ne sont à la hauteur du potentiel de pertes que pourrait générer un incident majeur. Ces crises sont fondatrices parce qu'elles laissent entrevoir ce potentiel et nous rappellent notre

vulnérabilité, en non parce qu'elles constitueraient un mètre-étalon pour l'anticipation des catastrophes futures.

### Approche historique, approche par scénarios

Pour projeter les conséquences du risque, il faut donc passer d'une approche historique (c'est-à-dire basée sur l'analyse et la reproduction de standards passés) à une méthode par scénarios. Dans le domaine, le rapport de l'Institut Montaigne<sup>11</sup> donne un aperçu glaçant des conséquences à envisager. En-dehors de ce rapport datant de plus de cinq ans (une éternité à l'échelle des évolutions du cyber), il est bien difficile de recenser des études précises pouvant servir de base à des scénarios quantitatifs. La culture populaire, elle, a pris les devants en proposant, via la fiction, de nombreux cas d'études, du déclenchement de la troisième guerre mondiale par des pirates informatiques dans *Wargames* (J. Badham, 1983), au récent *Leave the world behind* sur Netflix (S. Esmail, 2023) où une attaque cyber déclenche la désagrégation des États-Unis. L'empressement de certains experts de la cybersécurité à commenter le blockbuster de Netflix (sur le mode réaliste - irréaliste) montre, outre l'aspect médiatique, que ces fictions ont le mérite de stimuler la réflexion sur l'anticipation des crises. L'Agence de l'Innovation de Défense finance d'ailleurs des équipes d'auteurs de science-fiction pour imaginer les périls qui menacent la société<sup>12</sup>.

Pour autant, l'exercice ne satisfera pas complètement l'expert quantitatif. Si l'on veut définir les contours de l'assurabilité du risque cyber, la posture de prophète de l'apocalypse n'est pas satisfaisante. Car projeter les pertes au moyen de l'étude de scénarios repose sur une approche scientifique, où il ne s'agit pas seulement de laisser divaguer l'imagination vers des situations toujours plus extrêmes, mais de hiérarchiser ces hypothèses de travail de la façon la plus scientifique possible.

L'Autorité européenne des assurances et des pensions professionnelles (EIOPA) propose, dans son papier méthodologique sur la mise en œuvre de *stress tests* cyber<sup>13</sup>, une tentative de rationaliser une telle démarche. On pourra critiquer l'éventail restreint des situations considérées, ou encore reprocher des

**C'est au fond l'idéal que doit poursuivre le développement de l'assurance cyber, accompagner le mouvement de la société vers une meilleure intégration des démarches vertueuses en termes de cybersécurité.**

imprécisions, néanmoins le document présente le mérite indéniable de réfléchir à un cadre suffisamment clair permettant de formaliser l'exercice. Pour un scénario particulier, il s'agit de définir les caractéristiques clés qui permettront de simuler son impact, des aspects techniques (le temps d'interruption d'un service *cloud*, par exemple) aux réactions humaines (le degré de préparation des plans de continuité d'activité). Charge au modélisateur d'alimenter ces paramètres en valeurs crédibles.

Ce n'est pas la moindre des tâches, et il faut ici dissiper une confusion qui entoure trop souvent les approches par scénarios: si ces approches visent à étudier des situations qui n'ont jamais été rencontrées dans le passé, elles doivent, pour espérer être efficace, être alimentées par des données statistiques. Il faut débarrasser ce terme de sa connotation purement rétrospective. La grande difficulté, dans le cas présent, est de faire le tri entre des informations de natures diverses (données

quantitatives, rapports d'expertise, analyses de la menace, données parfois non-structurées), et d'éliminer le bruit causé par celles qui se révèlent inadéquates ou obsolètes, alors que la cacophonie des études envoie des signaux contradictoires.

Ce n'est que par la mise en œuvre d'une démarche statistique transparente et scientifiquement auditable que l'on pourra atteindre une quantification suffisamment réaliste et précise des impacts d'une crise cyber d'ampleur. Or, cette quantification est bien le préalable à tout dialogue sur le partage des risques entre les différents acteurs (assureurs, assurés, États). Elle seule peut clarifier les besoins en capital, et de là les conditions d'indemnisation qui permettent de répondre au mieux aux besoins de couverture de la société sans mettre en danger la solvabilité des compagnies. Elle doit également devenir le socle d'une politique de prévention efficace. Dans le domaine, d'immenses progrès ont été notés, comme le souligne le rapport 2023 de l'enquête LUCY de l'AMRAE. Les chiffres encourageants du secteur de l'assurance cyber, en 2022, sur le marché français, s'expliquent, si l'on se fie à l'analyse des concepteurs de l'étude, par une amélioration considérable du niveau de sécurité des entreprises françaises.

Car c'est bien là le second volet d'un mouvement vers une plus large assurabilité du cyber: une meilleure quantification des risques ne doit pas se contenter d'une analyse figée de la menace. Elle appelle à cibler les efforts des différents acteurs sur la prévention des risques les plus critiques. C'est au fond l'idéal que doit poursuivre le développement de l'assurance cyber: accompagner le mouvement de la société vers une meilleure intégration des démarches vertueuses en termes de cybersécurité. Un parallèle est souvent effectué avec le rôle historique de l'assurance dans le domaine de l'incendie, l'émergence des premières compagnies anglaises dans le sillage du grand incendie de Londres (1666) ayant contribué à développer les brigades d'intervention et les normes qui conduisirent à une réduction spectaculaire du risque. S'il est souhaitable de s'inspirer d'un tel exemple, le chemin reste long. Car si, comme pour l'incendie, le risque cyber est essentiellement affaire de comportement des acteurs (l'hygiène cyber étant la clé), sa perception reste plus abstraite pour les individus comme pour les organisations. La



### Notes

- <sup>1</sup> <https://edition.cnn.com/2021/04/12/business/jerome-powell-cyberattacks-global-threat/index.html>
- <sup>2</sup> Commissariat à l'Energie Atomique. "L'enjeu de la cybersécurité". Les Défis du CEAN 242 (2021)
- <sup>3</sup> Forbes : <https://www.forbes.com/sites/forbestechcouncil/2023/05/08/the-hidden-costs-of-cybersecurity/?sh=5c4aa93023e3>
- <sup>4</sup> LUCY : LUmière sur la CYberassurance, AMRAE, [https://www.amrae.fr/recherche?search\\_api\\_fulltext=lucy](https://www.amrae.fr/recherche?search_api_fulltext=lucy)
- <sup>5</sup> Y. Bessy-Roland, A. Boumezoued, C. Hillairet, C. (2021). Multivariate Hawkes process for cyber insurance. *Annals of Actuarial Science*, 15(1), 14-39.
- <sup>6</sup> A. Boumezoued, Y. Cherkaoui, C. Hillairet. Cyber risk modeling using a two-phase Hawkes process with external excitation, (2023). <https://arxiv.org/abs/2311.15701>
- <sup>7</sup> Hillairet, C., & Lopez, O. (2021). Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, 1-24.
- <sup>8</sup> Hillairet, C., Lopez, O., d'Oultremont L. & Spooenberg B. (2022). Cyber-contagion model with network structure applied to insurance. *Insurance: Mathematics and Economics*, Volume 107, November 2022, Pages 88-101.
- <sup>9</sup> Market Bulletin, LLOYD'S
- <sup>10</sup> La crue de la seine en île-de-France, CCR
- <sup>11</sup> Institut Montaigne (2018). Cybermenace : avis de tempête. <https://www.institutmontaigne.org/ressources/pdfs/publications/cybermenace-avis-de-tempete-rapport.pdf>
- <sup>12</sup> La Red Team Défense dévoile les scénarios de sa saison 2, Communiqué de presse
- <sup>13</sup> L'EIOPA publie un document sur les principes méthodologiques des tests de résistance des assurances sur les cyber-risques

très forte adaptabilité des écosystèmes criminels rend également nécessaire une vigilance de chaque instant pour maintenir dans le temps les efforts de prévention et les adapter aux changements d'usage. 



# Ratio combiné : combler l'écart entre le coût des sinistres et les primes grâce à l'IA

Le secteur de l'assurance traverse actuellement une période de turbulences, où les coûts des sinistres et les frais de gestion s'approchent dangereusement des montants des primes perçues. Selon le Insurance Information Institute aux États-Unis, cette situation devrait se poursuivre jusqu'en 2025, tandis que le secteur a manqué de peu de terminer l'année 2023 avec un ratio combiné moyen dépassant les 102 %. Dans l'Hexagone, France Assureurs confirme que « l'équilibre technique des différentes branches (IARD) s'est dégradé<sup>1</sup> » depuis l'année dernière. Face à la nécessité d'améliorer le ratio combiné, l'intelligence artificielle a un rôle stratégique à jouer.



**JEREMY JAWISH**  
CEO et Cofondateur,  
Shift Technology

**Dans un marché très compétitif où les résultats des assureurs sont tendus, l'intelligence artificielle est un moyen efficace pour améliorer le ratio combiné à condition d'agir sur l'ensemble de la chaîne de valeur ajoutée : gestion administrative, lutte contre la fraude, méthodes de souscription.**

Deux événements ont récemment fait grimper le coût des indemnités pour les assureurs : la rupture des chaînes d'approvisionnement et la montée de l'inflation. En parallèle, l'augmentation de la fréquence et de l'intensité des incidents météorologiques et autres catastrophes naturelles a eu pour effet d'accroître les montants à rembourser, tout comme le nombre de sinistres. Ceci à un niveau tel qu'une nouvelle hausse

tarifaire des réassurances était attendue à la fin de l'année 2023 après une augmentation déjà conséquente l'année précédente<sup>2</sup>. En tant que partenaire technologique de nombreux assureurs de premier plan en Europe et à travers le monde, Shift Technology occupe une position privilégiée pour observer l'ampleur de ce phénomène. L'augmentation des primes annuelles est un phénomène complexe à gérer. Elles ne peuvent, en effet, pas être revues à la hausse

simplement pour compenser l'augmentation des coûts, et la forte concurrence du marché rend la hausse des tarifs risquée.

Malgré cela, le prix des assurances ne cesse de grimper. Certains assurés auto ont vu le montant de leurs primes dépasser les mensualités versées pour payer leur voiture elle-même tandis que dans certaines régions, certains acteurs historiques se retirent du marché face à l'impossibilité de garantir la rentabilité de leur activité.

## Améliorer le ratio combiné, mode d'emploi

Face à ce constat, le secteur s'est mis en quête de solutions alternatives pour améliorer les ratios combinés. Parmi celles-ci, l'optimisation des processus de gestion des sinistres grâce à l'automatisation et à la digitalisation s'impose comme la plus efficace. À condition de l'utiliser avec méthodologie et savoir-faire, en faisant appel à des experts pour éviter d'ouvrir la porte à d'autres types de fraudes et ce, dans des proportions toujours plus importantes. Dans ce cas de figure, les assureurs compensent en effet tout gain d'efficacité par une augmentation des pertes liées à la fraude.

Les compagnies d'assurance peuvent toutefois aller encore plus loin dans leurs stratégies d'amélioration des ratios combinés. En redoublant de vigilance au moment de la souscription, il leur est par exemple possible de limiter les risques liés à une police ou un contrat d'assurance. Elles peuvent également songer à aborder de manière différente leur gestion des recours.

## Réduire l'impact de la fraude grâce à l'IA

Nous avons récemment démontré, dans notre « Rapport comparatif 2023 sur nos observations en matière de fraude » (« *Claims Fraud Benchmark Report* »), à quel point la détection de la fraude grâce à l'IA pouvait impacter les résultats des compagnies d'assurance. L'analyse par nos solutions de millions de sinistres nous a par exemple indiqué que les assureurs IARD étaient en mesure de bloquer jusqu'à 55 000 euros – pour l'assurance habitation, et 41 000 euros pour l'automobile – par

millier de sinistres analysés. Au bout du compte, une stratégie efficace de réduction des fraudes grâce à l'IA peut entraîner une amélioration du ratio combiné de l'ordre de 1 point.

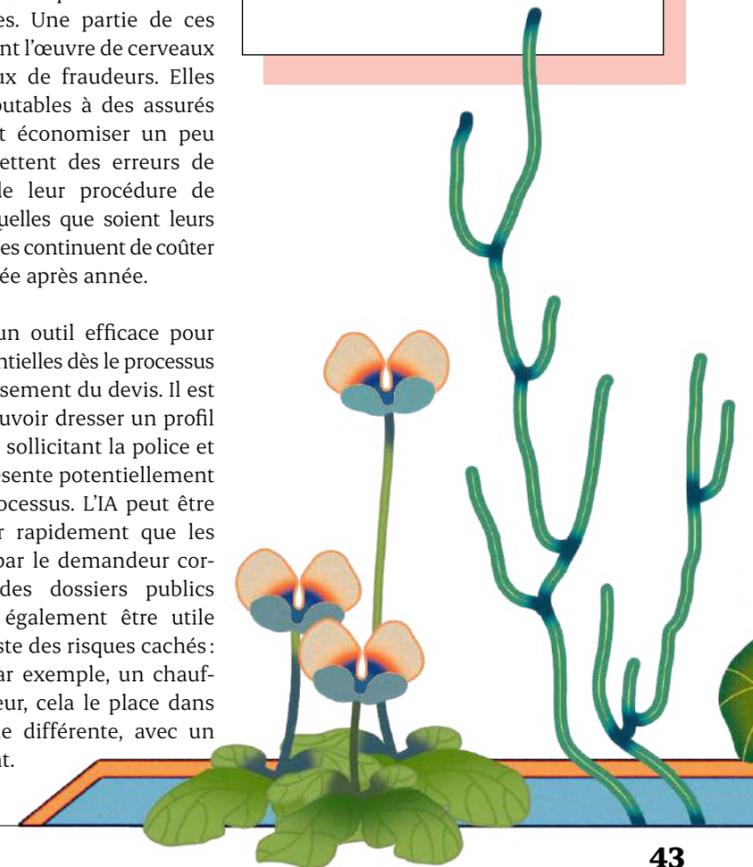
## Éviter les polices non rentables

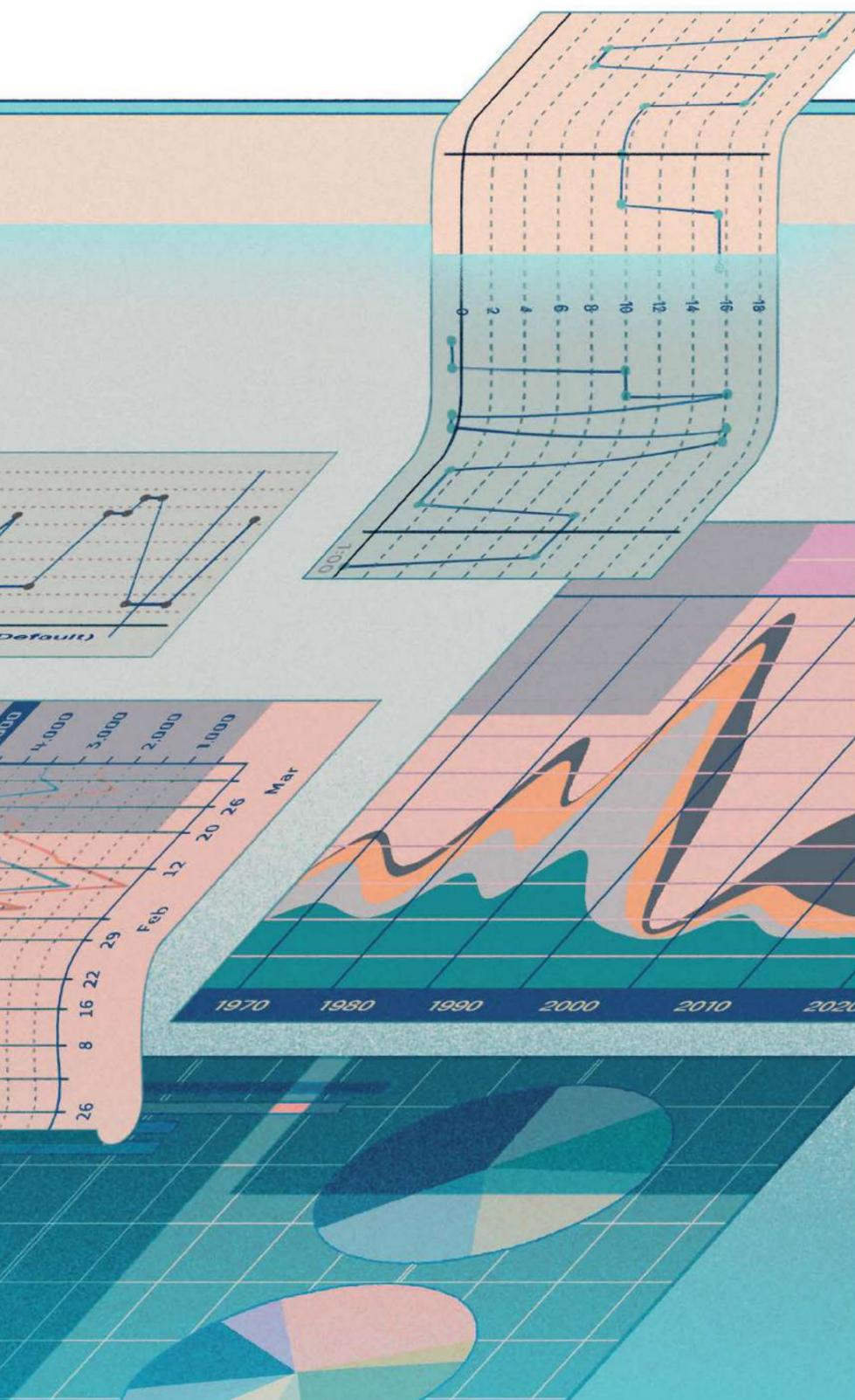
La détection des fraudes grâce à l'IA permet de faire baisser les coûts des sinistres et d'améliorer les ratios combinés. Mais n'est-il pas possible d'intervenir plus tôt dans le cycle de vie des polices ? Nos données indiquent que le recours à l'IA dès le processus de souscription peut aider à réduire le ratio combiné de manière significative, permettant au passage d'éviter les pertes futures. Notamment en comprenant bien et en identifiant les risques associés à une police ou à un assuré, et en utilisant ces connaissances pour prendre les meilleures décisions possibles quant aux actions à mettre en place pour les réduire au maximum.

Les assureurs subissent généralement des pertes de l'ordre de 10 à 15 % par an dues aux seules pertes de primes. Une partie de ces pertes n'est pas forcément l'œuvre de cerveaux criminels ou de réseaux de fraudeurs. Elles peuvent aussi être imputables à des assurés ordinaires qui espèrent économiser un peu d'argent ou qui commettent des erreurs de bonne foi au cours de leur procédure de demande d'adhésion. Quelles que soient leurs causes, ces fuites de primes continuent de coûter cher aux assureurs, année après année.

L'IA s'est révélée être un outil efficace pour identifier ces pertes potentielles dès le processus de demande et d'établissement du devis. Il est en effet essentiel de pouvoir dresser un profil complet de la personne sollicitant la police et des risques qu'elle représente potentiellement avant de finaliser le processus. L'IA peut être utilisée pour confirmer rapidement que les informations fournies par le demandeur correspondent à celles des dossiers publics disponibles. Elle peut également être utile pour déterminer s'il existe des risques cachés : si le demandeur est, par exemple, un chauffeur de taxi ou un livreur, cela le place dans une catégorie de risque différente, avec un barème de taux différent.

**Une stratégie efficace de réduction des fraudes grâce à l'IA peut entraîner une amélioration du ratio combiné de l'ordre de 1 point.**





### La montée en puissance de la fraude digitale

Alors que certains secteurs ont vu les incidents de fraude numérique diminuer de près de 15 %, celui de l'assurance est de plus en plus pris pour cible par des fraudeurs 2.0. Cette fraude visant les assureurs aurait augmenté de 130 à 160 % (!) au cours des dernières années. Contrairement à la plupart des fuites de primes mentionnées précédemment, il s'agit bien ici de fraudes perpétrées avec une intention délictueuse évidente.

Les fraudeurs profitent de l'anonymat, un corollaire du numérique à l'origine destiné à simplifier le processus d'achat d'une assurance, que ce soit directement auprès de l'individu souscripteur ou par l'intermédiaire d'un agent ou d'un courtier. Le digital facilite la falsification d'informations, la dissimulation d'identité et la mise en place de nouvelles méthodes telles que le « courtage fantôme », procédé par lequel les fraudeurs utilisent les canaux numériques et les médias sociaux pour vendre de fausses polices d'assurance à des consommateurs peu méfiants. L'IA, à son tour, facilite la détection des signaux indiquant que des escrocs numériques tentent d'utiliser le portefeuille d'affaires d'un assureur à des fins malveillantes. Elle peut, par exemple, aider à repérer l'utilisation récurrente d'informations personnelles identifiables (PII) dans des demandes d'indemnisation censées n'avoir aucun rapport entre elles, ce qui peut indiquer la présence d'un réseau de fraude.

La capacité à détecter les fraudes sophistiquées, en bandes organisées ou en réseaux – l'un des risques majeurs pour les acteurs du secteur –, revêt une importance cruciale quand on sait que le ratio sinistres à primes de cette catégorie peut être jusqu'à six fois supérieur à la moyenne du portefeuille d'un assureur. Identifier et prévenir ce risque en amont aura forcément une incidence notable et extrêmement positive sur le ratio combiné. Ceci se vérifie également pour des pratiques frauduleuses, telles que le courtage fantôme, les comportements malhonnêtes des intermédiaires, l'endossement en blanc ou encore le détournement de polices. Soit toutes les stratégies pouvant avoir un impact négatif à la fois sur les pertes liées aux sinistres et sur les primes encaissées.

**Nos recherches ont en effet démontré que les assureurs utilisant l'IA dans le cadre de la gestion des recours pouvaient récupérer en moyenne jusqu'à 7% supplémentaires de la valeur totale des sinistres.**

### Optimiser la gestion des recours

Pour les assureurs opérant à l'étranger, le coût des opportunités de recours manquées ou ignorées peut également atteindre des montants considérables. L'identification et la poursuite de ces opportunités est un processus fastidieux, long et manuel, pour lequel nombreux sont ceux qui estiment que le jeu n'en vaut pas la chandelle.

Considérant les difficultés auxquelles le secteur fait face actuellement, il pourrait néanmoins s'avérer pertinent de réexaminer certaines d'entre elles dans le but d'améliorer les ratios combinés. Nos recherches ont en

effet démontré que les assureurs utilisant l'IA dans le cadre de la gestion des recours pouvaient récupérer en moyenne jusqu'à 7% supplémentaires de la valeur totale des sinistres.

### L'IA comme multiplicateur de forces

L'intelligence artificielle peut donc être appliquée à différents processus tout au long du cycle de vie des polices en vue d'améliorer les ratios sinistres à primes. Or, l'amélioration de ceux-ci, ne fût-ce que d'un seul point, peut faire la différence entre subir une perte, atteindre le seuil de rentabilité ou réaliser un bénéfice. Le recours à plusieurs de ces solutions de manière combinée est ainsi susceptible d'avoir un impact très important, permettant de réduire ces ratios de 3 à 6 points.

L'épineuse question du ratio combiné n'est pas près de disparaître et la totalité des assureurs se verront contraints de mettre au point des stratégies en vue de la résoudre à plus ou moins long terme. En attendant, certaines mesures peuvent d'ores et déjà être prises. Notamment, la mise en place d'une combinaison puissante mêlant efficacité des processus et réduction des coûts.

L'IA se révèle efficace pour détecter les activités suspectes, raccourcir les cycles d'investigation et éviter de déboursier de l'argent pour des sinistres frauduleux. Elle permet également d'améliorer de manière significative la gestion des recours. Enfin, l'IA peut aider les assureurs à démarrer avec un portefeuille d'affaires propre, en évitant les déficits futurs liés à une mauvaise évaluation des primes à verser. Prises individuellement, ces approches sont précieuses. Ensemble, elles sont inestimables. ❗



### Notes

<sup>1</sup> L'Argus de l'Assurance, « 2022, une année chahutée pour l'assurance », 19/04/2023.

<sup>2</sup> L'Agefi, « La hausse des prix de la réassurance maintient les assureurs sous tension », 11/09/2023.



ANALYSES & DÉFIS

# Les risques géostratégiques

La géopolitique s'organise autour de trois motifs de conflits susceptibles d'éclater seuls ou par deux ou par trois simultanément : les conflits territoriaux, les conflits idéologiques et religieux, les conflits économiques enfin. La conjoncture actuelle nous en donne plusieurs exemples. La guerre entre l'État d'Israël et le Hamas à Gaza est une illustration parfaite de conflit territorial. L'idéologie sous sa forme religieuse n'y est pas absente, mais elle n'est pas mise en avant par les protagonistes. Quant à l'enjeu économique, on peine à l'identifier. →



**DANIEL ZAJDENWEBER**  
Comité éditorial, *Risques*



→ Le territoire en feu, Gaza, n'a pas de richesses minérales ou agricoles qui pourraient justifier une occupation par l'un ou l'autre des adversaires, tandis que la partie de la Cisjordanie occupée par l'État d'Israël, actuellement en paix relative, a certes des richesses agricoles, mais on peut douter de leur importance réelle dans le déclenchement d'un conflit militaire, si celui-ci devait advenir. Scénario pessimiste, la ressource en eau douce du côté du fleuve Jourdain, si elle venait à manquer, pourrait être à l'origine d'un futur conflit entre l'État d'Israël et le Royaume de Jordanie, allié ou non à des organisations terroristes. Le motif économique dominerait alors le motif idéologique, mais n'anticipons pas. Les guerres menées par l'Iran, d'abord militairement contre l'Irak puis à travers des organisations terroristes dans le Proche-Orient, au Yémen et même dans le monde entier par le moyen d'attentats, sont des exemples parfaits de conflits d'origine idéologique et religieuse. Sauf quelques différends à ses frontières avec le Pakistan, l'Iran ne revendique pas de territoires. La seule richesse dont il dispose, le pétrole, n'est pas instrumentalisée dans les conflits. Au contraire, dans la mesure où le pétrole iranien fait l'objet d'un embargo et où toute l'économie de l'Iran subit les interdictions internationales, on peut dire que le motif économique est négatif par rapport au motif idéologique et religieux. Il en va de même avec la guerre entre la Russie et l'Ukraine où nous avons un exemple du couplage de deux motifs, l'idéologique et le

territorial, couplage qui sacrifie l'économie de la Russie en raison de la perte de ses marchés européens et des investissements faits par les Européens et les Américains. Or, les richesses économiques de l'Ukraine ne sont pas telles qu'elles justifieraient un conflit fondé sur la prédation. Le charbon, par exemple, dont la province du Donbass est dotée, a pu être convoité par le passé. Il ne l'est plus aujourd'hui dans le contexte de la restriction de la production mondiale de gaz à effet de serre. Quant au blé, ou aux autres ressources agricoles de l'Ukraine, il n'est pas utile d'envahir le pays pour en disposer, le marché mondial y pourvoit y compris pour les blés russes.

La guerre initiée par la Russie rappelle à quel point une autre guerre, la froide, couplait les motifs idéologiques, territoriaux et économiques. On avait alors une parfaite superposition des territoires (l'ouest d'un côté l'est de l'autre) et des régimes économiques dominés par une idéologie (le capitalisme et le socialisme), superposition que la disparition de l'URSS a pulvérisée.

Le motif économique est évidemment à l'origine du conflit entre la Chine et les États-Unis. Il y a bien un conflit territorial latent qui peut devenir manifeste, Taïwan, mais pour l'heure il est secondaire par rapport aux nombreuses mesures prises par les États-Unis à l'encontre de l'économie chinoise. D'aucuns pouvaient opposer l'idéologie de la Chine à celle des États-Unis. Mais, entre le capitalisme de l'un et

le capitalisme de l'autre, il y a surtout l'importance d'un parti communiste très puissant, qui n'a pas pour autant empêché la croissance d'un important secteur privé compétitif dans le commerce mondial. Et c'est bien là toute l'originalité des conflits économiques par rapport aux conflits idéologiques ou territoriaux. Les protagonistes ont des intérêts communs, mieux ils sont entremêlés, comme le montre le conflit entre la Chine et les États-Unis. La Chine est à la fois le premier marché pour les exportations occidentales et américaines, le premier fournisseur de marchandises comme les textiles, l'électroménager, les jouets, bientôt l'automobile électrique, les batteries etc. Elle est aussi l'un des sous-traitants essentiels d'Apple pour la fabrication de ses smartphones et l'un des acheteurs importants (avec les Européens) de bons du Trésor américain, faisant ainsi de la Chine tout à la fois le concurrent, le client, le fournisseur et le financier des États-Unis.

Dans le contexte conflictuel actuel, l'assurance mondiale est non seulement confrontée à une sinistralité aggravée, mais aussi à une position inconfortable car elle se trouve en quelque sorte «entre le marteau et l'enclume», par exemple lorsqu'elle est confrontée au dilemme d'indemniser une partie en conflit quand l'une, les États-Unis, interdit de le faire par le biais de l'exterritorialité du droit américain. Les cinq articles de ce dossier analysent chacun les divers facteurs de cette sinistralité due aux conflits géopolitiques en cours.



## EN UN COUP D'ŒIL

### Lexique



Si le mot «*géostratégie*» est employé en anglais dès 1944, son entrée dans la langue française daterait de 1975.



### Le saviez-vous ?

Dans le cadre des sanctions contre la Russie, depuis le 5 décembre 2022 (pétrole brut) et le 5 février 2023 (produits raffinés), les assureurs sont tenus de ne plus offrir de services d'assurance qu'aux navires dont le chargement a été acquis à un prix inférieur au maximum.

### Pour prolonger votre réflexion sur les sanctions économiques

● ACPR. (2021). Lignes directrices conjointes de la Direction générale du Trésor et de l'Autorité de contrôle prudentiel et de résolution sur la mise en œuvre des mesures de gel des avoirs.

● Imbs, Jean and Pauwels, Laurent, (2023). «An Empirical Approximation of the Effects of Trade Sanctions with an Application to Russia», *Economic Policy*, Forthcoming.

● Trainar P. (2023). « Le bilan des sanctions économiques ». *Commentaire*, 184, hiver 2023-24.

### Les chiffres à retenir

# 75 %

des experts interrogés dans le cadre du rapport annuel AXA sur les risques émergents considèrent que les risques sont de plus en plus interconnectés.

# 60 %

des sondés de l'étude estiment que notre société doit prendre des risques pour progresser.

# Des risques géopolitiques enchevêtrés, aggravés par le jeu des anticipations



**GILLES ANDRÉANI**

Président de chambre à la Cour des comptes et Président de la Commission du secret de la Défense nationale (CCSDN)

**Gilles Andréani développe une dimension inquiétante des conflits en cours, celle d'engendrer des conflits à venir, due aux jugements des dirigeants des principales puissances mondiales en conflit : la Russie en guerre avec l'Ukraine, mais potentiellement aussi avec l'Europe et les États-Unis, la Chine avec Taïwan et possiblement avec les États-Unis, la Corée du Nord avec les États-Unis, etc. sans oublier les attaques non-étatiques menées par des groupes terroristes, toujours imprévisibles.**

Avec l'invasion de l'Ukraine par la Russie, le retour des menaces et de la guerre entre États a eu tendance à faire oublier les risques-non étatiques et transnationaux, qui étaient la source majeure de désordres à l'échelle mondiale depuis la fin de la guerre froide. Or, les premières ne se sont pas substituées aux seconds. Les deux types de tensions coexistent.

La superposition de risques non-étatiques persistants et de nouvelles rivalités ouvertes entre les États représente une conjonction dangereuse. Ces deux catégories de tensions, en effet, ne sont pas isolées l'une de l'autre : elles tendent au contraire à se renforcer mutuellement.

Non seulement leurs rivalités empêchent les États de coopérer pour gérer les risques globaux, mais elles les poussent à les instrumentaliser pour les retourner contre leurs rivaux. Dans ce contexte, le jeu des anticipations, l'appréhension que le rapport de forces ne se détériore avec le temps, conjugués avec l'excès de confiance en soi, pourraient mener à une aggravation des risques géopolitiques.

## Un retour des menaces, dans un cadre international déréglé

Il faut commencer par la guerre en Ukraine et se demander ce qu'elle signifie pour l'évolution du risque géostratégique.

Après la guerre froide, le mot « menace » avait disparu des communiqués de l'OTAN et des doctrines stratégiques occidentales qui lui substituèrent le mot « risque ». Vus d'un Occident qui dominait le système international, seuls des États comme l'Iran, la Corée du Nord, ou l'Irak de Saddam Hussein se présentaient encore comme des menaces, marginales et résiduelles, et d'ailleurs gérables : on était dans un monde où un conflit entre puissances majeures était devenu impensable.

La violence politique subsistait, mais prenait d'autres formes : décomposition violente des États multinationaux, comme en Yougoslavie ; guerres civiles entre ethnies ou groupes religieux rivaux qui débouchaient sur la faillite des États concernés, la violence de masse, voire, dans le cas du Rwanda, le génocide ; terrorisme déterritorialisé indépendant des stratégies étatiques sur le modèle d'Al-Qaïda.

Ces phénomènes n'étaient pas, pour l'Occident, un motif d'inquiétude existentielle, tant qu'ils ne convergeaient pas avec d'autres facteurs susceptibles d'en démultiplier les dangers, comme la prolifération des armes de destruction massive, les migrations de masse ou la criminalité transnationale, en particulier numérique.

L'opinion générale à l'Ouest était que ce monde était, à tout prendre, moins dangereux que celui de la guerre froide puisque le spectre d'un conflit direct entre puissances nucléaires avait disparu, mais aussi moins prévisible et rempli de risques à venir, non identifiés, qu'il fallait néanmoins s'efforcer de prévenir : « il y a des inconnues connues et des inconnues inconnues », dit ainsi en 2002 Donald Rumsfeld, secrétaire américain à la Défense, aphorisme resté célèbre visant à justifier par avance l'attaque préventive de l'Irak.

En février 2022, avec l'agression russe de l'Ukraine, l'on est revenu à un monde dominé

par les tensions entre puissances majeures et la menace de guerre. Deux séries de tensions géopolitiques dominant aujourd'hui les relations internationales : celle qui oppose la Russie à l'Occident, dont l'appui financier et militaire à l'Ukraine lui a permis de résister jusqu'ici à l'offensive russe ; celle qui oppose la Chine et les États-Unis, et qui se nourrit d'une série de griefs mutuels, commerciaux, politiques et stratégiques, le plus dangereux étant la question de Taïwan.

Sont-ils l'un et l'autre susceptibles de dégénérer en guerre ouverte ?

Pékin assume la possibilité d'attaquer Taïwan au cas où « l'île rebelle » franchirait une ligne rouge comme celle consistant à déclarer son indépendance, et Washington a dit que, dans ce cas, il défendrait Taïwan ; la réponse est clairement qu'une telle guerre est possible.

Or, sur le plan économique et stratégique, il est difficile de concevoir un risque de magnitude supérieure à celle d'un conflit ouvert entre les États-Unis et la Chine : interruption des échanges entre les deux principales économies du monde, dont les chaînes de production sont étroitement intégrées, recul massif du commerce international, etc. Ce serait un retour en arrière dans la mondialisation des échanges qui plongerait dans le chaos l'économie globalisée.

Rien à voir avec la guerre en Ukraine, qui met aux prises des puissances secondaires sur le plan économique, au rôle près de la Russie sur le marché de l'énergie, dont on a vu qu'il constituait pour Moscou un levier d'influence médiocre dans le conflit (mais, à court terme, une source persistante de revenus.)

Vladimir Poutine, quant à lui, dit mener une guerre défensive contre un Occident qui l'a agressé en incitant l'Ukraine à se détacher de la Russie ; il s'estime donc déjà en guerre avec nous. L'Occident soutient l'Ukraine dans le cadre d'un consensus fort, consistant à ne pas s'impliquer dans les combats ni à entrer en guerre aux côtés de l'Ukraine.

La réponse, s'agissant de la Russie et de l'Occident est donc plutôt négative : entre eux, la guerre est indirecte et verbale ; mais le sentiment d'hostilité grandit et la situation militaire, dans l'impasse, incite les deux côtés à l'escalade pour en sortir.

**Après la guerre froide, le mot « menace » avait disparu des communiqués de l'OTAN et des doctrines stratégiques occidentales qui lui substituèrent le mot « risque ».**

Dans le meilleur des cas, une confrontation prolongée et indécise entre la Russie et l'Ukraine risque d'être une source d'instabilité permanente pour l'Europe, comme la question du Cachemire l'est pour l'Inde et le Pakistan. Elle va durablement marginaliser la Russie, qui va rester une puissance au ban de la communauté des États européens et plus largement, du monde développé. Sa seule voie de sortie, dans ces conditions, sera une inféodation croissante à la Chine.

Le monde se retrouve ainsi avec quatre pôles de puissance majeurs, les États-Unis, la Russie, la Chine, et l'Europe. Chacun regarde deux des autres comme une menace active (ou potentielle pour ce qui est de la relation de la Chine avec l'Europe, moins dégradée qu'avec les États-Unis et non affectée – du moins pas directement – par la question de Taïwan, mais peu confiante en tout état de cause).

Le système international est-il en mesure de gérer ces tensions et comporte-t-il des éléments stabilisants permettant de réduire les risques qui leur sont associés ? Plusieurs évolutions récentes de ce système incitent plutôt au pessimisme à cet égard.

Le système international est devenu multipolaire: les alignements permanents qui contribuaient à sa stabilité se sont relâchés et sont à présent intermittents et opportunistes: l'Inde, amie historique de la Russie peut l'aider à contourner les sanctions américaines, tout en faisant cause commune avec les États-Unis contre la Chine; la Turquie, aider l'Ukraine en lui vendant des drones, et s'opposer à un élargissement de l'OTAN qui consolide la coalition pro-ukrainienne; dans la guerre de Gaza, Israël ignore superbement les objurgations d'un président américain qui est sans doute le plus pro-israélien depuis une génération.

**Des risques non-étatiques qui convergent avec les menaces**

Dans ce monde de nations rivales ou, en tout cas, qui n'écourent que leur intérêt, où nationalisme et populisme ont partout l'ascendant, chez les pays établis comme chez les puissances émergentes, l'on se sent de moins en moins tenu par les règles et les cadres multilatéraux: l'OMC n'a pas produit d'accord général depuis vingt ans, et son système de règlement des différends est en crise. Le Conseil de sécurité de l'ONU est à nouveau paralysé, comme au temps de la guerre froide. L'Union européenne elle-même est traversée de forces politiques qui défient ses principes et les disciplines communes les plus élémentaires.

Au total, l'on ne peut guère compter sur les institutions multilatérales, ni sur le patronage des plus grandes puissances pour prévenir les crises et limiter leurs effets.

Les plus visibles et les plus dangereuses sont aujourd'hui le fait des États et du retour de la guerre comme instrument normal de la politique. Cependant, pendant que les menaces liées à la dégradation des relations entre États montent, les risques non-étatiques n'ont pas disparu: à la croisée du terrorisme, de la prolifération des armes de destruction massive, de la criminalité transnationale, de la cyber-délinquance et de la montée des sentiments identitaires corrosifs pour la cohésion des États, ils sont toujours présents.

Ces risques croissent à l'abri des tensions entre les États, qui coopèrent moins pour les juguler, quand ils ne les exploitent pas à leur profit

**De tout cela résulte un brouillage de la frontière entre risques et menaces, entre guerre ouverte et guerre asymétrique, entre les tactiques de l'un et l'autre types d'affrontement, qui nous renvoie à une situation de ni paix ni guerre qui, avec des fins et des modalités très différentes, était celle de la guerre froide.**

contre leurs adversaires, quitte à les aggraver. Autrefois relativement unis pour tenter de trouver une solution aux deux problèmes majeurs de prolifération que sont l'Iran et la Corée du Nord ou, en tout cas, éviter qu'ils ne dégénèrent en crise ouverte, les puissances se divisent: la Russie, qui a besoin de leurs fournitures de missiles, d'obus et de drones, soutient ouvertement l'Iran et la Corée du Nord, dont elle ne cherche plus à modérer les comportements, ni la Chine, qui tout en restant ostensiblement à l'écart de ces deux problèmes, y jouait naguère un rôle discrètement utile. On a vu en Afrique la conjonction des intérêts

d'État russes et de la fragilité de plusieurs pays consolider les juntes militaires qui y avaient pris le pouvoir et leur faciliter l'éviction de la présence française. En mer Rouge, les armements antinavires fournis par l'Iran aux milices houthies a permis à celles-ci d'y compromettre le trafic maritime; l'escorte des navires marchands par les marines occidentales a été insuffisante pour contrer cette menace, et les bombardements de représailles anglo-américains n'ont pas suffi à décourager les Houthis.

À la faveur de la guerre en Ukraine, l'on voit progresser des technologies telles que des mini drones armés fabriqués en 3D, dont la diffusion aux mains de groupes terroristes serait hautement déstabilisante, mais dont l'Occident favorise l'acquisition par l'Ukraine. Des attentats comme celui contre les gazoducs Nord Stream en septembre 2022, attribué initialement à la Russie, puis, de façon plus vraisemblable, à l'Ukraine, démontre la porosité entre les tactiques du terrorisme ou du combat clandestin, d'un côté, et celles de la guerre ouverte de l'autre; porosité illustrée avec éclat du côté russe par le recours massif à l'espionnage, à la désinformation, voire à l'intimidation, à l'assassinat et à l'empoisonnement.

Plus généralement, la compétition dans la sphère de l'information numérique, la diffusion de fausses nouvelles ou le combat informationnel sont aujourd'hui des tactiques communes aux États et aux organisations non-étatiques, celles-ci servant souvent de paravent aux premiers.

De tout cela résulte un brouillage de la frontière entre risques et menaces, entre guerre ouverte et guerre asymétrique, entre les tactiques de l'un et l'autre types d'affrontement, qui nous renvoie à une situation de ni paix ni guerre qui, avec des fins et des modalités très différentes, était celle de la guerre froide.

**Entre le jeu des intérêts et la revanche des passions: le danger des anticipations**

Les rivalités ouvertes reviennent au centre de la politique internationale, et s'expriment à travers une gamme de moyens, réels ou virtuels, où la guerre ouverte revient, aux côtés des instruments de la guerre asymétrique.

**Dans les deux cas, avec la peur, il y a le désir de dominer, ou du moins de projeter une image de force conforme à l'idée qu'on se fait de son pays.**

Cela compromet, cela va sans dire, la maîtrise par les États des grands enjeux collectifs tels que les luttes contre le changement climatique ou pour la promotion maîtrisée des nouvelles technologies comme l'IA.

Au lendemain du 11 septembre 2001, l'on avait vu dans cet événement la marque d'une haine sans limite, d'une revanche des passions sur un monde que prétendaient unir le progrès de la démocratie et l'intégration économique globale. Alors que les causes de désordre et les risques non-étatiques n'ont pas disparu, et que reviennent les tensions entre États, du moins pourrait-on espérer que ceux-ci les gèrent dans le cadre rationnel de la défense de leurs intérêts, les passions demeurant l'affaire des opinions nationales et des partis, des groupes transnationaux extrémistes et des religions.

L'incrédulité qui régnait à l'Ouest sur l'invasion de l'Ukraine par la Russie (États-Unis et Grande-Bretagne exceptés) tenait à l'idée que Poutine, dirigeant rationnel, n'allait pas se lancer dans une guerre qu'il n'avait pas les moyens de gagner; il ne le ferait donc pas.

Ce serait oublier qu'entre le jeu rationnel et modérateur des intérêts d'État et l'extrémisation des esprits par les passions, existent les liens

que sont la peur et l'instinct de domination<sup>1</sup>. C'est l'appréhension de perdre l'Ukraine et le sentiment que le temps joue contre la Russie qui poussent Vladimir Poutine à prendre la décision insensée de l'envahir. Chez George W. Bush, l'exagération de la menace terroriste, le désir de venger l'outrage du 11 septembre, aboutissent au fiasco de l'invasion de l'Irak en 2003.

Dans les deux cas, avec la peur, il y a le désir de dominer, ou du moins de projeter une image de force conforme à l'idée qu'on se fait de son pays. Le jeu des anticipations fait se représenter à Poutine le risque de perdre l'Ukraine et de diminuer la stature de la Russie, à Bush celui que la convergence de la menace terroriste et d'un Irak doté d'armes de destruction massive n'aboutisse à ce risque inacceptable, un Al-Qaïda nucléaire; et, dans les deux cas, un excès de confiance en soi, qui aboutit à la décision de prévenir le risque en recourant à la guerre.

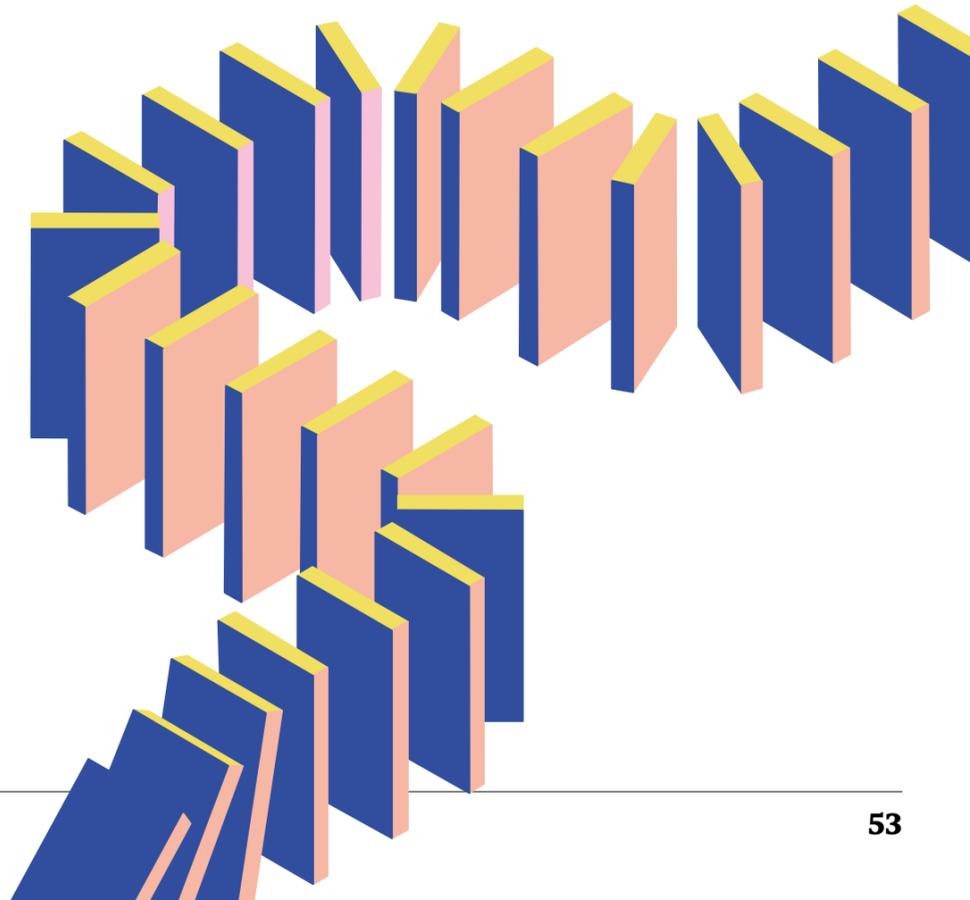
Cette conjonction du désir de puissance et de la crainte, de l'excès de confiance en soi et d'une appréhension, elle aussi excessive, est intrinsèquement dangereuse. Or plusieurs sont aujourd'hui les puissances et les leaders

**Notes**

<sup>1</sup> Sur ce thème, il faut lire *La Revanche des Passions, Métamorphoses de la violence et crise du Politique*, Pierre Hassner, Fayard, 2004

susceptibles d'éprouver cette double pulsion: la Chine de Xi Jinping, l'Inde de Narendra Modi, la Turquie de Recep Tayyip Erdogan.

Dans un monde où reviennent les tensions, où s'enchevêtrent des risques multiples, les anticipations biaisées par le jeu des passions, l'appréhension et l'excès de confiance en soi, risquent d'aboutir à des erreurs de calcul lourdes de conséquences; et l'on peut craindre que, dans cet univers, la force de modération et de confiance dans la raison politique, qu'avec toutes ses limites, l'Europe continue de représenter, soit impuissante à gérer les risques enchevêtrés de la mondialisation et de la rivalité des puissances, et qu'elle ne se retrouve dangereusement isolée.



# Les assureurs face au risque géopolitique dans un monde en polycrise



**FRANÇOISE GILLES**  
Directrice des risques,  
Groupe AXA



**PAUL-LOUIS MORACCHINI**  
Responsable des risques émergents, Groupe AXA

Trois milliards d'électeurs sont appelés aux urnes en 2024, dans un contexte de fortes tensions sociales et politiques. L'instabilité géostratégique est de plus en plus présente dans un monde en polycrise, où l'interconnexion avec les risques technologiques ou bien la crise climatique peuvent avoir des conséquences majeures. Qu'il s'agisse de leurs investissements, de la réglementation, ou de leurs produits et services, les compagnies d'assurance doivent relever de nombreux défis.

**Françoise Gilles et Paul-Louis Moracchini analysent tous les facteurs de risque que doivent prendre en compte les assureurs dans un monde en « polycrise ». Ainsi le risque géopolitique s'ajoute au risque climatique, puisque les conflits en empêchent une saine gestion, de même le risque de cyberattaques liées aux actions des États ou aux groupes terroristes constitue une menace permanente pour le monde entier.**

**Avec le cyber et le changement climatique, l'instabilité géopolitique est l'une des principales menaces de la décennie**

C'est ce que révèle le rapport annuel d'AXA sur les risques émergents (Future Risks Report 2023) auxquels le monde devra faire face au cours de la prochaine décennie.

L'instabilité géopolitique est ainsi classée troisième au niveau mondial par les experts du Groupe (3 500 répondants), après le climat et le cyber. Le risque géopolitique occupe cependant toujours la deuxième place en Europe. Cette question est d'ailleurs présente dans le top 5 de ce rapport depuis 2018 au moins, la guerre en Ukraine et les tensions au Moyen-Orient ayant fait substantiellement croître les préoccupations liées à ce risque dans le classement.

Par ailleurs, les résultats de cette étude annuelle nous indiquent aussi que 75 % des experts interrogés considèrent que les risques sont de plus en plus interconnectés, dessinant un monde de crises parallèles et multiples. Un monde en polycrise.

Le risque géopolitique fournit un exemple concret de cette interconnexion. Il agit comme un catalyseur, rendant plus complexe encore la lecture des évolutions du monde pour les entreprises et les assureurs.

Il est en effet directement impacté par le changement climatique. Les catastrophes naturelles extrêmes peuvent causer des migrations de populations, des conflits territoriaux, des tensions autour de ressources rares, mettant finalement à jour des fragilités politiques sous-jacentes. Les tensions territoriales en Arctique, dans le Pacifique, mais aussi les migrations de populations africaines ou sud-asiatiques, illustrent les nombreux exemples de ces connexions entre fragmentation politique, conflits territoriaux et perturbations climatiques.

Le risque géopolitique agit par ailleurs fortement sur la montée des risques liés aux nouvelles technologies, avec des cyberattaques sponsorisées par des États-nations, ou

**Le risque géopolitique agit comme un catalyseur, rendant plus complexe encore la lecture des évolutions du monde pour les entreprises et les assureurs.**

encore une nouvelle géopolitique de l'intelligence artificielle en plein essor qui impacte directement la sécurité et la stabilité internationale. Les pays en proie à des conflits géopolitiques cherchent à recourir à des technologies pour renforcer leur positionnement, afin d'accélérer leur indépendance et leur capacité d'action. Les acteurs de ces conflits visent également à s'emparer d'une avance technologique qui leur donnera une supériorité militaire, économique ou encore informationnelle. L'IA est véritablement devenue la nouvelle frontière de la compétition entre grandes puissances mondiales.

Enfin, il agit sur la fragmentation sociale, notamment par la désinformation, la propagation des *fake news* et les tentatives de manipulations de l'opinion, dans un contexte électoral crucial mentionné en introduction, et souligné récemment par le World Economic Forum. Ces phénomènes, accélérés par les développements technologiques, peuvent avoir un impact direct sur les élections, la composition des gouvernements et à terme sur la gestion des risques par les pouvoirs publics.

En somme, la géopolitique est un risque majeur, et agit sur l'ensemble des autres risques auxquels nous sommes et serons confrontés.

**L'assureur doit appréhender le retour en force du risque géopolitique pour faire face à de nouveaux défis**

Le risque de guerre est en général exclu des contrats d'assurance. En réalité, il ne l'est pas vraiment. L'assureur assure en effet du risque politique avec des couvertures, produits et services d'assurance directement concernés par la montée du risque géopolitique.

On peut citer concrètement les couvertures *Political Risk, Credit & Bonds* (PRCB), ou encore *War, Terrorism, & Political Violence* (WTPV) proposées par AXA. Ces lignes ont été développées pour aider les entreprises et les investisseurs à se protéger contre les risques liés à des événements politiques ou économiques imprévus qui pourraient impacter leur activité. L'assureur apporte ainsi une couverture sur mesure adaptée aux besoins de chaque entreprise. Le produit comprend également des services complémentaires de conseil et de gestion des risques.

Les assurés peuvent bénéficier ainsi d'une forte expertise pour évaluer les risques politiques et le suivi des procédures de compensation des sinistres. Ce type d'assurance propose une protection pour des pertes subies en lien plus précisément avec l'expropriation, l'annulation de licences, des troubles civils, des conflits armés ou encore des retards de paiement. Il couvre également les impayés clients ou fournisseurs, ainsi que les pertes financières subies en raison d'un défaut de paiement de la dette souveraine. Ces couvertures sont de plus en plus fondamentales pour soutenir les projets commerciaux et d'investissement des assurés, ce qui inclut le soutien à la transition énergétique aussi bien qu'à l'adaptation climatique dans de nombreux pays en voie de développement.

Par ailleurs, les conséquences du risque géopolitique aussi sont souvent assurées. On peut penser notamment à l'impact direct sur les couvertures AXA *Cyber, Business Interruption* et *Contingent Business Interruption*, ou encore

## Top 5 des risques émergents selon les experts



### 1 CHANGEMENT CLIMATIQUE

les risques liés à cet enjeu arrivent en tête de liste, pour les experts comme pour le grand public, dans toutes les zones géographiques.



### 2 RISQUES DE CYBERSÉCURITÉ

un expert sur huit les classe au premier rang, contre un sur dix l'an dernier.



### 3 INSTABILITÉ GÉOPOLITIQUE

les tensions géopolitiques se maintiennent à la deuxième place en Europe en 2023, mais reculent dans d'autres régions pour atteindre la troisième place au classement général.



### 4 RISQUES LIÉS À L'INTELLIGENCE ARTIFICIELLE ET AU BIG DATA

l'intelligence artificielle alarme davantage les experts (4e place vs 14e en 2022) que le grand public (11e place vs 19e en 2022).



### 5 RISQUES ÉNERGÉTIQUES

les risques liés à l'approvisionnement énergétique perdent une place cette année.

Source : AXA Future Risks Report 2023

Strikes, Riots & Civil Commotion (SRCC) pour le volet tensions sociales. Enfin, les assureurs doivent accepter une vision large du risque, qui peut toucher par exemple les lignes *Construction*, ou *Cargo/Marine* en cas d'impact sur les chaînes de valeur et le prix des matériaux.

Il ne faut pas oublier que l'impact de la géopolitique sur le risque financier demeure une dimension clé (augmentation des taux, etc.), en raison de la volatilité des marchés liée à la situation géopolitique incertaine. Celui-ci apparaît néanmoins contenu à ce stade. La gestion des portefeuilles requiert donc un suivi continu des tensions géopolitiques et des différents scénarios d'impacts sur les variables financières.

Enfin, un nouveau défi se pose avec celui de l'impact des risques géostratégiques sur l'image de la compagnie d'assurance. Un assureur global peut aujourd'hui être attaqué par les parties prenantes d'un conflit pour son soutien supposé (et fantasmé) à la partie adverse.

### La fragmentation géopolitique entraîne des divergences réglementaires, malgré un besoin croissant de solutions globales

L'assureur doit être particulièrement attentif aux conséquences du risque géopolitique sur les développements réglementaires, qui peuvent fortement entraver la compétitivité et la capacité d'action d'une entreprise globale. Les assureurs peuvent être soumis à des restrictions commerciales ou réglementaires impactant lourdement leur activité, en lien avec des tensions régionales ou internationales.

On peut prendre pour exemple le cas récent de la réglementation en matière d'ESG, avec l'émergence d'un *ESG backlash* venu des États-Unis et nourri par la montée des populismes. La divergence réglementaire sur ce type de sujet peut créer un environnement complexe pour les institutions financières qui soutiennent la transition. Les autorités européennes développent ainsi une vision de la « double matérialité » (analyser les risques

pour l'entreprise, mais aussi l'impact de l'entreprise sur l'environnement), tandis que la réglementation américaine ne se focalise que sur la matérialité financière pour la compagnie. On pense aussi aux divergences de vue sur l'intelligence artificielle et la régulation des réseaux sociaux, ou bien sur les partenariats public-privé en matière de couverture d'assurance.

Les fragmentations réglementaires liées aux tensions politiques peuvent également entraîner des demandes croissantes de la part d'autorités locales envers les assureurs, obligeant par exemple les compagnies à développer des couvertures pour couvrir certains risques, ce qui favorise les compétiteurs locaux par une taxation inégalitaire, ou utilisant le secteur financier et assurantiel comme un moyen de sanctionner une partie adverse (on parle alors de « *weaponization of finance* » comme cela a pu être le cas avec l'invasion de l'Ukraine en 2022). Certains acteurs étatiques sont aussi amenés à prendre des sanctions économiques directes (embargo, gel d'avoirs, réquisition de personnels...) envers les institutions financières, en particulier les banques et les assureurs, afin de pénaliser un adversaire dans le cadre d'un conflit. Les assureurs doivent donc tenir compte de ces évolutions réglementaires liées aux événements géostratégiques dans la gestion de leurs risques et dans leur relation avec les pouvoirs publics.

Malgré les tensions géostratégiques croissantes, notre rôle d'assureur doit être de rappeler l'importance de solutions globales et holistiques pour faire face aux grands risques de demain qui menacent nos sociétés. L'étude annuelle d'AXA sur les risques est rassurante en ce sens : pour la majorité des experts et du public interrogés (respectivement 54 et 52 %), des solutions prises à l'échelle globale s'imposent pour répondre aux futurs risques émergents. Les chiffres sur la perception de la globalisation sont eux aussi optimistes : près de 60% du public interrogé au niveau mondial est persuadé que la globalisation va se poursuivre à long terme, étant donné ce besoin de trouver des solutions communes aux grands risques.

Le risque géopolitique est un sujet en constante évolution qui nécessite une action proactive et de croire au dialogue pour minimiser les risques. Les gouvernements, les entreprises et les organisations internationales doivent

**Les fragmentations réglementaires liées aux tensions politiques peuvent également entraîner des demandes croissantes de la part d'autorités locales envers les assureurs**

travailler ensemble pour répondre efficacement aux crises actuelles et à venir. Une coopération indispensable pour faire en sorte que le futur ne soit pas un risque.

# Assurance et conflit : Protéger la continuité de la chaîne logistique



**JEAN-ÉTIENNE  
QUINTIN**

Membre de l'Académie de marine  
Directeur de clientèle  
Département Transports  
et Spécialités,  
DIOT SIACI

Nous vous proposons d'aborder dans cet article les expositions aux risques de la chaîne logistique de l'industrie avec pour illustration le domaine de la construction automobile. Puis nous envisagerons les garanties que le marché de l'assurance peut mettre en place dans un contexte géopolitique de conflits, pour enfin aborder les risques non garantis par le marché de l'assurance et les perspectives d'alternatives de transferts.

**Jean-Étienne Quintin développe toutes les conséquences fâcheuses des conflits pour l'assurance mondiale en général et en particulier sur les chaînes logistiques, comme celles qui relient les fournisseurs et les sous-traitants de l'industrie automobile. Les retards peuvent être tout aussi dommageables que les naufrages ou les incendies et les pertes d'exploitation sont difficilement indemnifiables lorsqu'il n'y a pas de dommages à la marchandise.**

## Les expositions aux risques de la chaîne logistique de l'industrie automobile : entre maîtrise et impact des aléas

Dans le prolongement des Trente Glorieuses, l'industrie mondiale ne s'est guère souciée de la résilience de sa chaîne d'approvisionnement. Les fournisseurs étaient multiples, les flux logistiques terrestres maritimes et aériens étaient peu empêchés par les risques climatiques ou par les risques politiques, à l'exception de quelques conflits localisés. Dans un contexte de concurrence mondiale plus forte, les industries occidentales ont revu leur modèle en délocalisant leurs fabrications et fournisseurs vers les pays émergents. En parallèle de ce mouvement, les industriels ont largement rationalisé les sources d'approvisionnement en limitant leur nombre de fournisseurs.

Dans cette situation d'optimisation, il ne manquait plus que la survenance de facteurs extérieurs, tels que des événements climatiques majeurs comme l'éruption du volcan Eyjafjallajökull en 2010, les inondations en Thaïlande en 2011, et un tsunami au Japon la même année pour venir perturber très fortement la chaîne logistique mondiale de certaines industries. À ces événements, nous pouvons ajouter les impacts d'origine humaine tel que l'échouement dans le canal de Suez du porte-conteneurs *Ever Given* en mars 2021. À cette liste d'expositions en risques, l'actualité des conflits mondiaux est venue rappeler à nos civilisations et aux industries manufacturières et de transformation que la géopolitique mondiale redevenait une source de perturbations majeure dans les ruptures d'approvisionnement.

Depuis l'après-guerre, l'industrie automobile a connu un développement exponentiel porté par la croissance économique et les avancées technologiques. Cette évolution a également influencé la chaîne logistique de l'industrie automobile, avec une décentralisation des fournisseurs et des chaînes d'approvisionnement mondiales de plus en plus complexes.

Tous les composants, toutes les pièces d'une automobile sont strictement nécessaires à sa production. Les industriels doivent disposer de plans de résilience malgré la complexité et

**L'actualité  
des conflits  
mondiaux  
est venue  
rappeler à nos  
civilisations  
et aux industries  
manufacturières  
et de transfor-  
mation que  
la géopolitique  
mondiale  
redevient  
une source de  
perturbations  
majeure dans  
les ruptures  
d'approvision-  
nement.**

la diversité des pièces. Certains composants ne sont pas seulement propres aux automobiles mais peuvent également être utilisés par d'autres industries comme les télécoms, le transport, l'électronique, l'aéronautique. Le sujet des ruptures d'approvisionnement va donc bien au-delà de l'industrie automobile.

Les premiers risques liés aux conflits géopolitiques sont les pertes et les destructions, mais aussi les perturbations dans la chaîne d'approvisionnement. Le blocage des routes et des ports crée des ruptures d'approvisionnement en amont, c'est-à-dire de composants, matériaux provoquant de possibles ruptures de production. Mais ces mêmes blocages peuvent également affecter les livraisons en aval vers les consommateurs, créant un accroissement de stock de produits finis.

Plusieurs types de réponses peuvent être envisagées, allant du double approvisionnement à l'utilisation de routes alternatives ou de moyens d'affrètements alternatifs, jusqu'à la coûteuse création de stocks tampons. Toutes ces solutions sont souvent temporaires et doivent être suffisamment agiles pour être mixées entre elles en cas de long conflit. Aucune n'est parfaite.

Lorsque les plans de mitigation sont épuisés, des arrêts de production peuvent malheureusement survenir, créant des effets collatéraux

importants: les fournisseurs non-impactés doivent réduire leur cadence de production pour éviter les surstocks et l'usine terminale doit arrêter sa chaîne de montage, provoquant du chômage technique et une gestion de stock hors flux de production.

Ces ruptures d'approvisionnement ont évidemment des conséquences financières pour l'industrie, outre la perte de revenus directs liés à la diminution ou l'arrêt d'activité, l'insatisfaction des clients pénalisés par la mise à disposition tardive de produits, voire l'absence de livraison.

Les départements achats et logistiques des industriels doivent ainsi s'adapter aux circonstances aléatoires comme après l'échouement d'un navire (*Ever Given* en mars 2021 dans le canal de Suez), avec le constat qu'un reroutage par le cap de Bonne-Espérance génère des coûts et des délais supplémentaires. En cas de conflits armés, il convient d'élaborer des plans de continuité d'activité via de nouvelles routes logistiques.

Les sites de production, tant ceux des industriels que ceux des fournisseurs, sont calibrés pour répondre à des capacités de production précises permettant un niveau de qualité répétable et irréprochable.

Le multi-approvisionnement imposerait de prévoir potentiellement de dépanner la production d'un site par l'activation d'un second, qui dispose déjà de son propre programme de production. Cela reviendrait donc à prévoir des unités de productions surdimensionnées et donc travaillant en sous-capacité ce qui n'est pas une solution économiquement viable ni pertinente.

La recherche de fournisseurs alternatifs est parfois une solution. Mais la particularité de certains composants, impose parfois le choix du fournisseur, la propriété intellectuelle attachée au produit le rendant en effet incontournable.

Enfin, l'industrie automobile se distingue par sa complexité. La conception et la fabrication d'un véhicule impliquent des processus longs et coûteux, allant de la recherche et développement aux essais très rigoureux, en passant par les phases de production en série garantissant un niveau de qualité répétable sur de très importants volumes. Une nouvelle source

d'approvisionnement implique de nouvelles phases de validation, car tous les composants d'un véhicule sont en interaction.

### Les assurances mobilisables en cas de rupture d'approvisionnement: les assurances des risques de guerre

Lorsqu'un conflit armé survient, comme cela a été le cas le 24 février 2022 entre la Russie et l'Ukraine, même si certaines prémices étaient apparues, la chaîne logistique de l'approvisionnement de matières premières comme les commodités liquides (pétrole), ou sèches en vrac comme les grains en provenance de la mer Noire, a été très rapidement stoppée. Le conflit entre le Hamas et Israël a désormais des conséquences jusque dans le détroit de Bab-el-Mandeb et dans le sud de la mer Rouge. Des navires ont été touchés, déroutés, détenus, et les marchandises à bord de ces navires ont subi le même sort. Désormais la gestion des risques à travers les cartes de notre planisphère devient un outil de pilotage indispensable. Mais les industries, manufacturières notamment, sont-elles bien garanties dans ces circonstances ?

Avant d'envisager les transferts de risques spécifiquement liés aux transports, il convient de rappeler qu'à l'occasion d'un conflit armé pouvant entraîner des conséquences directes sur l'outil industriel ou commercial d'un assuré dans une zone de conflit, il est possible de mobiliser des garanties de type violences politiques. De la même manière, ces couvertures peuvent comprendre des garanties de carences de fournisseurs.

Traditionnellement, le marché de l'assurance maritime mondial des risques de guerre et assimilés couvre les conséquences des risques de guerre, qu'il s'agisse des navires ou des marchandises. Ainsi, les dommages subis par les navires devraient être indemnisés par les assurances corps (œuvres vives, hélice, safran, appareils de propulsion), mais aussi les coûts relatifs aux renflouements et au remorquage. Bien qu'il s'agisse de mêmes attaques et de mêmes événements, les marchés d'assurances demeurent distincts entre ceux qui garantissent les navires et ceux qui garantissent les marchandises transportées à bord.

## L'assurance des risques de guerre a pour but de garantir l'armateur et les chargeurs contre les conséquences dommageables qui résultent de la guerre civile ou étrangère.

L'assurance des risques de guerre a pour but de garantir l'armateur et les chargeurs contre les conséquences dommageables qui résultent de la guerre civile ou étrangère. Tandis que le risque de mer est d'une fréquence relativement constante ou, en tout cas, n'évolue que très lentement en fonction des perfectionnements techniques et permet, par conséquent, l'établissement de statistiques facilitant, par catégorie de navire ou de navigation, la mesure approximative du prix du risque encouru, le risque de guerre est d'une intensité intrinsèquement variable.

En temps de paix générale, le risque est par définition très faible. En période de tension internationale, il s'accroît rapidement. Dès qu'une guerre, déclarée ou non, se déclenche, il peut prendre des proportions d'une extrême importance et les surprimes risques de guerre peuvent évoluer dans un rapport de 1 à 10 selon les zones et les périodes. L'évolution se fait en fonction des éléments géopolitiques du moment dans les zones fréquentées.

Les tarifications varient par ailleurs sensiblement en fonction de l'analyse du risque suivant la typologie de navire, son pavillon, les valeurs assurées, la zone de transit, et les mesures de sûreté envisagées comme le BMP5<sup>1</sup> ou l'embarquement de gardes armés.

Les assureurs risques de guerre à travers le monde suivent les appréciations de risques du JWC Joint War Committee s'agissant de l'assurance risque de guerre des navires et du JCC Joint Cargo Committee pour l'assurance risque de guerre des marchandises transportées du marché de l'assurance de Londres.

Pour le marché français, c'est le CESAM<sup>2</sup> qui établit une liste de notation des zones à risques à travers le monde.

Ainsi, les assureurs couvrant les risques de guerre se réservent la possibilité d'annuler les garanties (au moyen d'une « NOC » *Notice of Cancellation*), pour ensuite réétudier la tarification d'assurance pour toute exposition dans ces zones sur la base d'une déclaration préalable et de termes à définir au cas par cas.

### Les risques non-garantis et les perspectives d'alternatives de transferts

Au-delà de la destruction de biens lors de conflits armés, et afin de répondre aux problématiques de risques d'un certain nombre d'industriels en matière de rupture de la chaîne logistique, certaines compagnies aidées de consultants spécialisés et de courtiers ont tenté, il y a quelques années, de mettre au point des polices d'assurance autonomes de pertes financières dites « assurances de la *supply chain* » incluant les dommages, le risque d'insolvabilité, les risques politiques mais destinés à un nombre limité de fournisseurs. La mise au point de ce type de police nécessite cependant des études très approfondies sur l'ensemble de la chaîne de fournisseurs critiques quel que soit leur rang afin d'évaluer les vulnérabilités grâce aux facteurs de risques identifiés. Dans ce type d'étude, il est possible d'identifier le cas d'industriels qui réalisent des marges commerciales annuelles très conséquentes grâce aux produits de fournisseurs dont les coûts d'achats peuvent s'avérer relativement faibles.

L'étude de ces risques demeure toutefois très complexe en raison de la cartographie de la chaîne logistique des industries manufacturières comme la construction aéronautique ou automobile. Par ailleurs, le niveau de prime lié à ces risques demeure élevé faute de mutualisation suffisante.

À travers ce type de garanties, c'est bien une perte d'exploitation qu'un assuré cherche à transférer alors que ce dernier n'a en réalité subi aucun dommage : il s'agit du concept de la perte d'exploitation sans dommage que le marché de l'assurance a du mal à envisager. L'assurance des pertes d'exploitation (PE) a émergé en France au début des années 1980. Elle n'a cessé de se développer depuis lors étant désormais souscrite par la majorité des entreprises assurées. Cependant, ces pertes d'exploitation ne sont indemnisées qu'à la suite de dommages eux-mêmes indemnisés durant une période comprise habituellement entre douze et dix-huit mois durant les reconstructions de sites. Dans le cadre des politiques de production à flux tendus (zéro stocks), les industries manufacturières sont donc tributaires des approvisionnements et des flux logistiques. En cas de ruptures d'approvisionnement notamment sans dommages à la marchandise, il n'existe pas de véritables solutions de transfert du risque vers l'assurance.

Afin de répondre à ces problématiques de risques, il convenait d'imaginer un système d'indemnisation qui vise à couvrir les pertes d'exploitation ne résultant pas de dommages matériels, comme les blocages d'accès causés par les Gilets jaunes, les événements climatiques (éruption du volcan islandais Eyjafjallajökull en 2010 et blocage de la circulation aérienne), les pandémies. Les événements de type risque politique ou risque de guerre peuvent faire partie des risques garantis à travers des garanties d'assurance de pertes d'exploitation sans dommage. Faute de pouvoir trouver un marché d'assurance mature, la solution consiste, pour les assurés disposant de captives d'assurances, de garantir ces risques via des polices d'assurances dites « de pertes pécuniaires diverses ».

Nous avons pu voir à travers les quelques lignes qui précèdent que la chaîne logistique de l'industrie automobile notamment est très délicate à piloter dès lors que des conflits naissent à travers le globe. Si l'outil de transfert de risque que constitue l'assurance permet de protéger le bilan de l'entreprise durant certaines périodes où l'aléa est présent, en revanche l'assurance ne peut être une solution sur le temps long dès lors que des conflits perdurent et bouleversent les approvisionnements. Les répercussions du conflit entre le Hamas et Israël se sont



### Notes

<sup>1</sup> Best Management Practices to Deter Piracy and Enhance Maritime Security.

<sup>2</sup> Comité d'Études et de Services des Assureurs Maritimes et Transports (CESAM).

<sup>3</sup> Navigating troubled waters: Impact to global trade of disruption of shipping routes in the Red Sea, Black Sea and Panama Canal UNCTAD - 22 février 2024.

déportées sur le sud de la mer Rouge et le détroit de Bab-el-Mandeb. À l'heure de la rédaction de cet article, le trafic du canal de Suez avait baissé de 42% et les transits hebdomadaires de navires porte-conteneurs avaient chuté de 67% comme le montre une étude de la Conférence des Nations unies sur le commerce et le développement (CNUCED)<sup>3</sup>.

L'organisation souligne la nécessité d'une adaptation rapide de l'industrie du transport maritime et d'une coopération internationale solide pour gérer le remodelage du commerce mondial. Les industriels tels que les fabricants automobiles seront donc non seulement contraints par les circonstances géopolitiques du moment, mais aussi par les injonctions politiques liées au climat (émissions de carbone des moyens de transport), et par les nécessités d'aide au développement des pays aux économies vulnérables. ⓘ

# Après le choc, quel nouveau paysage pétrolier?



**PATRICE  
GEOFFRON**

Professeur d'économie,  
Université Paris-Dauphine-PSL

La guerre en Ukraine n'a pas débouché sur un choc pétrolier de plus, mais sur une fragmentation et une recomposition structurelle du marché du brut et de ses dérivés. Conjugée au retour d'une instabilité au Moyen-Orient, cette rupture s'inscrit dans un contexte où la COP28 a (prudemment) inscrit dans ses conclusions la nécessité d'une transition hors des fossiles, renforçant la perspective d'un pic prochain de la demande de pétrole. Dans le moyen terme, ces turbulences font peser des risques macroéconomiques qui constituent un sujet majeur pour le monde de l'assurance. Au-delà de notre décennie, la plausible accélération de la décarbonation, notamment induite par ces tensions sur les marchés d'hydrocarbures, permettra de mieux contenir des risques climatiques qui s'annoncent difficilement assurables.

**Patrice Geoffron décrit toutes les conséquences des conflits sur l'approvisionnement en pétrole et en gaz. Globalement il n'y a pas pour l'heure de risque de pénurie, puisque tous les pays importateurs ont pu diversifier leurs fournisseurs, en revanche le marché mondial subit une fragmentation qui renchérit les coûts de transport et aggrave les émissions de gaz à effet de serre.**

## Hydrocarbures : la résurgence brutale de l'insécurité d'approvisionnement

Pour la première fois depuis les chocs pétroliers des années 1970, les contraintes d'approvisionnement en hydrocarbures ont dominé la scène énergétique en 2022, conduisant depuis à un aggiornamento de leurs marchés. Le conflit en Ukraine a conduit l'Union européenne à rompre les liens énergétiques avec la Russie (modulo ceux relatifs à la filière nucléaire) via des embargos sur le charbon (en août 2022), puis sur le pétrole (en décembre) et ses dérivés (en février de l'année suivante), et à subir une attrition massive des flux de gaz en provenance de ce fournisseur « historique » (largement imputable aux Russes qui ont réduit leurs livraisons par gazoducs « à la carte », selon des modalités qui ont varié d'un client à l'autre). Les conséquences de cette rupture énergétique se sont diffusées bien au-delà de l'Europe, en perturbant à la fois les routes mondiales et les processus d'acheminement des hydrocarbures (avec notamment des restrictions sur l'assurance des cargaisons russes de pétrole), le niveau et la variabilité des prix et même les modalités de leur formation (avec l'introduction de mécanismes de prix-plafond).

Dans l'urgence, l'UE a resserré ses liens avec d'autres de ses fournisseurs « historiques » de gaz, tels que la Norvège et l'Algérie et, surtout, s'est diversifiée en important massivement du gaz liquéfié des États-Unis, et en provenance de producteurs d'Afrique et du Moyen-Orient, comme le Qatar; cela avec une certaine efficacité, puisque les volumes importés de Russie ont été réduits des trois quarts entre 2021 et 2023. Les embargos sur le pétrole brut et sur les carburants ont impliqué également d'organiser de nouvelles routes d'approvisionnement, en provenance du Moyen-Orient, du golfe du Mexique ou d'Afrique de l'Ouest (ainsi que de l'Inde pour les produits raffinés, comme le diesel, particulièrement important en France).

Le marché pétrolier s'est ainsi réorganisé, réorientant les flux de bruts et des produits raffinés, mais selon des chaînes logistiques « désoptimisées » sous l'effet du choc, avec des produits parcourant des routes plus longues. Dan Yergin, fondateur du Cambridge Energy Research Associates (CERA), en tire des

conclusions radicales: «Le marché mondial du pétrole tel que nous le connaissons depuis trente ans – c'est-à-dire marqué par la chute du Mur de Berlin et l'intégration de la Chine dans l'économie mondiale – fait aujourd'hui partie du passé. Nous vivons un changement historique, avec le passage d'un marché pétrolier mondialisé vers un marché fragmenté» (Yergin, 2022).

Ainsi, sous l'effet des embargos, le monde pétrolier se partage désormais entre un segment « russe » (les pays qui acceptent d'acheter du brut et des carburants de cette provenance) et le marché « non-russe » (le reste du monde, dont la plupart des pays de l'OCDE). Il est notable, toutefois, que cette fragmentation n'a pas mis à mal le fonctionnement de l'OPEP+ (i.e. l'Arabie saoudite, la Russie et leur vingtaine d'alliés), coalition inédite qui s'était formée en 2016 pour tenter de faire remonter les cours du baril (avec efficacité), après leur effondrement en 2014. L'entrée en guerre n'a pas distendu ces liens, y compris lorsque le président américain a tenté d'infléchir la position saoudienne en 2022, au plus fort de la crise énergétique, en enjoignant à augmenter ses volumes de production (cela, sans effet aucun). La crise a révélé un positionnement de l'Arabie saoudite équilibré entre Russie et États-Unis, confirmant un éloignement stratégique avec les premiers (malgré les liens scellés au sortir de la Seconde Guerre mondiale). Le conflit en Ukraine a confirmé que les États-Unis, premier producteur mondial de pétrole désormais, sont tout autant des concurrents que des partenaires de l'Arabie saoudite.

L'impact macroéconomique de ces perturbations sera massif et nécessitera des interventions drastiques sur les marchés de détail de l'énergie pour atténuer en partie l'affolement sur les marchés de gros: selon les calculs du groupe de réflexion Bruegel (Sgaravatti et al, 2023), les gouvernements européens (y compris le Royaume-Uni) alloueront environ 700 milliards d'euros de dépenses publiques en 2022 pour amortir l'impact sur les ménages et les entreprises les plus vulnérables (un ordre de grandeur confirmé par d'autres études, telles que Colgan et al. 2023). Le coût de la fourniture d'énergie a atteint plus de 9 % du PIB de l'UE, contre 2 % en 2020, soit un niveau proche de celui du deuxième choc pétrolier de 1979-1980 et plus du double de celui des États-Unis en 2022.

**Que le pic de la demande soit proche ou lointain, les tensions géopolitiques continueront à couvrir.**

Fatih Birol, directeur exécutif de l'Agence internationale de l'énergie (AIE), estime que le conflit aura constitué un accélérateur de la transition énergétique: «Les efforts déployés par la Russie pour obtenir un avantage politique et économique en faisant grimper les prix de l'énergie ont incité les gouvernements, non seulement dans l'UE mais aussi dans de nombreux pays du monde entier, à accélérer le déploiement d'alternatives plus propres et plus sûres. [...] les répercussions de la guerre en Ukraine remodelent l'avenir de l'énergie mondiale, avec un pic de la demande en combustibles fossiles clairement visible pour la première fois et qui devrait se produire avant la fin des années 2020» (Birol, 2023). Ce rehaussement des risques fait partie des facteurs qui ont contribué aux avancées (non dénuées d'ambiguïtés) en conclusion de la COP28, avec l'inscription d'un objectif d'orientation vers la sortie des fossiles («*transitioning away from fossil fuels*»).

**Vers un pic de demande, sous menace de nouveau choc pétrolier?**

Certes, le prix du baril navigue depuis la fin 2022 aux alentours de 80 dollars, mais en cela le cours de l'or noir reste très en deçà des 120 dollars atteints (et même par moment dépassés) à l'été de cette même année, au plus

fort des turbulences créées par la guerre. Cette observation suggère que le marché pétrolier s'est réorganisé de manière efficace et que, même si l'OPEP+ conserve une ligne restrictive, elle ne suffit pas à contrebalancer la progression des producteurs externes à la coalition, comme les États-Unis, le Canada, le Brésil et la Guyane.

Une part essentielle de l'explication concernant la modération (relative) des prix est cependant à rechercher du côté de la demande, dont l'AIE prévoit une augmentation très modérée en 2024 (+1,2 million de barils par jour contre +2,3 millions en 2023) (AIE, 2024). Même tirée par la Chine, l'Inde et le Brésil, la progression de la demande est contenue dans un contexte de croissance mondiale peu dynamique, alors que le déploiement des énergies renouvelables, la pénétration du véhicule électrique et les mesures d'efficacité énergétique contribuent également à un affaissement des besoins en produits pétroliers.

Ces indices viennent corroborer la thèse de l'AIE qui envisage un pic de demande pétrolière d'ici à la fin de la décennie (et une décroissance plus ou moins marquée au-delà); thèse à laquelle s'oppose l'OPEP avec force, anticipant des besoins en produits pétroliers bien plus durables (jusqu'en 2045 dans les dernières perspectives pétrolières de l'Organisation). Cette divergence apparaît dans les prévisions pour 2024, où l'OPEP voit un rythme de progression deux fois supérieur à celui de l'Agence (+2,25 millions de barils par jour).

Cette «joute» entre l'AIE et l'OPEP a les apparences d'une querelle picrocholine entre experts, mais les enjeux sous-jacents sont critiques: si le pic de la demande était atteint dans les années à venir, le «début de la fin» de l'ère des fossiles présenterait un caractère moins hypothétique qu'au sortir de la COP28. Et, dès lors, pays exportateurs et importateurs ont un intérêt à inscrire dans le paysage des narratifs distincts, susceptibles d'influer sur les anticipations des acteurs (et leurs stratégies d'investissements). En quelque sorte, l'opposition entre l'AIE et l'OPEP prolonge les lignes de fractures traditionnellement observées dans la COP, y compris la dernière.

Mais, que le pic de la demande soit proche ou lointain, les tensions géopolitiques continueront à couvrir.

En premier lieu, parce que le périmètre des embargos sur les produits pétroliers russes est susceptible d'évoluer, tant que le conflit en Ukraine se poursuivra. Au cours des premiers mois qui ont suivi l'entrée en vigueur des sanctions sur le pétrole, fin 2022, la Russie a subi à la fois un recul en volume et en prix (pour sa référence de brut «Oural» et ses produits dérivés), les rabais offerts étant destinés à pénétrer plus largement les marchés asiatiques (notamment l'Inde et la Chine en première ligne, mais également la Turquie) pour réorienter des volumes qui étaient jusqu'alors destinés à l'OCDE. Mais, au long de l'année 2023, la décote du pétrole russe s'est réduite: tout d'abord vendu aux alentours de 45 dollars (soit nettement sous le plafond des 60 dollars établi dans le cadre de l'embargo et, plus encore, sous le prix de marché), le baril russe est remonté vers 80 dollars en fin d'année (CREA, 2024). L'arme principale des pays désireux de restreindre les recettes pétrolières russes (en fermant leur marché et en tentant d'imposer un *price-cap* de 60 dollars) consistait à contraindre le transport, dès lors que les membres du G7 sont à la tête des flottes les plus importantes et, au-delà, sont les premiers assureurs des tankers (couvrant 90% des cargaisons). Mais, durant l'année 2023, Moscou a progressivement étendu sa flotte de navires, certains qualifiés de «fantômes», car camouflés derrière des sociétés écrans, pour gagner en autonomie.

Ainsi, l'efficacité des contraintes imposées à la Russie en matière pétrolière semble s'être rapidement érodée et, si les difficultés militaires ukrainiennes se confirmaient, les sanctions nouvelles qui s'imposeraient pourraient avoir une influence sur les volumes et/ou les prix. Autrement dit, la recomposition de l'ex-marché pétrolier mondial, sous l'effet du conflit en Ukraine, est loin d'être achevée et, même la paix revenue (perspective hypothétique à ce stade), un retour au *statu quo ante* est hautement improbable.

En second lieu, la résurgence des tensions géopolitiques au Moyen-Orient marque certes le retour de menaces «classiques» en matière pétrolière, mais qui s'inscrivent cette fois dans un contexte déjà singulièrement complexe, au regard de la fragmentation résultant de l'agression russe. Pour comprendre ce qui est en jeu, il convient de noter que, en 2023, 10% du commerce maritime mondial de pétrole et 8% du commerce mondial de gaz naturel liquéfié ont

**Dès lors que les coûts de transformation et d'acheminement du brut ont augmenté plus spécifiquement vers l'Europe, zone économiquement fragile et dont les dettes publiques sont sous examen, un sursaut des prix du pétrole restera une menace latente et sérieuse.**

transité par la mer Rouge (AIE, 2024). Les attaques de navires dans cette zone par les Houthis et les frappes menées en retour par les États-Unis et le Royaume-Uni ont conduit à dérouter des pétroliers et à les orienter vers le cap de Bonne-Espérance, avec des surcoûts (en fret et assurance, en mobilisant plus longuement les tankers) qui pèsent surtout sur l'Europe. Si le conflit changeait d'échelle, en s'étendant au détroit d'Ormuz, c'est alors le transit de plus d'un quart du commerce mondial de pétrole qui pourrait subir des perturbations. Les exportations de gaz naturel liquéfié en provenance du Qatar, désormais essentielles pour l'UE; seraient également concernées.

Ajoutons enfin que le cycle politique américain fait également partie des facteurs d'incertitude qui pèsent sur les hydrocarbures, pétrole compris. Comme on le sait, la politique de Joe Biden s'inscrit dans l'Accord de Paris et c'est dans ce cadre qu'il a déployé l'Inflation Reduction Act, ainsi qu'un récent moratoire sur des infrastructures d'exportation de gaz naturel liquéfié (sous des motifs environnementaux). Si Donald Trump venait à lui succéder, on peut imaginer qu'il reviendrait à une politique de puissance via les hydrocarbures (en incitant à forer tous azimuts, y compris sur les terres fédérales), et sans faire de zèle par ailleurs dans le déploiement des renouvelables ou l'encouragement à l'adoption d'une mobilité électrique. Des volumes de production accrus ne manqueront pas de tirer les prix pétroliers vers le bas (comme cela a été violemment le cas au milieu de la décennie 2010), avec des conséquences difficiles à imaginer dans un paysage pétrolier fragmenté par la guerre, mettant sous tension la capacité de l'OPEP+ à réguler les cours (en réduisant ses volumes de production). Mais, il est également possible d'imaginer (sur le fondement de l'expérience que nous avons acquise lors du «premier» mandat de Donald Trump), que les hydrocarbures pourraient constituer un outil de pression sur les alliés. Dans un contexte où le pacte de l'OTAN pourrait être mis en question, la dépendance des Européens à l'égard du gaz naturel liquéfié américain constitue un facteur de préoccupation additionnel...

**Quels enseignements pour le monde de l'assurance ?**

Les enseignements dépendent de l'horizon d'observation. Pour cette décennie, les tensions géopolitiques qui prévalent laissent planer la menace de nouveaux chocs, dans un contexte où les chaînes logistiques pétrolières en ont été recomposées dans l'urgence et où les trois premières grandes zones de production (Moyen-Orient, Russie, mais également États-Unis) sont soumises à des incertitudes inédites dans leur nature et les combinaisons possibles sur lesquelles elles pourraient déboucher. Certes, depuis le pic de 2022, les cours du brut sont restés dans une zone d'équilibre (70-80 dollars) qui ne met pas les pays importateurs sous pression extrême; mais, dès lors que les coûts de transformation et d'acheminement

du brut ont augmenté plus spécifiquement vers l'Europe, zone économiquement fragile et dont les dettes publiques sont sous examen, un sursaut des prix du pétrole restera une menace latente et sérieuse. Cela d'autant que les prix du gaz y seront structurellement plus élevés qu'avant le début du conflit en Ukraine (et, singulièrement, bien plus qu'aux États-Unis). Au total, pour les années à venir, le pétrole restera en Europe une préoccupation macroéconomique de premier rang, en se souvenant des effets et coûts sociaux des chocs récents, comme celui qui a conduit à la crise des Gilets jaunes en 2018.

Mais, à la condition de se projeter au-delà de notre décennie, les fracturations pétrolières (combinées aux recombinaisons gazières) en cours constituent un accélérateur de la transition vers des modèles énergétiques décarbonés, évolution historique dont il convient de bien saisir la portée. L'atteinte, plausible, d'un pic pétrolier déboucherait sur une «terra incognita»: d'un côté, une réduction des émissions de gaz à effet de serre permettra de contenir les dérives (et donc les risques physiques associés), mais, de l'autre, la sortie de l'ère des fossiles sera accompagnée de son lot de risques dits «de transition» (dont l'émergence massive de «stranded assets»).

Autrement dit, contenir la température aux alentours de 2 °C doit permettre de réduire les risques non-assurables mais, pour cela, l'impérative progression vers des modèles de sociétés décarbonées ouvrira sans doute sur des turbulences macroéconomiques inédites. 



**Bibliographie**

AIE, Oil Market Report, February 2024

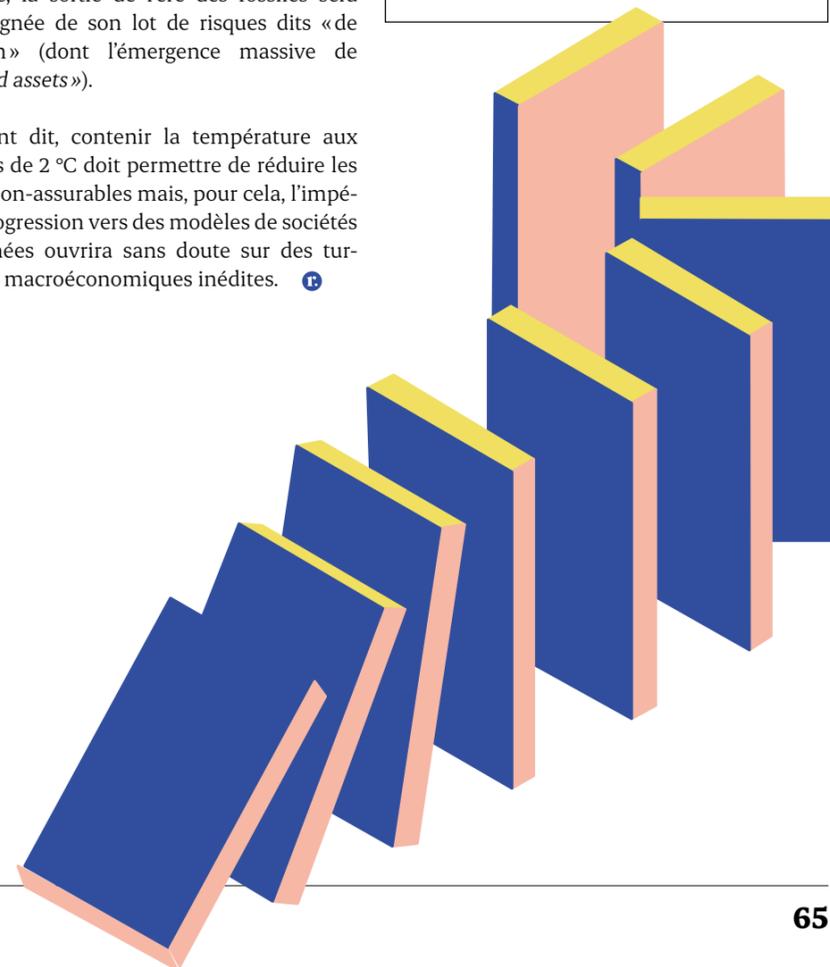
Birof F., Clean energy is moving faster than you think, Investment in new large-scale fossil fuel projects is now a risky proposition, *Financial Times*, 13 April 2023.

Colgan J.D., Gard-Murray A.S., Hinthorn M., Quantifying the value of energy security: How Russia's invasion of Ukraine exploded Europe's fossil fuel costs, *Energy Research & Social Science*, Volume 103, 2023.

CREA, One year of sanctions: Russia's oil export revenues cut by EUR 34 bn, 5 December 2023.

Sgaravatti G., S. Tagliapietra, C. Trasi et G. Zachmann, National fiscal policy responses to the energy crisis, Bruegel, June 2023.

Yergin D., Un peu de modestie sur la transition énergétique ne serait pas du luxe, *L'Écho*, 22 décembre 2022.



# Sanctions économiques : Quel coût pour le secteur de l'assurance ?



**PIERRE-CHARLES PRADIER**  
Économiste

Un conflit étranger comme la guerre actuellement menée par les Russes entraîne pour les assureurs des pertes d'activité limitées – quoique concentrées sur certains acteurs – en raison de l'interdiction expresse ou indirecte des opérations d'assurance et un alourdissement général des listes de gel des avoirs et donc des coûts liés à la conformité. En revanche, l'effet sur la valeur des filiales, mais aussi des contrats d'assurance des grands risques, peut être considérable, même s'il est entouré par le brouillard de la guerre et ne se découvre pleinement qu'après la signature des traités de paix.

**Pierre-Charles Pradier montre que les conflits n'envoient pas que des bombes, des obus ou des drones sur les militaires et les civils exposés, mais aussi des armes tout aussi efficaces, bien que non létales, qui se nomment : embargos, gels d'avoirs, interdiction d'utiliser le dollar ou tout intermédiaire américain etc. Autrement dit, ces armes financières et commerciales, puissamment utilisées par les États-Unis grâce à l'exterritorialité de leur droit contribuent à la désintégration du commerce mondial. Ce n'est qu'après la paix revenue que le monde pourra évaluer les coûts des conflits en cours. À cet égard, l'auteur évoque le traité de Versailles en 1919. Devons-nous être rassurés ?**

Après avoir été une arme dans la « guerre contre le terrorisme » sous l'égide des Nations Unies, les sanctions sont devenues une arme contre les États voyous. Dans un article récent de la revue *Commentaire*, Philippe Trainar dresse un « bilan des sanctions économiques » qui ne craint pas d'affronter la complexité : au-delà de leur efficacité ponctuelle sur le pays ou l'organisation visée, l'addition des sanctions produit un effet de composition qui tend à fragmenter l'espace économique et politique international. En particulier, il paraît maintenant difficile de constituer des majorités dans un monde où 110 pays sur les 193 membres des Nations Unies font l'objet de sanctions de la part de l'Union européenne ou de ses alliés. Sous les radars de la politique et de l'économie internationales, les entreprises mettent en œuvre et supportent les coûts des politiques de sanctions, qui peuvent s'avérer particulièrement élevés. Le présent article adopte une perspective résolument microéconomique pour faire le point sur les conséquences des sanctions pour les entreprises d'assurances. Pour cela nous distinguerons trois séries de causes : ❶ l'interdiction des opérations d'assurance, qu'elle soit expresse ou procède de l'interdiction

du commerce de certains biens et services, ❷ le gel des avoirs et enfin ❸ les interdictions découlant des sanctions étrangères. Pour finir, nous examinerons des réponses spécifiques ❹ notamment les « clauses sanctions » et le retrait des pays soumis aux sanctions.

## Embargo contre un État : interdiction expresse ou indirecte des opérations d'assurance

L'Union européenne peut adopter des « mesures restrictives » dans le cadre de sa politique extérieure de sécurité commune : conformément à l'article 215 du TFUE, le Conseil statue seul à la majorité qualifiée. C'est ainsi que l'Union a voté des sanctions contre la Corée du Nord puis l'Iran en 2007, et plus récemment le règlement 833/2014 « concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine ». C'est ce texte, augmenté de nouveaux « paquets » de sanctions, qui dispose une série d'interdictions directes ou indirectes de commercer avec les entités russes. Est notamment défendue expressément l'assurance « des biens et technologies propices à une utilisation dans le secteur de l'aviation ou l'industrie spatiale » s'ils sont utilisés par des personnes physiques ou morales russes. Une interdiction indirecte intervient pour toute « aide financière », y compris « tout type d'assurance ou de réassurance » (article 1), à l'exportation de matériel militaire ou à double usage (c'est-à-dire d'usage tant civil que militaire) (art. 2), de matériels et de technologiques pour l'exploration ou la production pétrolière (art. 3), comme pour l'aéronautique ou l'astronautique. La même interdiction s'étend désormais à l'importation de produits sidérurgiques et de diamants. Il n'est donc possible de fournir aucune forme d'assurance pour ce type de commerce, notamment pas d'assurance-crédit et pas d'assurance de transport.

Le commerce du pétrole fait l'objet de dispositions spécifiques et complexes depuis la formation d'une coalition pour le contrôle de son prix (*Oil Price Cap Coalition* comprenant outre l'Union européenne, le G7 et l'Australie). Depuis le 5 décembre 2022 (pétrole brut) et le 5 février 2023 (produits raffinés), les assureurs sont tenus de ne plus offrir de services d'assurance qu'aux navires dont le chargement a été acquis à un prix inférieur au maximum. Dans

**110**  
pays sur les 193 membres des Nations Unies font l'objet de sanctions de la part de l'Union européenne ou de ses alliés.

les faits, la mise en œuvre s'avère compliquée : les autorités des pays membres de la coalition ont reconnu des cas de falsification des documents ou de dissimulation des éléments importants du contrat<sup>1</sup>.

Ces interdictions ciblées, qui ont pour objectif de diminuer les ressources financières de la Russie belligérante et de limiter sa capacité de production d'armes modernes, ont donc pour effet de priver les assureurs européens d'une partie de leur activité : Imbs & Pauwels (2023) estiment cette perte de chiffre d'affaires à moins de 1% (même si elle est concentrée sur les assureurs crédit et transport).

## Sanctions individuelles : gel des avoirs

Les mesures de gel des avoirs touchent potentiellement tous les assureurs. Il s'agit cette fois de mesures ciblées à l'encontre de personnes physiques et morales : au premier janvier 2024, elles étaient plus de 1950 à être désignées par le règlement 269/2014 consolidé. Quel est l'effet d'une inscription sur la liste des personnes sanctionnées ? D'après la Foire Aux Questions du site de la Commission européenne, les entités du secteur financier, et particulièrement les entreprises d'assurance « ne peuvent mettre des fonds ou des ressources économiques à la disposition d'une personne inscrite sur la liste, directement ou

indirectement, par don, vente, troc ou tout autre moyen, y compris la restitution des ressources propres de la personne inscrite sur la liste. La conséquence d'une inscription sur la liste est que la prestation de services à la personne inscrite sur la liste, y compris les services d'assurance, doit cesser ». Il existe toutefois un certain nombre de dérogations, en particulier ❶ si le contrat en vertu duquel le paiement est fait est antérieur à la décision (d'inscription sur la liste) et si le paiement est fait vers un compte également gelé, ❷ une dérogation peut être accordée par le superviseur de l'État membre si la personne inscrite sur la liste ne peut subvenir à ses besoins fondamentaux (en France, l'autorisation de la DG Trésor est réputée automatique pour les contrats d'assurance obligatoires). Enfin ❸ des dérogations ponctuelles peuvent être accordées, conformément aux lignes directrices édictées par l'ACPR et la DG Trésor.

Le gel des avoirs introduit donc une complexité certaine car certaines opérations d'assurance sont interdites (notamment celles qui se traduisent par un versement au profit d'une personne inscrite sur la liste) mais pas celles qui visent à dédommager les tiers (les organismes d'assurance sont néanmoins tenus de « détecter toute tentative de mise à disposition indirecte de fonds au profit d'une personne ou entité désignée ou de contournement de la mesure de gel »). En outre, comme les mesures de gel s'étendent aux entités possédées, détenues ou contrôlées par les personnes inscrites sur la liste ; les sociétés d'assurance ont un devoir de vigilance (*due diligence*) étendu à l'égard de leurs clients personnes morales, et doivent donc recueillir les informations sur leur structure de propriété, leur gouvernance et leur bénéficiaire effectif pour s'assurer qu'elles ne sont pas visées par le gel des avoirs.

Cette obligation de vigilance n'est pas seulement ponctuelle. Le test de l'inscription sur la liste n'est jamais définitif. Les lignes directrices de l'ACPR précisent : « il est attendu des organismes financiers qu'ils effectuent un filtrage avant toute entrée en relation d'affaires ou d'exécuter une opération occasionnelle [n. i.] », comme l'indemnisation d'un sinistre. En outre, on n'attend pas une concordance exacte mais un « taux de concordance » (ACPR 2021 § 72) qui tolère donc des faux positifs devant être vérifiés à la main. Bref, la mise en œuvre du

dispositif de gel des avoirs oblige à repenser radicalement la relation avec le client et à construire un service dédié au filtrage préalable à toute opération significative.

Les assureurs de dommages qui n'avaient aucune activité à l'étranger ont pu croire jusqu'assez récemment que ce dispositif de gel des avoirs était superfétatoire et ne les concernait pas : ils ont compris, à la faveur d'un contrôle sur place, qu'ils n'étaient pas moins assujettis à la réglementation que les autres. Le recueil de jurisprudence de l'ACPR témoigne d'une mise en conformité progressive des assureurs en matière de dispositif de gel des avoirs ; les amendes récentes se comptent en millions d'euros. On peut penser que les coûts de mise en conformité entraînent une dépense initiale du même ordre de grandeur (maîtrise d'ouvrage du changement plus filtrage de l'ensemble de la clientèle), et une dépense annuelle récurrente (embauche pour le filtrage en continu) inférieure d'un ordre de grandeur à peine. Ces dépenses ne sont pas liées aux opérations militaires en cours, mais l'usage des sanctions dans la stratégie décidée par la politique extérieure de sécurité commune augmente les coûts de filtrage en étendant la liste des personnes visées par le gel des avoirs, et donc le nombre des faux positifs.

Outre les sanctions européennes, les entreprises financières doivent parfois observer les sanctions décidées par des États tiers.

### L'effet des sanctions étrangères

On mentionne pour mémoire les sanctions suisses ou britanniques, qui doivent être respectées par les personnes domiciliées dans ces pays, ce qui paraît aller de soi. En revanche, les sanctions américaines ne nécessitent pas nécessairement une domiciliation américaine mais l'implication d'une *US person* ou d'un *US nexus*. La première catégorie désigne une personne physique ou morale américaine, bénéficiant du statut de résident (*green card* par exemple) ou simplement de passage aux États-Unis qui serait partie à la transaction ; la deuxième catégorie est plus étendue, puisqu'il suffit d'une opération en dollars ou de l'implication même indirecte d'une *US person* (qui aurait par exemple négocié ou serait intervenue comme conseil dans l'opération en cause). Bref, il suffit de l'intervention d'une *US person*

ou d'un paiement en dollars pour que les sanctions américaines s'appliquent. C'est au nom de ce principe que BNP Paribas avait été condamné le 1<sup>er</sup> mai 2015 à 8,9 milliards de dollars d'amende par la justice américaine pour des opérations en dollars avec des clients cubains, iraniens et soudanais – aucune *US person* n'intervenait dans l'affaire mais le *US nexus* était constitué par les paiements en dollars. Il est remarquable que le montant de l'amende soit égal au montant des opérations violant les sanctions US : il n'y a ainsi rien à gagner à les enfreindre. D'autant qu'en plus de la condamnation pénale, une entreprise qui violerait les sanctions américaines, si elle ne s'avérait pas coopérative, pourrait se voir infliger des sanctions secondaires, c'est-à-dire apparaître à son tour sur la liste des personnes dont les avoirs sont gelés (*Specially Designated Nationals And Blocked Persons*) : des transporteurs maritimes libériens ou émiratis ont eu l'honneur d'une telle inscription en février 2024<sup>2</sup>, de même que des fournisseurs de composants électroniques asiatiques<sup>3</sup>.

Les entreprises européennes du secteur financier risquent donc d'être condamnées, voire elles-mêmes soumises aux sanctions américaines si elles acceptent des paiements en dollars, des clients américains ou si elles font intervenir des *US persons*. Ce dernier point mérite un examen attentif, puisqu'on peut n'avoir aucune activité américaine autre qu'un traité de réassurance négocié par un courtier qui a fait intervenir ses équipes américaines. C'est un point à éclaircir au moment de la signature des traités. De manière générale, on doit s'assurer que ses fournisseurs comme ses clients ne recourent pas à des *US persons* : c'est évidemment un sujet particulièrement délicat pour les entreprises avec une forte exposition internationale, aussi bien en matière de souscription, d'achat de services que de gestion d'actifs.

Comme les sanctions européennes, les sanctions américaines ont une double nature : un embargo sur l'exportation et la fourniture de services (notamment) d'assurance résultant d'*executive orders* du président américain, et une série de sanctions ciblées sur des personnes. Si on n'a pas vocation à exporter, il n'y a pas à se soucier du premier point, en revanche, le second point peut être un problème y compris sur le marché domestique, puisque les personnes bloquées par les

sanctions américaines n'apparaissent évidemment pas en tant que telles sur le registre de la DG Trésor. Il faut donc recourir à un service tiers, comme World Check, qui agrège toutes les listes de sanctions du monde entier. Dans le cas des personnes morales, l'obligation de vigilance doit s'étendre aux propriétaires puisque les sanctions américaines visent également les entités possédées par les personnes inscrites sur la liste<sup>4</sup>.

Les Européens ont un temps pensé s'abstraire des sanctions américaines avec le vote du Règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996, réactualisé quand Donald Trump a décidé de se retirer de l'accord de Vienne sur le nucléaire iranien en mai 2018. Ce texte dispose que les entreprises de l'Union ne doivent pas se conformer aux sanctions étrangères. Pour protéger de sanctions secondaires les entreprises européennes, un instrument (INSTEX, INstrument in Support of Trade EXchanges) fut créé conjointement par l'Allemagne, la France et le Royaume-Uni. Ce bricolage aventureux a finalement été abandonné en 2023<sup>5</sup>, et INSTEX a été démantelé : les velléités européennes d'échapper aux sanctions américaines doivent donc emprunter d'autres chemins.

### Autres mesures d'adaptation aux sanctions

Les entreprises particulièrement exposées aux sanctions peuvent limiter leur exposition en introduisant dans les contrats des « clauses sanctions », voire en quittant le pays qui fait l'objet d'un embargo.

Les assureurs ont pris acte de la généralisation des sanctions en introduisant dans leurs contrats une « clause sanction » relativement uniforme qui les dispense de fournir aucune prestation si cela devait les exposer à des sanctions. Toutefois, en juin 2022, la Cour d'appel de Paris a débouté AIG Europe qui refusait de couvrir les frais de défense des dirigeants de Lafarge S.A. dans le cadre des procédures pénales ouvertes à Paris et à Bruxelles, en raison des activités de l'entreprise en Syrie entre 2013 et 2014 qui l'exposaient à des sanctions. La cour a jugé que cette clause était effectivement une *clause d'exclusion*, or l'article L. 113-1 du code des assurances qui dispose que les clauses d'exclusion doivent être



### Bibliographie

ACPR. (2021). Lignes directrices conjointes de la Direction Générale du Trésor et de l'Autorité de contrôle prudentiel et de résolution sur la mise en œuvre des mesures de gel des avoirs.

Imbs, Jean and Pauwels, Laurent, (2023). «An Empirical Approximation of the Effects of Trade Sanctions with an Application to Russia», *Economic Policy*, Forthcoming.

Trainar P. (2023). Le bilan des sanctions économiques. *Commentaire*, 184, hiver 2023-24.



### Notes

<sup>1</sup> Price Cap Coalition. (2024). Price Cap Coalition – Oil Price Cap (OPC) Compliance and Enforcement Alert.

<sup>2</sup> US Dept of Treasury. (2024a). Treasury Targets Price Cap Violation Network and Implements G7 Ban on Russian Diamonds. 8<sup>th</sup> Feb. 2024.

<sup>3</sup> US Dept of Treasury. (2024b). T On Second Anniversary of Russia's Further Invasion of Ukraine and Following the Death of Aleksey Navalny, Treasury Sanctions Hundreds of Targets in Russia and Globally. 23<sup>rd</sup> Feb. 2024.

<sup>4</sup> OFAC. (2023). Entities owned by blocked persons (50% rule).

<sup>5</sup> Décision du Tribunal de l'UE numéro = T-8/21, IFIC Holding / Commission.

<sup>6</sup> *Onopriienko, Andrii et alii, Analysis of foreign business exits from Russia* (November 29, 2023). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.4648135>

<sup>7</sup> Sonne P., Ruiz R. R. (2023). How Putin Turned a Western Boycott Into a Bonanza. *New York Times*, Dec. 17.

<sup>8</sup> NSK = *Нефтяная страховая компания*, la « compagnie pétrolière d'assurance » est une entreprise kazakhstanaise.

<sup>9</sup> Zaozirny S. Pinnick T. (2023). Deal over jets stranded in Russia may serve as blueprint. Téléchargé de : <https://www.brownejacobson.com/about/news-media/deal-over-jets-stranded-in-russia-may-serve-as-blueprint>

*formelles et limitées*, ce que n'était donc pas la clause mise en cause (Cour d'appel de Paris 21 juin 2022 / n° 20/10832). Voilà donc une insistance remarquable du dicton « qui trop embrasse mal étreint » ! La clause sanction est désormais réécrite comme une clause *suspensive* (« L'exécution de ses obligations par [la Société] de couvrir un risque, de payer une somme d'argent ou de fournir une prestation en application du présent contrat, est suspendue, de plein droit et sans formalités, dans la mesure où cette exécution contreviendrait à une ou plusieurs Mesures de sanctions Internationales\* auxquelles [l'Assureur] [la Société] est soumis[e]. Cette suspension cesse à compter du jour où les Mesures de sanctions internationales cessent d'affecter l'obligation de [la Société]. »)

Si l'ajout dans les contrats de clauses sanctions opportunément rédigées paraît une nécessité pour les assureurs situés en dehors des pays en conflit, elle n'est évidemment pas une solution pour les assureurs installés dans les pays en conflit. Plus généralement, les filiales des groupes européens établis dans un pays visé par des sanctions se trouvent exposées à des difficultés juridiques inextricables : si elles respectaient les mesures restrictives, elles s'exposeraient à exercer une discrimination à l'encontre de certains clients actuels ou potentiels. Le choix est donc de vendre tout ou partie des filiales étrangères – une participation inférieure à 50 % exempte de l'obligation de se soumettre aux mesures restrictives de l'Union (comme des États-Unis). L'opacification des flux via une entité *ad hoc* située dans un pays tiers, comme une marque française de cosmétiques la pratique actuellement (d'après une

étude de l'École d'économie de Kyiv<sup>6</sup>), outre le risque de voir révélée une conduite contraire au discours public, est tout simplement impraticable pour une entité régulée.

L'appropriation des entreprises étrangères par les pays belligérants est un grand classique des situations de conflit, et pose la question du moment optimal pour sortir. Tout le problème est que les règles ne sont pas connues à l'avance, ce qui rend difficile l'application des modèles simples de la théorie des jeux. L'étude de l'École d'économie de Kyiv permet de constater que certains assureurs ont choisi de quitter la Russie et donc de chiffrer leurs pertes dès que possible, d'autres ont préféré annoncer qu'ils renonçaient à de nouveaux investissements en Russie ou qu'ils allaient désinvestir, d'autres encore ont opté pour le non-renouvellement des contrats (*runoff*) ou pour la vente de la part du capital qui les rendait majoritaires : autant de stratégies d'attente qui conduisent à une incertitude sur l'évaluation des pertes, d'autant que c'est l'acheteur qui détermine le prix de sortie<sup>7</sup>.

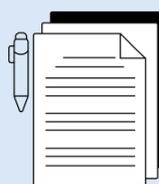
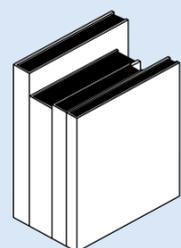
Un cas particulier d'incertitude sur l'évaluation des pertes des assureurs est celui des avions qui ont été bloqués en Russie depuis la fin février 2022. Ces avions étant assurés, les loueurs ont demandé à être indemnisés pour la perte des avions : les assureurs ont fait valoir que le contrat prévoyait une indemnisation pour perte totale au cas où des dommages physiques à un appareil dépassaient un

tantième de sa valeur, mais pas en cas de perte de jouissance. En juin 2022, les loueurs se sont portés partie civile devant les tribunaux britanniques pour forcer les assureurs à payer ; le procès doit avoir lieu en octobre 2024. A l'automne 2023 cependant, une transaction a eu lieu entre AerCap, le principal loueur, Aeroflot et NSK<sup>8</sup> : les termes de cet accord ne sont pas connus de manière certaine, mais des sources indiquent que les Russes auraient racheté les avions aux deux tiers de leur valeur, toutefois le loueur aurait pu récupérer les réserves de maintenance évaluées à une dizaine de pourcents de la valeur des avions, d'où une perte d'environ 25 %<sup>9</sup>. Il reste à observer dans quelle mesure cet accord qui porte sur 645 millions d'euros pourra être répliqué, non seulement pour le reste des avions d'AerCap, mais encore pour les avions des autres loueurs. En outre, même si on peut penser que ces arrangements limitent considérablement l'exposition des assureurs, il n'est pas possible de se prononcer sur les termes d'accords qui sont restés confidentiels.

On rappelle encore, à toutes fins utiles, que les conflits ont vocation à s'achever par des traités de paix : le traité de Versailles contenait des dispositions remarquables sur les contrats d'assurance. Et de manière générale, c'est seulement après la guerre qu'on mesure pleinement les coûts que celle-ci ont fait peser sur les belligérants, comme sur les personnes qui ont apporté leur concours : les assureurs ne font, à cet égard, pas exception.

DOSSIER

# Études



# débats



# Partage des données, à qui profite le crime?

Récemment, la Commission européenne a posé les bases d'un nouveau cadre d'accès aux données financières (FIDA, ou Financial Data Access), permettant aux consommateurs et aux entreprises d'autoriser des tiers à accéder à leurs données détenues par des institutions financières, y compris les assurances. Nous nous concentrons ici sur l'utilisation que pourraient faire les assureurs de davantage d'informations: cette ouverture de l'accès aux données compromet largement l'idée même de mutualisation et de partage des risques.

Un des principaux arguments en faveur de la réglementation FIDA est la transparence, ou comme le disent les textes «*promoting financial transparency*». Or il est difficile d'être contre la transparence, à moins d'avoir quelque chose à cacher. C'est le fameux argument «*nothing to hide, you've got nothing to fear*». Comme le rappelle Solove (2011), le gouvernement britannique l'avait utilisé comme argument pour installer des caméras de surveillance: «*if you've got nothing to hide, you've got nothing to fear*». L'universitaire Shoshana Zuboff est beaucoup plus réservée, «*if you have nothing to hide, then you are nothing...*». Partager des données personnelles sans limites, ni responsabilité quant à la manière dont ces informations

sont utilisées, est dangereux, pour la personne qui le fait, mais aussi collectivement.

## Partager les données, pour quoi faire?

Partager et regrouper des informations est a priori une idée pleine de bon sens.

En 1988, le fichier FVI (fichier des victimes indemnisées) a été mis en place pour répondre aux obligations résultant de l'article 26 de la loi du 5 juillet 1985 (dite «*loi Badinter*»), pour toutes les victimes d'un accident de la circulation. Les assureurs et les magistrats ont depuis l'obligation de communiquer les montants des

indemnités versées pour des dommages corporels survenus lors d'accidents automobiles. L'objectif était de permettre à toute victime de connaître les montants des indemnités auxquelles elle pourrait prétendre. Mais surtout, collectivement, elle permet de mieux suivre et de mieux comprendre, par exemple, les écarts constatés entre différentes cours d'appel pour des situations comparables. Plus généralement, l'ouverture des données en lien avec les accidents de la route permet d'aider la sécurité routière et la prévention. Il est possible de quantifier l'impact d'un changement de régulation sur les vitesses autorisées sur la route sur les décès sans données d'assureurs. Mais si on



**LAURENCE BARRY**

Co-titulaire de la chaire PARI



**ARTHUR CHARPENTIER**

Professeur à l'UQAM, Université du Québec à Montréal

souhaite analyser les dommages corporels, il faut des données plus fines, que possèdent les assureurs. En utilisant des données d'assureurs, Retting (2017) montrait que les SUV causent des dommages bien plus graves lors d'accidents avec des piétons, par exemple. De la même manière, les modèles climatiques permettent de prévoir le climat à moyen terme, ou ses conséquences sur la puissance des tempêtes hivernales, sur les risques de sécheresse ou sur le nombre de jours de canicule. Mais prévoir les conséquences économiques nécessite d'autres données, données que possèdent cette fois les assureurs. Pour analyser les impacts de telle ou telle règle d'urbanisme, les assureurs ont

des données qui permettraient une analyse robuste, par exemple. Lors de la récente pandémie de Covid, de nombreux débats ont eu lieu quant à la libération de données de santé, afin de mieux prévoir et anticiper la propagation. En matière de santé publique, un partage de données<sup>1</sup>, collectées de manière sécurisée, permettrait de faire réellement de la prévention, et bénéficierait réellement à tous. Partager des données permet en effet de faire des études scientifiques pour mieux cartographier les risques, et ainsi les réduire. Le danger est bien entendu le partage de données sensibles, ou plus subtiles, permettant d'inférer des informations sensibles, comme le rappelle l'idée de discrimination par proxy. Ainsi le projet de règlement FIDA exclut explicitement les données de santé du champ des données ouvertes, mais on peut utiliser à la place des indicateurs indirects, comme les achats dans les bureaux de tabac ou les paiements de services de soins pour inférer les pathologies des personnes. De la même manière, en observant les endroits où une personne utilise sa carte de paiement, les restaurants fréquentés par exemple, il est possible d'inférer ses pratiques religieuses; connaître l'historique de navigation permet d'inférer une sensibilité politique... Comme le fait remarquer Daniel Solove, des données a priori anodines peuvent ainsi être révélatrices d'informations sensibles. Mais surtout, ce partage de données avec des tiers, qui pourraient vendre des couvertures d'assurance et «*améliorer*» leur tarif, n'est pas sans danger sur l'équilibre du système, surtout si on s'intéresse à l'accessibilité financière pour tous.

## Petite histoire de la segmentation tarifaire

Les *collegia veteranorum* des légionnaires romains sont une illustration des premiers exemples de mécanisme d'assurance, comme

le raconte Ginsburg (1940). Au <sup>xvii</sup> siècle en France, les caisses de prévoyance des corporations se développent, jusqu'à leur disparition en 1791 par la loi Le Chapelier, avant de se réorganiser ensuite en «*sociétés de secours mutuel*». Chaque adhérent verse un montant à sa mutuelle, sa cotisation, et les fonds ainsi accumulés servent à indemniser un dommage subi par l'un des membres. En Angleterre, ce sont les «*amicales*» (*friendly society*) qui joueront ce rôle. Dans la seconde moitié du <sup>xix</sup> siècle, ces sociétés de secours mutuel se développent, sur une base corporatiste et géographique. Les tisserands de Lyon (canuts) étaient regroupés dès 1828 au sein de la Société du Devoir Mutuel, dont laquelle ils devenaient membre en versant un droit d'entrée de 3 francs, et une cotisation mensuelle d'un franc, comme le raconte Bron (1968). Un fonctionnement similaire se retrouve à la Société typographique de Paris. Comme l'explique Da Silva (2020), «*les mutuelles fonctionnent sur un principe de solidarité dans la mesure où les contributions ne sont pas nécessairement liées au niveau de risque.*»

Mais l'idée d'introduire une approche plus scientifique fait son chemin, comme en témoigne Hubbard (1852). Pour citer Da Silva (2020), «*alors que les mutualistes voient dans la figure de l'actuaire la fin programmée de la solidarité, les républicains y voient la rationalisation de l'aide.*» La tarification sur la base du risque va tranquillement s'imposer au cours du <sup>xx</sup> siècle, avec une tarification différenciée sur la base d'une segmentation en quelques classes tarifaires simples, constituées sur la base d'informations facilement collectées (avec un questionnaire par exemple, ou un rapide examen médical). Et surtout, cette pratique sera légitimée théoriquement sur la base du concept d'équité actuarielle (*actuarial fairness*).

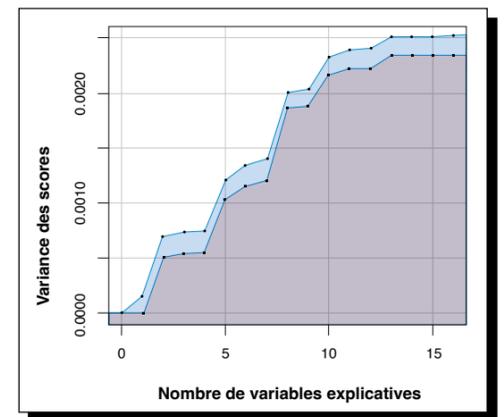
## De l'équité actuarielle

Depuis que le régulateur du Kansas a posé, en 1909, qu'une tarification devait être à la fois «*adéquate*» (donc suffisamment élevée pour éviter la ruine de l'assureur) et «*non-discriminatoire de façon inéquitable*» (*not unfairly discriminatory*), les discussions sont allées bon train dans le monde actuariel pour déterminer le sens de cette équité. Dans un premier temps, il est apparu que deux risques identiques ne devaient pas payer des primes différentes: dans cette acception, si tous les assurés d'un portefeuille paient la même prime quel que soit leur risque, cette tarification est tout à fait équitable. Mais la concurrence aidant, très vite la discussion a tourné autour de la définition de risques

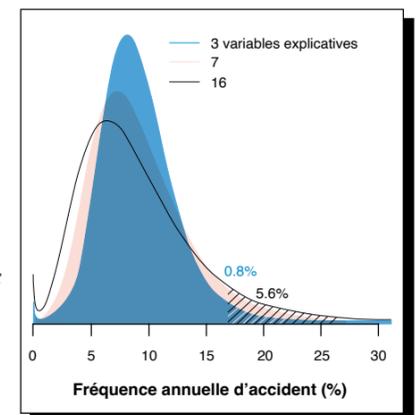
«*identiques*»: il faut segmenter pour éviter l'antisélection, mais il faut segmenter en étant capable de distinguer des risques «*identiques*» afin de rester équitable... d'où la nécessité d'avoir des variables de plus en plus granulaires qui délimitent les contours de cette identité de risque, comme le rappelle Barry (2020).

La théorie du choix rationnel qui prend son essor après-guerre sur la base des travaux de von Neumann et Morgenstern est assez rapidement appliquée à l'assurance par Friedman et Savage mais surtout Arrow, et transforme cette notion d'équité actuarielle. En effet, alors que jusque-là il s'agissait de mutualiser les primes, la notion d'assuré comme *homo oeconomicus* bouleverse cette approche: si, comme le décrit la théorie du

Fig. 1



Évolution de la variance de la fréquence de sinistre en haut (en bleu foncé, une régression logistique classique, et en rose pastel, avec du lissage de trois variables continues), et distribution des scores, en bas, avec des modèles à 2, 7 et 16 variables explicatives.



choix rationnel, toute personne est capable d'attacher des probabilités à des événements futurs, alors l'ajustement de la prime au risque devient un outil de communication entre l'assuré et l'assureur. La prime comme « signal du risque » devient un outil de prévention, et tout écart par rapport à cette prime « exacte » est une forme d'injustice vis-à-vis de l'assuré puisqu'elle ne lui permet pas de prendre les bonnes décisions en situation d'incertain (voir Barry 2023). La segmentation, qui était jusque-là présentée comme une contrainte concurrentielle, se justifie à présent par des considérations d'équité.

### La théorie mathématique de la segmentation

En s'inspirant de De Wit & Van Eeghen (1984), il est possible de montrer que davantage d'information augmente la segmentation, et la dispersion des primes (les plus risqués contribuant de plus en plus, et les moins risqués de moins en moins). Notons  $p(x)$  la fréquence d'accident prédite (le score) pour un assuré de caractéristiques  $x$ , autrement dit,  $p(x)=E[Y|X=x]$ , et notons  $\theta$  le paramètre de risque sous-jacent, capturant parfaitement le risque de l'assuré. Dans ce cas, la variance des scores

est  $Var[p(X)] = Var[Y] - (E[Var[Y|\theta]] + E[Var[E[Y|\theta]|X]])$  où les deux premiers termes sont incompressibles, avec la variance du risque dans le portefeuille, et la variabilité fondamentale, liée au risque sous-jacent<sup>2</sup>. Le dernier terme est celui qui explique à quel point les variables explicatives  $X$  capturent de l'information permettant d'approcher  $\theta$ . Plus on dispose de variables explicatives, plus on se rapprochera a priori de  $\theta$ . Autrement dit, la variance du score augmente mécaniquement avec le nombre de variables explicatives<sup>3</sup>.

### Un cas d'école

Mais il est possible d'aller plus loin que cette analyse de la variance des primes pures. Sur des données d'assureurs, en assurance automobile, on peut s'intéresser simplement à la fréquence d'accidents impliquant la garantie responsabilité civile<sup>4</sup>. Les variables explicatives sont ordonnées par ordre d'importance (la plus importante étant l'ancienneté du permis de conduire, et parmi les moins importantes, on aura par exemple le statut marital du conducteur). Sur la partie gauche de la Figure 1, on retrouve visuellement le théorème précédent: ajouter des variables prédictives augmente la variance des scores, des prédictions de fréquence de sinistres. Mais surtout, la distribution des scores est de plus en plus étalée, comme on le voit à droite. Alors que la fréquence annuelle globale d'accidents est de 8.5 %, on peut noter que la proportion d'assurés ayant une prévision supérieure à 17 % (traduit en prime pure, on regarde la proportion d'assurés payant une prime deux fois plus élevée que la prime moyenne) passe de moins de 1 % avec 2 variables prédictives à plus de 5 % avec 16 variables. Et ce pourcentage, obtenu avec une régression logistique, est très conservateur comparé à un algorithme d'apprentissage machine

plus complexe (une forêt aléatoire), où 15 % de la population se voit prédire une fréquence aussi élevée (Figure 1).

On peut aussi visualiser l'écart relatif entre le quantile à 90 % et 10 % en fonction du nombre de variables explicatives, comme sur la figure 2, à gauche. Autrement dit, avec une seule variable explicative, les 10 % les plus risqués payent 50 % de plus que les 10 % les moins risqués, et quatre fois plus avec 15 variables (huit fois plus avec un algorithme d'apprentissage machine). Si on compare la prime moyenne entre les deux déciles (les 10 % les plus risqués et les 10 % les moins risqués), le ratio passe presque de 1 à 8 – 13 si on compare les 5 % les plus risqués. Les risques les plus élevés se voient demander, en moyenne, treize fois plus que les risques les plus faibles<sup>5</sup>. Là encore, les modèles économétriques sont très conservateurs par rapport aux modèles d'apprentissage machine (Figure 2).

Si les valeurs numériques dépendent fortement de la base de données utilisée<sup>6</sup>, il faut surtout retenir que rajouter des variables explicatives pertinentes pour prédire le risque augmentera mécaniquement la dispersion des primes et réduira la mutualisation dans le portefeuille. Et si certaines variables n'étaient pas collectées par l'assureur pour construire son tarif, c'était peut-être parce qu'elles étaient considérées comme sensibles, voire interdites. Et en collectant des données personnelles par d'autres sources, une discrimination par proxy se met en place (peut-être parce qu'il se met à utiliser une information très corrélée avec un handicap, par exemple). On peut le visualiser sur la Figure 3, qui montre l'évolution de la fréquence moyenne prédite pour les hommes et les femmes, en augmentant le nombre de variables explicatives, sans que le genre du conducteur ne soit utilisé lors de

la construction du modèle. Même en excluant la variable sensible de la base servant à construire les modèles, l'algorithme apprend à reproduire une différence qui existe dans les données (les hommes ayant une fréquence annuelle de sinistre de presque 9% et les femmes 8,2%)

### Qui profitera de l'ouverture des données?

Prétendre que les consommateurs vont bénéficier de cette ouverture des données, c'est oublier que les bénéficiaires ne seront pas du tout répartis uniformément. L'assurance était fondamentalement une histoire de mutualisation<sup>7</sup> donc de « partage de gâteau »: s'il y a des gagnants, il y aura des perdants. Comme on vient de le voir, les faibles risques auront de fortes chances de voir leurs primes baisser en augmentant l'information disponible, et les personnes les plus à risque auront de fortes chances de se retrouver exclues, ne trouvant de prime à un prix abordable. Si actuariellement cette personnalisation des primes peut faire sens, et aussi flatter le consommateur, persuadé qu'il est un bon risque (et que s'il a un accident, c'est la faute des autres), avec l'ouverture des données, l'idée de mutualisation des risques fond comme neige au soleil. Et si collectivement, nous accordons un peu de valeur aux idées de solidarité et de justice, on se doit de constater que cette approche réglementaire ne va pas dans la bonne direction. **Ⓢ**



### Notes

- Le projet de règlement (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0360>) exclut, en l'état, les « données de santé » (sans pour autant les définir clairement, ce qui soulèvera forcément beaucoup de questions dans les années à venir, par exemple : est-ce que l'achat de perruques ou de livres sur le cancer ne révélerait pas une information sur moi, ou un membre de ma famille?)
- Si la probabilité d'avoir un accident est connue parfaitement (par exemple 11,847 %), la réalisation du risque pendant l'année de couverture reste fondamentalement aléatoire et imprévisible.
- Dans les modèles linéaires, c'est le résultat bien connu qui affirme que, dans des modèles emboîtés, le modèle ayant le plus de variables explicatives aura le plus grand R2, ou formulé autrement, la plus grande variance des prévisions.
- Le code est en ligne sur <https://github.com/freakonometrics/fida/> basé sur des données utilisées dans Charpentier (2014).
- Dans le mécanisme bonus malus, le bonus maximum est de 0,50 soit 50 % et le malus maximal est de 3,50 soit 350 %, soit un ratio de 7 entre les deux bornes.
- En particulier, le plateau observé à droite des courbes est artificiel, et vient du fait que les variables sont ordonnées par importance : les dernières variables ajoutées ont ici un faible pouvoir prédictif (mais sont disponibles dans la base de données).
- Pour reprendre l'expression classique en économie du bien-être, comme Brams & Taylor (1996).



### Bibliographie

- Arrow, K. J. (1951). Alternative approaches to the theory of choice in risk-taking situations. *Econometrica*, 404-437.
- Barry, L. (2020). Insurance, big data and changing conceptions of fairness. *European Journal of Sociology/Archives Européennes de Sociologie*, 61(2), 159-184.
- Barry, L. (2023). From Small to Big Data: (Mis) Uses of Insurance Premium for the Government of Hazards. *Journal of Cultural Economy*, 1-16
- Brams, S. J., & Taylor, A. D. (1996). *Fair Division: From cake-cutting to dispute resolution*. Cambridge University Press.
- Bron, J. (1968). *Histoire du mouvement ouvrier français*. Éditions Ouvrières.
- Charpentier, A. (Ed.). (2014). *Computational actuarial science with R*. CRC press.
- Charpentier, A. (2024). *Insurance, biases, discrimination and fairness*. Springer
- Da Silva, N. (2023). *La bataille de la Sécu: une histoire du système de santé*. La fabrique éditions.
- De Wit, G. W., & Van Eeghen, J. (1984). Rate making and society's sense of fairness. *ASTIN Bulletin: The Journal of the IAA*, 14(2), 151-163.
- Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online?. *Telematics and Informatics*, 65, 101717.
- Frezal, S., & Barry, L. (2020). Fairness in uncertainty: Some limits and misinterpretations of actuarial fairness. *Journal of Business Ethics*, 167, 127-136.
- Friedman, M., & Savage, L. J. (1948). The utility analysis of choices involving risk. *Journal of political Economy*, 56(4), 279-304.
- Ginsburg, M. (1940). Roman military clubs and their social functions. *Transactions and Proceedings of the American Philological Association* 71, 149-156.
- Hubbard, N. G. (1852). *De l'organisation des sociétés de prévoyance: ou, de secours mutuels, et des bases scientifiques sur lesquelles elles doivent être établies; avec une table de maladie et une table de mortalité dressées sur des documents spéciaux*. Guillaumin et cie.
- Retting, R. (2017). Pedestrian traffic fatalities by state. *Governors Highway Safety Association: Washington, DC, USA*.
- Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- von Neumann, J. & Morgenstern, O (1944) *Theory of Games and Economic Behavior*. Princeton University Press.
- Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs

Fig. 2 Évolution du ratio entre les quantiles à 90 % et 10 % de la fréquence de sinistres, et évolution du ratio entre la moyenne dans les deux déciles. En bleu foncé, une régression logistique classique, et en rose pastel, avec du lissage de trois variables continues.

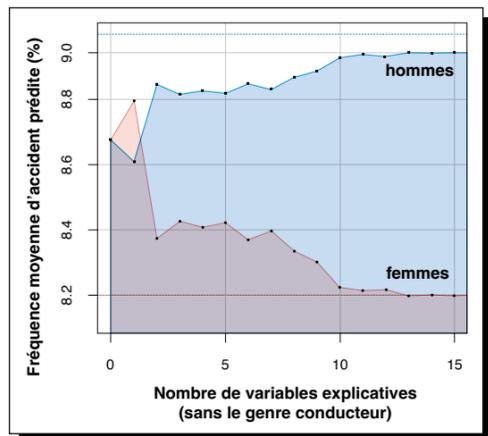
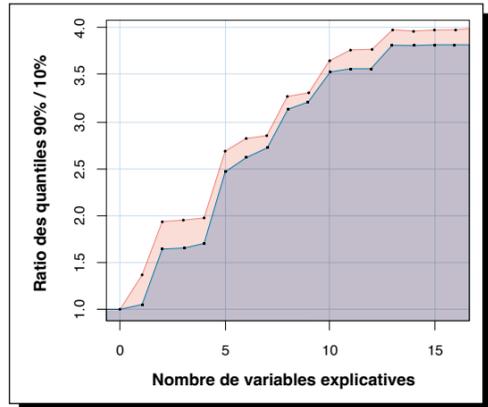


Fig. 3 Évolution de la fréquence moyenne prédite pour les hommes et les femmes

# Le risque géostratégique : l'éternel retour ?

« L'Histoire est liberté. La géographie est contrainte », rappelait l'historien Jules Michelet (1798-1874). La géostratégie mêle en réalité intimement les deux dimensions, qui s'imposent d'ailleurs dans la formation des historiens-géographes en France depuis le début du XIX<sup>e</sup> siècle. Le retour de la guerre dans le monde du XXI<sup>e</sup> siècle, perçu par l'Occident comme une régression, illustre la réalisation du risque géostratégique majeur. Nous allons ici essayer de démontrer que le risque géostratégique participe de la construction et de l'exercice de la puissance.



**PIERRE MARTIN**  
Historien

## L'utopie : la fin du risque géostratégique

Pour cerner le « risque géostratégique », il convient de définir ce qu'est la géostratégie, souvent confondue avec la géopolitique. Le géographe Philippe Boulanger, spécialiste de cette question, a récemment fait le point sur les débats épistémologiques liés à la géostratégie<sup>1</sup>. Il rappelle l'étymologie du concept : « Provenant des racines *stratos* (armée) et *agein* (pousser devant soi), la stratégie est forcément un mouvement dans l'espace<sup>2</sup>. » Si le mot est employé en anglais dès 1944, son entrée dans la langue française daterait de 1975<sup>3</sup>. Le regain d'intérêt pour la

géostratégie en France serait alors synchronique de celui pour la géopolitique. Si les définitions de géostratégie font l'objet de débats pointus, il y a cependant consensus pour dire que la géostratégie est très liée à la réflexion stratégique à des fins militaires et ce dès l'Antiquité, comme le rappelle d'ailleurs la racine grecque du mot. C'est pour cette raison que réflexion et pratique géostratégiques s'épaulent au gré des conjonctures historiques fortes, souvent liées à la surexposition au risque de guerre. Guerre froide et retour de la guerre coïncident ainsi avec une demande sociale de réflexion géostratégique. Comme le résume magnifiquement Philippe Boulanger : « la finalité de la

géostratégie consiste ainsi à proposer des hypothèses sur les risques, les menaces et les vulnérabilités afin de guider l'action stratégique en fonction de ses propres capacités stratégiques comme de celles de ses adversaires. » La paix perpétuelle<sup>4</sup>, la der des ders<sup>5</sup>, la terre est plate<sup>6</sup>, la fin de l'Histoire<sup>7</sup>... D'Emmanuel Kant à Francis Fukuyama en passant par le pacte Briand-Kellog mettant « la guerre hors la loi »<sup>8</sup>, on n'en finirait pas d'énumérer les textes proposant la fin définitive du risque géostratégique. On aurait pu ajouter la Déclaration de paix au monde, un décret du 22 mai 1790 : « la nation française renonce à entreprendre aucune guerre dans la vue de faire des conquêtes et

[déclare] qu'elle n'emploiera jamais la force contre la liberté d'aucun peuple. » Notons qu'il s'agissait ici moins d'une déclaration de paix universelle que du vote d'un texte éminemment politique qui visait à limiter les pouvoirs de Louis XVI, un temps monarque constitutionnel (1789-1793). Pas sûr que les populations européennes vaincues et grâce auxquelles les armées françaises ont financé leurs campagnes à partir de 1792 en aient été convaincues...

D'autres éléments poussent à l'utopie de la fin du risque géostratégique : la stabilité (apparente) de l'ordre mondial. L'année 1815 marque par exemple la fin du cycle de guerres révolutionnaires et impériales initié par la France, que les Anglais appellent « *French Wars* ». Dans son ultime ouvrage, *L'ordre du monde*, Henry Kissinger (1923-2023) revient sur le traité de Vienne accueilli et coordonné en 1814-1815 par le diplomate autrichien Metternich. Le système européen d'équilibre des forces qui en sort vise précisément à annihiler le risque géostratégique par le « concert des nations institutionnalisés par des conférences diplomatiques rassemblant périodiquement les chefs de gouvernement des alliances, pour définir leurs objectifs communs ou faire face à des crises émergentes. Ce mécanisme de concert des nations était une sorte de préfiguration du Conseil de sécurité des Nations Unies<sup>9</sup> ». Toute nation européenne qui sortirait du rang et aurait de trop grandes prétentions sur le continent devait être assez rapidement contrainte de respecter les engagements scellés à Vienne en 1815. Les nations d'Europe se révélèrent assez autorégulatrices en termes d'ambitions de puissance puisque ces principes garantirent une certaine paix, ou du

moins participèrent à anesthésier le risque géostratégique. La guerre ne disparaît donc pas d'Europe, mais elle est cantonnée dans des limites acceptables par toutes les puissances. Le « système Metternich » est censé avoir fonctionné un siècle, de 1815 à 1914. En réalité, le risque géostratégique est de retour dès 1866. La victoire des armées prussiennes sur celles d'Autriche à Sadowa cette année-là montre que l'unité des États allemands non seulement s'accéléra, mais en plus sous la houlette de la Prusse militariste. La guerre franco-prussienne de 1870-1871 est en germe, et c'est elle qui parachève l'unité de l'Allemagne proclamée le 18 janvier 1871 dans la galerie des glaces à Versailles, avant la signature du traité de Francfort le 10 mai 1871. « La France est une nation de zéros » a osé dire le chancelier allemand Otto von Bismarck... De facto, le risque géostratégique est de retour. La France est désormais obsédée par « la ligne bleue des Vosges » et le retour des provinces perdues, Alsace et Lorraine, intégrées à l'Allemagne unifiée. Autre exemple où le risque géostratégique semble avoir disparu : la période d'après la guerre froide, entre le démantèlement de l'URSS fin 1991 et les attentats du 11 septembre 2001 contre les tours jumelles du World Trade Center de New York. C'est à ce moment que l'Occident pense avoir concrétisé l'utopie d'Emmanuel Kant. L'Occident se croit alors éternellement à l'abri de l'« hyperpuissance » américaine selon le mot heureux du chef de la diplomatie française Hubert Védrine : les États-Unis cumulent alors tous les facteurs de puissance sans rival de taille. L'Europe va encore plus loin, se désarme sur le plan militaire, accélère la construction d'un espace marchand unifié,

## Un peu d'étymologie...

**Le terme « géostratégie » provient des racines *stratos* (armée) et *agein* (pousser devant soi). Si les définitions de géostratégie font l'objet de débats pointus, il y a cependant consensus pour dire que la géostratégie est très liée à la réflexion stratégique à des fins militaires et ce dès l'Antiquité.**

Source : Philippe Boulanger (géographe)

l'Union européenne, tout en faisant l'impasse sur le risque stratégique. Le voisinage de l'Union est alors considéré comme « le cercle des amis » selon le mot de Romano Prodi. Rares sont les lucides comme l'historien Élie Barnavi pour souligner que « contrairement à une idée largement répandue, l'Europe unie n'est pas la cause de la paix, mais sa conséquence<sup>10</sup>. » C'est dans un « entre-deux-risques géostratégiques » que le recul – confortable – permet de qualifier de parenthèse, que nombre d'intellectuels occidentaux théorisent la mort définitive du risque géostratégique et la convergence des nations vers un mode de vie démocratique apaisé. La Chine n'adhère-t-elle pas à l'OMC en 2001, avec l'appui des États-Unis ? « Le doux commerce » étiqueté par Montesquieu au XVIII<sup>e</sup> siècle sous la forme de la mondialisation généralisée était censé guider le Monde d'une « main invisible » vers une planète d'heureux consommateurs satisfaits. Cette insouciance naïve faisait alors quasiment consensus en Occident : c'est ainsi qu'en 1998 qu'Alain Minc publie *La mondialisation heureuse*. Un optimisme (ou une inconscience ?) généralisé(e), à l'exception toutefois des élites

militaires et de certains cercles de réflexion à l'époque bien peu audibles. À l'occasion en 2014 de la sortie de son livre *Dix thèses sur la guerre*, l'historien israélien Élie Barnavi considère que l'Europe a depuis 1945 effectivement rangé les armes au placard... mais que c'est bien le seul continent à l'avoir fait.<sup>11</sup> ».

## La réalité : la permanence du risque géostratégique

« La période située entre 1948 et le début du nouveau siècle a constitué un bref moment de l'histoire humaine où l'on a pu parler d'un ordre mondial naissant, fait d'un mélange d'idéalisme américain et de notions traditionnelles d'équilibre des forces<sup>12</sup>. » Pour le théoricien et le grand praticien des relations internationales Henry Kissinger, le désordre et partant le risque géostratégique sont la norme. L'ordre et le risque géostratégique contenu constituent bien l'exception. En 2003, l'historien Alexandre Adler publie *J'ai vu mourir le Monde ancien*. Pour lui, les attentats du 11 septembre 2001 sont au XXI<sup>e</sup> siècle ce que 1914 a été au XX<sup>e</sup> siècle. C'est la fin d'une

triple illusion: de l'hyperpuissance américaine, de la rationalité politique, de l'utopie d'une marchandisation universelle. Rappelons que de 1991 à 2001, le renseignement américain avait quasiment abandonné le risque géostratégique pour se concentrer sur l'espionnage industriel. Le seul conflit envisagé par l'Occident était alors la « guerre économique », théorisée dès les années 1970 par le conseiller du Président Pompidou Bernard Esambert<sup>13</sup>. Le 11 septembre 2001 apparaît donc comme la faillite majeure du renseignement, de la doctrine et de la prévention du risque géostratégique par les États-Unis d'Amérique. À court terme, l'attaque coordonnée d'Al-Qaïda à New York et Washington marque la fin de la sanctuarisation du territoire américain qui, hormis Pearl Harbor à Hawaï le 7 décembre 1941, avait toujours échappé à la destruction de guerre. À moyen terme, les États-Unis entrent dans un cycle délétère de vingt ans de guerre. Un risque géostratégique que les États-Unis peinent à assumer. Ils entraînent donc avec eux leurs alliés pour en porter le fardeau. Un risque initialement justifié pour éradiquer les racines du risque en Afghanistan. Si Ben Laden est éliminé en 2011, escompter implanter la démocratie en Afghanistan relevait d'une analyse totalement erronée du risque géostratégique régional. L'évacuation catastrophique de Kaboul par l'armée américaine le 15 août 2021 en est la sanction, et rappelle cruellement la débâcle de Saigon en 1975. La géographie se venge et se moque des armées surpuissantes inadaptées à des théâtres d'opération où l'ennemi est dans la montagne, la forêt tropicale ou dans la ville comme poisson dans l'eau. La seule

solution, difficilement applicable, consiste à enlever l'eau: ce qu'a fait l'armée française lors de la bataille d'Alger en 1957.

Dès 2016, le géographe et diplomate français Michel Foucher met les Européens en garde contre un « nouvel environnement géostratégique<sup>14</sup>. » Dans un rayon de trois heures de vol de l'Union européenne se trouvent désormais des foyers de crises qui déterminent un tout nouveau voisinage pour l'Europe, désormais entourée d'un « cercle de feu » selon l'expression du haut fonctionnaire autrichien Johannes Hahn en 2015. Citons l'État failli en Irak qui donne naissance à Daech en 2014, cet « enfant adultère de l'intervention américaine en Irak » pour le géopoliticien de terrain Gérard Chaliand<sup>15</sup>, qui a son pendant en Libye depuis 2011 et la chute de Khadafi. Citons également la guerre sans fin en Syrie, le risque géostratégique consubstantiel à Israël depuis 1948, la guerre civile larvée en Égypte entre le pouvoir militaire et le pouvoir islamiste des Frères musulmans, qui a aussi son pendant en Algérie depuis les années 1990. Citons enfin le retour d'une vieille menace nationaliste et impériale sur la frontière occidentale de la Russie où une partie des élites (ultra)-nationalistes n'a jamais vraiment admis la fin de l'URSS en 1991. La négociation avec la Russie a pu ponctuellement marcher, Michel Foucher également ambassadeur en Lettonie de 2007 à 2015 peut en témoigner. La diplomatie du chéquier de l'Union européenne a ainsi permis d'éviter que l'oblast de Kaliningrad, ex-Königsberg récupérée par l'URSS en 1945 et conservée par la Russie après 1991, ne devienne un abcès géopolitique et un risque géostratégique explosif au regard de ses

frontières terrestres. Mais depuis que Poutine a réouvert un cycle de guerre en 2014 en Crimée, et plus encore en février 2022 sur la frontière est de l'Ukraine, la Russie est redevenue un risque géostratégique majeur pour l'Europe. Même l'Allemagne pacifique d'après 1945 le reconnaît. Avant l'invasion russe de l'Ukraine, le diplomate SPD Sigmar Gabriel, ministre des affaires étrangères du gouvernement Merkel de 2017 à 2018 confessait avec humour: « Nous Européens pensions être des herbivores dans un monde d'herbivores. Nous découvrons que nous sommes des herbivores dans un monde de carnivores. Et avec le Brexit qu'allons-nous devenir: des végans? ». Le nouveau chancelier Olaf Scholz tente dans sa « grosse coalition » – en réalité déchirée – de faire admettre le « changement d'époque » en reconstruisant, après février 2022, une armée allemande totalement obsolète. Un fonds d'urgence de 100 milliards d'euros est voté pour sa modernisation quand l'Allemagne s'engage à consacrer 2 % de son PIB à la Défense.

L'innovation géostratégique peut modifier le risque géostratégique. Jusqu'en 1914, les armes se déployaient dans deux dimensions: la terre et la mer. La Première Guerre mondiale intègre l'air. L'arme aérienne permet de projeter la destruction au loin: l'armée française puis les villes du Royaume-Uni subissent les assauts de la Luftwaffe en 1940, avant que les métropoles de l'Allemagne nazie ne connaissent le même sort, l'US Navy est surprise par une attaque aérienne à Pearl Harbor en 1941, quand l'aéronavale américaine retourne la situation lors de la bataille des Midway en 1942. Le deuxième changement d'échelle a lieu avec les

bombardements atomiques d'Hiroshima et de Nagasaki en 1945. Pour Albert Camus, l'humanité entre dans une « ère prométhéenne », quand Raymond Aron conceptualise « l'âge planétaire<sup>16</sup> ». Pour le philosophe, l'arme nucléaire participerait paradoxalement à la limitation du risque géostratégique. Avec des arsenaux nucléaires massivement détenus par le duopole des deux superpuissances, États-Unis et URSS, et reposant sur le principe d'emploi en second pour infliger une réplique considérable, qui dissuade de l'employer en premier, l'arme nucléaire serait un des ingrédients majeurs de cette « guerre impossible, paix improbable ». La nucléarisation aurait ainsi minoré le risque géostratégique. Pour autant, l'innovation géostratégique est sans doute en train de bousculer ces attendus. Dès les années 1960, l'espace extra-atmosphérique revêt aussi une dimension militaire avec les satellites, d'observation puis tueurs. Dans les années 1980, les États-Unis relancent la course aux armements avec des boucliers antimissiles. Sur le plan technologique, les premiers missiles porteurs d'ogives nucléaires avaient une portée limitée: c'est une des raisons de l'implantation de fusées soviétiques à Cuba et de l'OTAN en Turquie. Or les grandes puissances travaillent désormais à des missiles hypersoniques capables d'atteindre des vitesses de Mach 5 (de plus de 5 000 km/h). Et des puissances nucléaires comme la Russie et la Chine entretiennent le doute sur la charge conventionnelle ou nucléaire de ces nouveaux vecteurs. Ce qui participe d'un flou géostratégique sur la doctrine d'emploi de l'arme nucléaire en second. Dans son dernier ouvrage, l'historien Thomas Gomart estime

## +

### Pour en savoir plus



Raymond ARON,  
*Penser la guerre, Clausewitz. 2. L'âge planétaire*, Gallimard, Tel, 1976.



Philippe BOULANGER,  
*Introduction à la géostratégie*, Repères, La Découverte, 2023.



Francis FUKUYAMA,  
*La fin de l'histoire et le dernier homme*, 1992.



Emmanuel KANT,  
*Vers la paix perpétuelle*, 1795.

que le risque géostratégique nucléaire est clairement de retour, notamment en Asie du Sud-Est autour de la Chine voire de la Corée du Nord: « Depuis 2015, la « Force des missiles de l'Armée Populaire de Libération », mise en place par Xi Jinping, a pour mission de conduire des frappes conventionnelles et nucléaires. Elle combine en son sein deux logiques: la première basée sur le postulat de l'efficacité militaire, la seconde basée sur le non-emploi et l'effet politique. D'un point de vue américain, cette dualité pourrait s'avérer particulièrement délicate à apprécier en cas de crise, et receler un potentiel élevé d'escalade accidentelle. Le développement par la Chine et par la Russie de missiles hypervéloces manœuvrants (vitesse supérieure à Mach 5) accentue ce risque dans la mesure où ils entretiennent une ambiguïté sur la cible visée, ainsi que sur la charge embarquée (conventionnelle ou militaire)<sup>17</sup>. » Dans *Penser la guerre*, Clausewitz<sup>18</sup> publié en 1976, Raymond Aron écrit un épilogue intitulé « Adieu aux armes ou la grande illusion »: le risque géostratégique n'a en réalité jamais disparu. Il correspond à la définition de la guerre par Clausewitz: « un caméléon ». Pour autant, comme pour tous les risques, la probabilité du risque géostratégique n'est pas la même toujours et partout.

### L'exposition au risque géostratégique varie

Dans son dernier ouvrage, Thomas Gomart analyse des « nœuds géostratégiques » majeurs. Qu'est-ce donc qu'un « nœud géostratégique »? Dans son analyse des « espaces stratégiques en réseaux »,

Philippe Boulanger précise: « Les zones pivots, les centres de gravité et les nœuds stratégiques constituent une autre grande catégorie de concepts géostratégiques dans la mesure où les grandes puissances se donnent pour priorité de les contrôler. Un zone pivot est, par définition, un centre de gravité dans un espace de conflictualité, lequel commande un espace plus large, tandis que le nœud stratégique est le point de convergence de différentes voies de transport qui assure la logistique de projection de forces<sup>19</sup>. » Point précisément nodal en ce qu'il est un carrefour de routes stratégiques, le « nœud » est au cœur de la construction des Empires maritimes. On peut ici parler d'une grande continuité géostratégique: le Portugal au xv<sup>e</sup> siècle, le Royaume-Uni au xix<sup>e</sup> siècle, les États-Unis d'après 1941 ont sécurisé les mêmes nœuds géostratégiques pour tenir les mêmes routes de navigation mondiales au fondement de leur thalassocratie. Thomas Gomart (2024) en analyse trois: Taïwan, nœud entre la Chine et le Monde, Ormuz, nœud entre la péninsule arabique et l'Iran, le Bosphore, nœud entre la mer Noire et la Méditerranée<sup>20</sup>. À chaque nœud, situé sur des artères de la mondialisation, un produit géostratégique d'intérêt mondial: les puces et semi-conducteurs du détroit de Taïwan, le pétrole, marchandise la plus naviguée du monde, du détroit d'Ormuz, le blé de Russie et d'Ukraine du détroit du Bosphore. Des espaces essentiels, des points de passage restreints pour des flux maritimes considérables: s'agit-il pour autant de lieux illustrant le risque géostratégique maximal? Ces « nœuds » ont toujours été particulièrement sécurisés: avant-hier par la marine portugaise, hier par la

Navy britannique, depuis 1945 par l'US Navy. La montée en puissance exponentielle de la Chine, couplée à son basculement maritime, participe de la crainte d'un affrontement pour la maîtrise de ces nœuds, à commencer par Taïwan<sup>21</sup>. Les enjeux sont maximaux, assurément: « Au cours des six premiers mois de 2022, près de la moitié du trafic de porte-conteneurs a transité par le détroit de Taïwan<sup>22</sup>. » Le détroit de Taïwan illustre le risque géostratégique majeur car Xi pousse à « régler la question de Taïwan de son vivant ». Une « réunification<sup>23</sup> » ferait basculer toute la mer de Chine dans l'orbite de Pékin: Taïwan est une zone pivot qui illustre aussi le risque impérial aux frontières. Pékin a d'ailleurs un différend frontalier, notamment maritime, avec la quasi-totalité de ses voisins, à l'exception récente et notable de la Russie<sup>24</sup>. Une vieille histoire que l'on croyait définitivement passée que celle du risque géostratégique nationaliste d'expansion armée. Russie, Chine, Turquie incarnent pourtant le retour de ce risque particulièrement bien analysé par Nicolas Baverez: « La Chine reste obsédée par la revanche sur les traités inégaux imposés par les puissances européennes au xix<sup>e</sup> siècle, Vladimir Poutine cherche à rejouer la Grande Guerre patriotique<sup>25</sup> en prétendant contre toute raison « dénazifier » l'Ukraine. Recep Tayyip Erdogan vit dans la nostalgie de l'Empire ottoman qu'il entend ressusciter<sup>26</sup>... Le risque géostratégique expansionniste impérial est bien de retour et place l'Occident, singulièrement l'Europe, en position délicate. Deux de ces trois puissances sont en effet voisines de l'Europe, quand la troisième, la Chine, est devenue omniprésente.

## Une vieille histoire que l'on croyait définitivement passée que celle du risque géostratégique nationaliste d'expansion armé. Russie, Chine, Turquie incarnent pourtant le retour de ce risque.

« nœud » géostratégique. On se souvient de l'obstruction du canal de Suez, qu'il commande plus au nord, à l'occasion de l'échouage du porte-conteneur d'Evergreen en 2021. On se souvient moins de sa fermeture consécutive à des opérations de guerre en 1956, et surtout de 1967 à 1975. Le risque géostratégique dans le détroit de Babel-Mandeb et aux environs, en mer Rouge et dans le golfe d'Aden, illustre la guerre asymétrique. Des pirates de Somalie ont pu hier arraisonner des bateaux au large de la Corne de l'Afrique: des opérations de police maritime internationale ont rétabli la

L'Europe n'a pas de Défense opérationnelle: depuis 1949 elle s'en est remise à l'OTAN, faute de mieux. Mais un retour possible de Trump au pouvoir remettrait de nouveau en cause la crédibilité de l'alliance. Les États-Unis, enfin, considèrent depuis Obama que la Chine incarne la menace systémique. Ils n'ont dès lors cessé de vouloir se retirer d'Europe et du Proche et Moyen-Orient. Or, l'attaque de l'Ukraine en février 2022 et celle d'Israël par le Hamas en octobre 2023 les contraignent à réassurer ces deux risques géostratégiques réalisés au détriment de celui grandissant de la Chine, leur grande rivale systémique.

Le dernier type d'exposition au risque géostratégique est celui, diffus, associé aux conflits asymétriques. Le détroit de Bab-el-Mandeb est aussi un

sécurité maritime. Fin 2023, ce sont les rebelles yéménites houthis chiites qui ont déclaré la guerre à Israël aux côtés du Hamas et attaquent des navires en mer Rouge. C'est un risque difficile à appréhender et à territorialiser caractéristique des guerres asymétriques, une guérilla aéronavale ici, qui s'appuie par exemple sur des drones. Un critère complémentaire est à convoquer: ce risque géostratégique peut naître et se développer dans des espaces en marge, dans des zones d'ombre délaissées par les stratèges. Al-Qaïda a ainsi essaimé en Afrique (Al-Qaïda pour le Maghreb Islamique), au Yémen précisément (Al-Qaïda pour la Péninsule Arabique), dans le désert sahélien, comme d'autres mouvements islamistes tel Boko Haram. Daech, avant-dernier âge du terrorisme islamique dans la typologie de

Gilles Kepel, a métastasé depuis l'Irak moribond, s'est autoproclamé califat du Levant avant d'être démantelé militairement par les grandes puissances. Mais Daech reprend vie depuis des cellules dormantes résistantes, activant un quatrième âge de l'islamisme, celui du « djihadisme d'atmosphère » défini par Gilles Kepel<sup>27</sup>. Ce risque géostratégique est partout et nulle part, il peut être très structuré et déclenché à distance comme les vagues d'attentats en France en 2015, les assassinats des professeurs Samuel Paty en octobre 2020 ou de Dominique Bernard en octobre 2023. Un risque qui vise à générer la terreur, mobiliser et occuper des forces de sécurité considérables, voire à semer la discorde dans la communauté nationale. Pour Gilles Kepel, les continuités l'emportent massivement sur les ruptures, faisant du bassin méditerranéen et de ses environs un creuset géostratégique depuis près d'un demi-siècle: « La Méditerranée et le Moyen-Orient ont connu dans les quarante ans écoulés des bouleversements immenses, inscrivant cette région au cœur des séismes qui accouchent du nouvel ordre du Monde au XXI<sup>e</sup> siècle. »<sup>28</sup>

Risque géostratégique majeur lié aux « nœuds géostratégiques » ou au renouveau impérialiste, risque géostratégique diffus associé aux conflits asymétriques et aux marges géographiques propices au développement de guérillas qui optimisent les innovations avec peu de moyens pour un rendement maximal. Le cardinal de Richelieu opposait au début du XVII<sup>e</sup> siècle la « guerre ouverte » à la « guerre couverte »: on pourrait reprendre son *distinguo* pour ce qui est du risque géostratégique. On aurait grand tort de considérer

que les analyses politiques de Lénine sont mortes avec lui il y a un siècle, le 21 janvier 1924. Dans *Les principes du socialisme et de la guerre de 1914-1915*, Lénine écrit: « La guerre est la continuation de la politique par d'autres moyens (à savoir la violence). Cette sentence célèbre appartient à Clausewitz, l'un des auteurs les plus pénétrants en matière militaire. Les marxistes ont toujours considéré avec juste raison cette thèse comme la base théorique de l'interprétation de chaque guerre donnée; c'est de ce point de vue que Marx et Engels ont toujours envisagé les différentes guerres »<sup>29</sup>. C'est exactement ce que proclame « pacifiquement » le XX<sup>e</sup> congrès du Parti communiste chinois d'octobre 2022, considéré par Bruno Tertrais comme « l'exact inverse de ce que fut celui de son homologue soviétique en 1956. »<sup>30</sup> La Chine tend explicitement à « l'accomplissement du communisme ». Or, ce projet désormais agressif, impérial et maritime heurte la puissance dominante en place des États-Unis. Une rivalité géostratégique qui ne peut durablement se maintenir sous la forme d'un « duopole », qui est « instable stratégiquement, car les États-Unis et la Chine veulent chacun le leadership mondial »<sup>31</sup>



### Notes

<sup>1</sup> Philippe Boulanger, *Introduction à la géostratégie*, Repères, La Découverte, 2023.

<sup>2</sup> Philippe Boulanger, *Introduction à la géostratégie*, Repères, La Découverte, 2023, p. 44. Le texte précise: « (selon) Lucien Poirier dans sa postface aux Transformations de la guerre du général Jean Colin, (1989) ».

<sup>3</sup> En 1975 dans le Larousse encyclopédique selon le dictionnaire *Trésor de la langue française*, article « géostratégie ».

<sup>4</sup> Emmanuel Kant, *Vers la paix perpétuelle*, 1795.

<sup>5</sup> La « der des ders », cri de ralliement des anciens combattants français après la Première Guerre mondiale pour dire que la boucherie à laquelle ils avaient échappé serait la « dernière des dernières guerres ».

<sup>6</sup> Thomas Friedman, *La terre est plate : une brève histoire du XXI<sup>e</sup> siècle*, 2005.

<sup>7</sup> Francis Fukuyama, *La fin de l'histoire et le dernier homme*, 1992.

<sup>8</sup> Le Pacte d'Aristide Briand et de Frank Kellogg, du nom du ministre français des Affaires étrangères et de son homologue secrétaire d'État américain, également appelé Traité de Paris, est signé le 27 août 1928. Soixante-trois pays « condamnent le recours à la guerre pour le règlement des différends internationaux et y renoncent en tant qu'instrument de politique nationale dans leurs relations mutuelles. »

<sup>9</sup> Henry Kissinger, *L'ordre du Monde*, 2014, édition française éditions Fayard 2016, chapitre II « Le système européen d'équilibre des forces et sa fin », p. 67.

<sup>10</sup> Élie Barvani, *Dix thèses sur la guerre*, Flammarion, 2014, p. 136.

<sup>11</sup> *Le Point*, 5 septembre 2014.

<sup>12</sup> Henry Kissinger, *L'ordre du Monde*, 2014, édition française éditions Fayard 2016, chapitre II « Le système européen d'équilibre des forces et sa fin », p. 340.

<sup>13</sup> Bernard Esambert, *Le troisième conflit mondial*, Plon, 1977 et *La guerre économique mondiale*, O Urban, 1991.

<sup>14</sup> Michel Foucher, « Le nouvel environnement géostratégique. Un aide-mémoire aux Européens », *Le Débat*, 2016/3, n°190.

<sup>15</sup> Gérard Chaliand, *Pourquoi perd-on la guerre ? Un nouvel art occidental*, Odile Jacob, 2016

<sup>16</sup> Raymond Aron, *Penser la guerre, Clausewitz. 2. L'âge planétaire*, Gallimard, Tel, 1976.

<sup>17</sup> Thomas Gomart, *L'accélération de l'Histoire. Les nœuds géostratégiques d'un monde hors de contrôle*, Tallandier, 2024, p. 35.

<sup>18</sup> Raymond Aron, *Penser la guerre, Clausewitz. 2. L'âge planétaire*, Gallimard, Tel, 1976.

<sup>19</sup> Philippe Boulanger, *Introduction à la géostratégie*, Repères, La Découverte, 2023, p. 102.

<sup>20</sup> Thomas Gomart, *L'accélération de l'Histoire. Les nœuds géostratégiques d'un monde hors de contrôle*, Tallandier, 2024, p. 171

<sup>21</sup> « D'origine économique, le basculement de la Chine vers la mer s'accompagne d'une montée en puissance navale spectaculaire. Entre 2008 et 2030, le réarmement naval de la Chine sera de +138 %. La marine chinoise dépasse d'ores et déjà la marine américaine en nombre de bâtiments et devrait aligner 450 unités contre 360 aux États-Unis à l'horizon 2030. À cette flotte s'ajoutent

les garde-côtes armés de 1000 navires et la milice maritime composée des bâtiments de la marine marchande utilisés à des fins de renseignement ou d'action hybride » Thomas Gomart, *L'accélération de l'Histoire*, 2024, p. 30.

<sup>22</sup> Valérie Niquet, « Taïwan : point nodal des enjeux de l'Indopacifique », *Conflits*, Mars 2023.

<sup>23</sup> Valérie Niquet, *Taïwan face à la Chine. Vers la guerre ?* Tallandier, 2023.

<sup>24</sup> « Un rappel d'importance : la Chine et la Russie n'ont plus de différend frontalier, contrairement à la Chine et l'Inde. », Alice Ekman, *Russie-Chine. Le grand rapprochement*, 2023, p.21.

<sup>25</sup> Nicolas Werth, *Poutine historien en chef*, Gallimard, 2022.

<sup>26</sup> Nicolas Baverez, *Démocraties contre empires autoritaires*, L'Observatoire, 2023, p. 27-28.

<sup>27</sup> Gilles Kepel, *Le prophète et la pandémie. Du Moyen-Orient au djihadisme d'atmosphère*, Gallimard, 2021.

<sup>28</sup> Gilles Kepel, *Sortir du chaos. Les crises en Méditerranée et au Moyen-Orient*, 2018, p. 449.

<sup>29</sup> Lénine, *Les principes du socialisme et de la guerre de 1914-1915*, t 21 p 314, cité par Raymond Aron, *Penser la guerre, Clausewitz. 2. L'âge planétaire*, Gallimard, Tel, 1976, p. 330.

<sup>30</sup> Bruno Tertrais, *La guerre des Mondes*, L'Observatoire, 2023, p. 106.

<sup>31</sup> Christian Saint-Etienne, *TRUMP et XI, les apprentis sorciers*, Chapitre 5 Un nouveau conflit mondial peut-il éclater d'ici à 2025?, *L'Observatoire*, 2020, p 190.

SECTEUR À LA LOUPE

# La presse écrite à l'épreuve des plateformes

Le marché publicitaire digital est de plus en plus dominé par les grandes plateformes américaines et chinoises. Que reste-t-il pour les médias traditionnels ?

Journaux, sites d'information, radios, télévision... les médias dits « traditionnels » sont de plus en plus confrontés au rouleau compresseur des plateformes numériques et des réseaux sociaux dont l'expansion continue. Tour d'horizon en données pour comprendre les enjeux du secteur.



**DOMINIQUE SEUX**  
Directeur délégué de la rédaction, *Les Échos*, éditorialiste France Inter

## La publicité digitale est en train de passer la barre des 10 milliards d'euros en France

Elle représente désormais près des deux tiers de la publicité totale dans notre pays. Et face à cette publicité en ligne qui a triplé en dix ans, la publicité à la télévision et dans la presse stagne, tandis que la publicité à la radio, si elle progresse un peu, reste très éloignée de ces niveaux.

Plus marquant encore, la publicité digitale se concentre davantage chaque jour sur quelques plateformes bien connues de tous : Google, YouTube, Instagram, Facebook, Amazon, Twitch, TikTok et X. Tous ces acteurs non-européens pèsent à eux seuls 78% du marché !

## Il ne reste pas beaucoup de place pour les supports tricolores

Ça, c'est le plus spectaculaire. Mais maintenant, le plus important est que dans cette centrifugeuse de la publicité, ce sont les éditeurs de contenus écrits, les médias écrits, en ligne, qui sont le plus en difficulté.

Ils essaient d'attirer de la publicité digitale, mais ils perdent le match du volume – celui des vidéos. Ils essaient de se financer par les abonnements, mais ont du mal à monter leurs prix et leur nombre ne peut pas grimper à l'infini.

Car tout le monde ne peut pas être le *New York Times*, qui a plus de 10 millions d'abonnés numériques, mais qui est une marque mondiale, en anglais.

## Bref, la presse écrite craint l'asphyxie

Comment faire ? Les éditeurs de presse généraliste, qui couvrent toute l'actualité avec des articles longs et des rédactions puissantes, cherchent tous azimuts des solutions.

Ils vont peut-être finir par se rallier un jour à des solutions non-libérales en demandant au législateur de contraindre les plateformes numériques à leur reverser plus d'argent quand elles utilisent leurs contenus. Ou forcer les annonceurs à mieux répartir les publicités comme Canal+ finance le cinéma.

## C'est insatisfaisant. Il faudrait trouver mieux

Mais il y a un enjeu d'information plurielle – n'ayons pas peur des mots.

Justement, un dernier mot, peut-être ? Sur la place de la pub en France (sous toutes ses formes, là). Sa place (en milliards) est deux fois moins importante ici qu'au Royaume-Uni et en Allemagne et 18 fois moins présente qu'aux États-Unis. La France, c'est le Canada, pas plus. Il y a un décalage entre la dénonciation fréquente ici de l'ultraconsommérisme et la réalité factuelle. Ce n'est pas la première fois.

## Note

Dominique Seux nous a aimablement donné son accord pour publier dans nos colonnes cet édito éco lu sur France Inter le 7 février 2024.

LES DÉBATS DE RISQUES

# La hausse des prix dans l'assurance est-elle une fatalité ?

  
**Débat animé par**  
**Jean-Hervé Lorenzi,**  
**directeur de la rédaction**  
**de la revue *Risques*,**  
**Pierre Bollon,**  
**Arnaud Chneiweiss**  
**et Pierre-Charles Pradier.**

Olivier Gayraud, juriste au sein de l'association Consommation, logement et cadre de vie (CLCV), Bertrand Labilloy, directeur général de CCR Re, Séverine Salgado, directrice générale de la Mutualité Française (FNMF), et Catherine Touvrey, directrice générale d'Harmonie Mutuelle, se sont réunis le 6 mars 2024 à l'invitation du comité éditorial de *Risques* pour débattre de la question de la hausse des prix dans l'assurance.



**OLIVIER GAYRAUD**



**BERTRAND LABILLOY**



**SÉVERINE SALGADO**



**CATHERINE TOUVREY**

## Risques Comment la hausse des primes d'assurance peut-elle s'expliquer ?

### Olivier Gayraud

Les primes d'assurance subissent, année après année, une forte augmentation. De plus en plus marquée, cette hausse n'est pas tenable et suscite, à juste titre, l'inquiétude de nos concitoyens. Présentée comme une quasi-fatalité, la situation est difficilement compréhensible. Lorsqu'on les interroge, les entreprises d'assurance justifient la hausse des prix en auto par le coût des pièces détachées ou encore par celui de la main d'œuvre. Pourtant, des dispositifs spécifiques existent et pourraient permettre de baisser les prix, comme le système des garages agréés ou le recours aux pièces de réemploi. En habitation, les démarches des entreprises d'assurance pour aider les assurés à lutter contre le vol, comme la télésurveillance, demeurent embryonnaires et pas suffisamment incitatives. Enfin, l'intensification des catastrophes naturelles soulève la question de l'aménagement du territoire : est-il encore raisonnable de continuer à construire partout ? Je redoute le moment où s'assurer deviendra trop cher pour certains consommateurs.

### Séverine Salgado

En vingt ans, les dépenses de santé ont été multipliées par deux. Elles sont passées de 109 milliards à 221 milliards d'euros. Sur la même période, les taxes sur les complémentaires santé ont été multipliées par huit. Or il n'y a pas d'argent magique ! La consommation de soins en France ne fait qu'augmenter, c'est assez logique d'un point de vue économique puisque la santé fait partie de ce qu'on appelle les *luxury goods*. Les dépenses de santé augmentent plus vite que la richesse nationale et que l'inflation, et elles augmentent pour tout le monde : + 36 % sur dix ans pour la sécurité sociale, + 37 % pour les organismes complémentaires et + 6 % pour les ménages. Dans le secteur des complémentaires santé, cette hausse se répercute mécaniquement sur les cotisations. Pour les mutuelles, celles-ci ont augmenté en moyenne de 8,1 % pour cette année, jamais un tel niveau n'avait été atteint. Naturellement, je rejoins M. Gayraud, une telle situation ne satisfait personne puisque nous avons tous la même préoccupation : celle de la soutenabilité des cotisations. Nous devons donc trouver un moyen de modérer la hausse des prestations et donc de casser la courbe des maladies chroniques et trouver une parade aux impacts du vieillissement démographique. On pourrait baisser le niveau des prestations et des garanties mais je ne suis pas sûre que les « consommateurs » en soient satisfaits. On peut également mener des actions de prévention, gérer le risque ou lutter contre la fraude par exemple, mais dans un premier temps cela se répercutera sur les frais de gestion. Il faut aussi parfois voir les dépenses comme des investissements même si ce n'est pas évident quand on reçoit son appel de cotisation, j'en ai bien conscience.

## Risques Pourquoi la concurrence, qui est très forte dans le secteur de l'assurance, n'a-t-elle pas fait baisser les prix ?

### Catherine Touvrey

La concurrence accrue dans notre secteur s'est au contraire traduite par une hausse des prix. On voit bien l'impact des coûts d'acquisition sur les frais de gestion car les taux de marge n'ont pas augmenté de façon significative. Une autre chose qui me frappe, c'est la part croissante des dépenses liées à la *compliance* et au déploiement d'outils numériques ou digitaux. Ces outils n'ont pas fait baisser les prix, avant tout pour des raisons d'échelle. Pour tirer le plein parti des investissements dans tous ces outils, il faudra avoir atteint de très gros volumes.

**Nous avons tous la même préoccupation : celle de la soutenabilité des cotisations.**

### Séverine Salgado

Si l'intensité concurrentielle en complémentaire santé ne s'est pas répercutée sur les prix, c'est aussi parce qu'il s'agit d'un marché très imparfait, très atypique à la fois hyper-concurrentiel et hyper-régulé, hyper-réglementé. Ainsi, les acteurs se sont concentrés pour pouvoir répondre à la concurrence tout en proposant à peu près les mêmes offres, les mêmes garanties. Le panier du contrat solidaire et responsable constitue un socle obligatoire qui est déjà très élevé, obérant les marges de manœuvre et d'innovation et donc la différenciation que l'on pourrait légitimement attendre d'un marché concurrentiel non-faussé.

### Bertrand Labilloy

Contrairement à beaucoup d'autres pans de l'activité commerciale et industrielle qui sont très largement délocalisés, l'assurance est un service 100 % local. L'ouverture des frontières a tiré la moyenne des hausses de prix vers le bas mais l'assurance n'a pas bénéficié de cet effet. Vous avez dit que l'assurance était un *luxury good* : j'observe qu'en ce qui concerne la garantie des catastrophes naturelles, on a élargi au fur et à mesure le champ de l'indemnisation en y ajoutant de nouvelles garanties sans en augmenter le prix. J'aurais tendance à faire le parallèle entre l'assurance et les

dépenses publiques. Beaucoup considèrent l'assurance comme une dépense forcée, à moitié publique. Ce n'est pas très clair dans l'esprit de nos concitoyens qui veulent toujours plus de services publics et toujours moins d'impôts : c'est la même chose pour l'assurance.

Enfin, il ne faut pas négliger le fait que l'assurance responsabilité, mais aussi certaines branches d'assurance dommages, sont des activités à déroulement long, avec un écart important entre le moment où l'on paye la prime et le moment où l'on touche une éventuelle indemnisation. Ce phénomène, qu'on nomme cycle inversé de l'assurance, est favorable pour tout le monde dans les phases de désinflation parce que l'on bénéficie de conditions et de services meilleurs que ce qui avait été tarifé ; inversement, dans les périodes de résurgence brutale de l'inflation, ce que nous avons vécu l'an dernier, c'est l'inverse qui se produit. J'ai été très surpris d'entendre les pouvoirs publics demander aux assureurs de bloquer les prix alors que le choc inflationniste avait déjà été encaissé au niveau de leur bilan. C'est quelque chose d'important à souligner.

**Nos concitoyens veulent toujours plus de services publics et toujours moins d'impôts : c'est la même chose pour l'assurance.**

## Risques La prévention est un axe de travail fort des assureurs. Comment l'envisagez-vous ?

### Catherine Touvrey

Il est nécessaire de s'interroger sur la manière dont les problèmes peuvent être évités au lieu de s'en tenir à les rembourser. Nous disposons d'un levier, celui de la prévention. Ce sujet est à la fois collectif et individuel. Collectif dans le sens où il y a des normes à renforcer, des interdictions à poser : en assurance santé, si je prends le seul sujet de l'alimentation, on voit bien à quel point la marge de progression est encore importante. Je pense notamment à l'alimentation des bébés que l'on habitue dès la naissance à certains goûts, ce qui ne va pas sans provoquer dès le plus jeune âge des addictions. Ajoutez à cela la sédentarité et

vous avez les problèmes de santé publique que l'on connaît aujourd'hui et qui commencent déjà à entraîner des répercussions sur l'assurance. Le sujet est aussi individuel puisqu'il nécessite de changer les comportements, d'informer, d'accompagner nos concitoyens pour passer d'une façon de vivre à une autre. J'ai l'habitude de dire que ce n'est absolument pas rationnel. Si ça l'était, aucun médecin ne fumerait car 100% des médecins savent que la cigarette n'est pas une bonne chose pour la santé, or ils fument autant que le reste de la population. Le sujet est émotionnel et relationnel : l'Institut Pasteur avec l'APHP et l'hôpital Robert-Debré soulignent dans une étude récente que sur 14 000 comptes rendus d'hospitalisation sur les trois dernières années pour tentative de suicide, le facteur explicatif principal est l'explosion des violences intrafamiliales pendant le Covid pour les filles entre 8 et 25 ans. On peut toujours proposer des applications de santé mentale, rembourser les consultations et assurer une prise en charge très onéreuse sur un sujet comme celui-ci, on a bien un sujet de lien social, d'organisation de la société. L'assurance est en quelque sorte une photo des évolutions difficiles de la société.

## Risques Pensez-vous possible que certains de nos concitoyens renoncent à s'assurer ?

### Séverine Salgado

Aujourd'hui, 96% de la population est assurée en santé mais la démutualisation est un risque qui nous préoccupe. L'enjeu est double car il conjugue inassurabilité et concentration du risque sur une partie de la population. Le risque, c'est que certaines franges de la population, notamment les retraités, les inactifs ou les très jeunes actifs, choisissent de ne plus s'assurer ou de souscrire des contrats « non-responsables », avec des garanties moins couvrantes, par exemple uniquement l'hospitalisation. Une solution utopique serait d'en finir avec cette segmentation du risque entre les actifs, les retraités, les personnes à revenus modestes avec la complémentaire santé solidaire, etc. Il y a aujourd'hui près d'une dizaine de régimes d'accès à la complémentaire santé. Une autre, plus réaliste, serait de réintroduire de la solidarité au niveau de la prise en charge de la sécurité sociale qui ne répond plus tout à fait à sa promesse initiale. S'il y a davantage de reste à charge sur les soins liés aux personnes âgées, c'est notamment parce que, contrairement à une idée reçue, le reste à charge hospitalier est très concentré et inégalitaire et n'est pas toujours le mieux pris en charge par la sécurité sociale. L'hôpital est le premier poste de dépenses des mutuelles, 25% de nos dépenses totales. On l'a vu avec le Covid et les séjours en réanimation, certains patients se sont retrouvés avec 10 000 euros de reste à charge !

### Bertrand Labilloy

En matière d'assurance habitation et notamment en dommages aux biens, les effets du changement climatique sont totalement avérés et cette dérive tendancielle est désormais intégrée. Concrètement, cela va se traduire pour les consommateurs par une hausse du taux de surprime de 12 à 20% à partir du 1<sup>er</sup> janvier prochain. Le coût de la garantie cat nat pour un ménage s'élève aujourd'hui à 25 euros en moyenne par an. Cette hausse est significative mais selon une étude récente réalisée par Elabe pour France Assureurs, pour 85% des Français, il faut continuer à assurer les dégâts liés aux conséquences du dérèglement climatique, même si le coût est important.

### Olivier Gayraud

Devant la hausse des cotisations, un assuré va logiquement aller faire jouer la concurrence, mais nos concitoyens maîtrisent assez peu leurs contrats d'assurance et sont tout à fait enclins à souscrire moins cher mais moins couvrant sans s'en rendre compte, ce qui constitue un autre risque très important.

## Risques Un travail de pédagogie vis-à-vis des assurés vous semble-t-il nécessaire ?

### Olivier Gayraud

Il y a un effet un relatif manque de clarté. N'oublions pas que le public a une connaissance très imparfaite de ce qu'est un contrat d'assurance. Il n'est pas rare qu'un assuré découvre qu'il n'est pas couvert au moment du sinistre. Certains de nos concitoyens se retrouvent confrontés à des dommages qui ne rentrent pas dans le cadre de la catastrophe naturelle et ils ne comprennent pas que leur dossier soit refusé alors qu'en parallèle les cotisations des contrats d'assurance pour les catastrophes naturelles augmentent.

### Catherine Touvrey

Je donnerai un exemple concret sur le sujet des montures optiques. Avant le 100% santé, la durée moyenne de remplacement des lunettes était de trois ans. Aujourd'hui, on est descendus à 2,4 années, ce qui représente 17 millions d'euros par an. Ne pourrait-on pas, grâce aux actions en faveur de l'économie circulaire et avec une incitation à un moindre gaspillage, remonter à trois ans ? Ne pourrions-nous pas engager avec les associations de consommateurs, les entreprises, nos propres adhérents, une démarche qui ne s'inscrirait pas dans de la pure consommation ?

En parallèle, nous devons aussi veiller à rendre compréhensibles des dimensions qu'on peut qualifier de macroéconomiques à l'échelle individuelle, ça me semble être un sujet absolument

déterminant. C'est la même chose que la question du dérèglement climatique : mon action individuelle est anecdotique et en même temps, c'est la somme d'actions individuelles anecdotiques qui fera changer les choses. On a donc un sujet à la fois collectif et individuel qui est assez déterminant. Je partage le fait qu'il y a des leviers d'action, des leviers de changement malgré le contrat responsable, malgré le 100% santé. On a besoin de dynamique collective et transparente.

## Risques Y a-t-il un enjeu de transparence vis-à-vis de vos assurés ?

### Catherine Touvrey

Chaque année, les complémentaires santé publient leurs taux de redistribution et celui relatif aux frais de gestion. Il s'agit d'une obligation qui pourrait être étendue à toutes les assurances. Les associations de consommateurs pourraient jouer un rôle dans ce domaine. Lorsque l'on regarde ces doubles indicateurs, on se retrouve parfois face à des situations extrêmement hétérogènes. On pourrait tout à fait imaginer dans l'assurance un certain nombre d'éléments conditionnés à ce double indicateur, qu'est-ce qui l'interdirait ? Chacun pourrait continuer à faire ses choix, à avoir des chargements très différents etc. Chez Harmonie Mutuelle, nous avons décidé de faire du taux de redistribution un engagement d'entreprise. 80% des cotisations appartiennent aux assurés. Si d'aventure, ce taux devait descendre en dessous de ces 80%, l'écart entre ce qui est « économisé » et 80% peut être doté à une provision pour ristourne qui doit être utilisée dans les deux ans, ou vient alors en supplément de prestations ou en économie de cotisation. Quand on explique cela aux assurés, ils ont le sentiment qu'on joue avec eux et pas contre eux. Il s'agit aujourd'hui de l'engagement d'un opérateur : j'invite plus d'opérateurs à prendre des engagements de ce type et à pouvoir les expliciter auprès de leurs assurés.

### Séverine Salgado

Pourquoi les consommateurs souscrivent-ils des contrats d'assurance où les taux de redistribution sont les plus faibles ? C'est là où l'on reboucle avec cette culture ou cette citoyenneté économique ou sociale, il y a vraiment quelque chose à jouer ensemble.

## Certaines compagnies d'assurance exemptent leurs assurés de franchise s'ils installent de la télésurveillance, voilà une bonne pratique !

### Catherine Touvrey

Je souhaiterais partager deux chiffres emblématiques. Si l'ensemble des complémentaires santé proposait un taux de redistribution de 80 %, 1,5 milliards d'euros pourrait être rendu aux assurés. Quant à la lutte contre la fraude, il s'agit d'un service aux assurés puisque c'est une protection de la mutualité contre des comportements déviants. Transposé à la sécurité sociale, cela représente près de 2 milliards d'euros. Ce sont des chiffres significatifs qui peuvent représenter un intérêt en termes de modération des prix. Il est nécessaire d'expliquer aux assurés l'utilité de mener ce travail.

### Olivier Gayraud

Les compagnies d'assurance doivent s'interroger sur la manière de réaliser des économies en interne. Comme on l'a vu, des dispositifs existent en auto ou en habitation : des garages ou des prestataires agréés existent depuis longtemps et je pense que ce sont des voies qui peuvent permettre de modérer les coûts. Certes des aménagements sont intervenus sur les pièces détachées automobiles, la main d'œuvre, la télésurveillance en habitation mais ceci reste encore trop timide. Les cambriolages sont en constante augmentation : pourquoi les assureurs ne pourraient-ils pas subventionner davantage certaines installations pour inciter les assurés à les souscrire ? Certaines compagnies d'assurance exemptent leurs assurés de franchise s'ils installent de la télésurveillance, voilà une bonne pratique ! Ces dispositifs ne sont pas compliqués à mettre en place. Il n'est pas possible que la solution soit exclusivement d'augmenter la facture de l'assuré chaque année.

### Risques

**Avez-vous chiffré ce qui, dans l'augmentation de vos coûts, relève de la réglementation ?**

### Catherine Touvrey

Les frais liés à Solvabilité II dans son ensemble représentent 1 % des primes et peuvent être comptés en surcoût. En revanche, tout ce qui est lié à la Directive sur la distribution d'assurances (DDA) correspond à de la protection du consommateur.

### Séverine Salgado

La CSRD qui va bientôt entrer en vigueur représente à elle seule 1 200 lignes de reporting extra-financier ! En deçà d'une certaine taille de mutuelle, nous avons davantage de salariés dédiés à la gestion de la réglementation qu'au développement même de l'activité de la mutuelle. Le coût de la réglementation qui évolue chaque année est loin d'être négligeable.

### Risques

**En assurance santé, pensez-vous que des discussions sur les paniers de garanties soient envisageables ?**

### Séverine Salgado

Le contrat solidaire et responsable est un outil très pratique pour les pouvoirs publics. Chaque fois qu'on a une nouvelle « bonne idée », on modifie le décret pour la faire figurer dans le contrat responsable. On y a, par exemple, mis les remboursements des fauteuils roulants. Or quand un individu est malheureusement en situation de handicap, il ne s'agit pas d'un aléa donc cela ne relève pas de l'assurance. Il s'agit d'un dispositif de compensation du handicap qui doit relever de la 5<sup>e</sup> branche, celle de la Caisse nationale de solidarité pour l'autonomie. L'intégration des remboursements des protections menstruelles dans le contrat responsable n'a pas de sens non plus puisqu'il n'y a pas d'aléa. Cela ne signifie pas, au contraire, que les mutuelles ne doivent pas proposer de solutions à ces besoins mais il faudrait imaginer d'autres mécanismes plutôt qu'un mécanisme purement assurantiel, des groupements d'achat par exemple ?

### Risques

**Introduire de la capitalisation en assurance santé pourrait-elle être une piste de réflexion ?**

### Catherine Touvrey

Cette idée ne me choque pas : les plans d'épargne retraite (PER) préparent la retraite, pourquoi ne pourrait-on pas imaginer un dispositif similaire pour les dépenses de santé qui augmentent elles aussi ? Aujourd'hui, on raisonne dans une logique annuelle de répartition : est-ce réellement la seule façon de réfléchir ? Je n'en suis pas sûre.

### Risques

**Des actions collectives pourraient-elles être menées ?**

### Olivier Gayraud

Je partage la nécessité de travailler tous ensemble. L'assurance est un contrat qui est mal connu et qui n'a pas forcément bonne presse auprès des gens. L'augmentation de tarifs tous les ans ne peut pas être le seul contact que l'assureur a avec ses assurés.

**Appelons à une forme d'états généraux de la protection sociale. Que veulent mutualiser, socialiser nos concitoyens ?**

### Séverine Salgado

Le terme « pouvoir d'achat » s'adapte aussi à l'assurance : la question est de savoir ce que l'on veut pouvoir « acheter » avec une cotisation assurantielle. Mettons-nous autour de la table, appelons à une forme d'états généraux de la protection sociale. Que veulent mutualiser, socialiser nos concitoyens ? Qu'est-on prêt à faire pour pouvoir ensemble, collectivement, s'assurer contre tel ou tel risque ? Nous poursuivons tous la même finalité, nous aurions donc collectivement intérêt à mieux nous connaître. Nous devons identifier des solutions tous ensemble et les moyens de les appliquer. Il n'y a pas de fatalité. Le chemin sera peut-être un peu long mais nous avons des leviers pour agir. 🗣️

# Pourquoi le secteur européen de l'assurance-vie doit-il innover?

L'Institut Louis Bachelier a organisé, le 23 janvier dernier, un webinaire consacré aux innovations assurancielles en matière d'épargne retraite. La conférence en ligne a réuni trois intervenants : Aymeric Kalife, CEO de iDigital Partners et professeur associé à l'Université Paris-Dauphine - PSL, Alexandre Mincier, expert en investissements pour l'assurance et les fonds de pension, Eric Baesen, senior Manager chez Nexialog Consulting et membre de la commission finance-gestion d'actifs de l'Institut des actuaires. Cette conférence a permis de partager des points de vue de praticiens pour éclairer la situation du secteur de l'assurance, fortement bouleversé par les politiques monétaires.

Depuis le premier semestre 2022, les principales banques centrales de la planète ont entamé une forte remontée des taux d'intérêt pour faire face à l'inflation. Nuls en 2021, les taux directeurs de la Banque centrale européenne (BCE) et de la Réserve fédérale des États-Unis (Fed) ont atteint respectivement 4,50% et 5,25% en janvier 2023. Cette forte hausse des taux directeurs, sur une période aussi courte, a généré un choc majeur sur le marché de la gestion actif-passif, comme l'a souligné Alexandre Mincier, expert

en investissements pour l'assurance et les fonds de pension, à l'occasion d'un webinaire organisé par l'Institut Louis Bachelier. Alors que la stratégie des assureurs a été conçue pour des taux structurellement baissiers, comme cela a été le cas au cours des dernières décennies, ce nouveau contexte restreint leur capacité à offrir du rendement à leurs clients. L'attrait des investisseurs pour les produits commercialisés durant la dernière décennie s'est donc réduit, en particulier pour l'assurance-vie.

## Les produits alternatifs ont montré leurs limites

La période de taux bas, voire négatifs est probablement révolue, ce qui oblige le secteur de l'assurance à réinventer ses produits. Ces dernières années, les investissements alternatifs, à l'image des fonds euros diversifiés, n'ont pas permis de répondre à la demande. Les produits proposés ne sont pas parvenus à garantir le « triptyque de l'assurance-vie », à savoir sécurité, disponibilité, rentabilité,

d'après Aymeric Kalife, CEO de iDigital Partners et professeur associé à l'Université Paris Dauphine - PSL. En effet, les structures alternatives se caractérisent par des limites importantes telles que des frais élevés, un manque de lien entre assureur et assuré, une absence de transparence et une faible attention portée aux événements de la vie.

La période actuelle, marquée par un stock massif de produits d'assurance – seulement 6 à 8% des investissements sont renouvelés

chaque année – et un dynamisme réglementaire (ESG, protection du consommateur) apparaît propice pour structurer des produits innovants. L'exemple américain, précurseur, peut servir d'inspiration. Des produits comme les rentes indiciaires, les mécanismes de protection à la baisse et les rentes viagères représentent aujourd'hui la majeure partie du marché outre-Atlantique. Les assurés profitent ainsi des opportunités de marché, tout en étant protégés en cas de baisse. De même, le capital-risque, apparu durant les années 1980 aux États-Unis, ne se développe que depuis une décennie en Europe.

## Gestion pilotée et garantie en capital

Des exemples de produits innovants existent tels que la gestion pilotée à horizon d'un plan d'épargne retraite (PER) couplée à une garantie en capital, comme l'a présenté Eric Baesen, senior Manager chez Nexialog Consulting et membre de la commission finance-gestion d'actifs de l'Institut des actuaires. Le produit combine les atouts des fonds en euros (garantie et prévisibilité) avec le dynamisme d'une gestion pilotée.

Le nouveau plan d'épargne retraite (PER), créé en 2019 par la loi Pacte en remplacement des plans d'épargne existants, permet de placer des sommes pour bénéficier à une date donnée – au départ à la retraite – d'une rente ou d'un capital. Le PER individuel est ouvert à tous les individus majeurs et les sociétés peuvent aussi proposer à leurs salariés un PER d'entreprise. Le PER individuel peut donner lieu à l'ouverture d'un compte-titre ou à l'adhésion à un contrat d'assurance de groupe et donc l'accès à un fonds en euros, où le

**Les assurés profitent ainsi des opportunités de marché, tout en étant protégés en cas de baisse.**

capital est garanti. En principe, le PER est géré suivant le principe de la gestion pilotée (75% des cas). Celle-ci a pour but d'orienter l'épargne vers l'économie productive, ce qui améliore les perspectives de rendements pour les souscripteurs. Le choix des actifs investis en gestion pilotée dépend de deux critères : la durée restante avant le départ à la retraite – plus il se rapproche, moins les actifs sont risqués et donc plus la part des fonds en euros augmente – et le profil d'investisseur (prudent, équilibré ou dynamique).

## La performance d'un produit avec capital garanti est satisfaisante

La solution retenue par Nexialog consiste à enrichir la gestion pilotée avec une protection du capital optionnelle. Cette garantie est facturée à l'épargnant par un taux de chargement plafonné sur l'encours. En contrepartie, l'assureur paye l'option capital protégé à l'échéance. Évaluer la prime de l'assurance revient ainsi à déterminer le prix d'un *put*, correspondant à une option de vente dans la célèbre formule de Black-Scholes. En supposant une sur-performance de la part des unités de compte de 4% sur un horizon de vingt ans et

aux conditions de taux actuel, la structure non-protégée réalise environ 3,3% de surperformance et la version protégée 2,9%. Cette solution protégée est ainsi une bonne alternative aux fonds en euros.

Des alternatives sont envisageables, susceptibles de rétablir le triptyque « sécurité, disponibilité, rentabilité ». Aymeric Kalife a présenté un « Fonds euros hybride » à deux facettes : 1 un Fonds en euros (30-40% de la prime, disponible à tout moment), 2 des unités de

compte à capital garanti (bruts de frais) et 4,5% de rendements annuels minimums garantis à terme (10 ans, en ligne avec la durée de détention usuelle d'un Fonds en euros). Ce type de structure à frais de gestion inférieurs à 2% (protection de l'assuré) offre à l'assuré un rendement global net de frais empirique supérieur à 5,5% par an, tandis qu'elle double les marges et réduit de deux tiers les risques et le coût du capital pour l'assureur (les risques de marché sont entièrement portés par le partenaire bancaire, les risques de rachats sont pris en compte via une tarification intégrant une efficacité et réactivité comportementale). L'expérience client peut être encore étendue via l'ajout à faible coût de garanties « cliquets », permettant de « locker » les périodes fastes et de profiter des rebonds de marché.

Alexandre Mincier a rappelé que l'élément clé pour le client est la garantie en capital. C'est ce qui différencie l'assurance d'une banque privée ou d'un gestionnaire d'actifs. Dès lors, la priorité des assureurs doit être d'offrir une protection à la baisse, tout en permettant à l'assuré de profiter d'un contexte de marché haussier. La coopération entre l'ensemble des acteurs (fonds d'investissements, banques,

assurances) est donc indispensable pour proposer des produits innovants, ce qui est d'ailleurs le cas aux États-Unis où la réglementation exige un dialogue entre les différents acteurs, contrairement à l'Europe.

## Facteurs comportementaux et réglementaires

Des interrogations persistent. La première sur les causes d'une différence entre les marchés américain et européen qui s'explique d'abord par l'aspect réglementaire : le régulateur américain oblige les acteurs à échanger, ce qui induit plus d'innovation. Mais la réticence des Européens à investir dans les actions est également un facteur différenciant entre les deux zones.

Ensuite, quelle attitude adopter dans une perspective de baisse des taux en 2024? Si une ou plusieurs baisses sont envisageables, les taux presque nuls de la dernière décennie ne reviendront probablement pas de sitôt. Toutefois, cette nouvelle donne devrait aussi inciter les gestionnaires d'actifs à se tourner vers les marchés actions, trop souvent délaissés.

Enfin, reste la question de la faible appétence des Européens pour le risque, qui serait d'abord générationnelle. Aymeric Kalife confirme qu'il observe chez ses étudiants un intérêt grandissant pour l'investissement. Il souligne, en particulier, les progrès de l'éducation financière. Toutefois, Alexandre Mincier y voit une limite. À l'avenir, les tarifs élevés de l'assurance pourraient refroidir des clients mieux informés, plutôt à la recherche de rendement chez des gestionnaires d'actifs que d'une garantie. En clair, le besoin d'innovation des assureurs européens devrait donc se maintenir pour satisfaire les épargnants. 📌

# Livres



Henry Farrell, Abraham Newman, **Underground Empire: How America Weaponized the World Economy**, Henry Holt.

Récemment, nous avons présenté dans ces colonnes les livres de Nicole Perloth et Mark Galeotti, qui décrivent l'instrumentalisation guerrière des hackers d'une part, et d'autre part de rien moins que «tout». L'ouvrage d'Henry Farrell et Abraham Newman donne une remarquable clé de lecture politique pour les décideurs économiques. Remarquable, car dans cette instrumentalisation guerrière devenue universelle, ni vous, ni votre entreprise ne pouvez vous abstenir de *prendre parti*. Il faut donc vous situer, et l'ouvrage vous aidera à le faire. Vous pourriez même y prendre un certain plaisir, tant les auteurs déploient de talent dans le récit des trente dernières années. Vous croyiez les avoir vécues? Il vous reste à visiter l'envers de l'histoire contemporaine.

Les trois premiers chapitres montrent la constitution de la puissance américaine: on parcourt d'abord «le monde de Walter Wriston», patron de Citibank entre 1967 et 1984. Cet homme réservé a cherché à soustraire son entreprise à l'emprise autoritaire des États: pour cela il a réinventé les métiers de la banque et ouvert la voie à la mondialisation. L'ironie de l'histoire est que c'est précisément la volonté de se mettre à l'abri des ingérences étatiques qui a permis de constituer une arme

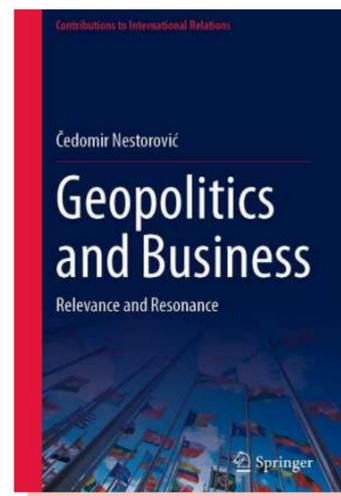
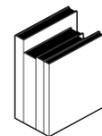
au profit de l'État américain, comme le montre la suite. Le deuxième chapitre détaille comment la National Security Agency (NSA) a réussi à reprendre le contrôle des communications numériques, donnant aux États-Unis un avantage décisif en termes d'information. Cela a permis au Trésor américain d'étouffer toute institution financière en s'assurant que ses sanctions soient respectées. Le troisième chapitre décrit la guerre entre les États-Unis et Huawei, qui a commencé lorsque Huawei a menacé le monopole américain sur les commutateurs Internet. Cette guerre a révélé deux nouvelles armes des États-Unis: l'accès à la technologie américaine et l'accès au renseignement américain pour les alliés. Au terme de ce parcours, il apparaît que Carrie Lam, la gouverneuse qui met Hong Kong au pas, ne peut se faire payer qu'en liquide car aucune banque même en Chine n'accepte de lui ouvrir un compte par crainte des sanctions secondaires. Aucun pays au monde ne peut rivaliser avec la capacité d'intimidation des États-Unis.

Aucun? Sauf peut-être l'Union européenne, qui a co-construit le gazoduc russe pendant les années 1990 malgré les menaces américaines. Le quatrième chapitre relatif à l'Europe mérite toute l'attention française. Notre pays est mentionné brièvement comme le seul État membre qui ait exprimé sans ambiguïté et de manière répétée par la voix du président de la République une volonté d'indépendance stratégique face au risque que représente la Russie, dans un contexte de montée de l'isolationnisme américain. Par contraste, les auteurs montrent comment la grande coalition allemande a écrasé depuis la guerre froide le débat sur l'indépendance stratégique pour bénéficier du double dividende de la paix d'une part et d'autre part de la stratégie russe de fournir le gaz à bas prix pour se doter le moment venu d'un instrument de chantage. Seuls les Verts ont combattu récemment le deuxième gazoduc et embrassé l'indépendance stratégique comme un sous-produit de la transition énergétique. Dans leur analyse nuancée des complexités allemandes, les auteurs soulignent le rôle tout à fait inattendu qu'Ursula von der Leyen a joué dans l'organisation d'une résistance européenne à l'agression russe en Ukraine, et qui n'a pas manqué de surprendre Vladimir Poutine autant que les Américains.

Le cinquième chapitre montre que les entreprises ne peuvent pas ne pas prendre parti. Entre autres exemples, on voit comment Microsoft a bâti un empire du lobbying, tenté de convaincre les États de la nécessité d'une convention «de Genève» pour protéger les civils des cyberattaques qui aurait permis aux entreprises du secteur informatique d'échapper à l'instrumentalisation guerrière... avant de mettre toute sa capacité technologique au service de l'Ukraine attaquée. Le récit du blocage de *Tornado Cash* par l'OFAC est remarquable à plus d'un titre: c'est un roman d'espionnage où les auteurs éclairent les enjeux, c'est-à-dire que même les cryptos ont plié le genou devant la puissance américaine. Nous ne pouvons plus nous dérober, il faut prendre parti.

Le dernier chapitre circonscrit les limites de la puissance: les entreprises comme les États font de leur mieux pour la contourner. En particulier, la Chine développerait à marche forcée son industrie des semi-conducteurs et sa monnaie numérique de Banque centrale en réponse aux menaces américaines, et les sanctions contre la Russie auraient traumatisé jusqu'à l'Arabie saoudite qui cherche les voies d'une indépendance stratégique dans la conversation à plusieurs voix. Autant dire que le monde change et que la primauté américaine est menacée, mais le propos des auteurs va au-delà du constat. Ils montrent d'abord que, contrairement à la guerre froide qui avait trouvé avec la théorie des jeux une représentation de la situation et un langage permettant de désamorcer l'escalade, l'absence de représentation partagée et de langage commun nous expose au risque d'embrasement. Pour *dé-risquer*, puisque c'est le terme à la mode, et qui résonne avec le titre de cette revue, les auteurs proposent un chemin de paix et de *prospérité partagée*. A la veille de l'élection présidentielle américaine, on aimerait croire qu'ils seront entendus. Et on lira avec profit et avec bonheur leur récit en attendant le sort des urnes, et en espérant avec Paul Claudel que le pire n'est pas toujours sûr.

**Pierre-Charles Pradier**



Cedomir Nestorovic, **Geopolitics and Business – Relevance and Resonance**, Springer, 2023.

Il y a vingt ans, Cedomir Nestorovic s'était fait connaître en publiant le manuel du cours de marketing «en environnement islamique»<sup>1</sup> à l'ESSEC. Il avait donc une demi-douzaine d'années d'avance sur la vogue de la finance islamique chez les professionnels, et deux sur le grand public. On peut donc s'attendre à ce que l'auteur ait des idées originales sur un sujet qui s'est installé dans l'actualité.

Le premier chapitre propose un cours de géopolitique tout ce qu'il y a de plus traditionnel en apparence: on y introduit les concepts de base – État-nation, empire, pouvoir – les questions fondamentales – pourquoi les États existent-ils? Qu'est-ce qui fait leur puissance? Y a-t-il un déterminisme géographique? – les auteurs classiques et les écoles de pensée. Nestorovic n'hésite pas à rappeler les problèmes de la discipline, comme l'association du concept de *Lebensraum* avec l'expansionnisme nazi, non pour se donner le rôle de procureur, mais pour inviter à prendre du recul. Le lecteur comprend assez rapidement que l'auteur le conduit à la frontière de l'Orient et de l'Occident, à la rencontre des générations montantes dans le souvenir de celles qui s'effacent pour ouvrir les horizons. Ce prof à

l'établissement singapourien de l'ESSEC fait dialoguer les auteurs allemands du siècle passé avec la pensée chinoise contemporaine, qu'elle s'exprime en République populaire ou à travers la diaspora, notamment dans les universités californiennes. Il écrit pour ses étudiants en école de management, et il entend évidemment mettre son savoir au service de l'action.

C'est là que l'affaire devient inhabituelle, puisque Nestorovic s'intéresse aussi aux pensées *marginales*. Par exemple la pensée *critique* développée notamment par les philosophes français et dans les sciences sociales au tournant des années 1960 et 1970 fait l'objet du deuxième chapitre. L'auteur ne prend pas de détour pour indiquer d'emblée que «la géopolitique critique n'a pas pour objet de résoudre les problèmes», mais, en substance, de comprendre *comment* un problème existe, ce qui peut permettre de le contourner ou de le penser différemment. Il présente donc un mini-manuel de pensée déconstructionniste à l'usage des personnes intéressées aux affaires, non seulement pour parfaire leur culture générale, mais aussi parce que l'entreprise peut avoir besoin d'une pensée clé en main pour asseoir sa légitimité face aux États, aux élites ou aux religions qui tenteraient de l'incriminer. La pensée critique au service du capitalisme entrepreneurial, il fallait y penser et le faire: Nestorovic montre par des exemples comment cela est possible.

Le lecteur de plus de 50 ans goûtera certainement, s'il a la patience de lire, le troisième chapitre consacré à la géopolitique féministe, qui n'est pas réduite à une géopolitique en faveur des femmes, c'est-à-dire à une forme d'idéalisme dans les choix politiques. Pour l'auteur, le féminisme c'est d'abord (mais pas exclusivement) une attention aux sujets *infra-politiques* comme la question du corps, de la propriété de soi, de «l'agentivité», c'est-à-dire de la capacité à agir volontairement en société. La domination n'étant pas l'exclusivité des femmes, l'affirmation féministe donne aussi la parole aux minorités, interroge les identités, la notion de réciprocité et bien sûr l'origine et les usages sociaux de la connaissance. On entend le prof attentif en dialogue avec ses élèves, on bénéficie de l'expérience



## Note

<sup>1</sup> Cedomir Nestorovic, *Marketing en environnement islamique*, Dunod, 2004.

de cet Européen qui sait se faire entendre d'une jeunesse dont les repères nous échappent. Le livre est particulièrement précieux pour cette mise en forme d'un air du temps qu'on voudrait enfermer dans la dénonciation du *wokisme*, et dont Nestorovic offre des clés de compréhension sans céder sur les principes universalistes.

Après cette mise en place assez touffue, l'auteur propose un chapitre de mise en œuvre de la *géopolitique des affaires*, qu'il présente comme une série d'études de concepts et de cas d'entreprises pour documenter les notions clés – espace, État, pouvoir – dans les trois registres de l'analyse classique, critique et féministe. Par exemple, la catégorie du *pouvoir* est présentée au prisme de la géopolitique classique, avec une réflexion sur la force militaire – et notamment la difficulté pour une gouvernance civile de maîtriser le complexe militaire-industriel – et sur le dessin des frontières, notamment sur la manière dont les entreprises de l'internet s'y prennent pour représenter l'appartenance territoriale des régions contestées. Par contraste, l'auteur reconnaît sans détour que les paradigmes critiques et féministes n'aiment pas les acteurs économiques, mais comme ils contestent toutes les formes de pouvoir, ils permettent de penser notamment la dialectique entre l'État et l'entreprise transnationale. L'étude de cas sur la stratégie hégémonique de la De Beers illustre de façon tout à fait intéressante la contribution de l'analyse critique. Le point de vue féministe montre que l'autonomisation (*empowerment*) des dominés peut n'être pas qu'un obstacle ou un prétexte mais aussi un levier pour les entreprises.

Les militants déploreront certainement la capacité de Cedomir Nestorovic à récupérer leur discours pour le compte des affaires. C'est évidemment une grande qualité de ce livre dense, nourri d'exemples précieux (par exemple sur le contentieux lié aux concessions minières) et d'une bibliographie très étendue et convoquée à point nommé.

**Pierre-Charles Pradier**

Créée en 1990 avec le soutien de la Fédération Française de l'Assurance, la revue *Risques* apporte des éléments d'analyse et de réflexion sur les grands débats de société et constitue une référence sur les questions de risque et d'assurance. Lieu de débat et de réflexion, cette revue à caractère scientifique réunit un comité composé d'universitaires de toutes les disciplines du risque et de praticiens de l'assurance.

Pour les numéros parus depuis 2000 (numéro 41 et suivants), sur le site <http://www.revue-risques.fr> vous pouvez consulter :

- les éditoriaux du directeur de la rédaction ;
- les chapitres introductifs des responsables de rubrique ;
- un résumé de chaque article ;
- de nombreux articles et entretiens dans leur intégralité.





# risques

n°137  
mars  
2024

ISSN : 1152-9253  
ISBN : 978-2-35588-108-4  
48€