Bulletin Juridique Des Assurances
BJDA
Anciennement Actuassurance
www.bjda.fr
LexisNexis®
www.lexisnexis.fr

Le développement de l'assurance du risque cyber : rapport de la Direction générale du Trésor

Antoine Touzain,
Professeur agrégé, Université Rouen Normandie,
CUREJ, UR 4703

Contrat d'assurance – Risque Cyber- Assurabilité

La Direction générale du Trésor a publié, au début du mois de septembre, son rapport dédié à l'assurance du risque cyber[1], dont elle appelle le développement. De façon habituelle, le rapport procède à un constat (I) avant de présenter plusieurs propositions (II).

I) Le constat de départ est celui d'une multiplication des cyberattaques, exposée par l'AMRAE[2] (p. 9-10), qui contraste avec le trop faible développement du marché de l'assurance cyber en France, notamment quant à la couverture des petites et moyennes entreprises (p. 12-13).

Or, le cadre juridique actuel ne serait pas adapté, le rapport reprenant plusieurs incertitudes qui ont déjà été pointées en doctrine[3] :

---

[1] Disponible en ligne : https://www.tresor.economie.gouv.fr/Articles/2022/09/07/remise-du-rapport-sur-le-developpement-de-l-assurance-du-risque-cyber. Sur ce rapport, v. les observations de S. Porcher, « L'assurance du risque cyber : quelques recommandations de la Direction générale du Trésor », *Dalloz actualité*, 26 sept. 2022.

[2] Le rapport se réfère notamment au rapport AMRAE, *Lumière sur la CYberassurance*, juin 2022, disponible en ligne : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4022&ref_type=publication&items=4022.

[3] P.-G. Marly et A. Valençon, L'assurance du risque cyber, *Dalloz IP/IT* 2019. 603.

- la garantie cyber serait souvent implicite (p. 14) car il y aurait des incertitudes quant à la couverture des risques cyber[4] : on voit pourtant mal en quoi il s'agit là d'un problème lié au « cadre juridique », car il s'agit surtout d'une imprécision des polices, ce que ne nie d'ailleurs pas le rapport qui évoque « un effort de clarification » des clauses des assureurs (p. 14) ;

- l'assurabilité du paiement des cyber-rançons, pourtant proposée dans de nombreux contrats d'assurance, demeure incertaine (p. 15-17) ;

- l'assurabilité des sanctions administratives serait rendue plus délicate avec le renforcement des obligations des responsables de traitement depuis l'entrée en vigueur du RGPD, que les contrats d'assurance couvriraient fréquemment malgré les doutes sur l'assurabilité (p. 17-18) ;

- l'absence de définition de la notion de cyberguerre créerait une incertitude quant à la qualification d'une exclusion légale, par application de l'article L. 121-8 du code des assurances, ce qui pourrait conduire à une multiplication des clauses d'exclusion en ce domaine.

Le rapport pointe également « la problématique de l'accès à la donnée », à savoir la difficulté qu'il y a à quantifier le risque cyber, en raison de l'absence de recul historique et de son caractère « évolutif et polymorphe », auquel s'ajoute le « flou autour des cyberattaques effectives », qui ne sont pas toujours déclarées, en raison du risque réputationnel qui pourrait découler des communications sur le sujet (p. 19).

Le rapport évoque en outre le caractère systémique que pourrait présenter le risque cyber de grande ampleur (p. 20) dès lors que les systèmes d'information sont interconnectés[5]. Il précise néanmoins que ce risque demeure assurable car maîtrisable, indiquant que 97 % des sinistres cyber couverts ont, en 2021, donné lieu à une indemnisation inférieure à 3 millions d'euros (p. 21). Pour autant, la dégradation de la sinistralité conduit à un durcissement des conditions d'assurance, qui pourrait rendre le coût d'assurance difficilement maîtrisable pour les entreprises (p. 21-22). Si le risque paraît absorbable grâce à des captives de réassurance, « l'écosystème français » y serait encore « insuffisamment favorable » (p. 22-23).

Enfin, le constat se termine par un rappel de la faible culture du risque en matière cyber : à la fois du côté des souscripteurs, qui demeurent trop peu couverts pour ce qui est des TPE et PME – tandis que la couverture des grandes entreprises est assez satisfaisante, même si le « niveau de maturité » des entreprises françaises n'est encore que de 46 % –, mais aussi du côté des intermédiaires d'assurance, qui n'auraient pas de compréhension suffisante des produits distribués (p. 24-25).

II) Des propositions sont ainsi formulées pour favoriser le développement de l'assurance du risque cyber.

Il est déjà proposé une « clarification du cadre juridique » (p. 26), pour répondre au premier constat :

---

[4] Sur cette question, v. aussi le récent rapport de l'Autorité européenne des assurances et des pensions professionnelles : S. Porcher, L'intervention de l'AEAPP face au risque de couverture silencieuse du risque cyber , *Dalloz actualité*, 13 oct. 2022.

[5] On rappellera à cet égard que le risque cyber faisait partie des risques systémiques contre lesquels alertait le CESE dans son récent rapport (v. A. Touzain, Appréhender les risques systémiques : les préconisations du Conseil économique, social et environnemental, *bjda.fr* 2022, n° 81).

- le rapport propose de promouvoir de bonnes pratiques de rédaction des contrats » (p. 26), passant notamment par la lutte contre les « couvertures silencieuses » et par des exclusions mieux rédigées : on peut s'étonner de ce que le rapport, qui rappelle la distinction entre les garanties « tous risques sauf » ou à « périls dénommés », ne prenne ainsi pas parti pour les secondes, qui permettraient de limiter les doutes quant à l'assiette de la garantie ;

- dans la même ligne, la DGT propose de renforcer l'information communiquée à l'assuré, de manière à mentionner explicitement la couverture ou son absence, afin de clarifier les garanties offertes (p. 27-28) : si la méthode n'est pas nouvelle, ne risque-t-on pas, en multipliant les informations, que celles-ci ne soient pas lues ?

- le rapport traite également la question essentielle de l'assurabilité des cyber-rançons, en proposant (comme un projet de loi du 7 septembre) de la subordonner au dépôt d'une plainte (p. 28), l'idée étant de concilier les intérêts des victimes (qui ont besoin d'être indemnisées), des assureurs français (puisqu'une telle assurabilité est admise dans d'autres États européens) et des pouvoirs publics (qui pourraient lutter contre la cybercriminalité grâce à la remontée d'informations)[6] ;

- le Trésor prend, à l'opposé, le parti de l'inassurabilité des sanctions administratives et notamment de celles pouvant être prononcées par la CNIL pour irrespect des obligations issues du RGPD (p. 29) : cette proposition n'apparaît guère discutable, étant donné que le caractère para-pénal de ces sanctions justifie un maintien de la logique punitive, qui n'est guère compatible avec une quelconque assurabilité ;

- enfin, le rapport évoque la question de la définition de la cyberguerre, rappelant que le rapport du Haut comité juridique de la place financière de Paris de janvier 2022 recommande d'actualiser la notion de guerre étrangère de l'article L. 121-8 du code des assurances pour y inclure la cyberguerre : la DGT conclut néanmoins à la nécessité de créer un groupe de réflexion sur cette question, tant la notion de cyberguerre est difficile à appréhender actuellement (p. 30).

En outre, des propositions sont faites pour améliorer la prise en compte de ce risque :

- il est ainsi suggéré d' « améliorer la prise en compte du risque cyber dans le pilotage de l'activité assurantielle », donc au titre de l'évaluation interne des risques (ORSA), ce qui permettrait, par effet boule de neige, une meilleure compréhension du risque encouru par les assurés (p. 31-32). À ce titre, le rapport recommande la consécration d'une catégorie identifiée au sein du code des assurances, rappelant néanmoins que cela supposerait de remédier aux garanties implicites (p. 33) ; il appelle « en complément » une branche dédiée au niveau européen (p. 34), niveau qui devrait pourtant être plus qu'un complément, étant donné l'importance fondamentale de l'appréhension du risque cyber aujourd'hui ;

- en outre, certaines propositions sont faites pour pallier le manque de données cyber, la DGT appelant de ses vœux l'élaboration d'une base de données cyber et, dans l'attente de sa constitution, l'usage de méthodes alternatives (notamment le recours à l'intelligence artificielle) afin de modéliser le risque (p. 34-35) ; surtout, le rapport suggère une proposition fréquemment avancée en matière de risques nouveaux, à savoir une mise en commun des données par les assureurs, tout en pointant les difficultés liées à la concurrence et à la réglementation des données (p. 36) ;

---

[6] Sur ce triple enjeu, V. P.-G. Marly, Vers un encadrement de l'assurance des cyber-rançons, *JCP E*, n° 40, 6 oct 2022. 807.

- par ailleurs, le rapport suggère, dans une démarche désormais habituelle, de procéder à une répartition des risques, ce qui passe par la promotion de l'auto-assurance via la constitution de captives de réassurance, qui pourraient à terme devenir des « captives par compartiment », lesquelles permettraient de mutualiser non pas les risques mais la structure captive (p. 38), sauf à constituer des mutuelles pour procéder à une réelle mutualisation du risque (p. 39) ; à long terme, le rapport propose également de transférer le risque aux marchés de capitaux notamment via des mécanismes de titrisation que sont les *insurance linked securities* (*ILS*) (p. 39), ce qui supposerait une meilleure connaissance du risque ; c'est pourquoi, à plus court terme, il est privilégié de recourir à l'assurance paramétrique, qui serait adaptée à la plupart des sinistres cyber qui sont de faible intensité, permettant une indemnisation rapide et adéquate (p. 40) ;

- enfin, le rapport insiste sur la nécessité de sensibiliser les entreprises, notamment par la diffusion de standards de sécurité afin d'inciter les entreprises à « renforcer leur résilience cyber »[7] (p. 41), ce qui passerait par une meilleure offre de formation (p. 43) mais aussi par la promotion d'une « *task force* » de l'assurance du risque cyber, adossée à Paris Europlace, dont le rôle serait de piloter la mise en œuvre des préconisations faites par le rapport (p. 43).

Ce rapport contient donc de fort intéressantes propositions et procède à une bonne synthèse de l'état des questions : on ne peut donc qu'en recommander la lecture.

[7] Ce qui rejoint le constat, déjà fait par le *Rapport préc* du CESE, d'une insuffisante « culture du risque » en matière de risques systémiques.