L'assurabilité des risques cyber

Michel Cojean, Délégué général de l'AEFR, a introduit la matinale en rappelant que le risque cyber est central pour toutes les entreprises et particulièrement dans le secteur financier. En outre, la couverture de ce risque suscite une attention spécifique des pouvoirs publics : le Trésor a lancé une concertation nationale sur l'assurance du risque cyber en 2021[1], et des initiatives européennes ont vu le jour, comme le Cyber Security Act[2] ou la proposition de règlement DORA sur la résilience opérationnelle numérique du secteur financier[3]. Enfin les cybermenaces se sont encore sensiblement renforcées au cours des dernières semaines, dans le contexte de la guerre en Ukraine.

Si un rapport récent du Sénat[4] recommande le recours à ces assurances, ce marché n'est pas encore totalement mature, et les offres aujourd'hui développées par les assureurs restent évolutives en termes de coût et de couverture. C'est l'objet de la présentation de Patrick Degiovanni, Directeur général adjoint de Pacifica, qui a rappelé la nature du risque cyber et la structuration des assurances en la matière. Il a également détaillé la structuration du programme d'assurance cyber du Crédit Agricole

Le marché de la cyber assurance reste aussi contraint par des freins issus de la réglementation française. C'est la raison pour laquelle le Haut Comité Juridique de la Place Financière de Paris (HCJP), sous l'impulsion du Trésor, a souhaité clarifier dans un rapport les questions juridiques soulevées par l'assurance du risque cyber. Les conclusions de ce rapport sont présentées par Pierre Minor, avocat, ancien Directeur juridique du groupe Crédit Agricole et Président du groupe de travail du HCJP.

Patrick DEGIOVANNI
Directeur Général Adjoint, Pacifica
Membre du GT du HCJP

Le risque cyber se définit comme un risque affectant un dispositif informatique. La caractéristique d'une cyberattaque est d'être invisible, intensive, incompréhensible, internationale, incertaine et intentionnelle (règle des 6i), ce qui explique la difficulté des assureurs de bien évaluer le risque pour proposer des réponses adaptées.
Les chiffres et évaluations aujourd'hui disponibles concernant le marché de la cyber assurance montrent que ce dernier reste encore modeste avec environ 130 M€ de cotisations, et un rapport

---

[1] *Lancement d'une concertation nationale sur l'assurance du risque cyber*- Rédigé par DG Trésor - Publié le 05 juillet 2021 : https://www.tresor.economie.gouv.fr/Articles/2021/07/05/lancement-d-une-concertation-nationale-sur-l-assurance-du-risque-cyber

[2] *Loi de l'UE sur la cybersécurité* : https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-act

[3] *Proposition de Règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier* : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0595

[4] *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?* Rapport d'information de Sébastien Meurant et Rémi Cardon - 10 juin 2021 : https://www.senat.fr/notice-rapport/2020/r20-678-notice.html

sinistres/cotisations difficile à évaluer. Ce marché ne mobilise aujourd'hui pas suffisamment de clients pour organiser une mutualisation efficace du risque cyber : selon les données de l'AMRAE[5], 87% des grandes entreprises ont une couverture cyber, 8% des ETI et 0,0026 % des PME, alors que des incidents de cybersécurité ont concerné 43% des PME en 2020.

L'approche du risque cyber par le marché de l'assurance doit s'articuler autour de trois piliers :
- la prévention : le diagnostic du risque cyber, des vulnérabilités des systèmes d'information et des protections déjà existantes au sein de l'entreprise ;
- la protection avec le traitement à froid des axes d'amélioration identifiés ;
- l'indemnisation, avec le traitement à chaud de la couverture du sinistre notamment au travers d'un contrat d'assurance et par la mise en place de process pour faire face aux conséquences d'un évènement.

Les réponses à ces différents points ne sont pas nécessairement entre les mains d'un même acteur, mais entre un assureur et potentiellement des spécialistes en matière de diagnostics, de remédiation, etc.

Concernant plus directement les solutions assurantielles, les garanties cyber peuvent se situer dans différents types de contrats : elles peuvent être intégrées au sein de contrats multirisques, sous forme historiquement de *silent cover*, car ces contrats n'excluaient pas ce type de risque. Ce qui a suscité une réaction des réassureurs qui craignaient qu'un grand nombre de contrats puissent être simultanément touchés par un même évènement. Par exemple, les professions médicales sont amenées à utiliser les mêmes logiciels comptables : en cas d'attaque de ces derniers par des hackers, si les contrats d'assurance multirisques de ces professions médicales contiennent une garantie cyber, explicite ou implicite, il y aurait alors un cumul de risques à indemniser. Aujourd'hui la tendance est d'isoler ces garanties cyber au sein d'offres dédiées que proposent beaucoup d'assureurs. Néanmoins la demande reste encore timide.

Enfin certaines offres comportent une proposition d'assurance complétée par une analyse préalable pour vérifier l'assurabilité du risque cyber. Elles concernent plus les grandes entreprises et ETI et permettent aux assureurs d'éviter de proposer un contrat dans une entreprise dont le SI présenterait de graves failles de sécurité.

Reste qu'il existe des tensions sur les capacités que peuvent apporter les assureurs sur ce risque. Cela provoque des augmentations de primes qui peuvent être significatives. Le cumul d'engagements contraint les assureurs à travailler sur les exclusions ou de restriction des garanties. L'assurabilité du risque cyber est également mise en cause du fait de la faible mutualisation et d'une insuffisance de la

[5] *Rapport LUCY : LUmière sur la CYberassurance*, AMRAE, mai 2021 : https://www.amrae.fr/recherche?type=All&search_api_fulltext=etat+du+marche

diversification du risque. Des questionnements subsistent en matière de règlementation. Globalement de nombreuses inconnues sur la manifestation de ce risque le rendent encore difficile à cerner.

Pierre MINOR
Avocat associé, Coat Haut de Sigy De Roux Minor
Ancien Directeur juridique du Groupe Crédit Agricole
Président du groupe de travail du HCJP

Le rapport du HCJP est consacré à l'assurabilité du risque cyber. Il s'est plus particulièrement penché sur trois sujets :

- peut-on couvrir les sanctions administratives par des mécanismes assurantiels ? Il existe un flou en droit français dans les contrats d'assurance sur ce sujet. Il s'agit aussi de savoir si les sanctions imposées par la CNIL en cas d'attaque cyber peuvent être assurées, qu'il s'agisse de sanctions pécuniaires ou de mesures correctrices ;
- Est -il possible de couvrir le cyber rançonnage par des mécanismes assurantiels ?
- Enfin, le risque de guerre usuellement exclu des assurances. Ce concept de guerre est-il de même nature lorsque le fait générateur est de nature cybernétique ?

Les couvertures des sanctions administratives

La doctrine est traditionnellement défavorable à l'assurabilité des sanctions administratives (prononcées par la CNIL, l'ACPR, l'AMF, etc…). Elle se fonde sur un arrêt de la cour de Cassation de 1960 qui qualifie les sanctions administratives de « peines », une position confirmée par la jurisprudence du Conseil Constitutionnel, de la CJUE, ainsi que par le Conseil d'Etat qui a considéré que relèvent du champ pénal les sanctions fiscales et pécuniaires prononcées par la Commission bancaire, le Conseil des marchés financiers, le Conseil de la discipline de gestion financière, ou encore la Commission des sanctions de l'AMF. Or il existe un principe intangible de personnalité de la peine repris à l'article 121-1 du Code pénal qui dispose que « *nul n'est responsable pénalement que de son propre fait* » et qui empêche qu'une personne autre que le prévenu puisse se substituer à lui dans l'exécution de sa peine.

La notion d'ordre public a aussi souvent été invoquée pour s'opposer à l'assurabilité des sanctions administratives. Ainsi une réponse ministérielle du 24 novembre 1997 précise que l'ordre public s'oppose à ce qu'un assureur prenne en charge les amendes pénales, de même que fiscales, douanières ou tout autre sanction pécuniaire prononcée par les autorités administratives.

Le groupe de travail du HJCP est donc arrivé à la conclusion qu'il n'était pas possible d'assurer des amendes administratives et des sanctions pécuniaires.

Il a abouti à la même conclusion s'agissant des sanctions pécuniaires des astreintes de la CNIL en s'appuyant sur la même analyse, mais également sur les dispositions spécifiques du RGPD qui précisent que les sanctions prévues (art. 83) doivent être effectives, proportionnées et dissuasives, ce qui parait exclure une assurabilité.

En revanche, les mesures correctrices demandées par la CNIL, pourraient faire l'objet d'une couverture assurantielle. Il s'agit par exemple de la remise en conformité des opérations de traitement, ou les conséquences pécuniaires de la mise en demeure de communiquer aux personnes concernées une violation des données à caractère personnel.

Pour clarifier le sujet, le groupe de travail recommande de modifier la loi de 1978, pour déclarer inassurables les astreintes et les autres sanctions pécuniaires décidées par cette loi ou par le RGPD, et de clarifier le sujet de manière plus générale s'agissant des autres autorités qui devraient suivre le même régime.

L'assurabilité du cyber rançonnage

L'assurabilité de la rançon en cas de cyberattaque, sujet très sensible, a été examinée sur le plan juridique.

- Au regard du droit civil, les assureurs qui remboursent des rançons pourraient se voir reprocher de faciliter de nouvelles infractions, ce qui irait à l'encontre de l'ordre public et des bonnes mœurs. Toutefois, il n'existe pas de jurisprudence sur ce sujet. La doctrine dit que l'assurance d'un risque est illicite à deux conditions alternatives : soit un texte spécial le prévoit, soit la garantie a directement pour objet une activité elle-même illicite. Ainsi l'assurance des rançons ne serait pas illicite car aucun texte n'est venu l'interdire et que le paiement de la rançon par l'assuré victime du chantage d'un hacker n'est pas non plus une activité illicite ou pénalement condamnable.
- Au regard du droit des assurances, aucun texte ni décision n'interdit aujourd'hui la couverture du risque de rançon, comme c'est le cas pour d'autres risques (assurance dite « retrait de permis »).
- Au regard du droit pénal, l'entreprise qui fait l'objet d'une demande de rançon suite à une cyberattaque est une victime et donc le paiement de la rançon n'est pas en soi une infraction pénale, puisque le paiement peut être considéré comme fait sous la contrainte. Avec cependant une limite qui est l'infraction de financement du terrorisme dans l'hypothèse où la rançon serait versée à un groupe terroriste. Cette infraction serait caractérisée par la connaissance que les fonds sont destinés à être utilisés en vue de commettre un acte de terrorisme. Toutefois, même dans cette hypothèse, une contrainte exonératoire du Code pénal pourrait s'appliquer dans certaines circonstances, compte tenu du montant de la rançon ou des conséquences d'un non-paiement pour l'entreprise visée.

  Concernant l'entreprise d'assurance, celle-ci n'encourt pas non plus de responsabilité pénale à prévoir le remboursement d'une cyber rançon, si elle n'a pas connaissance, en amont du règlement de la rançon par l'assuré, du fait que celle-ci va aller alimenter un réseau terroriste. Ce remboursement

n'apparait pas non plus comme pouvant tomber sous le coup de l'infraction de blanchiment, puisqu'il est fait avec des fonds légaux, sans aucun effet dissimulateur de sa provenance. Cette analyse permet de conclure à la possibilité au regard du droit pénal d'assurer le remboursement de la rançon.

Des limites figurent cependant dans le Code monétaire et financier pour les assureurs concernant la lutte contre le blanchiment et le financement du terrorisme. Il leur appartient de mettre en place des procédures de vérification dans le cadre de la vigilance courante et de la vigilance renforcée : déclarations à Tracfin, et suspension du paiement au titre de la garantie tant que Tracfin ne s'est pas prononcé. Le groupe de travail recommande de bien informer les assurés que la réglementation peut éventuellement entrainer une suspension de l'indemnisation par les assureurs.

Les assureurs sont également tenus de respecter les régimes de sanctions tant au regard de la législation française qu'au regard des législations étrangères, notamment dans le cas de gel des avoirs. Avant tout remboursement de rançon l'assureur doit s'efforcer d'identifier l'attaquant et de vérifier s'il n'est pas désigné par une mesure de gel des avoirs. Cela représente un risque juridique pour les assureurs étant donné l'obligation de résultat imposée par les textes, et le fait que les bénéficiaires des paiements sont souvent difficilement identifiables.

Enfin, le groupe de travail s'est intéressé au traitement de la rançon dans les autres pays. Une très grande majorité de pays n'interdit pas l'assurabilité du remboursement des rançons, celui-ci étant subordonné au respect des législations relatives à la lutte contre le blanchiment et le financement du terrorisme. De nombreux pays recommandent toutefois aux victimes de s'abstenir de payer les rançons, mais sans aller jusqu'à l'interdire. Une majorité de pays incitent également les entreprises à prendre des mesures techniques pour lutter contre ce type d'attaques et en limiter les effets. Autre trait commun, beaucoup de pays exigent que les autorités nationales soient informées d'une demande et du paiement d'une rançon, et que ce sujet soit traité de façon confidentielle.

Après avoir constaté qu'au regard du droit, l'assurance d'une rançon est envisageable, faut-il ou non, interdire ce type de contrat et le remboursement des rançons ? L'argument le plus souvent cité en faveur de l'interdiction est que le paiement de rançons nourrit un écosystème criminel et incite les hackers à multiplier les attaques. A contrario, interdire l'assurabilité de la rançon conduit à faire peser sur les entreprises victimes le poids financier de cette dernière et les conséquences du non-paiement, ce qui peut mettre en danger la survie de l'entreprise ; en outre les assurances peuvent être utiles pour apporter des mesures d'information et de formation, mais également des mesures techniques de protection que les entreprises pourraient ou devraient mettre en œuvre pour se protéger dans le cadre de la souscription des assurances.

Le groupe de travail s'est également interrogé sur les conséquences d'une interdiction qui resterait nationale. Celle-ci pourrait s'inscrire dans le droit européen parce que le sujet relève d'un domaine qui n'est pas harmonisé, ne ferait pas double emploi avec une règle déjà existante en France, et pourrait

être considérée comme poursuivant un objectif d'intérêt général. Mais elle entrainerait un désavantage concurrentiel pour les assureurs français, si ces règles ne s'appliquent pas également aux assureurs étrangers qui couvriraient des risques cyber situés en France dans le cadre de la libre prestation de services. Cela créerait également une distorsion de concurrence pour les entreprises françaises qui ne pourraient pas bénéficier d'une assurance de la rançon.

Se pose alors la question de la possibilité pour l'UE d'adopter un texte contraignant pour interdire l'assurance des rançons. Cela parait juridiquement possible mais non souhaitable, compte tenu du fait que la plupart des pays n'interdisent pas l'assurance de la rançon, et qu'il existe un réel besoin de protéger les entreprises et d'améliorer leur résilience vis-à-vis du risque cyber.

Le groupe de travail a formulé de nombreuses recommandations qui sont des mesures d'ordre opérationnel, règlementaire, et de prévention pour sensibiliser les opérateurs. Parmi les plus importantes, figurent le dépôt de plainte, et la facilitation des dépôts de plainte pour informer les différentes autorités publiques compétentes ; le renforcement des dispositifs publics de cyber-protection à la fois en moyens humains et financiers, et l'amélioration de la coordination entre les différentes autorités publiques compétentes(ANSSI, cybermalveillance.gouv, gendarmerie nationale, l'office central contre la criminalité liée aux technologie de l'information et de la communication, les autorités judiciaires…). Il serait utile d'instaurer une autorité publique unique ou centralisatrice qui puisse être leader sur ce sujet.

Le projet de loi LOPMI d'orientation et de programmation du Ministère de l'Intérieur, du 16 mars 2022, a repris un certain nombre de ces recommandations : pas d'interdiction d'assurer les rançons ; le Ministère de l'Intérieur serait désigné comme le chef de file de la lutte contre la cybercriminalité ; le paiement de la rançon et de l'assurance de la rançon est conditionné au dépôt de plainte avec la création d'un numéro « 17 cyber » pour faciliter les dépôts de plainte.

Le concept de cyber guerre dans les contrats d'assurance

Enfin le risque de guerre lors que le fait générateur est cybernétique est-il exclu des contrats d'assurance ? Le droit français est plus traditionnel dans son approche, et la guerre répond à une approche formaliste nécessitant une déclaration préalable des états attaquants, la Constitution précisant que « La déclaration de guerre est autorisée par le Parlement ». Toutefois une évolution intéressante peut être notée : trois alinéas ont été ajoutés en 2008 à la Constitution, pour introduire une nouvelle catégorie qui est celle de l'intervention des forces armées à l'étranger, impliquant d'informer le Parlement, ce qui contribue à un effacement de la notion de guerre comme catégorie ou institution juridique exclusive, au profit d'autres notions.

En revanche, les attaques cyber assimilables à des actes de guerre sont une réalité admise en droit international. Ainsi les Conventions de Genève de 1940 (article 2) s'appliquent en cas de guerre déclarée

ou de tout autre conflit armé surgissant entre des parties contractantes, même si l'état de guerre n'est pas reconnu par l'une d'elles. Cette approche échappe au formalisme classique d'une déclaration de guerre qui n'est pas le préalable à la qualification de cyberguerre. Les commentaires de 2020 de l'article 2 des Conventions de Genève considèrent que des actions cyber en parallèle d'actions militaires plus classiques constitueraient bien un conflit armé international.

De même la charte des Nations Unis s'applique à n'importe quel emploi de la force et des armes dont une opération cyber n'est pas exclue. Et il n'existe pas, en droit public international, d'obligation pour un Etat de prouver publiquement l'imputabilité d'un acte illicite dont il est victime à un autre Etat.

Le groupe de travail a proposé une modification de l'article 121-8 du Code des assurances pour clarifier ce sujet et ajouter au concept de guerre étrangère, celui de conflit armé international, quels que les moyens utilisés, militaires ou cybernétiques.

Couverture du risque cyber : l'exemple du groupe Crédit Agricole

L'expérience présentée par Patrick Giovanni couvre les activités assurantielles et bancaires, françaises et internationales, du groupe Crédit Agricole. La première étape a consisté à évaluer le risque et les conséquences financières potentielles en cas d'attaque. En dépit de la qualité de la prévention mise en place au sein du groupe, et même si la probabilité de survenance reste complexe à évaluer, le sinistre maximum possible auquel il pourrait être confronté a été évalué à plusieurs centaines de millions d'euros.

Une fois cette évaluation effectuée, il a fallu chercher sur le marché le montant correspondant de capacité. Or le marché sur des risques bancaires ou d'assurance est aujourd'hui très frileux. La seule façon de trouver des solutions suffisantes est de répartir ces risques entre quasiment tous les acteurs du marché, avec une première conséquence qui est que les marges de manœuvre pour négocier les primes d'assurance sont de ce fait limitées. Le groupe a dû faire face à une forte augmentation de ses primes d'assurances, en dépit de l'absence de sinistres au-dessus de la franchise conservée par le groupe en interne, qui se mesure en dizaines de millions d'euros. Cela a induit également un doublement de la conservation de risques en interne par le biais de l'entité d'assurance Pacifica et dans chaque entité du groupe. La plupart des grandes entreprises connaissent les mêmes contraintes.

Questions / Réponses

France Arnaud, présidente-fondatrice du courtier Solmondo, confirme que, pour les grands comptes, le marché est compliqué et la concurrence difficile à faire jouer. Concernant les PME en revanche, les tarifs sont beaucoup moins élevés, et il est difficile de comprendre pourquoi ces petites entreprises ne sont pas plus nombreuses à recourir à ces assurances. Elle espère que cette situation amènera l'administration française à revoir le régime fiscal des captives d'assurance, notamment en comparaison

de leur traitement au Luxembourg qui permet la constitution de provisions et le lissage dans le temps des éventuelles conséquences des sinistres. Il est souhaitable que les travaux qui ont débuté en France à ce sujet débouchent rapidement.

Différentes questions ont été posées à propos du projet de loi LOPMI, quant au délai nécessaire pour le faire aboutir (Michel Cojean) et les modalités prévues pour le dépôt de plainte (Marie Rémy-Bétolaud, Responsable juridique et conformité, France Assureurs). Le projet de loi LOPMI a été déposé auprès de l'Assemblée nationale, mais le débat parlementaire serait reporté après les élections présidentielles. Le projet de loi conditionne le remboursement de la rançon à un dépôt de plainte de la victime, qui doit intervenir au plus tard 48 heures après le paiement de la rançon : pourquoi le dépôt de plainte n'est-il pas prévu dès la demande de rançon ? Pierre Minor estime qu'il s'agit simplement de fixer un délai butoir.

Aymeric Pontvianne, conseiller finance innovation à la direction de la conformité de la CNIL, rappelle les commentaires faits devant le groupe de travail en début 2021 sur la proposition de modification de la loi Informatique & Libertés : il s'interroge sur le sort particulier fait aux sanctions prévues par la CNIL par rapport à celles d'autres autorités administratives. Une modification du Code des assurances pourrait cibler l'ensemble des sanctions administratives et pas uniquement celles du RGPD. Par ailleurs, Aymeric Pontvianne rappelle que la CNIL ne recommande pas le développement de garanties qui viendraient assurer les mises en demeure de la CNIL, dès lors que cette dernière a engagé une action répressive pour protéger l'ordre public économique. En outre la CNIL ne met généralement en demeure un responsable de traitement victime d'un cyber crime que dans des cas où elle constate des négligences graves de sa part eu égard à ses obligations de sécurité des données. Dans ce cas, la mise en conformité demandée au responsable de traitement va bien au-delà d'une simple remise en état des systèmes d'information. La CNIL estime également que la matérialité des garanties pourrait être questionnable et source de litiges compte tenu de la nature des mesures correctrices demandées. Les mesures répressives de la CNIL devraient être considérées sans distinguer les sanctions pécuniaires. Enfin, une telle offre d'assurance enverrait un effet de signal plutôt négatif en ce qui concerne l'efficacité des mises en demeure de la CNIL.

En réponse, Pierre Minor a expliqué que le groupe de travail s'est concentré sur le risque cyber et sur le cas des sanctions de la CNIL plutôt que celles émanant d'une autre autorité comme l'ACPR ou l'AMF. Mais le rapport indique que le raisonnement suivi pouvait s'appliquer à tout type de sanctions. Sur le deuxième commentaire, le groupe de travail a fait une distinction entre mesures correctrices et sanctions pécuniaires, mais cela ne veut pas dire que toutes les mesures correctrices doivent être assurées. Les assurances n'ont en effet pas vocation à financer la refonte d'un système qui n'était pas conforme au moment de l'attaque.

Elodie Lainé, Juriste, ACPR, a confirmé de son côté que l'ACPR n'avait pas forcément envisagé d'introduire dans le Code des assurances de disposition qui viserait l'intégralité des sanctions

pécuniaires des autorités administratives, mais il a été question de modifier la définition des risques de guerre pour l'adapter aux attaques de type cyber.

Raymonde Garella, Responsable de mission conformité, s'est interrogée sur une approche collective en cas de risque systémique sous la forme d'un fonds international créé pour faire face aux conséquences d'une pandémie mondiale cyber. Patrick Degiovanni a rappelé que ce sujet a émergé lors de la crise Covid, avec les réflexions des assureurs sur une garantie Capex pour des sinistres exceptionnels. Mais les assureurs au seul niveau français, n'ont pas réussi à faire émerger une solution de mutualisation associant le public et le privé, même si elle parait être la meilleure option possible sur les risques potentiellement systémiques mal maîtrisés.

France Arnaud a également souligné la difficulté pour les assureurs de répondre aux appels d'offre sur les contrats d'assurance cyber des entités publiques municipales, régionales, ou locales, compte tenu de leur manque de maîtrise de la gestion de ce risque. Un point de vue confirmé par Patrick Degiovanni qui a indiqué réfléchir avec la SMACL, la mutuelle des collectivités locales, à un programme d'assurance mais surtout d'accompagnement en amont des collectivités, notamment des hôpitaux concernés au premier chef par de sérieuses failles et qui portent un risque important compte tenu de la spécificité des données traitées.