RAPPORT SUR L'ASSURABILITÉ DES RISQUES CYBER

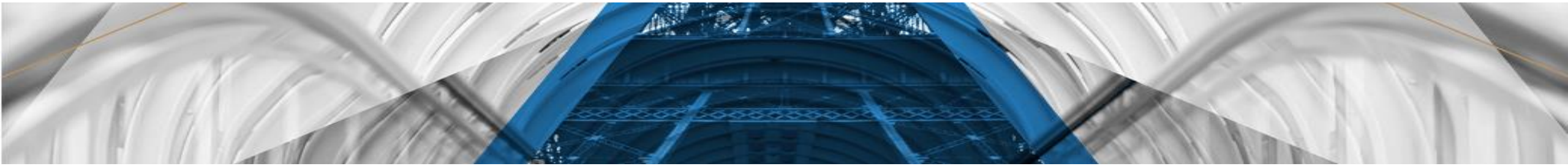
du Haut Comité Juridique de la Place Financière de Paris

Pierre Minor
Président du Groupe de Travail
Ancien Directeur Juridique Groupe Crédit Agricole
Avocat Associé, Coat Haut de Sigy de Roux Minor AARPI

Haut Comité Juridique de la Place financière de Paris

COAT HAUT DE SIGY DE ROUX MINOR AVOCATS

RAPPORT SUR L'ASSURABILITÉ DES RISQUES CYBER



I. La possibilité de couvrir les sanctions administratives par des mécanismes assurantiels

II. La possibilité de couvrir les risques de cyber rançonnage par des mécanismes assurantiels

III. Le cadre juridique actuel portant sur la couverture par les mécanismes assurantiels du risque de guerre est-il adapté dès lors que le fait générateur est de nature cybernétique ?

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

I. L'assurabilité des sanctions administratives et le cas particulier des sanctions prononcées par la CNIL

1.1 L'assurabilité des sanctions administratives, notamment pécuniaires ?

1.1.1 - L'approche traditionnelle défavorable à l'assurabilité des sanctions :

- Les auteurs, relativement à ce sujet, débattent dans une approche restrictive voire hostile.

- Se fondent sur un arrêt ancien dans lequel la question de la nature de « décimes additionnels » à une amende pénale avait posée à la Cour de cassation.

  - **Arrêt Com. 21 juin 1960**, Bull. civ. IV, n° 246.

  - Pour la Haute Juridiction, les décimes additionnels à l'amende pénale constituaient une peine accessoire qui prenait donc la nature d'une peine.

- Par ailleurs, en droit pénal, la notion de peine a connu une forte évolution. Dans ce contexte on a assisté à la multiplication des amendes civiles ou administratives qui visent à dépénaliser les sanctions mais qui ne leur ont pas fait perdre leur nature de peine.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- À travers deux décisions fondatrices de 1989 (décision N° 88-248 DC du 17 janvier 1989 et décision N° 89-260 DC du 28 juillet 1989) le Conseil Constitutionnel a admis que l'administration peut exercer un pouvoir répressif.

- Les arrêts de la Cour européenne des droits de l'homme ont aussi accompagné le juge administratif dans la construction du régime juridique de la répression administrative.

    - L'autonomie de « *l'accusation en matière pénale* » au sens de l'article 6§1 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales a permis une application de ses stipulations à un large panel de sanctions administratives.

        - CEDH, 8 juin 1976, Engel et autres c.Pays Bas, N°5100 /71

- Le Conseil d'État faisant sienne cette interprétation, a considéré que relevaient du champ pénal : ***les pénalités fiscales***, ***les sanctions pécuniaires*** prononcées par la **Commission bancaire**, par le **Conseil des marchés financiers**, par le **Conseil de la discipline de la gestion financière**, par la **Commission des sanctions de l'Autorité des marchés financiers**.

- Récemment, le Conseil constitutionnel a, dans le même esprit, affirmé la nature de peine des manquements et délits boursiers. Dans une décision du 18 mars 2015, il a décidé que le cumul des poursuites disciplinaires et pénales en matière boursière était contraire à la règle *non bis in idem* (Conseil constitutionnel, 18 mars 2015).

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- 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* ».

- À ce titre le Conseil d'État a précisé, dans un arrêt de 2007, que « *le principe constitutionnel de responsabilité personnelle en matière pénale est applicable aux sanctions administratives et disciplinaires* »
  - (**CE, avis, 29 octobre 2007**, Société sportive professionnelle LOSC Lille Métropole, n° 307736, Rec).

- Dans une autre mesure, la **notion d'ordre public** a aussi souvent été invoquée pour s'opposer à l'assurabilité des sanctions administratives.

- Cette notion d'ordre public n'est pas légalement définie, mais la doctrine considère que la notion d'ordre public correspond au bon fonctionnement des institutions indispensables à la collectivité.

- Deux réponses ministérielles sont venues apporter des précisions en faisant référence à l'ordre public :

  - Réponse ministérielle du 24 novembre 1997

  - Réponse ministérielle du 24 octobre 1991

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Par ailleurs, le ministère de l'économie dans le cadre de son pouvoir de contrôle préalable des contrats issus de l'ancien article L. 310-8 du Code des assurances (aujourd'hui abrogé) avait empêché la commercialisation de nouveaux contrats d'assistance offrant la possibilité de s'assurer contre les retraits de permis de conduire en bénéficiant d'un chauffeur durant la période de retrait au motif que :

  - *« l'objet de ces contrats paraît être en contradiction avec l'ordre public en ce qu'il tend à atténuer la rigueur d'une mesure destinée à sanctionner un comportement fautif et à entretenir l'assuré dans le sentiment d'une relative impunité ».*

- Position réitérée dans une réponse ministérielle du 15 février 1993.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

1.1.2 – Une jurisprudence peu éclairante :

- Deux arrêts :
  - Cass. civ. 2e, 14 juin 2012, pourvoi n° 11-17.367
  - Civ. 2, 13 juin 2019, n° 17-26.171

- Dans ces deux arrêts ce sont bien des questions d'assurance (faute intentionnelle, connaissance du sinistre) qui ont été traitées ; mais la question de fond de la validité de l'assurance d'une sanction administrative n'a jamais été évoquée.

En l'état du droit, il convient donc de conclure au caractère inassurable des amendes administratives et de toute sanction pécuniaire.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

1.2 Pour une assurabilité ciblée de certaines mesures prononcées par la CNIL

1.2.1 – L'inassurabilité des sanctions pécuniaires et de l'astreinte

- Aux termes du Règlement européen sur la protection des données (RGPD, préc.) 2016/679 il est nécessaire que les sanctions prévues soient « *effectives, proportionnées et dissuasives* » (article 83 et 84 du RGPD) ce qui parait exclure une assurabilité.

1.2.2 – Assurabilité des mesures correctrices faisant suite à la survenance d'un évènement de nature « *accidentelle* » de type cyberattaque

- Le RGPD distingue bien entre les sanctions qui doivent être aux termes de l'article 83 « *effectives, proportionnées, dissuasives* » des mesures correctrices de l'article 58 §2 ; ces mesures sont reprises à l'article 20 de la loi de 1978 comme mesures de mise en conformité mais également à l'article 21.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

II. L'assurabilité de la rançon en cas de cyberattaque

2.1 État des lieux du droit en France

2.1.1 – L'assurabilité du risque des ransomwares au regard du droit civil et du droit des assurances

2.1.1.1 – Au regard du droit civil

- Un contrat d'assurance doit, sous peine de nullité absolue, respecter l'ordre public et les bonnes mœurs.

- Le Code civil fait plusieurs fois références à l'ordre public et aux bonnes mœurs :
  - L'article 6 du Code civil
  - L'article 1102
  - L'article 1162

À cet égard, l'on pourrait reprocher aux assureurs qu'en remboursant les rançons aux victimes ils encouragent indirectement les cybercriminels à poursuivre leurs attaques et donc à commettre de nouvelles infractions ce qui irait à l'encontre de l'ordre public ou des bonnes mœurs.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Cette question de l'assurabilité des rançons n'a jamais été tranchée par les tribunaux, et en particulier la conformité de la question de la garantie d'assurance à l'article 6 du Code civil.

- Il a été avancé par la doctrine que « *l'assurance d'un risque purement pénal est illicite en tant que telle et que celle des autres risques est illicite à deux conditions alternatives : qu'un texte spécial le prévoie ou que la garantie ait directement pour objet une activité elle-même illicite* ».

- Si l'on tente d'appliquer ce raisonnement à l'assurance rançon, celle-ci n'est pas illicite en tant que telle puisqu'à ce jour aucun texte n'est venu l'interdire et que le paiement de la rançon par l'assuré victime du chantage des hackers ne constitue pas en lui-même une activité illicite ou pénalement condamnable.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.1.1.2 – Au regard du droit des assurances

- Le contrat d'assurance est par nature un contrat aléatoire qui fait de l'aléa un élément essentiel du contrat d'assurance. Ainsi, sont exclus du champ de l'assurabilité tous les risques dont la réalisation dépend de l'assuré.

- L'article L113-1 du Code des assurances dispose que :

  - *« l'assureur ne répond pas des pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré. »*

- La faute intentionnelle ou dolosive est la faute de l'assuré, or s'agissant de l'assurance rançon, l'assuré est une victime ; sauf à prouver qu'il était complice des cyber hackers...

- Aucun texte ou décision de jurisprudence n'interdit à ce jour la couverture du risque de rançon comme cela a pu être le cas pour d'autres risques (assurance dite « retrait de permis »).

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.1.2 – L'assurabilité du risque des ransomwares au regard du droit pénal et de la lutte contre le financement du terrorisme organisée par le Code monétaire et financier

2.1.2.1 – Au regard du droit pénal

- Dans le cas de l'entreprise-victime, le paiement de la rançon n'est pas en soi une infraction pénale, ce paiement pouvant être considéré comme étant fait sous la contrainte.

- En effet, une cyber-rançon s'analyse comme une extorsion à l'instar du délit d'extorsion prévu par **l'article 312-1 du Code pénal**.

- De plus, l'article **l'article 122-7 du Code pénal** prévoit que « *N'est pas pénalement responsable la personne qui, face à un danger actuel ou imminent qui menace elle-même, autrui ou un bien, accomplit un acte nécessaire à la sauvegarde de la personne ou du bien, sauf s'il y a disproportion entre les moyens employés et la gravité de la menace* ».

- Mais la question se pose par rapport à l'infraction de financement du terrorisme prévue par l'article 421-2-2 du Code pénal dans l'hypothèse où la cyber-rançon serait demandée par un groupe terroriste.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Cette infraction est caractérisée par la connaissance que les fonds fournis sont « destinés » à être utilisés, en tout ou en partie, en vue de commettre (un acte de terrorisme).

- L'existence d'une contrainte exonératoire de responsabilité pénale pourrait dans certains cas être invoquée par la victime ayant payé la rançon.

  - **Article 122-2 du Code pénal** : la personne doit avoir agi sous l'empire « *d'une force ou d'une contrainte à laquelle elle n'a pu résister* ».

- Pour l'entreprise d'assurance, celle-ci n'encourt *a priori* aucune responsabilité pénale à prévoir le **remboursement** d'une cyber-rançon par l'entreprise victime d'un cyber chantage.

- Ce remboursement n'apparaît pas outre pouvoir tomber sous le coup de l'infraction de blanchiment telle que définie par l'article 324-1 du Code pénal puisqu'il qu'il est fait, par hypothèse, avec des fonds légaux et n'a aucun effet dissimulateur de sa provenance.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Toutefois, lorsque l'entreprise d'assurance a connaissance en amont du règlement de la rançon par l'assuré du fait que cette dernière va alimenter un réseau terroriste, on ne peut exclure que l'assureur puisse être considéré comme complice et accusé de financement indirect du terrorisme du fait de la fongibilité entre les deux paiements.

- En revanche, si l'entreprise d'assurance apprend après le paiement de la rançon que celle-ci émane d'un groupe terroriste, le paiement fait au titre de la garantie doit être envisagé dans ses caractères propres, c'est-à-dire un paiement fait à un assuré sans reversement au groupe terroriste.

- Ce dernier schéma semble interdire une qualification de financement du terrorisme (article 421-2-2 du Code pénal) puisque le paiement par l'assureur va demeurer entre les mains de l'assuré et intervient après le paiement de la cyber rançon ce qui empêche de raisonner en termes de fongibilité entre les deux paiements.

2.1.2.2 – Au regard des mesures prévues par le Code monétaire et financier (articles L 561-2 et suivants du CMF)

- L'ensemble de ces dispositions s'appliquent aux assureurs dans le cadre de la couverture du remboursement des rançons. Ainsi, il leur appartient de mettre en place des procédures de vérification imposées aux assujettis dans le cadre de la vigilance courante (organisation et procédure interne L561-32 CMF) et de vigilance renforcée (L561-10-1 CMF) et faire les déclarations TRACFIN qui s'imposent.
- A cet égard, il **semble que les contrats d'assurance cyber explicitent peu ces procédures de vérification liées à la lutte contre le blanchiment des capitaux et le financement du terrorisme et les conséquences potentielles sur la garantie remboursement de la rançon**.

Respect des régimes de sanctions selon la législation française (articles L562-5 et L562-6 du CMF)

- Les assureurs sont tenus également de respecter les régimes de sanctions prononcés par les autorités internationales, européennes et nationales. Ces régimes peuvent conduire à la désignation de personnes pour lesquelles les fonds doivent être gelés.

- La mise en œuvre des mesures de gel est une obligation de résultat à la charge des organismes financiers. Ainsi, il existe toujours un risque juridique pour les assureurs étant donné l'obligation de résultat imposée par les textes, les bénéficiaires des paiements étant souvent difficilement identifiables.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.1.3.2 – Situation dans les autres pays du monde

- Il apparaît que la grande majorité des pays n'interdit pas l'assurabilité du remboursement des rançons en cas de cyber attaque mais :

  - subordonne le remboursement au respect des législations relatives à la lutte contre le blanchiment et le terrorisme,
  - recommande aux victimes de ransomware de s'abstenir d'effectuer le paiement des rançons,
  - incite les entreprises victimes à prendre les mesures techniques destinées à lutter contre ce type d'attaques et à en limiter les effets afin que l'éventuel paiement des rançons et sa prise en charge par les assureurs n'interviennent qu'en dernier ressort.

- À noter qu'en Allemagne l'autorité de contrôle (BaFin) a autorisé la couverture du risque de ransomware sous réserve du respect de certaines conditions dont l'exigence que cette garantie ne soit pas proposée seule mais dans le cadre plus large d'une police cyber contenant d'autres garanties et l'exigence de confidentialité.

2.2 Arguments pour et contre une éventuelle interdiction du remboursement par les assureurs des rançons versées par les victimes de cyberattaques

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.2.1 – Arguments en faveur de l'interdiction du remboursement des rançons

Notamment :

- Le paiement des rançons et leur remboursement potentiel par les assureurs nourrit un écosystème criminel.
- La confidentialité n'étant pas absolue, les entreprises assurées pourraient être plus exposées à ce type d'attaque.
- La France serait l'un des pays les plus touchés parce que « *les français payent* ».

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- La possibilité d'obtenir le remboursement d'une rançon en cas d'attaque cyber n'incite pas les entreprises à prendre les mesures de protection adaptées.

- Payer la rançon ne garantit aucunement la restauration des données, et le paiement de la rançon par une entreprise fragiliserait cette dernière, dans la mesure où elle serait alors potentiellement exposée à de nouvelles attaques en provenance des mêmes cyber criminels.

- La possibilité de remboursement des cyber-rançons par les assureurs augmente le risque de violation du régime des sanctions ou de celui applicable à la LCB/FT.

2.2.1 – Arguments en faveur de l'assurabilité

Notamment :

- Les victimes peuvent ne pas avoir d'autre choix que de payer les rançons. Interdire aux assureurs de prendre en charge la rançon n'empêchera pas les victimes de les régler.

- Faire peser sur la seule entreprise le poids financier de la rançon et les conséquences d'un non paiement (*pertes d'exploitation, mise en jeu de la responsabilité civile*), c'est mettre en danger sa survie.

- Le nombre d'entreprises bénéficiant d'une assurance cyber reste extrêmement faible en France. Ce n'est donc pas l'existence des garanties « remboursement des rançons » qui est à l'origine de l'existence des attaques par « ransomware ».

- Il n'existe aucune automaticité entre l'existence d'une garantie « cyber-rançon » et le paiement effectif par l'entreprise d'une telle rançon en cas de cyberattaque.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Une telle interdiction rendrait nécessairement moins attractifs les contrats d'assurance cyber proposés aux entreprises sur le marché.

- Un moindre encouragement à s'assurer et à adopter les bonnes pratiques en matière de protection contre la cyber criminalité.

- **Les conditions de souscription des contrats d'assurance cyber jouent un rôle important pour inciter les entreprises à adopter des bonnes mesures de protection cyber, mais également sur la mise en place effective de ces mesures**.

- Il convient de rappeler que les assureurs couvrent les conséquences du vol pour les victimes même si le vol est pénalement répréhensible.

- De même, les assureurs estiment qu'ils « n'encouragent » pas les assurés à régler les rançons.

- Les assureurs et les experts qui assistent les assurés en cas d'attaque cyber, privilégient les solutions alternatives lorsqu'elles existent.

- Se focaliser sur le remboursement des rançons par les assureurs ne permettra pas de mettre fin ni aux demandes de rançon, ni à la cybercriminalité, ni de réduire les coûts pour la société : pire cela conduirait à pénaliser certaines entreprises ou collectivités victimes des cybercriminels qui pourraient se retrouver en grande difficulté financière faute de pouvoir faire porter tout ou partie de leurs pertes sur l'assurance.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.3 Problématique européenne

2.3.1 – L'interdiction nationale

- Une interdiction purement nationale entraînerait un déséquilibre concurrentiel pour les assureurs français qui seraient soumis à ces règles si ces dernières ne s'appliquaient pas également aux assureurs étrangers couvrant des risques cyber situés en France.

- Une interdiction nationale qui ne s'appliquerait qu'aux seules entreprises françaises victimes de cyberattaques créerait un déséquilibre économique important au détriment de celles- ci vis-à-vis des entreprises situées dans un autre État Membre.

- Mais une interdiction nationale d'assurer le risque rançon pourrait satisfaire aux critères développés par les institutions communautaires.

- Une interdiction nationale n'empêcherait pas un assureur français de couvrir un risque de ransomware situé dans un État Membre qui n'interdit pas ce genre de couverture ; situation créant une distorsion de concurrence entre entreprises victimes.

- ***Se pose donc la question de la possibilité pour l'UE d'adopter un texte contraignant.***

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.3.2 – L'exercice par l'Union de sa compétence vis-à-vis d'un texte européen visant à interdire l'assurabilité des rançons en cas de cyberattaque

- Une action législative européenne visant à interdire l'assurabilité des rançons en cas de cyberattaque, *via* une disposition spécifique insérée dans un texte plus global, apparaît juridiquement possible.

- Cela permettrait d'assurer un niveau de concurrence égal à la fois pour les entreprises d'assurance mais également pour les entreprises victimes de ransomware, à tout le moins au sein de l'Union.

- ***Proposer un texte européen interdisant l'assurabilité des rançons n'est pas souhaité par les auteurs du présent rapport.*** Compte tenu des enjeux pour les victimes de cyberattaques, du besoin fondamental de protéger les entreprises et d'améliorer la résilience des entreprises vis-à-vis du risque cyber.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

2.4 Recommandations du groupe de travail HCJP

2.4.1 – Mesures d'ordre opérationnel : agir sur les dispositifs

i. Imposer et faciliter les dépôts de plainte.

ii. Renforcer/centraliser les dispositifs publics de cyber protection en moyens humains et financiers et améliorer la coordination entre les différentes autorités publiques compétentes.

- Élaborer au niveau national un cadre clair, accessible et commun à tous les opérateurs pour les assister et les aider à répondre aux attaques par ransomware.

- Instaurer une autorité publique unique ou centralisatrice qui puisse être contactée en ligne afin :
  - *D'abriter la procédure de dépôt de plainte obligatoire mentionnée ci-dessus.*
  - *D'apporter une assistance aux victimes dans la gestion des attaques et éventuellement aux assureurs pour les aider à identifier les attaquants et à respecter les mesures LCB-FT/gel des avoirs auxquelles ils sont soumis.*
  - *De permettre un échange d'informations, dans le cadre des demandes de rançon, qui pourraient être utilisées par les services publics en charge de la lutte contre ce type d'infraction. Mise en place par exemple d'une collaboration entre assureurs et autorités judiciaires ou policières.*

iii. Mener une action de partenariat entre assureurs et pouvoirs publics afin que :

- les entreprises ne communiquent pas dans leur rapport annuel des informations sur leur protection contre les risques cyber.

- les appels d'offres des organismes publics soumis à la procédure des marchés publics soient confidentiels sur ce type de couverture.

iv. Inviter les assureurs au niveau national et européen à préconiser des mesures de prévention et à mettre en œuvre les orientations suivantes :

- En matière de souscription :

  - ➢ sélectionner les risques sur la base d'une analyse technique détaillée et le respect d'un socle minimum de mesures de cyber prévention propre à chaque assureur.

  - ➢ adapter les conditions contractuelles *(franchises, capitaux assurés, plan de prévention)* en fonction du niveau de prévention exigé par chaque assureur.

  - ➢ envisager l'intégration de clauses de confidentialité dans les contrats.

  - ➢ sensibiliser les assurés au respect des mesures de gel des avoirs imposées par l'art. L562-4 CMF.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- En matière d'indemnisation :
  - ➢ conditionner la mise en jeu de la garantie rançon à un dépôt de plainte de la part des assurés victimes.
  - ➢ exiger de l'assuré une analyse systématique des solutions alternatives au paiement de la rançon.
  - ➢ inciter les assurés à n'envisager le paiement de la rançon, qu'en dernier recours.
  - ➢ analyser les transactions *blockchain* qui suivent le paiement de la rançon en cryptoactifs par l'assuré afin d'améliorer les chances d'identifier les cyberattaquants.
  - ➢ s'abstenir, par prudence, de garantir les rançons payées en cryptoactifs qui ne gardent pas l'historique des transactions.
- En matière de clarté des contrats :
  - ➢ clarifier les contrats sur les obligations et diligences LCB-FT et gel des avoirs à la charge des assureurs et des assurés lorsqu'ils sont assujettis.

2.4.2 – Mesures d'ordre réglementaires : agir sur les textes

i. Clarifier les textes nationaux/européens applicables aux obligations LCB-FT des assureurs en matière de remboursement rançon cyber afin de fixer le cadre dans lequel les assureurs pourraient s'inscrire pour s'assurer que les mesures qu'ils prennent sont suffisantes au regard de la loi.

ii. Agir au niveau européen pour un renforcement harmonisé de la cyber robustesse des entreprises afin d'aboutir à un écosystème sécurisé.

La mise en place par toutes les entreprises d'une véritable politique de gestion du risque informatique portée par un responsable et approuvée au plus haut niveau de l'entreprise.

Une cyber notation des différents acteurs économiques quelle que soit leur taille, par une agence européenne souveraine pourrait compléter le dispositif en maintenant un **niveau de confidentialité élevée** de la cyber notation.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

iii. Réglementer le marché/les échanges de crypto-actifs

Les attaques par ransomware se multiplient notamment grâce à la facilité d'utilisation des crypto- actifs qui peuvent notamment être transférés sans l'intervention d'un intermédiaire financier.

Risque : la possibilité de transférer des crypto-actifs sans l'intervention d'un intermédiaire assujetti à la LCB-FT.

Les transferts de crypto-actifs en « *peer to peer* » échappent par définition à tout contrôle ou réglementation (notamment la réglementation bancaire applicable à lutte contre le blanchiment des capitaux ou la réglementation KYC « *Know Your Customer* ») faute d'entité assujettie.

De ce constat découle l'idée **d'œuvrer à une régulation de ces échanges**.

Récemment, la Commission européenne, avec la publication de son paquet sur la lutte contre le blanchiment des capitaux présenté en juillet 2021, a proposé de tracer les transferts de crypto-actifs.

2.4.3 – Mesures de prévention : sensibiliser les opérateurs

i. Renforcer les actions de sensibilisation auprès des opérateurs publics et privés au risque cyber. (diffusion de guides pédagogiques).

ii. Réaffirmer les actions des entreprises d'assurance en matière de sensibilisation aux risques cyber auprès des entreprises.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

III. Le cadre juridique du risque de guerre et de ses mécanismes assurantiels dès lors que le fait générateur est de nature cybernétique

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Un fait générateur de nature cybernétique qui correspondrait à un acte de guerre et qui serait qualifié de cyberguerre ne répond pas à une définition en droit positif.

- Des attaques cyber assimilables à des actes de guerre sont une réalité admise en droit international. En l'état du droit français les moyens juridiques ouverts aux assureurs pour fixer les limites de l'assurabilité de ces actes de cyberguerre ne sont pas suffisamment précis.

- Il est recommandé une évolution du droit français au travers du régime légal de la présomption d'exclusion de l'article L121-8 du Code des assurances afin que sa portée soit clarifiée et que l'étendue des engagements à l'égard des assurés soit exempte d'une trop grande incertitude.

3.1 Le risque de guerre en droit des assurances

- L'intérêt de qualifier un fait générateur de nature cybernétique comme étant un acte de guerre, réside essentiellement dans la possibilité d'invoquer ou non l'exclusion de l'article L121-8 du Code des assurances.

- La cyberguerre, comme la guerre étrangère visée dans cet article a tous les attributs d'un risque systémique avec les mêmes logiques d'inassurabilité face à un évènement dont l'intensité va causer des dommages touchant de façon massive des biens. (inassurabilité technique en raison de l'impossibilité d'apprécier un tel risque et de le tarifer au moment de la souscription).

- Cette exclusion n'est susceptible de s'appliquer que quand elle est stipulée dans le contrat d'assurance.

- Une jurisprudence datée qui définit le fait de guerre comme correspondant à des opérations militaires (combats, bombardements, explosions, destructions) sans que le fait de guerre ne soit la cause unique ou directe du sinistre.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Une approche dite formaliste de la guerre, c'est-à-dire celle d'un conflit ouvert et déclaré entre la France et un autre État.

- Une évolution constitutionnelle intéressante (art. 35 de la Constitution du 4 oct. 1958 : « La déclaration de guerre est autorisée par le parlement ») en 2008 (3 juillet) qui introduit une nouvelle catégorie, celle d'une « intervention des forces armées » à l'étranger impliquant d'en informer le parlement.

- Effacement de la guerre comme catégorie ou institution juridique exclusive au profit d'autres notions.

3.1 Éléments du droit international public

- Certains éléments du droit international public ouvrent la voie pour accueillir la cyberguerre.

- Pas de définition de la guerre mais l'émergence de nouveaux concepts.

- Les conventions de Genève de 1940 relative au droit international humanitaire sont applicables (article 2) « *en cas de guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs Hautes Parties contractantes, même si l'état de guerre n'est pas reconnu comme l'une d'elles* ».

- Cette approche ouvre sur une une signification de la notion de guerre qui échappe au formalisme classique d'une déclaration de guerre qui pourrait donc ne pas être le préalable nécessaire à la qualification de cyberguerre.

- Les commentaires de 2020 autour de l'article 2 considèrent que des actions cyber en parallèle d'actions militaires plus classiques constitueraient un conflit armé international. L'analyse est identique pour des actes isolés entrainant des destructions de biens civils ou militaires équivalents.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- Pour ce qui concerne des attaques cyber avec des effets moins dévastateurs, les commentaires renvoient à la compétence des États qui devraient clarifier en droit si de telles opérations cyber pourraient être des actions armées constitutives de conflits armés soumises aux Conventions de Genève.

- Les commentaires de 2020 permettent de retenir le spectre le plus large possible des attaques cyber perpétrées par un État.

- Les Conventions de la Haye de 1899 et de 1907 restent sur une notion de guerre déclarée (concept inadapté à la cyberguerre).

- La Charte des Nations Unies (articles 2 et 51) s'applique à n'importe quel emploi de la force indépendamment des armes employées et dont une opération cyber ne peut être exclue.

- Il n'existe pas d'obligation en Droit Public International pour un État de prouver publiquement l'imputabilité d'un acte illicite dont il est victime à un autre État.

- S'agissant d'actes qui ne seraient pas menés par des États eux-mêmes au travers de leurs propres organes, le Droit Public International dégage des critères de contrôle effectif ou de contrôle global permettant d'imputer à un État les opérations en cause.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

- L'attaque NotPetya (juin 2017 attribuée à l'État Russe) a causé des dommages de grande ampleur et a touché de multiples entreprises. Certains assureurs ont pu opposer les exclusions conventionnelles des actes de guerre telles que stipulées dans les polices anglo-saxonnes.

- Mais la *Lloyd's Market Association* a publié de nouvelles clauses d'exclusions propres à la cyberguerre.

- Un tribunal américain a considéré récemment qu'une clause traditionnelle d'exclusion de la guerre ne s'appliquait pas à la cyberattaque NotPeya de 2017.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris

3.3 Recommandations du groupe de travail

- Modification souhaitée de l'article L 121-8 du Code des assurances pour ajouter au concept de étrangère celui de conflit armé international quels que soient les moyens utilisés (militaires ou cybernétiques) et les auteurs, dès lors qu'un État a opéré un contrôle sur l'action en cause ou les individus impliqués.

- Le concept de conflit armé international ne devrait pas être déterminé par une déclaration préalable formelle mais par une appréciation des faits et des critères propres entre un conflit armé entre États dont les moyens de Guerre seraient menés en partie ou exclusivement au travers d'opérations cyber.

COAT
HAUT DE SIGY
DE ROUX
MINOR AVOCATS

Haut Comité Juridique
de la Place financière de Paris