



Emerging Risks

Une évaluation du groupe de travail Emerging Risks
de la commission technique responsabilité civile de l'ASA

ÉDITION N°8, REVISION 2022

Éditeur

Association Suisse d'Assurances ASA
Conrad-Ferdinand-Meyer-Strasse 14
Case postale, CH-8022 Zurich

Comité compétent

Commission technique responsabilité civile, groupe de travail Emerging Risks

Interlocuteur

Patrizio Pelliccia
Secteur Non-vie
patrizio.pelliccia@svv.ch
Association Suisse d'Assurances ASA
Conrad-Ferdinand-Meyer-Strasse 14
Case postale
CH-8022 Zurich

Information juridique

La présente brochure s'entend uniquement comme un outil de diffusion d'informations et d'aide à la prise de décision dans un souci de faciliter les conclusions et les interprétations propres à chaque compagnie. En particulier, elle ne comporte aucune recommandation quant à l'assurabilité de ces risques ou la pertinence de leur exclusion des contrats d'assurance. Elle consiste en un simple état des lieux réalisé en juin 2022 ou plutôt en une sélection du groupe de travail de l'ASA dédié aux risques émergents. Le groupe de travail se réserve le droit de modifier et de procéder à une mise à jour de la brochure en temps voulu. La présente brochure n'a par conséquent pas la prétention d'être exhaustive ni exacte.

Sommaire

Éditeur	2	
Comité compétent	2	
Interlocuteur	2	
1	Résumé	4
2	Tableau des 10 risques émergents sélectionnés	5
2.1.	Remarques liminaires sur la présentation	5
3	Les 10 risques émergents de l'ASA en détail	6
3.1.	Industrie 4.0 / Internet des objets (IdO).....	6
3.2.	Mobilité autonome.....	9
3.3.	Cyberrisques / Cybersilencieux.....	13
3.4.	Robotique / Intelligence artificielle (IA).....	19
3.5.	Adaptation au climat et effets du changement climatique	21
3.6.	Matériaux de construction respectueux du climat	26
3.7.	Pandémie et dommages collatéraux.....	29
3.8.	Risques latents liés aux produits.....	32
3.9.	Responsabilité des entreprises (D&O).....	36
3.10.	Panne d'électricité (panne générale et pénurie d'électricité).....	42
4	Bloc théorique et définitions	46
4.1.	Définition des « risques émergents ».....	46
4.2.	Caractéristiques des risques émergents.....	46
4.3.	Risque lié aux changements – le paramètre spécifique à l'assurance.....	47
4.3.1.	Aspects sociaux / économiques.....	47
4.3.2.	Développements juridiques.....	48
4.3.3.	Développements technologiques et scientifiques	49
5	Risques émergents – Rôle de l'État.....	51
6	Risques émergents – Rôle de l'assureur responsabilité civile ...	52
6.1	Identification précoce des risques émergents par l'assureur	52
6.2	Analyse des risques émergents par l'assureur	53
6.3	Mesures des assureurs en matière de risques émergents	53

1 Résumé

Les nouvelles technologies et l'évolution de la société moderne sont porteuses d'opportunités, mais aussi de risques. Ces risques d'un nouveau genre sont appelés « risques émergents » et concernent notre vie future. Du fait de leur évolution dynamique justement, ils sont difficiles à identifier et à évaluer. La notion de « risques émergents » ne connaît pas de définition universelle. En assurance, elle désigne habituellement les risques susceptibles de survenir dans le futur et affichant une potentialité de sinistres élevée.

Les nouveaux risques peuvent avant tout être induits par le développement technologique (par exemple Internet / génie génétique / nanotechnologie) et les modifications de l'environnement (par exemple changement climatique) ou des dangers inhérents à la situation (par exemple cyberattaques). Mais tout changement de l'environnement social, du contexte politique ou de la situation économique peut également se traduire par des modifications en termes de risques. Ces dernières années, ce sont surtout les domaines de l'environnement, du génie génétique de la nanotechnologie ou/et de l'Internet des objets (IoT) c'est-à-dire de l'industrie 4.0, qui ont été l'objet de l'attention.

Les grands réassureurs et les compagnies d'assurances s'intéressent aujourd'hui de près à cette question. Les personnes chargées de la souscription ont pour mission d'identifier rapidement les nouveaux risques qui sont déjà « pris en compte ou inclus » dans la couverture existante, afin de les analyser en connaissance de cause et de les évaluer correctement.

Afin de soutenir les compagnies membres de l'ASA dans leur gestion des risques émergents, un groupe de travail de l'Association Suisse d'Assurances ASA a élaboré le présent document. Il contient une sélection de risques émergents qui, d'après lui, devraient, pour le moment, être suivis de près. Limités de manière purement subjective à dix risques, ceux-ci ne sont pas classés par ordre de priorité et sont présentés dans un ordre aléatoire :

- Industrie 4.0 / Internet des objets (IdO)
- Mobilité autonome
- Cyberrisques / cybersilencieux
- Robotique / Intelligence artificielle (IA)
- Adaptation au climat et effets du changement climatique
- Matériaux de construction respectueux du climat
- Pandémie et dommages collatéraux
- Risques latents liés aux produits
- Responsabilité des entreprises (D&O)
- Panne d'électricité (panne générale et pénurie d'électricité)

Outre cet inventaire, le groupe de travail présente également dans la brochure une partie théorique avec des définitions et un positionnement des différentes parties prenantes en matière de risques émergents. Fort de ces informations, le lecteur devrait être en mesure d'identifier, de classer et d'évaluer lui-même les risques émergents.

2 Tableau des 10 risques émergents sélectionnés

Industrie 4.0 / Internet des objets (IdO)
Mobilité autonome
Cyberrisques / cybersilencieux
Robotique / Intelligence artificielle (IA)
Adaptation au climat et effets du changement climatique
Matériaux de construction respectueux du climat
Pandémie et dommages collatéraux
Risques latents liés aux produits
Responsabilité des entreprises (D&O)
Panne d'électricité (panne générale et pénurie d'électricité)

2.1. Remarques liminaires sur la présentation

Du point de vue de l'assureur responsabilité civile, les risques émergents mentionnés ici portent en premier lieu sur l'évaluation de ce que l'on appelle les risques liés au changement, à savoir essentiellement les risques en lien avec les évolutions techniques, économiques, sociales et juridiques qui entraînent une modification du paysage des risques, y compris pour les assureurs.

Tous les risques ont été évalués selon une structure uniforme constituée des paramètres suivants :

- description du risque,
- état des connaissances scientifiques,
- perception du risque,
- pertinence en matière de responsabilité civile,
- pertinence en matière d'assurance de la responsabilité civile,
- horizon temporel pour les prétentions assurées.

3 Les 10 risques émergents de l'ASA en détail

3.1. Industrie 4.0 / Internet des objets (IdO)

Dernière adaptation en mai 2022

Description du risque

Ce que l'on appelle la quatrième révolution industrielle (Industrie 4.0) désigne l'utilisation et le rattachement de systèmes cyber-physiques. On entend par là l'association de composants logiciels à des systèmes de production. Ceci s'inscrit dans la droite ligne de l'utilisation des machines à vapeur et de l'introduction d'installations de production mécaniques (1^{re} révolution industrielle), de l'utilisation de l'énergie électrique comme base de la production de masse (2^e révolution industrielle) ainsi que de l'automatisation à grande échelle grâce à l'utilisation étendue des technologies de l'information et de l'électronique (3^e révolution industrielle).

Dans la quatrième révolution industrielle, il est possible d'appréhender toutes les phases du cycle de vie d'un produit – de l'idée d'un produit à son recyclage et son élimination, en passant par son développement, sa fabrication, son utilisation et son entretien. Il est désormais plus facile de concevoir des produits et des solutions sur mesure, qui épousent les souhaits individuels des clients, tout en réduisant parallèlement les coûts de production. La mise en réseau des entreprises le long de la chaîne de création de valeur permet d'optimiser l'ensemble de cette chaîne et pas seulement certaines étapes de production.

La numérisation et l'interconnexion croissantes de l'économie multiplient les points de recoupement entre les différents acteurs. Des normes et des règles uniformes entre les différents secteurs industriels, les questions liées à la sécurité informatique et à la protection des données ainsi que l'organisation future du travail ont ici un rôle central à jouer.

L'utilisation de machines et de robots autonomes et auto-apprenants constitue une autre évolution qui soulève la question légitime de savoir si le système juridique actuel tient suffisamment compte de ces nouveaux développements. Les machines et robots auto-apprenants acquièrent des capacités proches de celles de l'humain en analysant des informations et en prenant des décisions de manière autonome. Dans quelle mesure la législation en matière de responsabilité civile doit-elle être révisée ? Cette question fait actuellement l'objet de discussions au sein du Parlement européen. L'une des interrogations porte sur l'introduction ou non d'une nouvelle catégorie, celles des « personnes électroniques » (*electronic person*) qui, à l'instar des personnes physiques et morales, seraient dotées d'une personnalité juridique propre et devraient assumer une responsabilité (civile). Cela peut ressembler à de la science-fiction, mais c'est la réalité.

La technologie liée à la quatrième révolution industrielle consiste en la connexion d'objets à l'Internet (Internet des objets / IdO, *Internet of Things / IoT*) qui acquièrent de la sorte la capacité de communiquer entre eux de manière autonome via l'Internet (informatique ubiquitaire, *pervasive computing*). Ainsi, des mini-ordinateurs / capteurs / puces de plus en plus petits et intégrés dans les produits sont censés aider les utilisateurs sans que ceux-ci aient besoin d'interagir. Citons pour exemple les « *wearables* », comme les bracelets et montres de fitness connectés ou les capteurs et puces implantés dans le corps, les puces d'identification injectables pour les animaux (également appelées transpondeurs de biopuce), les capteurs de pression des pneus ainsi que les réfrigérateurs qui reconnaissent automatiquement la date de péremption des aliments enregistrés. Dans le

domaine professionnel, le pendant consiste en la surveillance des fonctions corporelles (par exemple la durée du sommeil) comme l'un des éléments de la sécurité au travail.

Le déploiement généralisé des réseaux mobiles 5G favorisera l'évolution des applications IdO en augmentant la transmission des données et la stabilité du réseau. D'un autre côté, l'introduction de la 5G et la densité d'antennes / de pylônes qu'elle induit font l'objet de controverses et pourraient donner lieu à des actions en responsabilité civile si de nouvelles preuves scientifiques devaient être apportées concernant la nocivité des champs électromagnétiques. Outre les effets des champs électromagnétiques sur le bien-être physique, les bandes de fréquences prévues et la puissance des antennes peuvent également entraîner des complications d'un autre ordre, comme le montre l'exemple du débat sur les perturbations possibles des systèmes de contrôle aérien à proximité des aéroports.

La connexion des processus de production à l'Internet et leur contrôle à distance sont tout aussi réels que l'utilisation accrue d'appareils IdO dans la vie quotidienne. Il s'agit par exemple du contrôle et de la commande à distance des systèmes de support de vie, des activités de loisirs, des installations de sécurité et des installations domestiques.

Perception du risque

Les possibilités offertes par l'utilisation de l'Internet et les risques inhérents ne sont pas encore totalement connus dans toute leur ampleur. Les pannes de l'Internet ou la manipulation de données peuvent affecter des pans entiers de l'économie, comme en témoignent les attaques de pirates informatiques (voir Cyberrisques). L'introduction du réseau 5G fait l'objet de controverses, notamment en ce qui concerne les effets potentiellement nocifs pour la santé.

Le passage de la production conventionnelle à l'Industrie 4.0 risque de s'accompagner de problèmes d'interfaces. En particulier lors de la phase de transition, il s'agit d'assurer les recoupements entre la production traditionnelle et la nouvelle production numérique et en réseau.

La panne d'une installation de production pourrait avoir de graves conséquences. En effet, en raison de l'interconnexion accrue des composants, ce ne sont pas uniquement les systèmes directement défaillants qui sont affectés, mais aussi les sous-traitants et fournisseurs éventuellement en lien avec eux. Un tel scénario de sinistres risquerait de déclencher souvent les « couvertures conditionnelles d'interruption de l'activité ».

Pertinence en matière de responsabilité civile

Les principales dispositions légales régissent la responsabilité pour les produits défectueux, le non-respect des dispositions relatives à la protection des données et la responsabilité liée aux activités dangereuses (par exemple l'utilisation de véhicules à moteur). Dans quelle mesure la législation actuelle relative à la responsabilité civile tient-elle compte de ces évolutions ? Cette question fait l'objet de discussions au sein de différentes instances (par exemple : Parlement, industrie, secteur de l'assurance).

Pertinence en matière d'assurance de la responsabilité civile

Assurance de la responsabilité civile d'entreprise

Il s'agit en premier lieu de l'assurance de la responsabilité civile pour les dommages corporels et matériels provoqués par des produits défectueux, des services de qualité médiocre et des activités dangereuses ainsi

que de l'assurance de la responsabilité civile de l'employeur. Si des produits défectueux ou des éléments de ces produits entraînent des dommages corporels et matériels, ceux-ci sont généralement couverts par l'assurance de la responsabilité civile d'entreprise. L'utilisation de systèmes autonomes peut modifier la fréquence des sinistres. Au regard des investissements élevés dans les nouvelles technologies, l'ampleur des dommages matériels risque d'augmenter. L'assurance des frais de rappel des produits défectueux ainsi que celle des dommages pécuniaires résultant de l'interruption de l'exploitation et de la perte de jouissance revêtent également une importance croissante.

Assurance de la responsabilité civile professionnelle / cyberassurance

Les erreurs de programmation de logiciels (par exemple algorithmes défectueux, vulnérabilité aux attaques de pirates, fuites de données) peuvent entraîner des dommages corporels, matériels et pécuniaires assurés.

Horizon temporel pour les prétentions assurées

La quatrième révolution industrielle a déjà commencé et ne manquera pas de modifier en profondeur le monde du travail ces prochaines années. L'utilisation de machines et de robots pensants et auto-apprenants dans le domaine privé (par exemple robots de soins / domestiques) et professionnel (par exemple commande automatique de machines et de processus de production) est une réalité. La connexion de la vie quotidienne avec l'Internet bénéficie d'une popularité croissante (par exemple bracelets de fitness).

3.2. Mobilité autonome

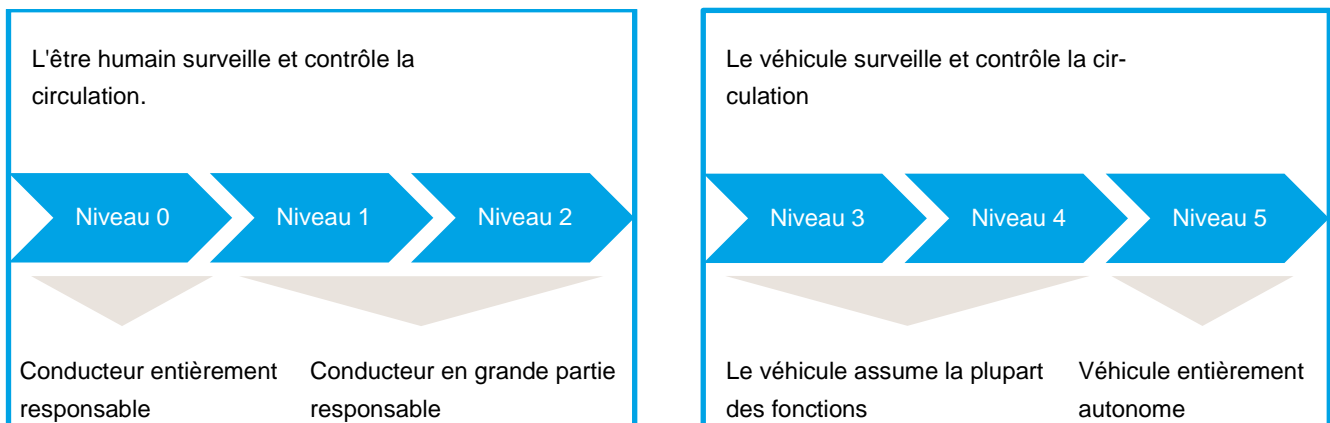
Dernière adaptation en mai 2022

Description du risque

La notion de « mobilité autonome » englobe d'une part la conduite autonome et d'autre part l'utilisation de drones. Les explications ci-dessous traitent exclusivement de la conduite autonome. Les risques liés aux drones ne sont pas couverts par la définition des risques émergents mentionnée ci-dessus.

De nos jours, nous ne pouvons plus imaginer nos véhicules sans systèmes électroniques et sensoriels d'assistance à la conduite. Les derniers véhicules arrivés sur le marché offrent des assistances à la conduite de plus en plus nombreuses et raffinées, voire prennent totalement en charge la conduite du véhicule dans certaines situations. La question n'est donc pas de savoir si la mobilité autonome sera un jour possible, mais simplement jusqu'où ira l'autonomie et quand sera-t-elle effective.

La mobilité autonome comprend essentiellement cinq niveaux :



Niveau 0

Absence d'automatisation. La conduite est assurée par le seul conducteur (*Driver only*). Le véhicule est uniquement équipé de systèmes d'avertissement et d'alerte.

Exemples : avertisseur anticollision, système d'alerte de franchissement involontaire de ligne (AFIL).

Niveau 1

Certains systèmes d'assistance apportent une aide lors de l'emploi du véhicule (par exemple, régulateur de vitesse et de distance).

Exemples : régulateur automatique de vitesse et de distance, système d'alerte de franchissement involontaire de ligne (AFIL).

Niveau 2

Automatisation partielle, systèmes combinés de guidage et d'accélération.

Exemples : système automatique d'aide au stationnement, système de guidage longitudinal, assistant à la conduite dans les embouteillages

Niveau 3

Mode automatisé, le conducteur n'a pas besoin de surveiller le véhicule en permanence. Le véhicule assume certaines fonctions de manière autonome.

Exemple : Le conducteur n'intervient « plus que » dans quelques situations. Des alertes sonores et visuelles invitent le conducteur à reprendre le contrôle du véhicule.

Niveau 4

Automatisation élevée, le système prend en charge la conduite du véhicule de manière durable.

Exemple : Le système assure la conduite du véhicule aussi longtemps qu'il est capable d'accomplir les tâches correspondantes. Si ce n'est pas le cas, le conducteur est invité à reprendre le contrôle du véhicule.

Niveau 5

Autonomie totale du véhicule. Le véhicule prend en charge toutes les fonctions de conduite.

Exemple : Le véhicule est guidé de manière totalement autonome par le système. Il n'est pas équipé de volant et peut se déplacer sans conducteur.

Situation actuelle

De nos jours, circulent sur les routes essentiellement des véhicules équipés de systèmes de niveaux 0 à 2. Il ne s'agit pas seulement de véhicules de gammes moyenne à supérieure, mais aussi, et de plus en plus, de petites voitures. Au regard de la rapidité des progrès technologiques, le coût de tels systèmes ne manquera pas de baisser, ce qui les rendra prochainement accessibles à toutes les catégories de véhicules. Le nombre de véhicules équipés de ces systèmes d'assistance à la conduite va donc augmenter.

Quelques véhicules de niveau 3 circulent d'ailleurs déjà sur nos routes. Pour le moment, il s'agit surtout de véhicules des catégories supérieures. Or, le développement de l'automatisation de la conduite progresse rapidement. La tendance à l'automatisation est inéluctable, de sorte que les systèmes de niveau 3 équiperont bientôt aussi les véhicules des catégories inférieures.

Les véhicules équipés de systèmes de niveau 4 et 5 ne circulent pas encore sur nos routes. Plusieurs essais de véhicules à conduite autonome (niveau 4 et / ou 5) ont eu lieu et se poursuivent dans le monde entier. Cette tendance se maintiendra certainement dans les années à venir. Ce ne sera probablement qu'une question de temps avant que les véhicules équipés de systèmes de niveau 3, 4 et 5 ne fassent partie de notre paysage routier.

La grave pénurie mondiale de chauffeurs de camion ne manquera pas de stimuler le développement des camions autonomes. Outre les essais réalisés sur la voie publique, les camions autonomes (niveau 5) sont déjà testés en pratique par certaines entreprises (par exemple Walmart¹). Les experts estiment que les camions de niveau 4 seront produits en série d'ici 2030² et qu'ils modifieront le paysage routier.

¹ <https://qz.com/2086940/walmart-is-using-driverless-trucks-for-its-grocery-business/>

² https://www.daimler.com/magazine/technology-innovation/autonomous-trucks.html#anchor_1691078

L'actuelle législation sur la circulation routière est pour l'instant en retard par rapport à cette évolution. Elle prévoit que le conducteur doit à tout moment avoir le contrôle de son véhicule et pouvoir intervenir. Or, dès que des véhicules équipés de systèmes de niveau 4 et 5 circuleront sur nos routes, cette condition ne sera plus remplie que dans une certaine mesure, voire plus du tout. Il faudra bien que la législation sur la circulation routière s'adapte tôt ou tard à cette nouvelle donne.

Perception du risque

La mobilité autonome suscite régulièrement l'intérêt des médias qui se focalisent alors généralement sur les systèmes de niveaux 4 et 5. Les articles et reportages sur les systèmes des niveaux 1 à 3 sont beaucoup plus rares. Cela s'explique sans doute par le fait que nombre de ces systèmes d'aide et d'assistance à la conduite équipent déjà nos véhicules des nouvelles générations et qu'ils ne sont donc plus si inhabituels.

La conduite entièrement autonome présente de nombreux avantages. Des études partent du principe que la mobilité entièrement autonome aura un effet positif tant sur la fluidité du trafic en soi que sur le nombre d'accidents et donc sur celui des victimes de la route. En outre, il est probable que les véhicules entièrement autonomes contribueront à améliorer la mobilité des personnes âgées en particulier et, par ricochet, leur qualité de vie.

Comme souvent, l'émergence de nouvelles technologies s'accompagne également de risques d'un genre nouveau et suscite de multiples interrogations. Outre les questions de responsabilité civile, d'autres questions se posent portant sur la fragilité et la vulnérabilité de tels systèmes.

Au regard notamment de la durée d'utilisation moyenne d'un véhicule, il faut tenir compte de la fragilité de la mobilité entièrement autonome. En combien de temps le logiciel utilisé devient-il obsolète au point qu'une mise à jour logicielle ne suffit plus à garantir la sécurité de la conduite ? Que se passe-t-il si le détenteur du véhicule refuse d'effectuer une mise à jour nécessaire ?

Par ailleurs, dans quelle mesure les systèmes utilisés sont-ils vraiment sûrs ? Sont-ils suffisamment protégés contre les cyberattaques ? Des pirates informatiques peuvent-ils manipuler un véhicule de sorte à entraver certaines de ses fonctionnalités, voire à en prendre totalement le contrôle ?

Une autre thématique porte sur les aspects éthiques. Plusieurs articles récents ont abordé la question de savoir s'il était acceptable d'un point de vue éthique qu'une machine prenne certaines décisions. Le cas de figure portait sur un véhicule entièrement autonome confronté à une collision imminente. La collision en elle-même était inévitable. Mais dans cet exemple théorique, la question s'est posée de savoir quelle décision prendrait le système. Doit-il protéger les occupants du véhicule et donc éviter une collision avec l'obstacle – en l'espèce, un camion ? Pour éviter la collision, le véhicule devrait toutefois se déporter vers la droite ou vers la gauche. En cas d'évitement par la droite, le véhicule écraserait un couple de retraités et, en cas d'évitement par la gauche, une mère et son jeune enfant. Bien qu'il s'agisse d'un exemple théorique, il illustre néanmoins parfaitement les problèmes qui se posent. Il est tout à fait légitime de se demander si le traitement d'une telle question éthique peut vraiment être confié à une technologie. Qui devrait ensuite justifier la décision prise et qui devrait en assumer la responsabilité ?

Pertinence en matière de responsabilité civile

Comme nous l'avons déjà mentionné, la plupart des législations sur la circulation routière ne sont pas adaptées aux nouvelles technologies ou ne tiennent pas encore suffisamment compte de la mobilité autonome. L'évolution du droit en la matière devra être observée de près.

En Suisse, il ne faut pas s'attendre à une adaptation fondamentale du reste du droit de la responsabilité civile, notamment de la législation sur la responsabilité du fait des produits. Les réglementations en vigueur semblent être suffisantes pour la mobilité autonome.

Pertinence en matière d'assurance de la responsabilité civile

Il est probable qu'avec les progrès de l'automatisation, les dommages se déplaceront également de l'assurance responsabilité civile des véhicules à moteur vers l'assurance responsabilité civile d'entreprise, que ce soit dans le cadre de l'élévation de recours par les assurances de véhicules à moteur ou directement par les personnes lésées. Plus le niveau des systèmes utilisés est élevé, plus les recours formulés directement à l'encontre des constructeurs ou des fournisseurs devraient se multiplier.

Dans le domaine de la mobilité autonome ou de ses fabricants, il faut s'attendre à une augmentation des dommages en responsabilité civile du fait des produits. Cela devrait avoir des répercussions non seulement sur la responsabilité civile produits des constructeurs automobiles, mais aussi sur celle des concessionnaires automobiles. Par ailleurs, la fréquence et l'ampleur des rappels de produits ne manqueront vraisemblablement pas d'augmenter, en raison de la vulnérabilité de la technologie et des logiciels utilisés.

Horizon temporel pour les prétentions assurées

La mobilité autonome ne sera probablement pas introduite à une date précise. L'intégration des systèmes correspondants dans notre quotidien sera au contraire progressive. Cette introduction progressive s'accompagnera d'un déplacement des sinistres de l'assurance des véhicules à moteur vers l'assurance de la responsabilité civile d'entreprise. Il faudra cependant attendre encore quelques années avant que les véhicules totalement autonomes fassent vraiment partie de la circulation routière.

3.3 Cyberrisques / Cybersilencieux

Dernière adaptation en mai 2022

Description du risque

Les entreprises privées comme les entreprises publiques dépendent aujourd'hui des systèmes informatiques, ceci quels que soient leurs domaines d'activité. Elles sont, de fait, très exposées et, donc, particulièrement vulnérables aux dysfonctionnements dus à de potentielles cyberattaques. La complexité de la sécurité de l'information est en constante évolution, et les risques afférents sont souvent sous-estimés. La sécurité de l'information comprend entre autres la protection de la confidentialité des informations et des données (*confidentiality*), la protection de l'intégrité des données (pas de modification possible par des tiers non autorisés ; *integrity*) et la garantie de la disponibilité des systèmes informatiques dits « critiques », comme ceux des systèmes de paiement, des hôpitaux ou de l'approvisionnement en énergie. Différentes catégories de risques sont identifiables :

- défaillance ou interruption des infrastructures critiques des technologies de l'information et de la communication (*Critical Information Infrastructure = CII-Breakdown*) telles que l'approvisionnement en électricité et les entreprises de transport ;
- sécurité des données et des informations en ligne (*online data and information security*, par exemple, l'informatique en nuage [*cloud computing*]) au regard de la perte éventuelle de données ou de modifications malveillantes de données ;
- vol d'informations (cybervol) ;
- espionnage informatique (cyberespionnage) ;
- guerre de l'information et cyberterrorisme (*cyber war and cyber terrorism*).

Les dangers liés à l'Internet sont multiples et comprennent les traditionnels virus, vers, chevaux de Troie et logiciels espions, qui peuvent entraîner la perte irrémédiable de données, l'atteinte à la vie privée, la divulgation de secrets professionnels ou d'informations sur des partenaires commerciaux. Parmi les risques figurent également des activités telles que l'hameçonnage de données (*phishing*), qui peut par exemple conduire à l'utilisation frauduleuse de cartes de crédit, les courriers indésirables (*spams*), en général juste agaçants et chronophages, ainsi que les « cryptoverrouilleurs » – (*cryptolockers* en anglais ; également appelés virus de cryptage, chevaux de Troie de chantage ou rançongiciels [*ransomware*]) – qui rendent les fichiers illisibles et peuvent généralement être décryptés contre le paiement d'une rançon en crypto-monnaies telles que le « Bitcoin », « Ethereum », etc. Vous trouverez des détails sur ces différents dangers après des sources suivantes :

- Le Centre national pour la cybersécurité (NCSC) propose des informations actualisées sur la sécurité des systèmes informatiques et de l'Internet ainsi que sur la protection des infrastructures critiques suisses (<https://www.ncsc.admin.ch/ncsc/fr/home.html>).

Outre des rapports semestriels détaillés, le NCSC publie une lettre d'information et alimente un blog sur la situation actuelle en matière de cybersécurité. En Suisse, les tentatives d'escroqueries, d'hameçonnage

ou de chantage se sont nettement multipliées (rapport semestriel 2/2021). Parallèlement, les événements ci-dessous sont cités à titre d'exemples :

- Tentatives de manipulation de l'approvisionnement en eau en Floride

En février 2021, le curseur de la souris d'un ordinateur chargé du système de traitement de l'eau potable d'Oldsmar, en Floride, s'est mis à bouger tout seul. Le technicien de service a tout juste eu le temps d'intervenir alors qu'un intrus tentait à distance de faire monter la teneur d'hydroxyde de sodium à un niveau dangereux pour la santé. Ce dernier avait réussi à accéder à l'appareil de commande du traitement de l'eau par le biais d'un logiciel d'accès à distance insuffisamment sécurisé, qui a bien failli être fatal à l'infrastructure de la ville.

- SITA : Vol de données concernant les passagers

Le premier fournisseur mondial de systèmes d'enregistrement de passagers de l'industrie aéronautique (Société Internationale de Télécommunications Aéronautiques (SITA)) a été la cible d'une cyberattaque. Les données des passagers de diverses compagnies aériennes ont ainsi été « récupérées ». L'incident a touché des serveurs sur lesquels sont stockées les données des passagers de diverses compagnies aériennes.

- Exemples tirés du rapport de l'Office fédéral de la sécurité des technologies de l'information (BSI) « Die Lage der IT-Sicherheit in Deutschland 2021 » (État des lieux de la sécurité informatique en Allemagne en 2021) :

- Attaque de rançongiciel contre un hôpital universitaire en Rhénanie du Nord-Westphalie

Le 10 septembre 2020, une attaque de rançongiciel aux conséquences non négligeables s'est produite dans un hôpital universitaire. Il s'agit de l'un des six hôpitaux universitaires de Rhénanie du Nord-Westphalie (NRW), piliers des soins aux patients dans le Land le plus peuplé d'Allemagne et à la pointe de la recherche et de l'enseignement. Il semble que les malfaiteurs ne visaient pas en premier lieu les soins ambulatoires ni stationnaires délivrés aux patients, mais plutôt l'université elle-même.

En dépit de cette attaque, l'hôpital a pu fournir les soins médicaux aux patients déjà hospitalisés, mais n'a pas pu assurer les soins d'urgence pendant treize jours consécutifs en raison de la panne de ses systèmes centraux. Les traitements planifiables et ambulatoires ont été annulés ou reportés, et l'admission de nouveaux patients a été suspendue.

- Cyberattaque de DarkSide (*ransomware-as-a-service*) contre la compagnie Colonial Pipeline

Le 7 mai 2021, l'exploitant d'oléoducs américain Colonial Pipeline Company a été victime d'une cyberattaque contre son infrastructure informatique. Colonial Pipeline Company se présente comme l'exploitant du plus grand système d'oléoducs pour produits raffinés aux États-Unis. La compagnie occupe une position-clé dans l'approvisionnement des clients en produits raffinés le long de la côte Est des États-Unis. Du fait de l'attaque, l'exploitant de l'oléoduc a déconnecté son réseau administratif et

a dû suspendre l'exploitation de l'oléoduc par mesure de précaution. Cette suspension a provoqué des pénuries régionales et un effet de panique suivi d'achats en masse, notamment d'essence.

Ces derniers temps, les déclarations de vol, de falsification ou de destruction de données personnelles enregistrées électroniquement, comme les informations relatives aux cartes de crédit ou les données médicales (par exemple dans les hôpitaux), par des pirates informatiques ont augmenté. Selon le *Beobachter*, près de 3000 entreprises en Suisse ont été victimes de cyberattaques en 2020³. Les nouvelles technologies, telles que l'informatique quantique (*quantum computing*), permettent un décryptage beaucoup plus rapide des codes de sécurité / mots de passe et risquent à l'avenir de provoquer une multiplication exponentielle des cyberattaques contre les entreprises suisses si elles sont utilisées par des personnes malintentionnées⁴.

Sont concernées toutes les entreprises et, de manière générale, les organisations devant stocker une grande quantité de données personnelles (par exemple données concernant les collaborateurs, les clients, les patients) pour l'exercice de leur activité. Elles sont tenues de mettre en œuvre des mesures adéquates pour la protection des données personnelles, la sécurité des données et leur récupération et de veiller à leur bonne application (devoir de diligence). Cela implique également des mises à jour régulières ou le remplacement de logiciels afin de combler d'éventuelles failles de sécurité. La cyberattaque « Wanna Cry » de mai 2017 a clairement démontré qu'il est indispensable de vérifier régulièrement les logiciels et de procéder aux adaptations correspondantes. Cette attaque a paralysé des dizaines d'hôpitaux en Grande-Bretagne, entraîné des pannes des chemins de fer allemands et perturbé les chaînes de production du constructeur automobile Renault. Au sein du *National Health Service* (NHS ; système de santé du Royaume-Uni), cinq pour cent environ des ordinateurs fonctionnent avec le système d'exploitation Windows XP qui n'est pratiquement pas protégé. « NotPetya », un logiciel malveillant visant la destruction de données et se propageant comme un ver, a été utilisé en 2017, essentiellement pour nuire à l'Ukraine. Or, un grand nombre d'entreprises actives à l'international ont également été touchées ; ces victimes collatérales ont subi d'importants dommages comme le logisticien Maersk (300 millions de dollars de dommages) ou l'entreprise pharmaceutique Merck (1,4 milliard de dollars de dommages). Lors des processus de couverture, les cyberassureurs ont argumenté que la cyberattaque consistait en un instrument de la Fédération de Russie et s'inscrivait dans le cadre des hostilités permanentes contre l'Ukraine⁵. Par conséquent, ce dommage ne serait pas assuré du fait de l'exclusion « ... des dommages causés par des actions hostiles ou belliqueuses en temps de paix ou de guerre ». Il reste à voir dans quelle mesure cette argumentation résistera à un jugement du tribunal. Ce cas constitue un excellent exemple de l'importance d'une formulation précise des exclusions.

Par ailleurs, les exigences légales se renforcent, notamment sur l'attitude à adopter en cas de perte de données. Aux États-Unis, toutes les personnes touchées doivent être informées d'un tel incident et, dans de nombreux cas, se voir proposer une surveillance (*credit watch*) afin de prévenir l'utilisation abusive de leurs cartes de crédit. Ces mesures entraînent des coûts supplémentaires.

³ <https://www.beobachter.ch/digital/sicherheit/dramatischer-anstieg-der-angriffe-hacker-sturzen-sich-auf-schweizer-firmen>

⁴ <https://www.weforum.org/agenda/2021/11/in-a-quantum-future-our-economy-needs-to-be-protected-a-cybersecurity-expert-explains-why/>

⁵ Spiegel Online Patrick Beuth 23 janvier 2022

Perception du risque

L'économie est tributaire des systèmes d'information, c'est indiscutable. La presse quotidienne publie régulièrement des articles sur les perturbations et les attaques illégales de toutes sortes de systèmes d'information. Les cyberattaques visent non seulement les données des particuliers et des entreprises, mais aussi des chaînes d'approvisionnement entières ; ces dernières peuvent d'ailleurs également être touchées comme simples victimes collatérales.

Pertinence en matière de responsabilité civile

Aux États-Unis et au Royaume-Uni, les pertes de données (confidentielles) débouchent de plus en plus souvent sur des actions en dommages et intérêts. Cette tendance s'observe également en Europe (et en Suisse). Il ne fait aucun doute que l'atteinte intentionnelle et illicite à des infrastructures critiques, ordinateurs, réseaux, données, etc., constitue un cas de responsabilité civile, même si les auteurs seront difficiles à identifier en cas d'actes de cybercriminalité. Si la personne assurée a contribué au dommage par son comportement, notamment du fait d'une manipulation négligente des données et / ou en raison d'une sécurité insuffisante des données, elle peut alors également être tenue pour responsable.

La responsabilité civile découlant de l'infraction au devoir de diligence des exploitants de systèmes informatiques et des fournisseurs d'accès à Internet (ISP) pour des dommages consécutifs est également tout à fait concevable (par exemple dommages corporels dans les hôpitaux, mais aussi dommages matériels ou atteintes à l'environnement).

Pertinence en matière d'assurance de la responsabilité civile

Assurance de la responsabilité civile d'entreprise

Les dommages corporels et matériels résultant du dysfonctionnement des systèmes informatiques sont assurés. Au regard de la quatrième révolution industrielle (industrie 4.0) et de la mise en réseau généralisée des machines, ce scénario est de plus en plus probable même si la sécurité informatique occupe désormais une place importante dans la stratégie de tous les types d'entreprises. Les dommages purement pécuniaires résultant de l'interruption de systèmes d'infrastructure et d'information critiques (comme les centrales électriques) peuvent être assurés en partie.

Sous réserve d'exclusion explicite des cyberrisques (par exemple CGA assurance responsabilité civile d'entreprise ou CGC Perte d'usage), les prétentions découlant de la responsabilité civile légale pour les dommages corporels, matériels ou purement pécuniaires peuvent être coassurées (couvertures silencieuses des cyber-risques, « *silent cyber* » cover).

Risques	Dommages / Couverture	CGA Assurance RCE
Responsabilité civile légale pour atteintes à la personnalité	Indemnisation de tiers pour des dommages corporels résultant de la divulgation par négligence d'informations confidentielles / personnelles	

Risques	Domages / Couverture	CGA Assurance RCE
Responsabilité civile légale en cas d'infractions à la sécurité informatique	Indemnisation de tiers pour des <u>dommages économiques purs</u> (dommages pécuniaires) résultant de la divulgation par négligence d'informations confidentielles / personnelles	Non assuré
	Indemnisation de tiers pour des dommages corporels / matériels causés en raison de la sécurité insuffisante du réseau du preneur d'assurance	Assuré
Dommages aux données / informations du PA sans endommagement du matériel informatique	Indemnisation de tiers pour des <u>dommages économiques purs</u> (dommages pécuniaires) causés en raison de la sécurité insuffisante du réseau du preneur d'assurance	Non assuré
	Frais de reconstitution de données volées, détruites ou corrompues à la suite d'une attaque informatique	Non assuré
Pertes de revenus du PA à la suite <ul style="list-style-type: none"> – d'attaques informatiques – de l'interruption de l'infrastructure (par exemple électricité) 	Pertes de revenus résultant de l'interruption des systèmes informatiques ou d'un traitement inadéquat des informations confidentielles	Non assuré
	Dépenses supplémentaires du PA découlant de cyberchantage à son rencontre, de l'usurpation d'identité	Frais d'investigations et de l'indemnisation des demandes de rançon Coûts / dépenses liés à l'usurpation d'identité.

 Assuré

 Non assuré

Le problème des cybercouvertures « intentionnelles » dans l'assurance responsabilité civile d'entreprise traditionnelle est un peu moins prononcé qu'en assurances de choses, mais ne doit pas être sous-estimé pour autant. Un logiciel de commande défectueux ou une cyberattaque sur le logiciel de commande d'une machine peuvent par exemple entraîner des dommages corporels ou matériels lors de l'emploi de celle-ci. Ce type de

dommages est en principe couvert par les assurances responsabilité civile d'entreprise ; or, il se peut qu'il ne soit pas suffisamment pris en compte dans les primes en raison du manque de recul en matière de sinistres.

Il en va autrement des éventuelles extensions de couverture – intentionnelles ou non – dans les assurances responsabilité civile d'entreprise, qui peuvent entraîner une double couverture par le biais de cyberassurances spéciales. Par exemple, l'extension de la notion de dommage matériel aux pertes de données sans dommage matériel préalable, la couverture de certains dommages économiques purs (dommages pécuniaires) à la suite d'un cyberincident (comme le non-respect des droits de la personnalité ou la responsabilité civile des médias), les frais de reconstitution de ses propres données, etc. De telles extensions de couverture peuvent s'avérer problématiques et entraîner des doubles couvertures involontaires. Il convient d'accorder une attention particulière à la formulation des conditions afin d'éviter tout litige portant sur l'étendue de la couverture.

Assurance responsabilité civile professionnelle (prestataires de services informatiques, fabricants de logiciels / de matériel, etc.)

Les dommages économiques purs (dommages pécuniaires) résultant d'une prestation de services non conforme sont assurables. En règle générale, les conventions de services prévoient toutefois des limitations de responsabilité.

L'offre de cyberassurances spéciales se multiplie au niveau international, mais aussi sur le marché suisse de l'assurance. En général, ces produits couvrent les dépenses entraînées pour la reconstitution des propres données et les pertes de revenus résultant de l'interruption de l'exploitation (couverture des risques propres, *first party coverage*) ainsi que les prétentions de tiers au titre de la responsabilité civile légale (assurance de tiers, *third party coverage*) pour les dommages liés par exemple au non-respect des droits de la personnalité et à l'utilisation abusive des informations de cartes de crédit.

Assurance responsabilité civile D&O

Des contrôles inadéquats et des normes de sécurité insuffisantes peuvent entraîner des dommages financiers importants, voire la faillite de l'entreprise. Les responsables de l'entreprise risquent dès lors de devoir répondre de ces manquements devant les tribunaux. En règle générale, les polices d'assurance ne prévoient pas d'exclusion pour les dommages liés à une sécurité informatique déficiente.

Horizon temporel pour les prétentions assurées

Le problème est d'actualité. L'ensemble de ces risques peuvent entraîner à tout moment l'élévation de prétentions.

3.4 Robotique / Intelligence artificielle (IA)

Dernière adaptation en mai 2022

Description du risque

La robotique englobe des pans de l'informatique, de l'électrotechnique et de la construction mécanique et est également utilisée comme terme générique pour l'Internet des objets (IdO ; *Internet of things, IoT*) ainsi que pour la mobilité autonome (par exemple voitures, trains, bateaux, avions / drones).

L'intelligence artificielle (IA) est déjà utilisée pour de nombreuses applications par des entreprises privées et, de plus en plus, par les pouvoirs publics, et elle est devenue incontournable dans notre monde d'aujourd'hui. L'IA est ainsi utilisée dans les systèmes de reconnaissances vocale et faciale, les moteurs de recherche, les logiciels d'analyse d'images, les assistants virtuels, les applications de l'Internet des objets, la mobilité autonome, etc.

Les machines autonomes auto-apprenantes sont de plus en plus nombreuses à être utilisées dans l'industrie (par exemple production et système de stockage automatisés) et dans le secteur de la santé (par exemple chirurgie robotique, robot d'assistance et de services). L'utilisation de robots industriels est un phénomène bien connu dans le cadre de processus répétitifs relevant de l'automatisation, comme dans la fabrication automobile.

La pénurie de personnel soignant dans les hôpitaux et les maisons de retraite entraîne un débat mondial sur la question de savoir dans quelle mesure les robots soigneurs et les robots auxiliaires peuvent être utilisés pour accomplir des tâches routinières. Les robots sont capables d'accompagner les patients aux examens, de porter leurs affaires, de distribuer de la nourriture et des médicaments, de bavarder et de discuter ou, plus généralement, de les aider à passer le temps. Dans les pays férus de nouvelles technologies, de tels robots sont déjà utilisés, comme le montrent des exemples en provenance du Japon et de la Chine. Il faut également s'attendre à ce que les robots envahissent de plus en plus la sphère privée (par exemple aspirateurs ou tondeuses robots).

Perception du risque

Les effets négatifs potentiels de cette évolution font l'objet de discussions dans les milieux scientifiques et juridiques. Il s'agit notamment de savoir dans quelle mesure la législation en vigueur en matière de protection des données, de sécurité des produits et de responsabilité du fait des produits tient suffisamment compte de ces évolutions.

Pertinence en matière de responsabilité civile

Un robot défectueux peut provoquer des dommages corporels et matériels. De tels dommages relèvent de la législation portant sur la responsabilité civile liée aux produits ainsi que des dispositions générales de responsabilité civile. La question qui se pose ici est notamment celle de savoir qui doit répondre finalement de la faute. Est-ce le détenteur / propriétaire du robot, par analogie avec la responsabilité civile des détenteurs d'animaux ou de véhicules à moteur ? Est-ce le fabricant final du robot dans lequel le logiciel est intégré ou est-ce le programmeur du logiciel défectueux ? Le robot doit-il être doté d'une personnalité juridique propre et,

en tant que tel, voir sa responsabilité engagée de manière autonome (en tant que personne électronique en complément de personnes physiques et morales) ? Ces questions font l'objet d'intenses discussions au sein du Parlement européen et de la Commission européenne. L'extension de la directive sur la responsabilité du fait des produits est également à l'ordre du jour, afin de mieux protéger les consommateurs. Par ailleurs, l'introduction d'une assurance responsabilité civile obligatoire pour les produits défectueux est en discussion.

Pertinence en matière d'assurance de la responsabilité civile

L'assurance responsabilité civile d'entreprise et l'assurance responsabilité civile produit du fabricant offrent une couverture d'assurance si un robot défectueux (par exemple, une erreur de programmation dans le logiciel d'IA) provoque des dommages corporels ou matériels. Est également couverte la responsabilité civile légale du détenteur du robot, ainsi que celle des exploitants des systèmes requis par les systèmes autonomes, tels que les systèmes de navigation ou de télécommunication. L'assurance responsabilité civile professionnelle des développeurs de logiciels couvre les prétentions en responsabilité civile à la suite de dommages (corporels et matériels) que le robot a causés à des tiers du fait d'une programmation erronée, ainsi qu'à la suite des dommages (dommages matériels / pécuniaires) causés aux robots eux-mêmes fabriqués par des tiers. De même, des erreurs de programmation dans des solutions et applications numériques reposant sur l'intelligence artificielle (par exemple recrutement de personnel, conseil juridique numérique, dispositifs de commande de machines et de véhicules) peuvent entraîner des dommages corporels et matériels classiques ainsi que des dommages économiques purs (dommages pécuniaires).

Horizon temporel pour les prétentions assurées

Comme les robots et l'intelligence artificielle vont de plus en plus faire partie de notre vie quotidienne et prendront en charge différentes tâches / procédures, il faut s'attendre à voir se multiplier les élévations de prétentions pour dommages corporels, matériels et, s'ils sont assurés, pour dommages économiques purs (dommages pécuniaires). Quant à savoir quels seront les produits d'assurance responsabilité civile concernés, cela dépendra de l'allocation future des prétentions en responsabilité civile. Entrent par exemple en ligne de compte le propriétaire, le détenteur ou l'utilisateur du robot, le fabricant du robot ou un sous-traitant, le développeur de logiciels, le fabricant de produits défectueux fabriqués avec le robot (impression 3D) ou encore un opérateur de système (par exemple une entreprise de télécommunications).

3.5. Adaptation au climat et effets du changement climatique

Dernière adaptation en mai 2022

Description du risque

En Suisse aussi, le changement climatique a des répercussions sur l'environnement, l'économie et la société. À l'heure actuelle, des mesures permettant de s'adapter à ces changements sont déjà nécessaires ; elles prendront encore plus d'importance à l'avenir.

État des connaissances scientifiques

Le Conseil fédéral a adopté, le 2 mars 2012, la stratégie d'adaptation aux changements climatiques, dans laquelle il définit les objectifs et principes en la matière, identifie les champs d'action pour neuf secteurs et décrit les défis transversaux que la Confédération devra relever.⁶

- Gestion des eaux
- Économie forestière
- Agriculture
- Tourisme
- Santé
- Énergie
- Développement territorial
- Gestion des dangers naturels
- Gestion de la biodiversité

Le changement climatique affecte les systèmes écologiques et influence les multiples interactions entre eux. Le réchauffement provoque l'augmentation de la température de l'eau, ce qui modifie les conditions de vie pour les organismes aquatiques. L'intensification des précipitations entraîne une érosion accrue et un lessivage des nutriments des sols. Une multiplication de situations anticycloniques stables favorise la présence de couches d'inversion et la formation de smog. L'augmentation de la sécheresse entraîne ici et là une pénurie d'eau, modifie les habitats et l'aire de répartition des espèces et des populations.

Inversement, le climat est influencé par les systèmes naturels. Par exemple, les océans, les marais, d'autres sols organiques ainsi que les forêts constituent d'importants réservoirs de CO₂ dont la modification agit sur le climat. Les activités humaines telles que l'étalement urbain, la mobilité, la surexploitation des ressources et la pollution exercent un impact négatif sur les écosystèmes. Du fait de la dégradation des systèmes naturels et de leurs services écosystémiques, les moyens de subsistance de l'être humain sont de plus en plus menacés. Ceci revêt une grande importance, surtout dans le contexte du changement climatique, car seuls des écosystèmes intacts et robustes sont en mesure de se montrer suffisamment stables et résilients pour arriver à surmonter les adaptations inévitables.⁷

⁶ Les risques et les opportunités liés au changement climatique (admin.ch)

⁷ Adaptation_aux_changements_climatiques_-_Plan_d'action_2020-2025.pdf

Le Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC) met en garde contre une multiplication des phénomènes météorologiques extrêmes en lien avec le réchauffement climatique tels que la sécheresse, les épisodes de fortes précipitations, le gel extrême, les tempêtes et autres phénomènes similaires. En outre, le GIEC s'attend à ce que les événements extrêmes soient également plus importants en termes de durée et de pics. Il est difficile d'extrapoler les modèles établis au niveau mondial à celui de la Suisse. Il est néanmoins possible d'affirmer que la Suisse ne pourra pas se soustraire à cette tendance. Outre les risques d'événements météorologiques extrêmes, cela implique également une fonte des réservoirs d'eau douce sous forme de fonte des glaciers et de dégel du permafrost. Ces deux phénomènes peuvent contribuer à des inondations, des laves torrentielles et des chutes de pierres.⁸

Depuis la fin de la conférence sur le climat de Glasgow en novembre 2021, il apparaît désormais fort peu probable que le monde atteigne l'objectif d'un réchauffement maximal de 1,5 degré Celsius par rapport au niveau préindustriel. Cela signifie qu'il faut plutôt s'attendre à des variations plus importantes en termes de répercussions.

Le Conseil fédéral envisage la mise à disposition entre 2025 et 2030 d'un total de 2,9 milliards de francs environ pour l'assainissement des bâtiments et le passage à des installations de chauffage respectueuses du climat. À cela s'ajoutent des fonds annuels alloués au développement d'infrastructures de recharge pour les véhicules électriques, à la conversion des flottes de bus à la propulsion électrique dans le trafic local et régional ou à la couverture des risques lors de l'extension des réseaux de chauffage urbain. Ces investissements dans les nouvelles technologies peuvent modifier le paysage des risques.

Il convient également de noter le nombre croissant de plaintes en rapport avec le changement climatique.⁹ Qu'il s'agisse de plaintes contre des entreprises pour infraction aux dispositions légales relatives à la protection du climat ou pour réduction insuffisante des émissions de CO₂ (par exemple plainte contre la compagnie Royal Dutch Shell : obligation de réduire les émissions de 45 pour cent d'ici 2030¹⁰) ou du fait de leur contribution au réchauffement mondial et du préjudice qui en résulte pour des tiers, susceptible d'engager la responsabilité civile (par exemple action climatique contre RWE : les émissions d'origine humaine responsables de l'effondrement des glaciers¹¹). Un autre exemple est celui des actions en justice contre le législateur pour omissions en matière de protection du climat et négligences en matière de protection des personnes vulnérables (actions contre la réglementation, par exemple plainte de personnes âgées contre la Confédération pour inaction climatique¹²). Les plaignants sont généralement des groupes d'intérêt public (par exemple des ONG), des particuliers, des investisseurs, des industries concernées (par exemple les pêcheurs du Pacifique) ou des gouvernements.

⁸ Sixth Assessment Report — IPCC

⁹ Setzer, J. & Higham, C. Global Trends in Climate Change Litigation: 2021 Snapshot (London School of Economics and Political Science, 2021).

¹⁰ <https://www.nzz.ch/wirtschaft/shell-klage-das-urteil-veraendert-die-welt-fundamental-ld.1629072?reduced=true>

¹¹ <https://www.germanwatch.org/de/19832>

¹² <https://www.klimaseniorinnen.ch/warum-wir-klagen/>

Perception du risque

Le secteur de l'assurance va devoir affronter des évolutions parallèles, à savoir

- les effets physiques du changement climatique et
- les conséquences de la transformation de l'économie pour surmonter le changement climatique.

Ces évolutions comprennent les tempêtes, les inondations, la grêle, les épisodes de fortes précipitations, la sécheresse, voire également les conditions nivologiques extrêmes. En outre, le risque de coulées de boue et de chutes de pierres augmentera avec l'affaiblissement du pergélisol (*permafrost*). Cela peut avoir des répercussions sur les fondations des bâtiments, les infrastructures de transport, les oléoducs et les lignes électriques. De plus, le dégel du pergélisol peut entraîner l'extension des zones exposées à des territoires déjà construits. Il en va de même pour les zones exposées au risque d'avalanches, si les forêts de protection souffrent du changement climatique. Les épisodes de fortes précipitations risquent de provoquer des inondations en dehors des zones inondables ; la sécheresse et le gel peuvent occasionner la perte des récoltes. Rien ne dit que les mesures de protection permettront effectivement de protéger les infrastructures contre de tels événements extrêmes ni si elles seront suffisamment efficaces.

Les aspects portant sur la responsabilité civile sont décrits ci-après. Le changement climatique risque de modifier également le paysage des risques d'autres couvertures d'assurance. Ainsi, il faut s'attendre à une multiplication des événements extrêmes en assurance de choses.

Pertinence en matière de responsabilité civile

Les entreprises et leurs dirigeants pourraient être accusés de ne pas avoir pris de mesures concernant les émissions de gaz à effet de serre ou d'avoir tardé à en prendre. Les actionnaires pourraient également poursuivre les dirigeants (plaintes D&O) pour réorientation insuffisamment rapide d'une entreprise vers l'ère post-fossile, prise de mauvaises décisions ou communication d'informations inexactes dans les rapports sur l'exposition de l'entreprise au changement climatique (par exemple durabilité, critères ESG [*Environmental/Social/Governance*]). Les secteurs les plus susceptibles de devoir engager des frais pour se défendre ou d'être confrontés à des prétentions assurées sont ceux qui émettent beaucoup de gaz à effet de serre. En Suisse, il s'agit par exemple des producteurs de ciment, des raffineries, de l'industrie des transports ou de l'agriculture.

Les actions en responsabilité civile contre des entreprises pour des dommages corporels et matériels dus à leurs émissions et à leur contribution au réchauffement mondial ne devraient pas aboutir en Suisse pour le moment, car il faut que la responsabilité individuelle de l'entreprise soit clairement engagée (pas de responsabilité fondée sur les parts de marché).

En cas d'endommagement d'infrastructures lors de phénomènes météorologiques extrêmes, les communes et les villes pourraient être poursuivies en responsabilité civile pour délimitation incorrecte des zones exposées sur leurs cartes des dangers. Les planificateurs et les conseillers qui participent à l'élaboration de la délimitation de ces zones risquent également de se retrouver devant les tribunaux pour infraction au devoir de diligence s'ils se sont insuffisamment tenus informés de l'état actuel des connaissances lors de la réalisation de ce travail de délimitation.

Par ailleurs, les promoteurs immobiliers qui construisent dans des zones encore indiquées comme non dangereuses sur les cartes des aléas, mais qui risquent fort de se retrouver davantage exposées à l'avenir au regard des informations facilement accessibles, pourraient être amenés à répondre de leurs actes si des bâtiments devaient se retrouver endommagés ou inhabitables en raison de l'apparition de nouveaux risques naturels dus au changement climatique. De la part des experts, une telle clairvoyance va de soi.

L'augmentation des températures et la sécheresse croissante pendant la période de végétation des forêts augmentent le risque d'incendie de forêt en Suisse. Le transport et la distribution d'électricité, la gestion de la végétation, mais aussi, par exemple, les entreprises de construction ou les chemins de fer peuvent déclencher de tels incendies de forêt par une étincelle et se retrouver alors poursuivis en responsabilité civile. Ce scénario s'est déjà produit à plusieurs reprises à l'étranger, notamment en Californie. Ce pourrait également devenir le cas en Suisse à l'avenir.

Les travailleurs sur les chantiers seront de plus en plus exposés aux vagues de chaleur et à l'augmentation des rayons UV. Une mortalité accrue soulèverait également la question de savoir si l'employeur protège suffisamment ses employés contre les conséquences du réchauffement climatique. Des scénarios comparables sont envisageables pour les exploitants de maisons de retraite ou les organisateurs événementiels.

Indirectement, le changement climatique pousse certaines branches à adapter leurs produits. Pour le secteur de l'assurance, les nouvelles technologies sont généralement synonymes d'incertitudes accrues et d'un paysage des risques modifié. Par exemple, la question de savoir si les véhicules électriques présentent un risque d'incendie accru lors de leur charge n'a pas encore été clarifiée. Les incendies de batterie dans les garages privés ou publics pourraient non seulement entraîner une multiplication des dommages matériels, mais aussi des dommages corporels du fait de l'émission de gaz toxiques. La responsabilité du fait des produits, les couvertures pour rappel de produits ou les assurances de la responsabilité civile pour véhicules à moteur pourraient être concernées à des degrés divers.

Pertinence en matière d'assurance de la responsabilité civile

Comme les risques liés au réchauffement climatique ou à l'adaptation au climat ne sont pas explicitement exclus de l'assurance responsabilité civile, ils sont donc couverts a contrario. Même si les liens de cause à effet entre les émissions et leur impact sur le climat mondial sont connus, il pourrait s'avérer difficile, dans certains cas, de délimiter clairement la contribution réelle d'une entreprise, en particulier si celle-ci a bien respecté la réglementation en vigueur.

Les émissions de gaz à effet de serre proprement dites sont progressives et ne devraient en général pas relever de l'assurance responsabilité civile des entreprises. En revanche, les rejets accidentels de polluants après un phénomène météorologique extrême pourraient être couverts, par exemple l'inondation d'une décharge à la suite de fortes précipitations ou des fuites de réservoirs de pétrole.

Il en va autrement des effets concrets du changement climatique. La responsabilité des personnes dont on doit attendre, dans le cadre de leur travail, qu'elles soient conscientes des risques particuliers liés au changement climatique (par exemple, les fortes précipitations) est engagée si elles ne satisfont pas à cette exigence

dans le cadre de leur devoir de diligence. En l'absence de restrictions de couverture, les assurances de responsabilité professionnelle pourraient être concernées (par exemple, celles des architectes et des planificateurs).

Les assurances D&O sont (également) en ligne de mire, comme le montrent les exemples évoqués ci-avant. Les décisions des dirigeants en lien avec un comportement insuffisant en matière de protection du climat ou des informations erronées quant à leur approche de la durabilité et leur application des critères ESG pourraient se traduire par des pertes financières et conduire à des actions en justice de la part des actionnaires.

Le secteur de l'assurance commence à peine à tenir compte correctement des changements climatiques dans ses contrats d'assurance. Certaines compagnies gèrent leurs participations de manière à ne plus proposer d'éléments de couverture aux branches ou aux activités les plus gourmandes en énergie (charbon, pétrole et gaz).

Horizon temporel pour les prétentions assurées

Les effets du changement climatique sont clairement visibles en Suisse, et l'adaptation au climat est déjà en cours. Ce sont surtout les conséquences directes de phénomènes météorologiques extrêmes qui se répercutent rapidement sur l'assurance responsabilité civile. La pertinence temporelle des plaintes climatiques contre les entreprises n'est pas encore claire.

Il va falloir surveiller de près les modifications de la législation et vérifier leur pertinence pour les assurances. Exemples : abaissement des valeurs limites d'émissions et d'immissions ou adaptations de la législation sur le CO₂.

Les demandes d'indemnisation risquent de s'accumuler également du fait de l'approfondissement des connaissances scientifiques, d'une attention accrue portée au changement climatique dans les médias, de la multiplication des actions des ONG ou du financement croissant de litiges par les investisseurs (*litigation funding*).

3.6. Matériaux de construction respectueux du climat

Dernière adaptation en mai 2022

Description du risque

Pour tenir compte de l'évolution des exigences dans le domaine de la construction (par exemple bâtiments plus hauts, réduction des coûts par la préfabrication en série / les importations, villes vertes, amélioration de l'efficacité énergétique), le secteur du bâtiment recourt de plus en plus à de nouveaux matériaux dont la sécurité est testée et approuvée conformément aux méthodes et procédures actuelles. Il ressort des sinistres déjà survenus que toutes les procédures de test ne garantissent pas la sécurité des matériaux de construction à court ni même à long terme.

Comme ils sont plus légers et possèdent de bonnes propriétés isolantes, les matériaux composites dits à ossature métallique (*Metal Composite Material, MCM*) ou les systèmes composites pour isolation thermique (*Exterior Insulation Finishing Systems, EIFS*) sont utilisés par exemple pour doubler les façades des bâtiments en construction. Ces revêtements inflammables à base de MCM peuvent potentiellement engendrer d'énormes dommages, car le mode de construction utilisé agit comme une cheminée en cas d'incendie et permet au feu de se propager plus rapidement, comme en témoigne les incendies survenus à Dubaï et à Londres (Grenfell Tower 2017). Une petite inattention – par exemple lors d'un barbecue sur la terrasse – ou le court-circuit d'un appareil électrique peuvent dégénérer en catastrophe en présence de tels matériaux composites.

À la suite des événements mentionnés, les procédures d'essai et de certification actuellement applicables à ces matériaux de construction ont subi un examen critique en vue de leur révision. Dans quelle mesure, ces procédures tiennent-elles suffisamment compte des propriétés particulières des nouveaux matériaux ? Cette question continue de faire l'objet de discussions. Citons quelques exemples.

La demande de matériaux de construction durables, dont l'empreinte carbone est réduite et / ou qui sont fabriqués à partir de ressources renouvelables, enregistre actuellement une forte hausse.¹³ Dans la perspective d'une économie circulaire, les fabricants de matériaux de construction, mais aussi les architectes et les ingénieurs, sont depuis peu tenus de boucler les cycles des matériaux le plus possible. Cela implique entre autres des constructions durables, l'optimisation de l'énergie utilisée pour la fabrication et le transport (réduction de l'énergie dite grise) ainsi que le tri et le recyclage complet des matériaux lors de la démolition d'anciens bâtiments. Par ailleurs, l'utilisation de matériaux combinant plusieurs fonctions (par exemple, les façades photovoltaïques) augmente. Les défauts ou dysfonctionnements des produits se multiplieront vraisemblablement, car plus d'un aspect de la performance risque de différer par rapport aux attentes (production d'électricité et / ou régime hydrique).

Les maîtres d'ouvrage exigent de plus en plus le recours à des matériaux de construction à énergie grise réduite pour la fabrication et le transport. La recherche actuelle porte par exemple sur le ciment modifié, dont la fabrication nécessite moins d'énergie, voire peut même piéger du CO₂. Ses propriétés demeurent toutefois encore largement inexplorées. En Suisse, de nouvelles prescriptions en matière de protection contre les incendies autorisent désormais la construction d'immeubles avec des éléments en bois. De plus, les techniques

¹³ Empa - Communication - *A recipe for eco-concrete*

d'assemblage et de collage du bois évoluent en permanence et peuvent partiellement remplacer l'acier et le béton armé.¹⁴ Les matériaux d'isolation à base de papier constituent un autre exemple de l'utilisation accrue de matériaux de construction renouvelables.

Un dernier point concerne les matériaux de construction auto-cicatrisants ou dotés de capteurs censés mettre en évidence les signes de fatigue à un stade précoce. Il s'agit toutefois de nouvelles technologies, raison pour laquelle il n'y a pas encore assez de recul sur le long terme en la matière.

Les réserves par rapport aux nouveaux matériaux de construction peuvent porter sur le risque de défaillance fonctionnelle prématurée, de problèmes de statique ou d'une détérioration du climat intérieur (*indoor-pollution*) ainsi que d'une lutte inefficace contre les incendies par les pompiers. Par ailleurs, les ouvriers ne disposent pas toujours des connaissances requises sur la manière d'utiliser ces nouveaux matériaux et de les intégrer dans la construction, ce qui peut être source d'un nombre plus élevé de défauts aux ouvrages.

Industries concernées :

fabricants et fournisseurs de matériaux de construction,
industrie du bâtiment,
architectes et ingénieurs.

Or, les maîtres d'ouvrage et les autorités d'autorisation / de surveillance ainsi que les propriétaires, les utilisateurs des bâtiments et les entreprises de gestion des bâtiments sont également concernés.

Perception du risque

En Suisse, des maisons ont été endommagées par l'humidité parce que les membranes de toiture n'étaient plus étanches dans des conditions météorologiques extrêmes, comme celles des régions montagneuses. Dans la plupart des cas, les dommages n'ont été découverts qu'après l'expiration de la garantie. Ces dommages s'expliquent notamment par le fait que les matériaux de construction sont parfois développés à la limite de leurs possibilités. Les membranes de toiture en question étaient censées laisser passer l'humidité sous forme de vapeur tout en prévenant les infiltrations d'eau, et ce pour une durée de vie de 30 ans¹⁵.

Des incendies survenus pendant la construction ou l'exploitation d'immeubles ont mis en évidence la problématique des revêtements inflammables à base de MCM qui sont plus ou moins dangereux en fonction du mode de construction utilisé ([par exemple The Address Downtown Dubai 2015, Grenfell Tower London 2017](#)).

Lorsque l'isolation thermique des bâtiments est inadaptée aux conditions climatiques locales, cela se traduit régulièrement par des dommages aux bâtiments dus à l'humidité. En Irlande, par exemple, l'humidité a provoqué des dommages en série à la suite de travaux d'isolation lors d'une rénovation visant à optimiser l'enveloppe des bâtiments existants (*cavity wall insulation*).

¹⁴ http://www.nfp66.ch/SiteCollectionDocuments/NFP66_Teilsynthese_1_Holzbau_FR.pdf

¹⁵ <https://www.srf.ch/sendungen/kassensturz-espresso/sika-will-nicht-fuer-undichte-dachfolien-haften>

Pertinence en matière de responsabilité civile

Les sinistres survenus jusqu'à présent ont mis en évidence l'importance que revêt la responsabilité civile pour un grand nombre d'entreprises impliquées. Les maîtres d'ouvrage, les architectes, les fabricants de produits, les fournisseurs et les entreprises de construction ne sont pas les seuls à devoir se défendre contre des prétentions en responsabilité civile. Les propriétaires des bâtiments, les services de gestion des bâtiments ou les entreprises responsables de l'entretien ainsi que les autorités de surveillance sont aussi régulièrement incriminés. Il leur faut envisager que la preuve puisse être apportée d'un lien de causalité adéquate entre, d'une part, le matériau composite défectueux en tant que cause du dommage et, d'autre part, les dommages corporels ou matériels survenus.

Dans quelle mesure invoquer l'exception en matière de respect des normes de sécurité correspondantes peut s'avérer efficace pour limiter la responsabilité engagée ? La question se pose.

Pertinence en matière d'assurance de la responsabilité civile

Ce risque n'est pas exclu en assurance de la responsabilité civile, c'est-à-dire qu'il est couvert à contrario. Cela concerne notamment l'assurance responsabilité civile professionnelle des architectes, l'assurance responsabilité civile d'entreprise et l'assurance responsabilité civile produit des participants à la construction ainsi que celle des fabricants et fournisseurs de matériaux de construction.

Le problème est aggravé par le fait que les matériaux sont parfois consommés et utilisés pendant des années avant qu'un défaut ne soit constaté. Le risque de dommages en série liés à l'utilisation de nouveaux matériaux est donc accru.

Horizon temporel pour les prétentions assurées

Dans les années à venir, il faut s'attendre à une augmentation des prétentions en responsabilité civile en rapport avec les nouveaux matériaux de construction.

3.7. Pandémie et dommages collatéraux

Dernière adaptation en mai 2022

Perception du risque

Répercussions sur le marché financier

La pandémie a entraîné une nette augmentation des risques financiers et une volatilité accrue sur le marché financier. Toutefois, les réactions individuelles dépendent indubitablement de la gravité de l'épidémie dans le pays considéré. Les interventions politiques non conventionnelles visant à stimuler l'économie peuvent néanmoins s'avérer problématiques sur le long terme. Citons pour exemple le rachat d'obligations d'État et d'autres obligations (*quantitative easing*) par la banque centrale aux États-Unis. Cette mesure risque de se traduire sur le long terme par une dévaluation de la monnaie locale et donc une hausse de l'inflation. Rétrospectivement, les diverses mesures politiques prises par les différents pays et la désintégration qui en résulte représentent une plus grande menace pour le monde que le virus lui-même.

Entreprises zombies

Le soutien non conventionnel de la politique fiscale et monétaire évoqué plus haut et apporté dans le sillage de la pandémie de Covid-19 a attisé la crainte que ces mesures ne favorisent l'émergence d'entreprises zombies. Il s'agit d'entreprises dont le modèle économique n'est plus viable, ce qui est néanmoins masqué aujourd'hui par les crédits bon marché octroyés dans le cadre de la crise du Covid-19, de sorte qu'elles ne feront faillite que dans le futur. À l'heure actuelle, il ne devrait y avoir qu'un petit nombre d'entreprises zombies en Suisse, tant parmi les entreprises privées que parmi celles cotées en bourse. Celles-ci se concentrent surtout dans l'industrie manufacturière et le commerce de détail et ne représentent qu'une petite partie des bénéficiaires des crédits accordés aux sociétés non financières. En outre, la proportion d'entreprises cotées en bourse qui peuvent être identifiées comme entreprises zombies obéit à un schéma cyclique : elle augmente en période de récession et diminue en période de reprise, ce qui est probablement dû à un mélange de chocs agrégés et de chocs sectoriels.

Mais ce sont surtout les entreprises cotées en bourse qui sont exposées aux risques D&O lorsque leur direction ou leur conseil d'administration tardent à adapter leur modèle économique du fait des crédits octroyés dans le cadre de la crise du coronavirus, alors qu'une telle mesure serait vraiment nécessaire. Cette inertie n'est pas dans l'intérêt des actionnaires.

Redémarrage d'entreprises à l'arrêt

L'objectif des normes industrielles en matière de conception d'installations et de processus d'exploitation consiste dans le fait de garantir la sécurité. La préservation de la sécurité des installations et des processus implique une maintenance continue par un personnel expérimenté et qualifié, c'est-à-dire du temps et de l'argent, ceci afin d'éviter toute interruption d'exploitation suivie de travaux de remise en état et de sécurité. Les enseignements tirés de la pandémie de Covid-19 ont également mis sous pression les tâches de maintenance et d'inspection. Cette crise économique mondiale a donc entraîné un resserrement des budgets de maintenance dans de nombreux secteurs et des retards dans les travaux déjà planifiés. Nombre d'entreprises des secteurs les plus divers ont décidé, par mesure d'économie, de mettre les installations à l'arrêt plutôt que de profiter de ces pauses pour en effectuer la maintenance. En outre, des collaborateurs qualifiés et

expérimentés ont soit été licenciés et / ou, du fait des restrictions de mobilité pendant le confinement, n'ont pas été en mesure de se rendre sur les lieux d'intervention.

La remise en service des installations mises à l'arrêt pendant le confinement dû à la pandémie risque de se dérouler dans l'urgence et sans les budgets nécessaires : en d'autres termes, dans des conditions impliquant une mise en service rapide et pas forcément bien planifiée.

Une fois la pandémie terminée et le retour à la normale, les assureurs devraient en conséquence tenir compte également des caractéristiques suivantes lors de leur évaluation des risques : « financement suffisant », « temps » et « disponibilité de personnel expérimenté et qualifié ».

Symptômes persistants du Covid-19

Souvent, des personnes touchées par le Covid-19 se plaignent de symptômes persistants, comme des dysfonctionnements cognitifs, des difficultés respiratoires et de la fatigue, qui apparaissent parfois même des mois après l'infection. On ne sait toujours pas combien de temps ces symptômes risquent de perdurer.

D'autres études scientifiques complémentaires s'imposent. Les symptômes persistants peuvent générer des coûts de santé plus élevés et des demandes d'arrêt de travail en raison d'une morbidité et d'une comorbidité graves, ainsi que des prétentions accrues en invalidité.

Par exemple, des interventions médicales ont été reportées à cause de la pandémie, et les patients n'ont pas effectué les examens préventifs réguliers ou – en cas de symptômes – ne se sont pas rendus chez le médecin. Du fait de leur diagnostic ainsi retardé, certaines maladies chroniques généreront des coûts médicaux plus importants et se traduiront par une mortalité accrue bien après la fin de l'épisode pandémique.

En outre, de nombreux soignants expérimentés ont quitté la profession, et on craint que les collaborateurs du secteur des soins dans les hôpitaux, les maisons de retraite, les foyers médicalisés et les institutions similaires soient encore plus nombreux à faire de même. Ce phénomène entraîne des pénuries de personnel dans des secteurs critiques tels que les hôpitaux et les établissements médico-sociaux, ce qui pourrait se traduire à moyen terme par un plus grand nombre d'erreurs médicales et de dommages corporels. Il convient d'observer dans quelle mesure l'initiative sur les soins infirmiers peut corriger à temps cette évolution.

Pertinence en matière de responsabilité civile

Lorsque des entreprises mises à l'arrêt redémarrent alors qu'elles sont sous la pression des coûts et avec du personnel potentiellement nouveau, les problèmes et autres dysfonctionnements ne sont pas à exclure, et cela peut dégénérer en dommages corporels, matériels et environnementaux. La pression des coûts et le manque de personnel qualifié peuvent se répercuter négativement sur l'assurance qualité et entraîner une augmentation du nombre de prétentions élevées en responsabilité civile (produits). Les décisions de la direction de l'entreprise peuvent être remises en question et, en cas de décisions erronées, donner lieu à l'élévation de prétentions en responsabilité civile.

Dans le secteur hospitalier et des soins, les dommages corporels risquent également de se multiplier si les « lacunes en matière de personnel » ne peuvent pas être comblées en temps voulu par du personnel qualifié et expérimenté.

La pandémie se traduira par une augmentation du travail à domicile ou à distance (*remote work*) et une diminution du travail en présentiel. La gestion de l'infrastructure informatique privée n'étant généralement pas confiée à des professionnels, le risque de cyberattaques et de dysfonctionnements informatiques augmente. Cela peut se répercuter de manière significative sur la sinistralité future.

Pertinence en matière d'assurance de la responsabilité civile

Les assurances responsabilité civile d'entreprise et professionnelle n'excluent pas les dommages corporels, matériels et environnementaux consécutifs au redémarrage d'entreprises mises à l'arrêt, pour autant que les sites d'exploitation soient encore au bénéfice d'une couverture d'assurance.

Les assurances responsabilité civile hospitalière et professionnelle dans le domaine des soins couvrent les dommages corporels causés par une organisation défectueuse, le manque de personnel et le surmenage des collaborateurs.

Il faudrait peut-être adapter les cyberassurances à l'évolution de la situation en matière de risques. Il conviendrait aussi de vérifier dans quelle mesure l'assurance couvre également les dommages causés par une infrastructure informatique privée lacunaire.

Horizon temporel pour les prétentions assurées

La pandémie n'est pas terminée et son évolution doit être surveillée de près. Les répercussions énumérées ci-dessus sont d'actualité surtout en cas d'apparition de nouveaux variants (et leur lot de nouvelles mesures) et en présence de nouvelles vagues d'infection.

Sources

New emerging risks insight, Swiss Re SONAR. (2021). Swiss Re Institute.

Changement structurel : repousser à plus tard n'est que partie remise. (2021). KPMG Switzerland Blog. <https://home.kpmg/ch/de/blogs/home/posts/2021/11/strukturwandel.html>

Policy Responses to COVID-19. (2021). International Monetary Fund. <https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19>

Quantitative Easing (QE). (2021). Investopedia. <https://www.investopedia.com/terms/q/quantitative-easing.asp>

3.8. Risques latents liés aux produits

Dernière adaptation en mai 2022

Description du risque

Qu'est-ce que le « temps de latence du produit » ?

Que signifie une longue période de latence dans le monde médical ? La période de latence désigne le temps qui s'écoule entre une exposition (exposition aux causes d'une éventuelle atteinte à la santé, par exemple à des rayonnements) et l'apparition des premiers symptômes d'une atteinte à la santé (par exemple un cancer). De nombreux facteurs liés à l'environnement n'exercent pas un impact uniquement au moment de l'exposition, mais induisent potentiellement des effets sur l'évolution de la maladie toute la vie durant. La longue période de latence entre l'exposition à un risque à un stade précoce de la vie et l'apparition ultérieure d'un trouble pathologique complique la détermination des liens de cause à effet.

Il en va de même pour le temps de latence du produit, d'une part la déclaration de sinistre et d'autre part le règlement du sinistre. Pour tenir compte du temps de latence dans les analyses d'expositions cumulatives, on utilise souvent des informations différées sur l'exposition. Le résultat dépend de l'étendue de la couverture concernée et du déclenchement de la couverture (*trigger*).

Quelle est l'ampleur du risque ?

Les risques liés à l'amiante existent potentiellement partout. L'expansion rapide de l'industrie chimique au siècle dernier a donné lieu à l'apparition de dizaines de milliers de produits chimiques différents. Notre mode de vie dans son ensemble ainsi que la nature de nos produits en ont été considérablement modifiés, parfois pour le meilleur, parfois pour le pire.

Presque chaque jour, des organisations ou des autorités restreignent ou interdisent l'utilisation de différents produits chimiques. Les répercussions de ces mesures sur l'industrie chimique (fabricants comme utilisateurs) dépendent de l'évolution de la législation, qui pourrait entraîner une multiplication des problèmes de responsabilité. Les propositions en faveur d'une lutte efficace contre les produits chimiques toxiques pourraient aller dans le sens d'une responsabilité élargie du fabricant, en vertu de laquelle ce dernier se verrait tenu de reprendre les produits en fin de vie, comme cela se pratique déjà dans l'industrie automobile.

Pour chaque action en justice potentielle, il convient de définir la partie défenderesse. Or, plusieurs actions en justice contre des fabricants de produits chimiques préoccupants ont permis d'identifier de nouvelles catégories de défendeurs potentiels. Outre contre les fabricants historiques de produits chimiques, une plainte peut également être introduite contre des détaillants, des distributeurs, voire des municipalités. C'est ce que nous montrent par exemple les plaintes déposées contre les PFAS (substances per- et polyfluoroalkylées). Il est actuellement difficile d'estimer quels pans des chaînes d'approvisionnement ne risquent pas d'être poursuivis en justice à l'avenir. Du fait de la sensibilisation croissante du public par le biais des médias sociaux et d'autres plateformes, conjuguée à la pression financière accrue sur les gouvernements ou à l'affirmation d'une conscience écologique, il faut s'attendre à une intensification des efforts visant à incriminer d'autres entreprises de la chaîne d'approvisionnement. Même si les Américains sont les plus prompts à porter plainte et obtiennent souvent des compensations faramineuses aux États-Unis, ce phénomène s'observe de plus en plus dans d'autres parties du monde.

Au cours des vingt dernières années, un nombre croissant de données ont démontré que certains produits chimiques (appelés « perturbateurs endocriniens ») exercent des effets nocifs sur le système endocrinien à des concentrations qui étaient auparavant considérées comme inoffensives. Les produits chimiques fabriqués par l'être humain et ayant des effets secondaires indésirables sur le système hormonal sont nombreux : additifs pour matières plastiques, retardateurs de flamme, produits chimiques industriels, pesticides, composants de produits cosmétiques, principes actifs pharmaceutiques, métaux et métalloïdes, etc. Leur large diffusion, leur stabilité chimique et leur accumulation via la chaîne alimentaire rendent les perturbateurs endocriniens exposés aux poursuites judiciaires. Cela peut avoir des répercussions sur l'industrie chimique où ces produits sont fabriqués ou sur d'autres secteurs industriels (par exemple, celui de l'alimentation humaine / animale) où ils sont utilisés. Les entreprises qui produisent, commercialisent ou transforment des produits chimiques dangereux peuvent être poursuivies en justice si ces produits provoquent alors des dommages qui étaient prévisibles. En conséquence, des incidences sur le secteur de l'assurance ne sont pas à exclure.

Qu'est-ce qui prolonge encore la période de latence ?

L'économie circulaire (*circular economy*) prolonge encore le temps de latence. L'économie circulaire consiste en un système régénératif dans lequel l'utilisation des ressources et la production de déchets, les émissions et le gaspillage d'énergie sont minimisés. Il en résulte que les produits sont conçus et fabriqués de manière à pouvoir encore être utilisés, améliorés ou réutilisés à d'autres fins après leur premier emploi. Plus les matériaux et les produits sont utilisés longtemps, plus la période de latence est importante et, par conséquent, plus les demandes d'indemnisation risquent d'être nombreuses.

Entrés en vigueur en décembre 2019, les nouveaux règlements européens sur les exigences d'écoconception et l'étiquetage énergétique ont force obligatoire depuis le 1^{er} septembre 2021. Ces mesures s'appliquent aux produits mis en circulation sur le marché de l'UE, ceci indépendamment de leur lieu de fabrication. Jusqu'en 2019, la directive sur l'écoconception se concentrait sur l'efficacité énergétique. Mais ce n'est qu'un début. À l'avenir, de plus en plus de secteurs seront concernés, surtout au regard de la prise de conscience grandissante de la population en faveur de la durabilité.

Comment la Suisse réagit-elle ?

En avril 2020, le Conseil fédéral a adapté l'ordonnance sur les exigences relatives à l'efficacité énergétique (OEEE). Cette révision de l'OEEE permet de reprendre dans le droit suisse les nouvelles prescriptions plus sévères de l'Union européenne (UE) en matière d'efficacité énergétique dans le domaine des installations et appareils fabriqués en série.

Adaptée en conséquence la nouvelle ordonnance sur l'efficacité énergétique est entrée en vigueur le 1^{er} septembre 2021.

Découvertes scientifiques

La réglementation sur les produits chimiques s'attache à leurs effets nocifs, ceci indépendamment de leur mode d'action sous-jacent. Par ailleurs, chaque pays réglemente à sa manière par le biais de lois et d'initiatives les perturbations et les effets nocifs qui résultent justement de ce mode d'action.

Il faudrait se tenir informé et lire régulièrement les études de l'Organisation mondiale de la santé (OMS) ou d'autres organisations renommées et influentes afin de tenir compte de leurs constats. Tous les résultats

publiés par l'OMS qui concluent qu'un produit chimique a des effets négatifs sur la flore, la faune et / ou l'environnement et qu'il représente un danger pour l'être humain ne manqueront pas d'être utilisés dans le cadre de procédures judiciaires aux États-Unis. Les condamnations se chiffrant à plusieurs millions de dollars liées au glyphosate (pesticide) sont en partie le fruit d'une divergence d'opinion entre l'OMS et l'Agence américaine de protection de l'environnement (USEPA) sur le lien entre l'utilisation de ce pesticide et la prolifération de cancers.

Perception du risque

Tant qu'il n'existe pas de preuves scientifiques solides qu'un produit chimique particulier est susceptible de causer des dommages aux animaux ou d'être tenu pour responsable d'effets nocifs sur la santé humaine, il est peu probable que les dépôts de plainte se multiplient. Toutefois, si une étude « révolutionnaire » établit un lien entre une substance chimique et des effets nocifs sur la santé humaine, des plaintes ne manqueront pas d'être déposées, en particulier, mais pas exclusivement, aux États-Unis. Il est tout à fait envisageable qu'un avocat décide de prendre la tête d'une action en justice afin de s'établir comme « meneur » dans de tels dossiers.

Si, dans le contexte de « l'économie circulaire » et du « droit à la réparation », les directives relatives à l'éco-conception sont étendues au delà des produits liés à la consommation d'énergie, beaucoup plus de produits ou de secteurs seront concernés. Les répercussions sur la protection des produits et des consommateurs sont évidentes. L'allongement des cycles de vie des produits entraîne un emploi plus long de ceux-ci et, par ricochet, une probabilité accrue de dommages. Il faut en outre s'attendre à ce qu'une telle évolution provoque une recrudescence des rappels de produits (plus fréquents et plus étendus que par le passé). Le législateur européen pourrait, d'une part, introduire une responsabilité causale aggravée en cas de non-conformité des produits et, d'autre part, adapter les délais de garantie légaux à la durée de vie des produits.

Pertinence en matière de responsabilité civile

Au regard d'une responsabilité pour dommages corporels et matériels, c'est surtout la responsabilité du fait des produits qui est en ligne de mire. Une responsabilité pour les dommages corporels est déjà envisageable aujourd'hui pour les fabricants. Par ailleurs, il ressort de divers litiges récents qu'outre le fabricant de produits inquiétants (produits chimiques / substances / matériaux), d'autres entreprises de la chaîne de création de valeur risquent de plus en plus de se voir mises en cause. Il ne faut pas exclure non plus une action en responsabilité civile pour dommages environnementaux.

Pertinence en matière d'assurance de la responsabilité civile

Si des dommages corporels et / ou matériels sont causés à des tiers en rapport avec un produit, ils sont en principe couverts par l'assurance responsabilité civile d'entreprise. Selon les cas, les dommages économiques purs (dommages pécuniaires) peuvent également être inclus dans l'assurance responsabilité civile. La couverture d'assurance dépend alors, d'une part, de l'étendue de la couverture accordée et, d'autre part, des circonstances concrètes qui ont conduit au sinistre.

Les secteurs fortement touchés par les nouvelles réglementations sur l'économie circulaire devront revoir leurs produits, ce qui peut se répercuter négativement sur la sécurité des produits et la qualité du risque dans le portefeuille des assureurs en responsabilité civile.

Horizon temporel pour les prétentions assurées

Afin de minimiser autant que possible les futures élévations de prétentions, il est nécessaire, dans une démarche de prévention, d'échanger activement avec les autorités sur les interdictions concernées ainsi que sur l'évolution des réglementations relatives à l'économie circulaire.

3.9. Responsabilité des entreprises (D&O)

Dernière adaptation en mai 2022

Pour se protéger contre les demandes de dommages et intérêts résultant d'une responsabilité insuffisamment assumée, les entreprises peuvent souscrire une assurance de la responsabilité civile dite des organes ou des dirigeants (*Directors and Officers Liability Insurance*). Une telle couverture est indiquée afin d'éviter qu'en cas de litige, les dirigeants, les membres des conseils d'administration ou d'autres instances (assemblée générale, organe de révision) ne soient tenus de répondre de leurs actes sur leur fortune privée en tant que personnes physiques. Les entreprises actives à l'international, en particulier, s'exposent à un risque de responsabilité accru, car les activités exercées sous des systèmes juridiques étrangers moins connus comportent de nombreuses incertitudes. Seuls les dirigeants les plus téméraires renonceront donc à souscrire une assurance D&O en dépit des activités exercées par leur entreprise à l'étranger.

Description du risque

La « responsabilité des entreprises » est communément assimilée – probablement en souvenir de la campagne de votation en faveur de l'initiative pour des multinationales responsables¹⁶ – à la responsabilité engagée en cas de dommages environnementaux ou d'atteintes aux droits humains. Mais la responsabilité des multinationales revêt bien d'autres facettes encore. Pour une entreprise, un comportement qualifié de responsable ne porte pas uniquement sur l'exercice de son activité proprement dite, mais aussi sur des aspects écologiques significatifs (durabilité, protection de l'environnement), des aspects en termes de postes de travail (relations avec les collaborateurs) ou sur l'échange avec les principaux groupes d'intérêts (parties prenantes comme les clients, les actionnaires, les fournisseurs).

Les décideurs d'une entreprise, concrètement les membres de la direction ou du conseil d'administration, sont légalement tenus¹⁷ de prendre leurs décisions dans l'intérêt de l'entreprise.

Perception du risque

Le scandale des gaz d'échappement (*Dieselmoteur*), les intoxications aux pesticides ou l'élimination inappropriée de déchets toxiques à l'étranger, l'esclavage moderne (travail des enfants, exploitation des travailleurs dans les mines) et autres violations des droits humains (par exemple privatisation de l'eau potable) ou encore le

¹⁶ En 2020, la Suisse s'est prononcée sur l'initiative pour des multinationales responsables. En vertu de cette initiative, les multinationales ayant leur siège en Suisse étaient tenues de respecter les droits humains et les normes environnementales internationales également en dehors de la Suisse. À cet effet, la responsabilité des multinationales devait pouvoir être engagée en cas de violation des droits humains et de non-respect des normes environnementales contraignantes, ceci quel que soit le lieu où les actes (ou omissions) correspondants avaient été commis. Lors de la votation populaire du 29 novembre 2020, l'initiative a certes obtenu la majorité du peuple avec 50,7 pour cent environ de voix favorables, mais elle a échoué à la majorité des cantons, également requise.

¹⁷ Art 717 al. 1 CO : « Les membres du conseil d'administration, de même que les tiers qui s'occupent de la gestion, exercent leurs attributions avec toute la diligence nécessaire et veillent fidèlement aux intérêts de la société. »

procès climatique intenté contre Shell¹⁸ ont sensibilisé la population à la responsabilité sociale des entreprises. Même si l'objectif principal d'une entreprise demeure le profit, la maximisation des bénéfices est relativisée par les attentes des parties prenantes, qui souhaitent que l'entreprise exerce son activité dans le respect des aspects éthiques et de manière aussi durable que possible.

Il est toutefois intéressant de noter que la plupart des actions en responsabilité civile sont engagées en raison de pertes financières subies par les actionnaires ou les créanciers, et non en raison de demandes d'indemnisation liées aux actes (moralement répréhensibles) mentionnés ci-dessus. Les actions en responsabilité intentées par des actionnaires ou des créanciers ne jouent évidemment qu'un rôle secondaire dans l'esprit du public, car elles sont rarement médiatisées, contrairement aux scandales environnementaux.

Pertinence en matière de responsabilité civile

Les membres du conseil d'administration ainsi que l'ensemble des personnes impliquées dans la direction de l'entreprise ou sa révision (organes) peuvent être tenus personnellement responsables des dommages qu'ils causent en enfreignant leurs obligations.

Il existe de nombreux cas dans lesquels la responsabilité d'un responsable peut être engagée. Exemples possibles :

- absence d'appels d'offres,
- absence d'autorisations fournies par d'autres instances,
- non-respect des directives des associés,
- gestion des risques déficiente,
- prises de mauvaises décisions,
- erreurs dans le bilan,
- corruption,
- détournement de fonds et fraude,
- infractions aux règles de la concurrence ou en matière de conformité,
- absence d'étude de marché,
- acquittement de factures alors que l'entreprise est déjà en faillite,
- fraudes fiscales ou fraudes concernant les cotisations aux assurances sociales,
- non-respect du devoir d'assistance prévu par le droit du travail (par exemple harcèlement moral [*mobbing*] / ou sexuel [*sex tortion*] d'employés),
- licenciements injustifiés.

Essentiellement en cas de faillite d'une entreprise, la responsabilité relevant du droit des sociétés anonymes risque de retomber sur ses instances.

¹⁸ Le 26 mai 2021, le groupe pétrolier Shell a été condamné à La Haye à réduire drastiquement ses émissions de CO₂ d'ici 2030. La plainte avait été déposée par des organisations de protection de l'environnement. Le jugement pourrait créer un précédent important.

Un exemple récent illustre à quel point la frontière peut être ténue entre une bonne et une mauvaise décision : une entreprise doit-elle se retirer du marché russe en raison du conflit en Ukraine ? Si la direction de l'entreprise prend une décision en ce sens, elle court alors le risque de se voir expropriée et dépossédée de son activité, qui sera alors reprise par l'État russe. Si cette même direction décide de ne rien faire, elle prend le risque d'une détérioration de son image de marque et, probablement, d'une défection des clients ou des investisseurs. C'est un vrai dilemme :

Quelle que soit la décision prise, les dirigeants de l'entreprise s'exposent à se voir potentiellement reprocher d'avoir pris une mauvaise décision.

En quoi la responsabilité des multinationales constitue-t-elle un risque émergent ?

Le risque que les membres des instances dirigeantes et autres organes décideurs des entreprises voient leur responsabilité engagée s'est accru ces dernières années. Ce phénomène s'explique par la complexité accrue de la législation du fait de la multiplication des dispositions, mais aussi par les risques nouveaux tels que les pandémies, les cyberattaques, la numérisation, la protection des données ou le changement climatique (ou par la prise de conscience de ces risques). Par ailleurs, depuis quelque temps, la problématique de la durabilité gagne en importance, que ce soit au niveau de la production, du transport, des chaînes d'approvisionnement, des investissements, voire des clients finaux.

Les sociétés d'acquisition ad hoc encore appelées sociétés d'acquisition à vocation spécifique (*Special Purpose Acquisition Companies, SPAC*) constituent un nouveau risque pour les dirigeants de voir leur responsabilité engagée. Une SPAC est une société fictive créée dans le seul but d'acquérir une société cible non cotée. La SPAC lève d'abord des capitaux par le biais d'une introduction en bourse (offre publique initiale, IPO). Elle investit ensuite les capitaux levés dans l'acquisition d'une société cible, cette dernière étant cotée en bourse dans le cadre de l'acquisition (de-SPAC).¹⁹ D'origine américaine, ces véhicules financiers peuvent être cotés et négociés à la *SIX Swiss Exchange* depuis le 6 décembre 2021, date à laquelle les marchés étaient d'ailleurs déjà volatils (en raison de la pandémie).

Ci-après, quatre exemples illustrent dans quelle mesure ces véhicules financiers risquent d'engager la responsabilité des entreprises.

Exemple de risques liés à la pandémie

Il ressort de l'expérience actuelle que le secteur du tourisme (hôtellerie, restauration), l'aviation, l'industrie automobile (chaînes d'approvisionnement interrompues) ou le secteur de l'événementiel, par exemple, ont été fortement impactés par les effets secondaires de la pandémie. Les dirigeants pourraient se voir reprocher de n'avoir pas été capables de réagir à temps et, par exemple, de n'avoir pas misé sur une deuxième activité ni reconstitué les stocks pour amortir les pertes.

Ou encore, cela concerne tous les secteurs, les employés reprochent à leur entreprise une mauvaise application des mesures sanitaires pendant la pandémie, le non-respect de son devoir d'assistance ou de la protection des données.

¹⁹ Définition tirée de : <https://www.six-group.com/fr/newsroom/media-releases/2021/20211116-spacs-six-ser.html> (consultée le 17.06.2022).

Il y a aussi des dossiers où le personnel navigant, licencié pour ne pas avoir voulu se faire vacciner, a porté plainte contre la compagnie aérienne en invoquant un licenciement abusif. Des parties prenantes revendicatrices pourraient également reprocher à la direction que ces licenciements ont été effectués à tort et qu'ils ont eu pour conséquence l'annulation de plusieurs vols en raison d'un manque de personnel, ce qui s'est répercuté négativement sur le résultat d'exploitation.

Exemple de cyberrisques

Du fait de la numérisation, de plus en plus de données – même extrêmement sensibles – sont stockées sur un serveur ou dans le *cloud* (nuage). Ces serveurs sont reliés électroniquement en réseau, ce qui permet aux pirates informatiques d'accéder aux données et de les télécharger. Elles peuvent alors être utilisées de manière abusive : être revendues, servir de monnaie d'échange pour faire chanter leurs propriétaires ou être exploitées pour ternir la réputation d'une personne. Par ailleurs, les cyberattaques sont dangereuses aussi parce qu'elles permettent la manipulation de systèmes informatiques entiers ou leur mise hors service.

Aujourd'hui, nous dépendons tous de l'informatique et sommes donc tous vulnérables. De nos jours, une entreprise de services est contrainte de cesser ses activités si son système informatique ne fonctionne plus. Une direction qui ne prend aucune mesure pour protéger son entreprise contre les cyberattaques, l'hameçonnage (*phishing*) ou les virus agit, dans la conception actuelle des choses, à l'encontre de la prudence la plus élémentaire et risque de voir sa responsabilité engagée en cas de dommages de ce type.

Exemple de risques liés à la durabilité

Les critères ESG sont devenus la norme en matière de placements durables (*sustainable finance*). ESG est l'abréviation de « *environmental, social and governance* » (environnement, social, gouvernance d'entreprise) et signifie quelque chose comme « responsabilité sociale de l'entreprise » (*Corporate Social Responsibility*). En résumé, la responsabilité sociale de l'entreprise recouvre un comportement entrepreneurial responsable qui intègre, de son propre chef²⁰, des préoccupations sociales et environnementales dans l'exercice de son activité et ses interactions avec les groupes d'intérêts et les parties prenantes.²¹ Dans l'idéal, un comportement responsable de l'entreprise se reflète aussi dans le choix des investissements qu'elle réalise.

²⁰ En Suisse, les nouvelles dispositions introduites dans le Code des obligations (CO) avec effet au 1^{er} janvier 2022 prévoient deux nouveautés importantes : d'une part, les grandes entreprises suisses devront, dans un esprit de transparence, rendre compte des risques engendrés par leur activité : elles devront établir un rapport sur les questions environnementales, les questions sociales, les questions de personnel, le respect des droits de l'homme et la lutte contre la corruption. Elles devront également présenter les mesures qu'elles ont adoptées dans ces domaines. D'autre part, les entreprises dont l'activité présente des risques dans les domaines sensibles du travail des enfants et des minerais et métaux provenant de zones de conflit ou à haut risque devront se conformer à une obligation d'établir des rapports et à des devoirs de diligence étendus. Les entreprises ont un an pour se conformer à ces nouvelles exigences.

²¹ Définition : Que signifie ESG (*environmental social governance*) ? | explication tirée de Fonds-Wiki | Glossaire EURAMCO (euramco-asset.de) (consulté le 11.4.2022).

Si la direction d'une entreprise « oublie » d'aligner sa stratégie sur les critères ESG, elle risque de voir ses investisseurs faire défection ou que cette omission porte atteinte à son image de marque. Dans les deux cas, cela constituerait des éléments engageant la responsabilité D&O.

Exemple de SPAC

Comme nous l'avons vu plus haut, les SPAC sont des véhicules financiers, sorte de « sociétés de chèque en blanc »²², qui servent à racheter une entreprise déjà établie et à l'introduire rapidement en bourse. Ces véhicules de placement reposent sur des structures de gouvernance et de rémunération complexes. L'évaluation des risques concernant les rendements attendus, qui évoluent au cours du cycle de vie de la SPAC, nécessite aussi une analyse approfondie. En outre, la direction de l'entreprise rachetée demeure en place et doit s'adapter, pour ainsi dire « du jour au lendemain », aux exigences en matière d'obligations de *reporting* et de transparence du marché des capitaux. Il va de soi que ce phénomène s'accompagne de risques accrus en responsabilité civile. La situation devient encore plus délicate lorsque l'entreprise se retrouve subitement entretenir un lien avec les États-Unis du fait de cette reprise. Premièrement, les actionnaires américains portent de plus en plus souvent plainte contre des sociétés étrangères.

Deuxièmement, la SEC, l'autorité de surveillance des marchés financiers américains, entend mettre un terme aux dérives des introductions en bourse d'entreprises aux coquilles vides en adoptant des règles plus strictes. À l'avenir, il faut que les investisseurs dans de telles SPAC soient aussi bien protégés que dans le cas d'une introduction en bourse normale (IPO).²³

Pertinence en matière d'assurance de la responsabilité civile

La responsabilité des dirigeants signifie que les dirigeants doivent assumer la responsabilité financière des erreurs commises. Afin qu'ils ne soient pas amenés à répondre sur leur propre patrimoine privé, l'employeur peut conclure une assurance responsabilité civile d'organes. Également appelée assurance D&O (*Directors and Officers*), cette assurance protège le patrimoine privé des membres de la direction et de ceux du conseil d'administration.

Les préjudices intentionnels tels que la gestion déloyale ne sont bien entendu pas couverts par l'assurance D&O. Dans le cadre du procès de Raiffeisen, Pierin Vincenz a été condamné pour divers délits contre le patrimoine²⁴, raison pour laquelle l'assurance D&O ne doit en principe pas prendre en charge les dommages causés. Toutefois, elle pourrait tout de même être tenue de fournir des prestations. En effet, si les irrégularités commises par l'ancien CEO de Raiffeisen auraient dû être détectées par le conseil d'administration ou l'organe de révision s'ils avaient témoigné de la diligence requise, alors ces manquements relèveraient bel et bien de l'assurance D&O.

²² Source : Neue Zürcher Zeitung, 19.2.2021, Spacs: Die Blankocheck-Firmen kommen wohl in die Schweiz (nzz.ch) (consultée le 11.4.2022).

²³ Source : Handelsblatt, 30.3.2022: US-Börsenaufsicht SEC will Spacs enger an die Kandare nehmen (handelsblatt.com) (consultée le 11.4.2022).

²⁴ Jugement du tribunal du district de Zurich du 13.4.2022 (NON passé en force de chose jugée, un appel sera déposé).

Le risque D&O n'a cessé de croître ces dernières années. Les exigences accrues en matière de protection des données, de numérisation et nouvelles technologies, de cyberattaques, de changement climatique, mais aussi le mouvement « #MeToo » ont aiguisé la situation en responsabilité civile et rendu possible l'élévation de nouvelles prétentions en assurance D&O. La couverture D&O a donc nettement gagné en importance.

Même si l'initiative sur la responsabilité des entreprises a échoué en Suisse à la majorité des cantons, la tendance au niveau de l'UE va dans le sens d'un net durcissement des règles. Il faut s'attendre à ce que la Suisse soit obligée de suivre cette évolution. Pour les assurances de la responsabilité civile, cela pourrait signifier qu'elles se verront de plus en plus confrontées à des plaintes élevées à l'étranger. Il convient également de se demander si une entreprise présente d'une manière ou d'une autre une exposition aux États-Unis, c'est-à-dire si elle entretient un lien commercial avec les États-Unis qui pourrait déclencher l'élévation de prétentions en D&O. Comme vous le savez, les demandes de dommages-intérêts formulées aux États-Unis s'élèvent généralement à un multiple de ce qui est réclamé en Suisse, et les victimes potentielles y sont en outre beaucoup plus promptes à porter plainte.

Au regard de la large palette de constellations imaginables en matière de responsabilité civile, il est devenu de plus en plus difficile pour les compagnies d'assurances d'évaluer les risques potentiels. Il convient de se demander si les assurances sont armées pour y faire face, et si les primes incluent également les risques en partie cachés. Une chose est sûre : le service souscription doit se montrer beaucoup plus pointilleux en assurances D&O (application du principe « Connais bien ton client », « *know your customer* »), ce qui pourrait conduire à des exclusions ponctuelles dans certains contrats. En Allemagne, ce phénomène a déjà entraîné des augmentations drastiques des primes des polices D&O²⁵, et certains assureurs se sont retirés du marché de l'assurance responsabilité civile des dirigeants.²⁶

Horizon temporel pour les prétentions assurées

Une caractéristique particulière des prétentions découlant d'une gestion négligente de ces assurances réside dans le laps de temps important entre la naissance des prétentions et leur élévation. Cet aspect complique encore l'évaluation du risque actuariel.

²⁵ Source : Handelsblatt, 16.12.2021, p. 23: « Haftungsrisiken für Manager nehmen zu » (Hausse des risques de responsabilité civile pour les dirigeants).

²⁶ Sources : Frankfurter Allgemeine Zeitung für Deutschland, 16.12.2021, p. 24: « Risiken für Vorstände und Führungskräfte nehmen zu » (Augmentation des risques pour les membres des conseils d'administration et des dirigeants) ainsi que : Chubb zieht Notbremse in D&O (Chubb tire la sonnette d'alarme en assurance D&O | Herbert Frommes Versicherungsmonitor (consultées le 1.4.2022)).

3.10. Panne d'électricité (panne générale et pénurie d'électricité)

Dernière adaptation en mai 2022

Au moins depuis la parution du roman à succès « Blackout - Demain il sera trop tard » de Marc Elsberg, tout un chacun peut s'imaginer le potentiel énorme de dommages qui résulterait de la disparition de l'énergie électrique. Un tel *black-out* ne représenterait pas seulement un défi financier, mais aussi un défi social et sociétal pour la région touchée. Tout cela n'est-il que fiction ? Dans la négative, qu'en est-il du risque de *black-out* ?

Description du risque

L'Office fédéral de la protection de la population (OFPP) a publié en novembre 2020 deux dossiers, l'un sur le risque de pénurie d'électricité et l'autre sur celui de panne d'électricité (*black-out*), dans lesquels il donne des définitions, fournit des exemples, précise les facteurs d'influence et présente des scénarios possibles. Pour l'essentiel, la pénurie d'électricité caractérise un état du réseau électrique où la production et la demande ne coïncident pas à un moment donné, c'est-à-dire que les capacités de production sont épuisées au niveau régional ou national et ne peuvent plus couvrir la demande. Ce « déficit d'électricité » doit alors être comblé « de l'extérieur ». Se pose alors immédiatement la question de la définition de la taille d'un réseau électrique. Le réseau électrique suisse est physiquement intégré au réseau européen, c'est-à-dire qu'il en fait partie. Les réseaux ne peuvent donc pas être fermés par des barrières comme les frontières. Par conséquent, une pénurie nationale d'électricité devrait être couverte par les réserves de production des pays voisins. Si celles-ci ne sont pas disponibles, il faut délester le réseau d'autant de consommateurs ou de sources de consommation que nécessaire pour que la demande corresponde à la capacité de production nationale. Ces délestages contrôlés et intermittents prennent la forme de pannes d'électricité locales et canalisées et permettent d'éviter un *black-out* incontrôlé à grande échelle.

D'une manière générale, une panne d'électricité à grande échelle peut être la conséquence directe d'un déséquilibre entre consommation et production en raison d'un manque de production (pertes ou insuffisance), d'un manque de capacité (surcharge), de problèmes de synchronisation, de chute de fréquence ou de tension. Ces problèmes peuvent être dus, outre aux pénuries d'électricité mentionnées ci-avant, également à des accidents ou des incidents (intempéries, négligence, sabotage, tempêtes solaires, etc.), à des perturbations météorologiques (foudre, tempête, gel, inondations, etc.), à la déconnexion ou à la défaillance d'installations (lignes, centrales, mécanismes de protection, etc.) ou à des défaillances humaines (failles de sécurité, prévisions faussées, manque de communication ou de coordination, prise de mesures erronées, etc.).

Le principal problème du système électrique européen réside dans le fait qu'il ne dispose pas vraiment de réserves ni de réelles possibilités de stockage. La production et la consommation doivent être physiquement synchronisées à tout moment. C'est notamment pour cette raison qu'il existe depuis plus d'un siècle une règle en matière d'approvisionnement en électricité en vertu de laquelle chaque pays et chaque région est responsable de son propre approvisionnement en électricité à partir de ses propres ressources, et ce à tout moment de l'année. Cette règle relativement simple est encore en vigueur aujourd'hui dans tous les pays européens. Cependant, ces dernières années, des situations se sont multipliées, essentiellement en hiver, où certains pays n'arrivaient plus à s'approvisionner seuls en électricité à certaines périodes, c'est-à-dire que leur production était confrontée à une demande supérieure à ce que leurs centrales électriques étaient en capacité de fournir.

L'exemple le plus récent remonte à janvier 2021, lorsque la France a dû arrêter 11 réacteurs nucléaires de différentes centrales à cause d'un manque de personnel à la suite de la pandémie de Covid-19. En outre, la situation en Allemagne était également tendue, car en raison de la sortie du nucléaire et du charbon, l'Allemagne n'était plus en mesure non plus de pourvoir à son propre approvisionnement. Les deux pays ont été obligés d'acheter des quantités considérables d'énergie à la Bulgarie et à la Roumanie pour combler leurs déficits en électricité.

En Bulgarie et en Roumanie, les centrales à charbon restantes, aussi anciennes soient-elles, ont alors dû fonctionner à plein régime afin d'assurer l'approvisionnement de ces deux pays. Des quantités gigantesques d'électricité ont ainsi été transportées à travers l'Europe, ce qui a provoqué une surcharge au niveau d'un tableau électrique, lequel est tombé en panne, et a entraîné une brusque chute de tension divisant alors le réseau électrique européen interconnecté. Il en a résulté une pénurie dans le nord-ouest, c'est-à-dire qu'en France et en Allemagne, toutes les réserves ont été connectées au réseau et des consommateurs ont parfois dû être déconnectés. En revanche, le sud-est de l'Europe a connu une suralimentation considérable, ce qui signifie que des centrales du même ordre de grandeur ont dû brusquement être déconnectées du réseau afin de maintenir la stabilité de la fréquence.

Cette situation a clairement mis en évidence le fait que si des pays ne sont plus en mesure d'assurer à tout moment leur propre approvisionnement et se retrouvent contraints d'acheter de l'énergie sur le marché, certaines portions du réseau électrique risquent d'être poussées à la limite de leurs capacités, ce qui affecte alors grandement leur résilience. Cela accroît le risque de *black-out*. Viennent s'ajouter d'autres facteurs aggravants de la transition énergétique comme l'augmentation de la consommation d'électricité due aux changements de comportement des utilisateurs (passage du chauffage à l'énergie fossile aux pompes à chaleur, électrification des transports individuels, etc.) ainsi que l'expansion et le commerce transfrontière, entre autres, de sources d'énergie renouvelables non garanties et l'abandon progressif, motivé par des raisons politiques, de l'énergie produite par les centrales nucléaires, à charbon et à pétrole, jusque-là productrices d'énergie garantie.

Au niveau des réseaux, ce tournant énergétique signifie avant tout des charges beaucoup plus élevées en raison des livraisons d'électricité interrégionales. La colonne vertébrale de l'infrastructure du réseau européen a été conçue au milieu du siècle dernier de manière que chaque pays soit en mesure de s'approvisionner par ses propres moyens. Cela signifie qu'en cas de survenance d'un dommage, comme la panne d'une centrale électrique, les lignes transfrontières sont dimensionnées de sorte que la panne d'une ou deux centrales électriques puisse être compensée pratiquement par-delà les frontières. Ces réseaux n'ont toutefois pas été construits pour que des pays entiers puissent s'approvisionner chez leurs voisins.

Une pénurie d'électricité telle que décrite ci-dessus pourrait en principe se produire à tout moment et entraîner des pannes générales d'électricité (*black-outs*) en cas de production insuffisante. La Suisse est surtout menacée à la fin de l'hiver, lorsque les lacs de retenue sont vides et que l'eau de la fonte des neiges ne peut pas encore être transformée en électricité par les centrales hydroélectriques. Si l'on ajoute à cela une vague de froid, une capacité de transport électrique limitée et la panne d'une centrale nucléaire, il faudrait se délester de certaines charges, ce qui pourrait conduire à des *black-outs*.

Découvertes scientifiques

Les transports d'électricité transrégionaux affaiblissent la résilience de la production décentralisée, le stockage de l'énergie et les consommateurs locaux en tant qu'entités stables (notamment en cas de situations de pénurie locales). Il faudrait que l'écologisation de la production ainsi que les changements de comportement des consommateurs qui se traduisent par une hausse de la consommation électrique soient compensés par une augmentation correspondante des capacités de stockage de l'énergie afin de préserver la sécurité d'approvisionnement habituelle. Les délestages pendant les périodes de pénurie d'électricité sont en outre des scénarios non éprouvés qui sollicitent énormément la résilience des réseaux électriques et peuvent, au pire, conduire à des pannes d'électricité généralisées de grande ampleur.

Perception du risque

Certes, les médias ont déjà traité la problématique de la panne générale d'électricité (*black-out*) par le passé. La télévision suisse alémanique (SRF) l'a également abordé dans le reportage « [Blackout – das Experiment](#) » (*Black-out – l'expérience*).

Le scénario de la pénurie d'électricité et d'une panne générale potentiellement à grande échelle, ainsi que les risques y afférents, ne sont néanmoins pas encore pleinement perçus par la population dans toute leur ampleur. Un *black-out* à grande échelle, s'étendant sur plusieurs pays, mettrait hors service l'ensemble de l'économie pendant plusieurs jours, voire plusieurs semaines, et pèserait significativement sur l'ordre public.

Comme nous l'avons déjà indiqué, les autorités responsables ont reconnu le risque de pénurie d'électricité ou de panne générale d'électricité (*black-out*). En ce qui concerne les [pannes d'électricité](#) (voir « *Domaine technique* »), l'OFPP décrit trois scénarios : « intensité considérable, intensité majeure et intensité extrême ».

Pertinence en matière de responsabilité civile

En matière de responsabilité pour dommages corporels et matériels, l'accent est mis sur les entreprises aux infrastructures critiques, lesquelles devraient disposer d'une alimentation électrique de secours en état de marche (hôpitaux, pouvoirs publics, industrie chimique, etc.).

Les hôpitaux et les médecins risquent de voir leur responsabilité civile engagée en cas de dommages corporels à la suite d'une interruption d'électricité, par exemple parce qu'ils ne peuvent alors plus accéder au dossier du patient et courent le risque de ne pas lui administrer les bons médicaments. Ou encore parce qu'ils doivent interrompre voire suspendre une opération chirurgicale puisqu'ils n'ont pas été en mesure d'assurer un approvisionnement électrique garanti. Dans l'industrie manufacturière, des atteintes à l'environnement sont également envisageables si les systèmes de sécurité ne fonctionnent plus correctement.

Une responsabilité pour des dommages pécuniaires ne saurait être exclue non plus, surtout pour les professions libérales (comme les avocats ou les fiduciaires). De tels professionnels concluent des contrats avec leurs clients selon le droit des mandats et doivent répondre de l'exercice d'une activité minutieuse. Même si, sans électricité, ils ne peuvent plus accéder à leurs fichiers informatiques, etc., il est fort probable qu'ils devront de toute façon remplir leurs obligations par d'autres moyens et avec tout le soin requis.

Pertinence en matière d'assurance de la responsabilité civile

Si, en raison d'une panne de courant, une activité / un service ne peut pas être exercée / fourni ou ne peut être exercée / fourni qu'imparfaitement et que cela provoque des dommages corporels et / ou matériels à des tiers (également en rapport avec des atteintes à l'environnement), ceux-ci sont couverts par l'assurance responsabilité civile d'entreprise dans le cadre des autres dispositions contractuelles.

Selon le groupe de risques assuré (comme les avocats, les fiduciaires), l'assurance responsabilité civile peut également couvrir les dommages économiques purs. La couverture d'assurance dépend alors des circonstances concrètes qui ont conduit à la survenance du sinistre.

Les assurances responsabilité civile pour les entreprises disposant d'infrastructures critiques sont les premières concernées. Il s'agit notamment des producteurs d'énergie, des exploitants de réseaux électriques, des hôpitaux, des pouvoirs publics, y compris des forces d'intervention d'urgence, des transports publics, de l'industrie chimique ainsi que d'autres entreprises d'approvisionnement.

Mais d'autres « consommateurs d'électricité » aussi (comme les avocats ou les hôpitaux) risquent également de ne plus être en mesure de fournir leurs services à leurs clients ou de ne plus pouvoir exercer correctement leur activité et devoir dès lors répondre de prétentions élevées par des tiers.

En règle générale, les assureurs responsabilité civile évaluent ces risques dans leurs scénarios de gestion des cumuls d'événements et en déduisent les mesures nécessaires.

Horizon temporel pour les prétentions assurées

Un *black-out* peut survenir à tout moment en Suisse, comme expliqué ci-avant.

Afin de minimiser autant que possible les éventuelles futures prétentions, un échange proactif s'impose avec les autorités ainsi qu'avec les entreprises disposant d'infrastructures critiques, ceci dans un souci de prévention.

4 Bloc théorique et définitions

4.1. Définition des « risques émergents »

La notion de « risques émergents » n'est pas définie uniformément dans le secteur de l'assurance. Le verbe « émerger » vient du latin et signifie « sortir de l'eau, se manifester, se produire ou encore apparaître ». Appliqué aux risques, cela exprime qu'ils apparaissent à l'horizon avec des contours flous et représentent un type de futur danger éventuel. Cette problématique s'est manifestée ces dernières années dans le domaine du changement climatique notamment, de la pandémie ainsi que dans les exemples suivants : cyberrisques, nanotechnologie, Internet des objets (*Internet of Things*) ou Industrie 4.0.

Les risques émergents se distinguent des risques « traditionnels » du fait qu'ils évoluent de manière dynamique – y compris sur une longue période, comme l'amiante – et que, normalement, leur potentiel de dommages ne peut être identifié dans toute son ampleur qu'a posteriori.

4.2. Caractéristiques des risques émergents

Les risques émergents possèdent souvent les caractéristiques suivantes :

- en raison du « principe tous risques » prédominant dans le secteur de la responsabilité civile (tout est couvert, sauf ce qui est expressément exclu), les risques émergents sont souvent déjà inclus dans les portefeuilles des assureurs sans qu'ils en aient vraiment conscience ;
- l'estimation traditionnelle des risques n'est pas applicable car la probabilité d'occurrence du risque ainsi que l'ampleur possible du dommage ne sont pas connues ;
- dans notre monde globalisé, les risques émergents ne peuvent pas être délimités par branches ni par zones géographiques ;
- les risques émergents sont difficilement identifiables. La perception du danger peut être très diverse, elle est compliquée à décrire et à évaluer ;
- le lien de causalité adéquate entre la source du risque (cause) et le dommage consécutif (effet) ne peut souvent pas (encore) être prouvé ;
- les risques émergents sont dynamiques, c'est-à-dire qu'ils évoluent en permanence. Les progrès technologiques, les nouvelles découvertes scientifiques, mais aussi les changements conjoncturels ou encore l'évolution des conditions d'exercice aux niveaux juridique ou social constituent ce que l'on appelle le « risque lié aux changements » et donnent du fil à retordre aux souscripteurs en responsabilité civile.

En fait, les risques émergents entraînent une modification de la nature et de l'étendue des risques. Pour l'assureur, l'important, c'est de tenir compte des engagements de couverture déjà pris. Il a défini ses tarifs de primes en fonction des risques existants et ne saurait imposer les augmentations de primes nécessaires pour couvrir les nouveaux risques supplémentaires et / ou l'étendue de la couverture concernant ces engagements au même rythme que cette aggravation des risques.

4.3. Risque lié aux changements – le paramètre spécifique à l'assurance

Du point de vue de l'assureur responsabilité civile, les paramètres qui sous-tendent les risques émergents peuvent être subdivisés comme suit :

- aspects sociaux / économiques,
- développements juridiques et
- développements technologiques et scientifiques.

Concernant les risques présentés ci-après, les différents aspects de ces développements et leur influence sur le paysage des risques doivent impérativement être considérés au regard du fait que nous évoluons ici dans un environnement extrêmement dynamique et que l'image des risques émergents décrits et, par conséquent, leur assurabilité peuvent bouger dans un sens ou dans l'autre.

4.3.1. Aspects sociaux / économiques

Notre perception du droit s'étant modifiée, nous rejetons de plus en plus l'idée qu'une personne lésée doive supporter elle-même un dommage comme son propre risque inhérent à la vie (mentalité revendicatrice). Certains risques se transforment avec l'évolution de la société et marquent de manière déterminante notre société du risque actuelle. Les changements suivants revêtent une importance particulière :

- besoin accru de sécurité et moindre acceptation du risque,
- informations de meilleure qualité et plus complètes sur les risques,
- influence des réseaux sociaux,
- modification de la perception des risques,
- intensification de l'action des groupes de pression sous forme de recours collectifs organisés,
- société de l'art de vivre et du jeunisme (chirurgie esthétique, thérapies hormonales, certains sports extrêmes, etc.).

Lorsqu'il s'agit de débattre sur les risques présumés et réels de la vie quotidienne, que ce soit l'électromog, les organismes génétiquement modifiés (OGM) utilisés dans les aliments ou bien les nanoparticules, les scientifiques, les responsables politiques, les associations de protection des consommateurs, les autorités ainsi que les médias, tous entendent bien contribuer à la discussion. La principale interrogation, à savoir l'ampleur réelle du ou des risques, demeure fréquemment sans réponse. C'est pourquoi la perception du risque de chacun revêt une importance particulière.

Paradoxalement, l'être humain accepte relativement facilement de courir des risques dont il croit connaître les conséquences possibles, voire probables. Il traverse lorsque le feu est rouge, il effectue des dépassements en voiture sans avoir de visibilité, il inhale la fumée de cigarette cancérigène, il ne se nourrit pas correctement ou encore il pratique des sports en vogue particulièrement risqués. Seuls les risques inconnus lui font vraiment peur.

Par expérience, les risques surestimés et ressentis comme dangereux sont principalement ceux qui sont présentés sous un angle dramatique, à grand renfort de photos et de vidéos, et dont la survenance brutale se

traduit par de nombreuses victimes, comme un crash d'avion. Les risques insidieux, qui se produisent à intervalles réguliers (cent accidents de la circulation causant un mort à chaque fois) sont à l'inverse ressentis comme étant moins graves.

À cet égard, il faut également prendre en compte le rôle des médias. Certains ont souvent tendance à déformer les faits et à mettre en avant des détails peu importants mais susceptibles d'influencer l'opinion publique et d'éveiller également des peurs ici et là. Cela entraîne chez de nombreuses catégories de la population un besoin de sécurité accru, souvent accompagné de mesures officielles adéquates.

Les multiples effets de la mondialisation peuvent être considérés comme un risque émergent s'inscrivant dans un contexte économique. Il s'agit ici notamment de la concentration géographique – déjà réalisée dans certains cas – des sites de production dans des pays à bas salaires, laquelle induit une production de masse, avec le risque que les critères de qualité escomptés ne soient pas respectés. La multiplication des rappels de produits électriques ou électroniques en dit long à ce sujet. Par ailleurs, la mise en place de réseaux de communication, de recherche, de commerce et de transport à l'échelle mondiale a créé des conditions permettant une diffusion à grande échelle et de plus en plus rapide des innovations et des produits.

Les distances spatiales perdent de leur importance et les risques cachés, au lieu d'être ponctuels et limités géographiquement, peuvent se manifester par des dommages étendus, cumulés et survenant dans le monde entier.

4.3.2. Développements juridiques

Les paramètres / sources à l'origine des risques émergents décrits précédemment entraînent régulièrement des modifications du cadre juridique. Celles-ci peuvent correspondre à des modifications de la loi, mais également à des évolutions de la jurisprudence.

En ce qui concerne les risques émergents s'inscrivant dans un contexte juridique, les personnes chargées d'appliquer le droit sont confrontées à la question de la responsabilité dans le cas des risques de développement. Il y a risque de développement si une chose ou un acte, au moment de sa mise en circulation (responsabilité du fait des produits), de l'émission (environnement) ou de la conclusion du contrat (responsabilité du fait du contrat), possède un potentiel de dommages que l'état des connaissances scientifiques et techniques (en tenant compte de la recherche et du développement au niveau mondial) ne permet pas d'identifier.

Une personne a par exemple lancé un nouveau produit sur le marché, et celui-ci a provoqué des dommages de développement qu'elle ne pouvait pas prévoir et qui ne sauraient lui être reprochés : est-elle néanmoins tenue de réparer les dommages commis, ou le lésé est-il condamné à les assumer ? En Suisse, mais également en Europe, cette question a été tranchée par le législateur de diverses manières en fonction de la norme de responsabilité applicable.

Les durcissements des règles de responsabilité sous diverses formes, considérés d'un point de vue global, s'avèrent également une source de risques émergents. Il s'agit par exemple de l'extension des responsabilités pour risques indépendantes de la faute, de la diminution des possibilités de décharge, du prolongement des délais de prescription ainsi que de l'augmentation des prestations de dommages-intérêts et des prestations

versées à titre de réparation morale. À cet égard, il faut mentionner également la mise en œuvre, dans plusieurs pays, de nouveaux instruments permettant de faire valoir plus facilement des prétentions en dommages-intérêts (par exemple les plaintes collectives).

Le système juridique américain, difficilement prévisible pour les Européens, et les décisions de justice qui en découlent, souvent incompréhensibles, doivent également être qualifiés de risque juridique émergent au sens large.

4.3.3. Développements technologiques et scientifiques

Le progrès scientifique et technique, toujours plus rapide, est non seulement à l'origine de technologies complètement nouvelles, comme le génie génétique ou l'application de l'intelligence artificielle, mais a également permis à des technologies déjà connues de prendre de nouvelles dimensions. Ces technologies seront amenées à changer le monde, comme l'ont déjà fait les technologies de l'information (IT). Il convient alors de se demander comment ces nouveaux domaines, et en particulier la part d'inconnu qu'ils renferment, doivent être gérés. Les opportunités résultant de ces (nouvelles) technologies doivent pouvoir être exploitées sans que les dangers qui y sont éventuellement associés dépassent les limites du raisonnable.

Au cours des dernières années, les assureurs responsabilité civile ont été confrontés à plusieurs reprises à des substances, produits et sources de risque dont les conséquences nocives pour la santé sont en partie avérées, mais en partie présumées seulement. Grâce à l'amélioration constante des méthodes de mesure techniques, médicales et scientifiques, il faut s'attendre à ce que d'autres produits et substances considérés jusqu'à présent comme inoffensifs soient identifiés comme nocifs. Des techniques toujours plus affinées permettent parallèlement de déterminer de manière encore plus précise le responsable des dommages et entraînent une multiplication des prétentions en dommages-intérêts.

La plupart de ces substances et sources de risque ont un point commun : les atteintes à la santé ne sont détectables qu'après un laps de temps considérable. L'ampleur complète des risques connexes en matière de responsabilité civile pour le responsable et son assureur sera donc également découverte uniquement a posteriori. Ce phénomène a été parfaitement illustré dans le cas de l'amiante. Pendant des décennies, l'amiante fut considéré comme le matériau des mille et une possibilités, car, contrairement à d'autres fibres, il possède des propriétés optimales pour de nombreuses applications techniques. Des produits contenant de l'amiante ont été utilisés comme panneaux, nattes ou matière à mouler pour la protection incendie et l'isolation thermique, comme garnitures de frein et d'embrayage dans le secteur de la construction automobile ainsi que comme joints en cas de sollicitations thermiques ou chimiques élevées. L'amiante a également été utilisé pour fabriquer des produits en fibrociment. L'amiante est dangereux lorsque ses fines particules sont inhalées et que celles-ci atterrissent par les voies respiratoires dans les poumons où elles sont susceptibles de provoquer différentes maladies comme le cancer de la plèvre (mésothéliome) ou des poumons. Bien qu'une interdiction générale de l'amiante ait été décrétée en 1990 en Suisse, des atteintes à la santé provoquées par l'amiante, notamment en cas de réalisation inappropriée des travaux de désamiantage, ne peuvent pas être complètement exclues aujourd'hui encore. Aux États-Unis, le fait de craindre une pathologie due à l'amiante (*fear of*

Asbestos) suffit à justifier une prétention de dommages-intérêts, sans nécessiter un diagnostic médical explicite.

Dans la problématique liée aux substances toxiques présentes dans les bâtiments ou dans les sols, il ne s'agit pas d'un nouveau risque de responsabilité civile. Bien au contraire : ce sont généralement des potentiels de risque parfaitement connus dans de nombreux cercles. Si certains polluants et leurs effets font régulièrement l'objet d'une attention particulière, c'est non seulement en raison des possibilités de détection plus fines des dommages évoquées plus haut, mais aussi de la sensibilisation accrue de la population et des autorités en charge de l'environnement et de la santé. En dépit des assainissements importants déjà effectués sur des bâtiments comportant des substances toxiques et des sols pollués, et malgré les interdictions dans ce domaine, les assureurs responsabilité civile se verront encore confrontés pendant des années à des demandes de dommages-intérêts élevées par des personnes contaminées, car des substances toxiques, pour certaines encore inconnues, sont toujours présentes dans de nombreux endroits. En l'espèce, on observe alors souvent un phénomène de risque dit « réémergent ».

La connexion d'objets avec Internet (l'Internet des objets (IoT), *Internet of Things* / Industrie 4.0) ne cesse de gagner en importance. Elle se caractérise par la miniaturisation et l'intégration de la microélectronique dans des objets, ainsi que par sa connexion sans fil. L'idée d'être en permanence entouré de nombreuses puces et capteurs communiquant entre eux suscite des craintes quant aux risques éventuels pour la santé, mais aussi pour la vie privée (attaque de la sphère privée). Que des objets réagissent également depuis peu à leur environnement sans nécessiter l'intervention de l'utilisateur laisse sceptique.

5 Risques émergents – Rôle de l'État

Poussé par les craintes et les sentiments souvent subjectifs du grand public, par les revendications de groupes de pression les plus divers et surtout par la pression des médias, l'État est, lui aussi, régulièrement amené à intervenir lorsque des risques émergents surviennent. Si les risques émergents se manifestent de façon très variée, il en va de même des mesures prises par l'État. Comme il est très difficile d'évaluer la probabilité de survenance d'un risque émergent et l'ampleur de ses dommages potentiels, la gestion des risques émergents représente, pour les pouvoirs publics aussi, un véritable défi.

Le besoin de protection de la population dans les cas de scénarios de sinistre parfois encore vagues est souvent confronté à des aspects économiques à ne pas négliger. En matière de risques émergents, non seulement le type de mesures retenues est extrêmement important, mais le moment où celles-ci doivent être prises l'est tout autant. Combien de fois – en particulier dans une perspective internationale – un État s'est-il vu reprocher, à juste titre, d'avoir attendu trop longtemps avant de prendre les mesures adéquates pour désamorcer des problèmes ?

En cas de nouveaux dangers potentiels, l'État dispose des instruments suivants (énumération non exhaustive) pour assumer sa responsabilité de puissance publique :

- fixation de valeurs limites,
- définition d'interdictions,
- directives pour procédures d'agrément spéciales,
- instauration d'obligations de déclaration et / ou de demandes d'autorisation pour certaines activités,
- introduction de réglementations pénales spéciales,
- durcissement des règles de responsabilité,
- introduction d'assurances responsabilité civile obligatoires.

6 Risques émergents – Rôle de l'assureur responsabilité civile

La problématique des « risques émergents », encore peu considérée en tant que telle il y a une quinzaine d'années, est aujourd'hui confiée à des spécialistes hautement qualifiés, surtout chez les principaux réassureurs. Il s'agit avant tout d'identifier les risques de demain.

La gestion des risques émergents représente un véritable défi pour les personnes chargées de la souscription dans la mesure où, compte tenu de l'évolution rapide de l'environnement juridique, social et technologique, il faudrait souvent être devin pour identifier à temps les développements problématiques. Il est donc nécessaire de mettre en place une stratégie de gestion prospective afin de réagir en temps voulu et de manière appropriée à la situation de menace spécifique générée par les risques émergents. Une telle approche devrait comporter les éléments suivants :

- détection précoce (et recensement) des risques émergents,
- analyse des risques émergents,
- application de mesures (de souscription).

Ce processus permet de réunir les conditions requises pour détecter les modifications du paysage des risques, à la manière d'un système d'alerte précoce ou de radar, et développer les solutions adéquates. Pour être utiles, les systèmes d'alerte précoce doivent convertir des signaux faibles, incompréhensibles et difficilement interprétables par les néophytes en critères de décision, voire en instructions, clairement compréhensibles.

6.1 Identification précoce des risques émergents par l'assureur

L'objectif de cette première phase consiste dans l'identification la plus précoce possible des signaux indiquant la présence de risques émergents potentiels. L'environnement de la responsabilité civile doit être « balayé » comme avec un radar à 360° afin de détecter les modifications susceptibles d'influer négativement sur le paysage des risques. Les évolutions techniques, scientifiques, sociales et juridiques occupent le premier plan de telles observations, car elles sont susceptibles de se traduire par l'occurrence d'un risque émergent.

Les articles parus dans la presse et les publications spécialisées, les recherches sur l'Internet, la participation à des séminaires ainsi que l'échange de renseignements avec des collègues, des clients et des spécialistes doivent être considérés comme autant de sources d'information.

L'art du dépistage précoce ne consiste pas à pressentir les futurs développements tel un devin mais à identifier le plus tôt possible des modifications qui se sont déjà produites, ainsi que leurs circonstances, à l'aide des moyens à disposition.

6.2 Analyse des risques émergents par l'assureur

Dans un deuxième temps, les risques émergents identifiés doivent être classés en fonction de leur pertinence pour l'assureur concerné à l'aide d'une codification des risques (par exemple échelle de couleurs « jaune, orange, rouge »), en tenant compte des aspects suivants :

- source des risques émergents constatés (par exemple nouvelle technologie) en tenant compte d'éventuelles interactions avec d'autres facteurs d'influence ;
- probabilité d'occurrence effective du risque ;
- types de dommages concernés (dommages corporels, dommages matériels, dommages économiques purs, dommages à l'environnement) ;
- propagation géographique possible ;
- degré de dangerosité au cas par cas (risques petits, moyens, grands, catastrophiques) ;
- potentiel d'éventuels dommages en série ;
- scénario catastrophe concernant l'ampleur possible des dommages au sein du portefeuille de l'assureur concerné, en tenant compte d'un éventuel potentiel de dommages cumulés ;
- mode de perception par le public (par exemple médias, débats politiques, associations de protection des consommateurs, etc.) ;
- pertinence en matière de droit de la responsabilité civile (par exemple preuve du lien de causalité par rapport à la source du risque et aux dommages consécutifs, ainsi que l'identification éventuelle d'un responsable avéré) ;
- mesures officielles éventuelles (par exemple interdictions, prescriptions de sécurité, durcissement des règles relatives à la responsabilité, obligations d'assurance, etc.).

Cette classification des risques émergents constitue une base pour déterminer le type et l'urgence des mesures à prendre.

6.3 Mesures des assureurs en matière de risques émergents

Dans le cadre de la gestion actuarielle des risques émergents, l'assureur responsabilité civile doit d'abord s'interroger sur l'assurabilité de tels risques. Les caractéristiques des risques émergents détaillées ci-dessus montrent que ces derniers ne sont pas d'emblée compatibles avec les critères généralement reconnus qui conditionnent l'assurabilité des risques. D'autre part, les assureurs vivent du fait qu'ils prennent en charge des risques. En conséquence, l'assureur responsabilité civile ne doit pas se soustraire à ses engagements, mais au contraire les respecter en tenant compte des besoins des entrepreneurs de la manière la plus exhaustive possible, tout en restant contrôlée. Pour l'assureur responsabilité civile, il s'agit donc de trouver le juste équilibre entre le refus de la prise en charge des risques (dont se plaint fréquemment l'industrie) et une souscription trop risquée (dont se plaignent les contrôleurs et analystes). Mais à cette fin, il a besoin d'un système sensoriel solide, axé sur les risques, pour faire face aux conséquences négatives radicales que peuvent entraîner les risques émergents.

Pour couvrir les conséquences négatives que peuvent avoir pour lui des dommages potentiels causés par des risques émergents, l'assureur responsabilité civile dispose par exemple des options suivantes :

- à l'aide d'obligations, faire en sorte que l'ensemble des possibilités techniques visant à limiter le risque soient exploitées et que les recommandations appropriées ainsi que les valeurs limites en vigueur soient respectées ;
- limiter les montants à couvrir en convenant de seuils pour certains risques ;
- au regard du potentiel que représente une multitude de personnes concernées, prévoir une clause efficace applicable aux dommages en série. Il convient de noter que le regroupement actuariel escompté de plusieurs dommages provoqués par une même cause dans le cadre d'un événement unique n'est efficace que si le risque émergent concerné est considéré comme la cause commune à tous les sinistres qui en résultent ;
- compte tenu de l'application approximative des dispositions légales dans certains pays (par exemple États-Unis, Canada), une restriction de la validité territoriale peut s'imposer ;
- les risques émergents étant souvent des risques à long terme, prévoir un rattachement précis des cas d'assurance à prendre en charge à une période d'assurance donnée, et donc à un contrat d'assurance donné. En règle générale, l'adoption du principe de la réclamation (principe « *claims made* ») s'impose pour définir le champ d'application temporel ;
- accord sur une garantie unique par année d'assurance ;
- accord sur des franchises supérieures ou spécialement aménagées ;
- exclusion de couverture du risque émergent concerné ou de certaines de ses composantes.

Jouent également un rôle important une communication claire sur la politique de souscription et la publication de directives de souscription spéciales concernant la gestion actuarielle des risques émergents ainsi que l'ouverture le plus tôt possible d'un dialogue sur les risques avec les entreprises concernées, les autorités et les autres organismes impliqués.

Une gestion professionnelle des risques émergents, fondée sur un système d'alerte précoce opérationnel, pourrait également offrir des opportunités au secteur de l'assurance. Ainsi, par exemple, le développement de produits d'assurance et de services innovants permettrait de générer de nouveaux champs d'activité.

ASA | SVV

Association Suisse d'Assurances ASA

Conrad-Ferdinand-Meyer-Strasse 14

Case postale

CH-8022 Zurich

Tél. +41 44 208 28 28

info@svv.ch

svv.ch