Haut Comité Juridique
de la Place financière de Paris

RAPPORT SUR L'ASSURABILITÉ DES RISQUES CYBER

du Haut Comité Juridique
de la Place Financière de Paris

28 janvier 2022

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

TABLE DES MATIÈRES

INTRODUCTION

La cybercriminalité constitue aujourd'hui l'une des menaces les plus importantes pour les entreprises et les institutions, susceptible de paralyser des rouages essentiels à leur fonctionnement et pouvant mettre en jeu leur survie ainsi que celles de leurs clients, fournisseurs ou sous-traitants ou, s'agissant des hôpitaux, de leurs patients.

Selon le rapport de l'ANSSI[1] « État de la menace ransomware à l'encontre des entreprises et des Institutions » datant du 1er mars 2021 : « *En matière de victimologie, aucun secteur d'activité ni zone géographique n'est épargné. Cependant, il est observé une hausse des attaques à l'encontre des collectivités locales, du secteur de l'éducation, du secteur de la santé et d'entreprises de services numériques.* »

La cybercriminalité revêt différentes formes mais selon le rapport de l'Institut Montaigne[2] sur le ransomware[3] (cyber-rançonnage) : « *Parmi l'ensemble des risques de cybersécurité touchant les entreprises, le ransomware représente la menace la plus régulièrement observée en 2020, et celle aux plus forts impacts sur la production, la réputation et les finances des victimes.* »

Face à ce risque grandissant, certaines entreprises choisissent de transférer une partie de leur risque de ransomware en souscrivant une assurance.

Des couvertures assurantielles sont ainsi proposées par certains acteurs du marché dont l'objet est de protéger les entreprises contre ce type d'attaque.

Mais l'on observe un faible développement de l'assurance cyber. En effet, le marché de l'assurance cyber demeure confidentiel à l'échelon international ou national. En 2018 le marché mondial de la cyber assurance était estimé entre 3 et 3,5 milliards de dollars, le marché américain captant 85 à 90 % de ces primes. L'Europe ne représente encore que 5 à 9 % de ce marché, soit un montant maximum de 255 millions d'euros (300 millions de dollars) de primes[4]. En 2020, le marché de l'assurance cyber est estimé à environ 7 milliards de dollars en primes émises brutes et devrait atteindre 20,6 milliards de dollars en 2025[5]. En France, France Assureurs (Fédération Française de l'Assurance (FFA)) l'estime à 135 millions d'euros par rapport à un encaissement global de l'assurance de dommage de près de 60 milliards d'euros.

---

[1] *Cf. infra page 17.*

[2] *Cf. infra page 18.*

[3] *« Un ransomware est un logiciel malveillant qui bloque l'accès à un appareil ou des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès ».*

[4] *Rapport d'information n° 678 du Sénat : La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?*

[5] *Source : Global Data, Cyber Insurance, 2021 Update - Thematic Research.*

Le développement en Europe et plus particulièrement en France de l'assurance cyber, se heurte, d'une part, à des difficultés de structuration tant au niveau de l'offre que de la demande, d'autre part au manque de clarté du cadre juridique national.

La plupart des études de marché démontrent en effet que les entreprises sous-estiment l'impact des incidents cyber sur leurs activités et soit elles trouvent le surcoût de ce type d'assurance exagéré par rapport à leurs contrats traditionnels, soit elles n'identifient pas clairement le contenu des offres proposées.

Au-delà des enjeux relevant strictement des logiques de marché sur ce segment en plein essor, il apparaît que l'émergence d'une véritable offre d'assurance contre les risques cyber est limitée par l'état de la législation et de la règlementation françaises. Selon de récents rapports de l'OCDE, les freins juridiques – y compris l'absence de norme – constituent les principaux facteurs de restriction du développement du marché. À cet égard, l'OCDE souligne la nécessité tant pour les organisations internationales et régionales que pour les États de revoir leurs normes, ou de les développer, afin que ces limitations au développement du marché soient levées.

Saisi par la Direction Générale du Trésor, le Haut Comité Juridique de la Place financière de Paris a constitué un groupe de travail[6] chargé d'examiner le caractère complexe des questions juridiques soulevées par le sujet de l'assurance des risques cyber afin de les clarifier. Cette clarification est attendue par les assureurs pour leur permettre de mieux apprécier les contours de leurs engagements. Cette clarification nécessaire au développement du marché des assurances du risque cyber va également bénéficier aux assurés qui cerneront de façon plus précise la portée des couvertures souscrites.

Ainsi le présent rapport, issu des travaux de ce groupe de travail, tente-t-il d'apporter des réponses à ces questions et de clarifier les trois thématiques suivantes :

1) Le cadre juridique actuel portant sur le régime des sanctions administratives notamment de nature pécuniaire et la possibilité de leur couverture assurantielle :

L'entrée en vigueur en mai 2018 du règlement général sur la protection des données (RGPD) fait peser de nouvelles obligations sur les entreprises responsables de traitement de données personnelles en matière de protection de ces données, créant ainsi un lien potentiel avec les risques de nature cyber (vol ou corruption de données, par exemple), susceptibles de voir engager leur responsabilité en cas d'infraction. De fait, la question de la nature juridique de ces sanctions pécuniaires et de leur prise en charge par des mécanismes assurantiels (notamment *via* des contrats de type responsabilité civile des mandataires sociaux) se pose avec une acuité nouvelle alors que le cadre juridique et jurisprudentiel national ne permet pas de conclure de façon certaine sur leur assurabilité.

[6] *Cf. liste des membres du groupe de travail en Annexe 1.*

2) La possibilité au plan juridique de couvrir le risque de cyber rançonnage des entreprises et des particuliers par les mécanismes assurantiels :

Dans un contexte où le risque de cyber rançon touche massivement les entreprises françaises, entraînant tant le versement d'importants montants de rançons que de nombreuses faillites d'entreprise, une solution assurantielle pourrait permettre de couvrir les pertes résultant de l'événement cyber tout en s'inscrivant dans le respect de la législation financière, notamment en matière de blanchiment des capitaux et de financement du terrorisme (LCB-FT).

3) 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 ?

D'un point de vue assurantiel, l'intérêt de la qualification d'un tel fait générateur de nature cybernétique, que l'on peut désigner par cyberguerre, réside essentiellement dans la possibilité d'invoquer ou non l'exclusion légale du risque de guerre fixée à l'article L121-8 du Code des assurances.

Le présent rapport aborde ces trois thématiques au plan strictement juridique et tente de clarifier la question de la licéité de l'indemnisation des amendes administratives et de celle de l'indemnisation du paiement des rançons en droit positif. Il se penche également sur l'opportunité, tant sur le plan du cadre juridique français qu'européen, d'une éventuelle interdiction du remboursement desdites rançons par les assureurs et propose également un certain nombre de mesures d'encadrement et d'axes d'amélioration visant à lutter au mieux contre la cybercriminalité. Enfin il suggère une nouvelle approche de la notion de guerre lorsque le fait générateur est de nature cybernétique. Il ne se prononce pas sur les enjeux relevant des logiques de marché de l'assurance du risque cyber, ni sur l'opportunité d'étendre le champ d'application des contrats d'assurances.

EXECUTIVE SUMMARY

Le présent rapport se prononce sur les trois thématiques précisées en introduction.

Sur la question des sanctions administratives

Le rapport rappelle tout d'abord que l'approche traditionnelle, tant réglementaire, que jurisprudentielle, est défavorable, voire hostile à leur assurabilité. En l'état du droit positif, il convient donc de conclure au caractère inassurable des amendes administratives et de toute sanction pécuniaire.

Toutefois et afin d'avancer sur ces questions de façon plus prospective, le rapport s'interroge, au regard de la variété des sanctions CNIL issues de l'adoption du RGPD, sur l'assurabilité de certaines de ces sanctions ou plus exactement de certaines de leurs conséquences.

Il convient en effet d'opérer une distinction entre :

- Les sanctions/amendes administratives, de l'article 83 du RGPD, 20 et 21 de la loi de 1978 (sanctions pécuniaires et astreintes) qui sont par nature inassurables et ;

- les mesures dites correctrices de l'article 58 § 2 du RGPD, qui sont dénommées mesures de mise en conformité à l'article 20, II de la loi de 1978 et que l'on retrouve également à l'article 21 dont certaines pourraient être légalement assurables dans certains cas.

S'agissant des sanctions administratives, le rapport propose l'insertion à l'article 21 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés d'un nouveau paragraphe V qui interdirait dans un souci de clarification l'assurabilité des sanctions pécuniaires et astreintes prévues par la loi de 78 et le RGPD.

En ce qui concerne les mesures dites correctrices, non visées par l'interdiction, le rapport ne propose pas de modification des textes mais appelle à la vigilance car en pratique l'assurabilité restera fortement limitée par les règles même de l'assurance.

Enfin, s'agissant des amendes et astreintes infligées par d'autres autorités (AMF, AFA etc...), le rapport précise qu'une modification des textes pourrait également être envisagée afin de préciser le caractère inassurable des sanctions pécuniaires.

Sur la question de l'assurabilité de la rançon en cas de cyberattaque

Dans un premier temps, le rapport dresse un état des lieux du droit tant en France qu'à l'étranger.

S'agissant du droit français, ni le Code civil, ni le Code des assurances, ni même la jurisprudence ne se sont prononcés sur une inassurabilité de ce genre de garantie, le paiement de la rançon par

l'assuré victime du chantage des hackers ne constituant pas en lui-même une activité illicite.

S'agissant du droit pénal, aucun texte ne vient pénalement sanctionner le paiement de la rançon par la victime ou son remboursement par l'assureur. Se pose toutefois la question de l'infraction pénale 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. Il apparaît que cette infraction pourrait être constituée si la victime ou son assureur ont connaissance en amont du règlement de la rançon du fait que les fonds fournis sont « *destinés à être utilisés, en tout ou en partie, en vue de commettre* (un acte de terrorisme) ».

Les risques juridiques de qualification d'infraction pénale pour les parties prenantes, y compris pour celles qui assistent les victimes, ne sont donc pas totalement inexistants[7].

Par ailleurs, les assureurs et les assurés (s'ils sont assujettis) sont tenus de respecter les dispositions du Code monétaire et financier sur la lutte contre le blanchiment/financement du terrorisme et le respect des mesures de gel de avoirs.

Le rapport comprend également un aperçu de la situation à l'étranger.

Il apparaît que la grande majorité des pays n'interdit pas l'assurabilité du remboursement des rançons en cas de cyberattaque mais la subordonne à certains conditions (notamment la lutte contre le blanchiment et le terrorisme). La situation aux États-Unis qui a fait de la cybersécurité une priorité est plus particulièrement étudiée. Un article détaillé rédigé par le cabinet Skadden, Arps, Slate, Meagher & Flom pour le présent rapport se trouve en annexe VI. Y sont mentionnés les risques de sanctions civiles et pénales susceptibles d'être infligées par les autorités américaines et notamment par l'OFAC (Département du Trésor américain) en cas de paiement ou de remboursement de rançon pouvant bénéficier à une entité listée.

Le rapport examine également les avantages et les inconvénients de l'assurabilité de la rançon en cas de cyberattaque et envisage finalement les conséquences juridiques d'une interdiction eu égard au marché européen dans lequel évoluent assureurs et victimes d'attaque par ransomware. Au plan juridique le rapport conclut à la possibilité qu'un texte européen puisse édicter une telle interdiction mais ne la recommande pas dans l'intérêt des victimes de cyber attaques. On note également qu'aucun État membre n'a interdit à ce jour ce genre de couverture.

Tirant les conclusions de l'analyse juridique décrite ci-dessus, le rapport ne préconise pas en effet d'interdire l'assurabilité du remboursement des rançons en cas de cyber attaque mais propose certains axes d'amélioration destinés à lutter au mieux contre les attaques par ransomware.

---

[7] *L'existence d'une contrainte exonératoire de responsabilité pénale pourrait dans certains cas être invoquée par la victime ayant payé la rançon (Art. 122-2 du Code pénal). Voir infra : « 2.1.2.1. Au regard du droit pénal ».*

Ces axes d'amélioration sont présentés selon trois catégories : des mesures d'ordre opérationnel, des mesures d'ordre réglementaire et des mesures de sensibilisation à l'égard des acteurs.

S'agissant des mesures d'ordre opérationnel,

Elles englobent l'obligation de déposer plainte, ou la facilitation du dépôt de plainte, le renforcement et la centralisation des dispositifs publics de cyber protection en moyens humains et financiers, et l'amélioration de la coordination entre les différentes autorités publiques compétentes. Le groupe de travail recommande également que les assureurs au niveau national et européen soient invités à préconiser des mesures de prévention tant au niveau de la souscription du contrat d'assurance que de l'indemnisation.

S'agissant des mesures d'ordre réglementaire,

Les recommandations du groupe de travail portent également sur la nécessité de clarifier les textes nationaux et européens applicables aux obligations LCB-FT des assureurs en matière de remboursement des rançons cyber afin de fixer le cadre dans lequel les assureurs pourraient s'inscrire pour s'assurer que les mesures qu'ils prennent pour satisfaire à leurs obligations LCB-FT sont suffisantes au regard de la loi.

Pour le groupe de travail il convient aussi d'agir au niveau européen pour un renforcement harmonisé de la cyber robustesse des entreprises afin d'aboutir à un écosystème sécurisé (voir Annexe VIII pour une analyse détaillée). La mise en place par toutes les entreprises, y compris les TPE-PME et les personnes publiques, d'une véritable politique de gestion du risque informatique portée par un responsable et approuvée au plus haut niveau de l'entreprise est une étape capitale dans la lutte contre les attaques informatiques par ransomwares.

À cet égard, pourrait être adopté au niveau européen[8] un texte trans-sectoriel visant à renforcer la cyber sécurité de l'ensemble des opérateurs. Mais au-delà du niveau européen, le sujet devrait être traité au niveau international, compte tenu du caractère mondial du risque cyber.

Enfin le groupe de travail recommande que soit mise en place un dispositif permettant d'assurer une traçabilité totale des transactions de cryptomonnaies ainsi qu'une régulation accrue et harmonisée du marché des crypto-actifs afin de réduire les risques liés à cette catégorie d'actifs.

Sur la question du cadre juridique applicable au risque de guerre et de ses mécanismes assurantiels dès lors que le fait générateur est de nature cybernétique

Le rapport mentionne l'article L121-8 du Code des assurances (exclusion, sauf convention contraire, des pertes et dommages occasionnés par la guerre) ; le caractère daté de la jurisprudence

[8] *Des travaux ont déjà été réalisés au niveau européen, et ont abouti à un corpus textuel déjà en vigueur. D'autres travaux sont en cours d'élaboration. Voir infra : « 2.4.2. Mesures règlementaires : agir sur les textes ».*

sur l'interprétation de cet article permet difficilement de mesurer aujourd'hui la portée de cette exclusion légale en cas de cyberguerre.

Dès lors, le rapport souligne qu'une clarification des limites de l'assurabilité en raison de l'ampleur des dommages susceptibles d'être générés par un acte de cyberguerre serait opportune.

Cette clarification devrait entrainer une modification de l'article L121-8 du Code des assurances avec pour objectif d'inscrire l'exclusion dans la contemporanéité du droit et des relations internationales, en ajoutant au concept de guerre étrangère, celui de conflit armé international.

Une définition de la notion de guerre étrangère devrait compléter l'article L121-8 pour une claire compréhension de la part des assurés. Elle serait rédigée selon une acception large incluant le 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.

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

Il convient de rappeler le contexte de l'assurabilité des sanctions administratives de façon générale (1.1) ; puis de voir plus avant dans quelle mesure les sanctions CNIL peuvent être assurées (1.2).

1.1 - La question de l'assurabilité des sanctions administratives notamment pécuniaires

Dans une approche traditionnelle de la question, l'assurabilité d'une sanction est déniée (1.1.1) ; la jurisprudence civile n'apporte pas d'éclaircissement sur ce point (1.1.2).

1.1.1 - Une approche traditionnelle défavorable à l'assurabilité des sanctions

La question de l'assurabilité d'une peine n'est pas nouvelle en assurance, les auteurs en débattent dans une approche restrictive, voire hostile (F. Leduc, *in Traité du contrat d'assurance terrestre*, Litec 2008, n° 142 ; L. Mayaux, Le risque assurable, *in Traité de droit des assurances*, dir. J. Bigot, T. III, Le contrat d'assurance, LGDJ 2002, n° 1104 à 1108).

Il se fondent sur un arrêt ancien dans lequel la question de la nature de « décimes additionnels » à une amende pénale avait été posée à la Cour de cassation (Com. 21 juin 1960, Bull. civ. IV, n° 246 ; RGAT 1961. 53, note A. Besson). La Cour d'appel avait estimé que l'assureur de responsabilité civile devait les prendre en charge. La Haute Juridiction avait censuré les juges du fond en indiquant clairement que les décimes additionnels à l'amende pénale constituaient une peine accessoire qui prenait donc la nature d'une peine (Com. 21 juin 1960, préc.). Par ailleurs, il est admis par les auteurs que le contrat d'assurance qui vise à pallier les conséquences du retrait d'un permis de conduire comporte un objet illicite (L. Mayaux, Le risque assurable, préc., n° 1106 ; F. Leduc, préc., n° 142). Le ministère de l'économie et des finances avait interdit en 1992, pour violation de l'ordre public, le contrat permettant de fournir un chauffeur en cas de suspension de permis (L. Mayaux, Le risque assurable, préc., n° 1106 ; F. Leduc, préc., n° 142 et V. G. Defrance, L'ordre public des assurances, Argus 21 février 1992, p. 16 s.).

En outre, en droit pénal, on observe que la notion de peine a connu une forte évolution. Aux peines d'emprisonnement et d'amende se sont adjointes d'autres formes de privations ou de restrictions de liberté, telle que par exemple la suspension du permis de conduire (Y. Mayaud, *Droit pénal général*, 5e éd., PUF, 2015, n° 503). 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.[9]

[9] *C.F dossier thématique du 9 janvier 2017 du Conseil d'État reproduit ci-après pages 5 et 6 et pages 12 et 13.*

« Dans 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.

Dans ces deux décisions le Conseil Constitutionnel a exigé le respect de principes fondamentaux dans l'exercice du pouvoir de répression administrative. Il juge « *qu'une peine ne peut être infligée qu'à la condition que soient respectés le principe de légalité des délits et des peines, le principe de nécessité des peines, le principe de non-rétroactivité de la loi pénale plus sévère ainsi que le principe des droits de la défense* » et « *que ces exigences concernent non seulement les peines prononcées par les juridictions répressives mais aussi toute sanction ayant le caractère d'une punition même si le législateur a laissé le soin de la prononcer à une autorité de nature judiciaire* ».

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. En effet, dès lors qu'elle remplit l'un des trois critères alternatifs posés par la Cour, tenant à la qualification de la mesure en droit interne, à la nature de l'infraction et à la sévérité de la sanction que la personne concernée risque d'encourir, une mesure doit respecter les principes posés par l'article 6§1 de la Convention (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 de l'article 6§1 les pénalités fiscales (CE, avis, Section, 31 mars 1995, Ministre du budget c/Auto-Industrie Méric, N° 164008) les sanctions pécuniaires prononcées par la Commission bancaire (CE, 29 novembre 1999, Société Rivoli Exchange n° 194721, Rec), par le Conseil des marchés financiers (CE, Assemblée, 3 décembre 1999, Didier, n° 207434, Rec) par le Conseil de la discipline de la gestion financière (CE, 31 mars 2004, Société Etna Finance et M.P. , n° 243579, T.) par la Commission des sanctions de l'Autorité des marchés financiers (CE, 24 février 2005, Société GSD gestion set M.G., n° 269001,Rec.). »

Plus 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, n° 2014-453/454 QPC et n° 2015-462 QPC). Il s'évince de cette affirmation que les amendes civile ou administratives revêtent bien la nature de peines.

Or, en cette matière, 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* ». Le principe de personnalité des peines empêche qu'une personne autre que le prévenu puisse

se substituer à lui dans l'exécution de sa peine. En effet pour remplir son rôle dissuasif la peine doit atteindre le coupable personnellement. Plusieurs réponses ministérielles ont rappelé qu'il était interdit d'assurer les conséquences pécuniaires des condamnations pénales ou qu'un assureur ne pouvait prendre en charge les amendes fiscales, douanières ou toute autre sanction pécuniaire prononcée par les autorités administratives.

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).

La notion d'ordre public a aussi souvent été invoquée pour s'opposer à l'assurabilité des sanctions administratives. Cette notion n'est pas légalement définie. L'article 6 du Code civil dispose qu'« *on ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* ». De même l'article 1102 du Code civil précise que « *chacun est libre de contracter, de choisir son contractant et de déterminer le contenu et la forme du contrat dans les limites fixées par la loi. La liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public* ».

La doctrine considère que la notion d'ordre public correspond au bon fonctionnement des institutions indispensables à la collectivité. En d'autres termes, il doit tendre à protéger les valeurs morales fondamentales et les intérêts essentiels d'une société en posant les frontières au-delà desquelles la liberté contractuelle ne peut plus s'exercer.

Une réponse ministérielle du 24 novembre 1997 précise qu' « *il est interdit d'assurer les conséquences pécuniaires des condamnations pénales. Cette interdiction se rattache aux règles générales du droit pénal, notamment au principe de personnalité des peines. L'ordre public s'oppose donc à ce qu'un assureur prenne en charge les amendes pénales, de même que les amendes fiscales, douanières, ou toute autre sanction pécuniaire prononcée par les autorités administratives.* »[10]

Une réponse ministérielle du 24 octobre 1991 a ainsi rappelé que le Conseil d'État avait estimé qu' « *une assurance ayant pour objet de couvrir la conséquence pécuniaire d'une suspension ou d'un retrait de permis de conduire pour celui qui en est l'objet, aurait pour résultat d'en réduire ou supprimer les effets, et porterait atteinte au principe de la personnalité des sanctions et des peines et à leur stricte application. Cette question relève néanmoins de l'interprétation souveraine des tribunaux* » et conclut que « *sous réserve d'un avis contraire des tribunaux, un tel contrat doit être considéré comme illicite car contraire à l'ordre public.* » (Avis du Conseil d'État du 17 juin 1969).

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

[10] *Question écrite n° 2988 relative à une clause de prise en charge des amendes pénales par l'assureur.*

commercialisation de nouveaux contrats d'assistance qui devaient offrir 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* ». Cette position a été réitérée dans une réponse ministérielle du 15 février 1993[11].

La jurisprudence civile ne déroge pas à ce principe ; à l'analyse elle n'apporte pas d'éclairage nouveau sur la question.

1.1.2 - Une jurisprudence civile peu éclairante

Un arrêt du 14 juin 2012 (Cass. civ. 2e, 14 juin 2012, pourvoi n° 11-17.367, Revue des sociétés 2012, p. 637, et la note ; Gaz Pal. n° 179-180, note B. Dondero ; JCP E, 2013 n° 36, pp. 30-31, obs. M. Asselain ; RTD com. 2012, p. 813, note N. Rontchevsky) a pu être interprété comme susceptible de marquer une évolution dans le traitement de l'assurabilité de la sanction administrative en visant non l'ordre public, mais le caractère intentionnel des faits reprochés.

En l'espèce, un dirigeant avait été sanctionné par l'AMF pour manquement à l'obligation d'information du public par diffusion d'informations inexactes. Dans cet arrêt, la Cour de cassation a validé l'interprétation des juges du fond (confirmée par la Cour d'appel) en ce qu'ils avaient considéré que la faute intentionnelle était « *exclusive du caractère aléatoire du contrat d'assurance* » afin de conclure que la garantie n'était pas due. Il a pu être soutenu que cet arrêt ouvrait une brèche dans le principe de l'inassurabilité des sanctions administratives. Toutefois, à aucun moment dans cette affaire la question de la licéité de la garantie n'a été posée à la Cour de cassation. Seul le caractère intentionnel de la faute de l'assuré a été débattu.

Le même raisonnement a été adopté dans un arrêt du 13 juin 2019 (Civ. 2, 13 juin 2019, n° 17-26.171, Rev. Sociétés 2020, p. 103) par la Cour de cassation qui a confirmé l'arrêt d'appel qui avait jugé que l'assureur était fondé à dénier sa garantie en vue de la prise en charge d'une sanction pécuniaire prononcée par l'AMF. En effet, le défendeur avait connaissance des faits dommageables ayant donné lieu à la procédure administrative avant la date de souscription du contrat. Cette connaissance du sinistre antérieure à la prise d'effet du contrat prive ce dernier d'aléa ; l'assureur ne doit donc pas sa garantie (C. ass. art. L124-5).

Dans ces deux arrêts ce sont donc 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

[11] *Réponse ministérielle n° 47504, JO 15/02/1993, p. 597.*

administrative n'a jamais été évoquée et n'a donc pas reçu de réponse. Il ne semble pas possible au Groupe de travail de pouvoir interpréter ces arrêts dans le sens d'une assurabilité possible des sanctions administratives fondées sur des fautes non intentionnelles.

En l'état du droit, il convient donc de conclure au caractère inassurable des amendes administratives et de toute sanction pécuniaire. Une clarification des textes dans le sens d'une inassurabilité de ces sanctions pécuniaires administratives parait souhaitable pour mettre un terme aux incertitudes qui demeurent dans beaucoup de contrats d'assurances envisageant une assurabilité des sanctions administratives, mais dans la limite permise par la loi.

Toutefois on peut s'interroger, au regard de la variété des sanctions CNIL issues de l'adoption du RGPD, sur l'assurabilité de certaines de ces sanctions ou plus exactement de certaines de leurs conséquences. Le sujet mérite un examen particulier dans la mesure où en cas de survenance d'une cyber attaque la CNIL pourrait être amenée à prononcer des sanctions du fait notamment de la perte ou de la divulgation de données protégées.

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

Le groupe de travail est d'avis qu'il convient d'opérer une distinction entre :

• les sanctions/amendes administratives, de l'article 83 du RGPD et 20, III et 21 de la loi de 1978 (sanction pécuniaire et l'astreinte) qui sont par nature inassurables (1.2.1) ; et

• les mesures dites correctives de l'article 58 § 2 du RGPD, qui sont dénommées mesures de mise en conformité à l'article 20, II de la loi de 1978 et que l'on retrouve également à l'article 21 dont certaines pourrait être légalement assurables dans certains cas (1.2.2). Les textes applicables figurent en Annexe III.

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. Une sanction assurable ne pourrait en effet avoir de caractère dissuasif. En outre, la position française des différentes juridictions rappelée ci-dessus conduit à déclarer inassurable les amendes administratives prévues à l'article 20 III, 7° de la loi de 1978.

Dans le même esprit, les astreintes prévues par les articles 20, III, 2° et 21, I, 6° de la loi de 1978 ne sont pas assurables.

En revanche, les mesures correctives prévues par l'article 58 § 2 du RGPD lorsqu'elles sont liées à un événement de nature « *accidentelle* » de type cyberattaque paraissent pouvoir être assurables.

1.2.2 - Assurabilité des mesures correctrices faisant suite à la survenance un événement 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 correctives 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 Toutes les mises en demeure de mise en conformité ou d'information qui figurent dans ces deux textes peuvent avoir des conséquences pécuniaires qui pourraient, en cas d'attaque cyber, être assurables car ce sont des mesures techniques correctrices. Ainsi par exemple :

• les conséquences pécuniaires des mises en demeure de communiquer aux personnes concernées une violation de données à caractère personnel ou de leur notifier les mesures prises (art. 20, II, 1 et art. 20, II, 4° al. 2 de la loi de 1978),

• la perte d'exploitation due à la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale (art. 20, III, 5° de la loi de 1978),

• la perte d'exploitation due à l'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois (art. 21, I, 1° de la loi de 1978),

• les conséquences pécuniaires de la mise en demeure de (re)mettre les opérations de traitement en conformité avec les dispositions applicables) lorsque cette conformité n'est plus assurée du fait de l'attaque subie (art. 20, II, 2 de la loi de 1978),

• la suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant ou de l'autorisation délivrée sur le fondement du III de l'article 66 de la loi (données de santé) (art. 20, III, 4 loi de 1978).

Il convient de rappeler que l'assurabilité de ces sanctions devra s'inscrire dans le cadre des règles propres au contrat d'assurance.

Ainsi, par exemple, la faute intentionnelle ou dolosive est en tout état de cause inassurable aux termes de l'alinéa 2 de l'article L. 113-1 du Code des assurances. Ensuite, le principe de non-enrichissement de l'assuré limite la réparation à un sinistre de nature accidentelle qui cause un dommage à un système fiable. Le rôle de l'assureur n'est pas de prendre en charge la mise à niveau d'un système informatique qui ne présentait pas les normes standard de sécurité et de fiabilité. C'est donc bien uniquement à l'occasion par exemple, d'une attaque informatique qui a entraîné une fuite de données dont la CNIL a eu connaissance et qui suscite une mise en demeure de sa part, que l'assureur pourrait alors indemniser les coûts techniques de ces mises en demeure.

À la lumière de ces analyses et réserves, le groupe de travail propose l'insertion à l'article 21 de la loi de 1978 d'un paragraphe V dans les termes ci-après :

Loi du 6 janvier 1978
Article 21

(…)
« V. - Les amendes administratives, les astreintes et autres sanctions pécuniaires prévues par la présente loi ou par le Règlement EU 2016/679 du 27 avril 2016 sont inassurables. »

S'agissant des amendes et astreintes infligées par d'autres autorités (AMF, AFA etc..) une modification des textes pourrait également être envisagée afin de préciser le caractère inassurable des sanctions pécuniaires.

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

Propos introductifs

« Un ransomware est un logiciel malveillant qui bloque l'accès à un appareil ou des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès »[12].

Selon le rapport de l'Institut Montaigne sur le ransomware : *« Parmi l'ensemble des risques de cybersécurité touchant les entreprises, le ransomware représente la menace la plus régulièrement observée en 2020, et celle aux plus forts impacts sur la production, la réputation et les finances des victimes. »*

Selon un rapport de l'IST (*Institute for Security and Technology* américain) d'avril 2021 intitulé « *combating ransomware* », une augmentation de 260% de la fréquence des attaques par ransomware a été relevée sur le marché américain avec un montant moyen - $338,669 - de la rançon en forte augmentation (47%). Dans un rapport de l'Association des superviseurs américains (NAIC) sur le marché de l'assurance cybersécurité en date du 20 octobre 2021, il est précisé que les attaques par ransomware ont augmenté de 62% depuis 2019.

Au niveau national, 192 attaques par ransomwares ont été traitées par l'ANSSI en 2020, contre cinquante quatre l'année précédente (255% de hausse).

La proportion des entreprises cyberattaquées a augmenté de 38% à 43% dans le monde. Sur ces entreprises attaquées, une sur six est touchée par une demande de rançon et plus de la moitié (58%) paie la rançon. Plus de 60% des entreprises payant les rançons se trouvent dans trois pays : les USA (21%), l'Allemagne (21%) et la France (19%). La demande de couverture autonome (*standalone cover*) a augmenté de 1% à 27%[13]. Source : Hiscox Cyber Readiness Report 2021.

---

[12] *Voir https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares.*

[13] *Attention ce chiffre est général sur l'assurance cyber et ne couvre pas spécifiquement l'assurance rançon.*

Cette forte augmentation de la cybercriminalité est essentiellement due :

• à la numérisation de l'économie qui s'est accélérée dans les dernières années, du fait entre autres de l'apparition du « *cloud* », du développement des ventes par internet et du télétravail en partie liés à la crise sanitaire,

• au manque de cyber robustesse des entreprises françaises, à tout le moins des TPE, PME et ETI par manque d'acculturation aux risques cyber dû en partie à un manque d'information et de formation des dirigeants et salariés,

• à l'absence d'équipes de forces de l'ordre et de justice spécialisées en la matière en nombre suffisant à même de traquer les cybers criminels, ainsi que

• à une coopération insuffisante tant au niveau européen qu'international.[14]

Selon le rapport de l'ANSSI « État de la menace ransomware à l'encontre des entreprises et des Institutions » datant du 1er mars 2021 : « *En matière de victimologie, aucun secteur d'activité ni zone géographique n'est épargné. Cependant, il est observé une hausse des attaques à l'encontre des collectivités locales, du secteur de l'éducation, du secteur de la santé et d'entreprises de services numériques.* »

Fin mars 2021, une cyberattaque visait d'ailleurs l'un des géants américains de l'assurance, CNA, rendant son site web inaccessible au public ; l'intérêt particulier pour un pirate de déployer une attaque cyber contre un assureur est de tenter d'avoir ainsi accès au détail des couvertures de chaque assuré. L'objectif est d'ainsi orienter les futures attaques vers des entreprises assurées contre les ransomwares facilitant ainsi le paiement de la rançon au bénéfice du pirate.

Face à ce risque grandissant, certaines entreprises choisissent de transférer une partie de leur risque de ransomware en souscrivant une assurance.

Des couvertures assurantielles sont proposées par certains acteurs du marché dont l'objet est de protéger les entreprises contre ce type d'attaque.

Peuvent être couverts, soit dans des contrats autonomes, soit dans des contrats de dommages aux biens et de responsabilité civile :

• les frais de gestion de crise : conseil juridique, frais d'expert informatique, frais de communication de crise,

• les frais de notification et frais de monitoring et surveillance,

---

[14] Voir sur ce point le Rapport d'information n° 678 du Sénat du juin 2021 : La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?

• les frais de reconstitution des données,

• les pertes d'exploitation,

• les frais d'enquête administrative,

• les frais de défense assurables dans le cadre d'une enquête,

• les recours de tiers : remboursement des préjudices subis par un tiers, frais de défenses et dommages et intérêts.

Les assureurs peuvent également proposer de garantir sous certaines conditions le remboursement de la rançon payée par l'entreprise victime de l'attaque à la demande expresse de l'assuré. Il convient de préciser que la mise en œuvre de cette garantie est peu fréquente par rapport aux autres garanties couvrant le risque cyber.

Au cours d'une audition au Sénat sur la cybersécurité des ETI et des PME qui s'est tenue le 15 avril 2021, l'ANSSI et le Parquet de Paris ont reproché aux assureurs d'encourager l'augmentation des cyberattaques par ransomware en acceptant de procéder au remboursement du paiement des rançons ; par ailleurs, dans un Rapport d'information du Sénat n° 678 daté du 10/06/2021, intitulé : « *La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?* » la proposition n° 12 propose d'interdire l'assurabilité du risque de paiement des rançons en cas d'attaque par ransomware. De même, en octobre 2021, dans un Rapport dédié à la cyber-assurance, la député V. Faure-Mutian a proposé, s'agissant de l'assurabilité de la demande de rançon en cas de cyber attaque : «*(...) il convient d'inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou d'indemniser la rançon et se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise.* »

Pour les assureurs, l'objectif premier est de couvrir les pertes pécuniaires des entreprises assurées victimes de ransomwares. Par ailleurs les assureurs indiquent mettre en place avant d'accorder la garantie remboursement, des mesures de prévention afin d'essayer d'identifier les personnes auprès desquelles est effectué le paiement de la rançon et à tout le moins de tenter d'obtenir des informations sur ces dernières pour leur permettre, dans la mesure du possible de s'assurer du respect de leurs obligations de déclarations au titre de la lutte contre le financement du terrorisme.

Les problématiques de paiement des rançons et du remboursement des rançons payées par les assureurs sont importantes mais le principal enjeu en matière de cybersécurité et de ransomware reste bien le manque de cyber robustesse des entreprises et des organismes publics et *a contrario* le dynamisme technologique des cyberattaques.

Par ailleurs, il est observé une faible pénétration de l'assurance cyber. En effet, le marché de l'assurance cyber demeure un marché confidentiel à l'échelon international ou national. En 2018 le marché mondial de la cyber assurance était estimé entre 3 et 3,5 milliards de dollars, le marché américain captant 85 à 90 % de ces primes. L'Europe ne représente encore que 5 à 9 % de ce marché,

soit un montant maximum de 255 millions d'euros (300 millions de dollars) de primes[15]. En 2020, le marché de l'assurance cyber est estimé à environ 7 milliards de dollars en primes émises brutes et devrait atteindre 20,6 milliards de dollars en 2025[16]. En France, la France Assureurs[17] l'estime à 135 millions d'euros par rapport à un encaissement global de l'assurance de dommage de près de 60 milliards d'euros.

Il ressort de l'étude de l'AMRAE[18] sur la cyber-assurance que seules 8% des entreprises de taille intermédiaire ont souscrit une assurance cyber. Et bien sûr tous les contrats cyber ne contiennent pas une garantie couvrant l'assuré contre le risque de ransomware.

Notons que les demandes de paiement des rançons ne résultent pas toujours d'une attaque par ransomware mais peuvent également résulter d'une menace de divulguer des données confidentielles, ou de données préjudiciables à l'entreprise[19].

2.1 - État des lieux du droit en France et aperçu de la situation à l'étranger

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

Le principe de l'assurabilité des risques est régi par les articles 6 et 1102 et 1162 du Code civil et l'article L.113-1 du Code 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.

Comme indiqué ci-dessus, aucune définition légale ne vient définir précisément l'ordre public ; il s'agit d'une notion assez générale qui désigne la paix, la tranquillité et la sécurité publique et dont les individus ne peuvent s'écarter par convention ; il s'agit de l'ensemble des exigences fondamentales considérées comme essentielles au fonctionnement des services publics et au maintien de la sécurité ou de la moralité.[20]

---

[15] *Rapport d'information n° 678 du Sénat : La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?*

[16] *Source : Global Data, Cyber Insurance, 2021 Update – Thematic Research.*

[17] *France Assureurs est le nouveau nom d'usage de la Fédération Française de l'Assurance.*

[18] *Lumière sur la Cyberassurance, édition 2021, AMRAE.*

[19] *Voir Rapport OCDE, The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage Box 3.3.*

[20] *Voir définition lexique juridique G. Cornu.*

Les bonnes mœurs, quant à elles, sont « *(...) des règles imposées par la morale sociale à une époque donnée, et dont la violation éventuellement constitutive d'infractions pénales, est susceptible de provoquer l'annulation d'une convention* »[21].

Dans le Code civil, il est fait plusieurs fois références à l'ordre public et aux bonnes mœurs.

L'article 6 du Code civil dispose que l' : « *On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs* ».

L'article 1102 précise que « *Chacun est libre de contracter ou de ne pas contracter, de choisir son cocontractant et de déterminer le contenu et la forme du contrat dans les limites fixées par la loi. La liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public.* »

L'article 1162 du même code ajoute : « *Le contrat ne peut déroger à l'ordre public ni par ses stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties* ».

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.

Cette question particulière de l'assurabilité des rançons n'a jamais été tranchée par les Tribunaux ; plus généralement, la question de la conformité de la garantie d'assurance à l'article 6 du Code civil a rarement été traitée par la jurisprudence, mais il est certain que, malgré la spécialité du droit des assurances, cet article s'applique aux contrats d'assurance comme cela a, d'ailleurs, été confirmé par la Cour d'appel de Paris[22], dans le cadre d'une procédure visant l'assurabilité des amendes administratives[23] [24].

Du côté de la doctrine, certains auteurs[25] se sont penchés sur la question du contour de l'ordre public appliqué aux contrats d'assurance et du critère permettant de savoir si oui ou non un contrat

---

[21] *Voir Serge GUINCHARD, Thierry DEBARD (dir.), Lexique des termes juridiques, Dalloz, 2013.*

[22] *Voir Arrêt CA Paris du 14 février 2012 (n° 09/06711).*

[23] *On rappellera que la notion d'ordre public a depuis fort longtemps été utilisée en Doctrine pour justifier certaines interdictions qui ont pu paraître pertinentes un temps. Ainsi l'assurance sur la vie a longtemps été considérée comme immorale avant que sa licéité ne soit reconnue en 1818. De même, on tendrait à oublier que la licéité de l'assurance de responsabilité civile a très longtemps fait débat et n'a été reconnue par la jurisprudence qu'en 1845 sous réserve de la faute intentionnelle. À l'époque les tenants du maintien de son interdiction craignaient un effondrement général de la moralité si tout à chacun pouvait être assuré contre les conséquences civile de sa faute.*

[24] *On citera également la décision de la Cour de cassation de 2014 annulant pour contrariété à l'ordre public une assurance destinée à couvrir le risque d'annulation d'une exposition qui mettait en scène des cadavres humains. Cass Civ. 1ère 2 octobre 2014.*

[25] *Voir notamment L. Mayaux « Assurance et ordre du public : à la recherche d'un critère » RGDA 2008, n° 3.*

d'assurance est licite au regard de l'ordre public. Il a été avancé 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.

2.1.1.2 - Au regard du droit des assurances

Le contrat d'assurance est par nature un contrat aléatoire[26] qui fait de l'aléa un élément essentiel du contrat d'assurance ; ce caractère nécessairement aléatoire du risque exclut du champ de l'assurabilité tous les risques dont la réalisation dépend de l'assuré.
Le Code des assurances ne contient aucune disposition affirmant le caractère aléatoire du contrat. Il interdit néanmoins la conclusion de certains contrats ne comportant pas (ou plus) d'aléa tels que ceux visant à assurer des « *pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré* » (L113-1 CA) :
« *Les pertes et les dommages occasionnés par des cas fortuits ou causés par la faute de l'assuré sont à la charge de l'assureur, sauf exclusion formelle et limitée contenue dans la police. Toutefois, 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...

En matière d'assurance cyber, au cas par cas, l'attitude de l'assuré pourrait faire disparaître l'aléa, mais ces hypothèses ne remettraient pas en question l'assurabilité du remboursement des rançons de manière générale.

Hormis ces références qui demeurent assez générales, aucun texte ou jurisprudence n'interdit explicitement à ce jour la couverture du risque de rançon comme cela a pu être le cas pour d'autres risques[27].

---

[26] *Même s'il n'est plus mentionné comme tel dans le Code civil ; art. 1108 civ. : définition du contrat aléatoire : « les parties acceptent de faire dépendre les effets du contrat, quant aux avantages et aux pertes qui en résulteront, d'un événement incertain ».*

[27] *Voir par exemple l'interdiction en 1992 de l'assurance dite "retrait de permis" (réponse parlementaire à la question n° 17035 publiée au JO du Sénat le 24/10/1991, page 2343).*

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

Le principe de l'assurabilité des risques est régi par les articles 6 et 1102 et 1162 du Code civil et l'article L113-1 du Code des assurances.

2.1.2.1 - Au regard du droit pénal

S'agissant de la situation 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 en une extorsion puisqu'elle vise à obtenir une remise de fonds sous la contrainte, ce qui correspond au délit d'extorsion prévu par l'article 312-1 du Code pénal (il convient de préciser que la contrainte morale est prise en compte au titre de l'extorsion). Il n'apparaît donc pas possible de reprocher pénalement un paiement fait sous une contrainte constitutive d'infraction pénale, la société payeuse étant la victime de cette infraction.

Par ailleurs, 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* ».

En revanche, la question se pose par rapport à l'infraction de financement du terrorisme prévue par l'article 421-2-2[28] du Code pénal dans l'hypothèse où la cyber-rançon serait demandée par un groupe terroriste. Cette infraction étant 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'entreprise payant la cyber-rançon est exposée à être poursuivie de ce chef. Cette poursuite suppose néanmoins que l'entreprise avait connaissance du fait que la demande de cyber-rançon émane d'un groupe terroriste. L'existence d'une contrainte exonératoire de responsabilité pénale pourrait dans certains cas être invoquée par la victime ayant payé la rançon[29]. Pour mémoire, pour que l'article 122-2 du Code pénal soit applicable la personne doit avoir agi sous l'empire « *d'une force ou d'une contrainte à laquelle elle n'a pu résister* ». Dans certains cas, la contrainte subie pourrait effectivement apparaître comme suffisamment irrésistible au sens de l'article 122-2 du Code pénal[30].

---

[28] *L'art. 421-2-2 prévoit que : « Constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte ».*

[29] *La contrainte de l'extorsion est distincte de la contrainte exonératoire de responsabilité pénale.*

[30] *Par exemple pour les activités des opérateurs de service d'importance vitale ou essentielle (OIV-OSE) comme les hôpitaux…*

En conséquence le paiement de la rançon par l'entreprise victime d'une attaque cyber n'est pas pénalement répréhensible sous réserve du cas de financement du terrorisme lorsque les conditions de l'art. 421-2-2 du Code pénal sont réunies.

S'agissant de 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 paiement étant *a priori* licite, il n'y a pas d'obstacle juridique à prévoir une telle garantie. En effet, celle-ci n'a ni un objet ni une cause illicite. Cette assurance est comparable à une assurance couvrant le risque de vol ou de destruction. L'entreprise d'assurance n'encourt donc pas de responsabilité pénale à rembourser à son assuré le montant de la cyber-rançon versée par celui-ci.

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[31] puisqu'il qu'il est fait, par hypothèse, avec des fonds légaux et n'a aucun effet dissimulateur de sa provenance.

Il n'existe donc pas aujourd'hui d'interdiction légale, formelle pour les assureurs de couvrir le remboursement de ce type de rançon prévu dans le cadre de polices d'assurance cyber.

Néanmoins, tout comme pour la victime, on peut s'interroger sur le point de savoir si l'infraction de financement du terrorisme pourrait être retenue à l'encontre de l'assureur ayant remboursé la rançon payée par la victime, même si la somme payée à l'assuré demeure entre ses mains, de sorte que les fonds versés à ce titre ne peuvent pas être qualifiés de fonds « *destinés à être utilisés, en tout ou en partie, en vue de commettre (un acte de terrorisme)* ».

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 schéma semble interdire une qualification de financement du terrorisme au sens de l'article 421-2-2 du Code pénal, puisque le paiement en cause 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.

Il doit être mentionné que d'autres infractions pourraient être retenues, dans des cas très particuliers, à l'encontre des intermédiaires, qui interviennent dans des opérations dites de remédiation

[31] *« Le blanchiment est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect. »*

(négociations/paiement), à l'occasion de demandes de cyber-rançon. Ces infractions[32], plus aisément qualifiables que le financement du terrorisme sont énumérées en note de bas de page ci-dessous.

Les risques juridiques de qualification d'infraction pénale pour les parties prenantes et notamment celles qui assistent les victimes, ne sont donc pas, dans certains cas, totalement inexistants.

2.1.2.2 - Le respect des mesures prévues par le code monétaire et financier

• Lutte contre le blanchiment des capitaux et le financement du terrorisme (notamment articles L561-2, L561-4-1, L561-5, L561-5-1, L561-6, L561-10-1, L561-15, L561-16, L561-32, R561-12-1).

Compte tenu des risques que représentent le blanchiment de capitaux et le financement du terrorisme pour la société, les pouvoirs publics imposent aux entreprises du secteur financier (banques et assurances) de déceler, de façon précoce, à travers les opérations réalisées, les personnes susceptibles de participer à des activités illicites. Cela se traduit notamment par des obligations d'identification, de connaissance de leur client et de vigilance constante. Le manquement à ces obligations peut entraîner des sanctions financières lourdes, voire des sanctions pénales. Pour cette raison, les assureurs peuvent être amenés régulièrement à poser des questions aux assurés et à leur demander des justificatifs (par exemple afin d'attester de l'origine ou de la destination des fonds).

Les entreprises d'assurance, en tant qu'entités assujetties aux obligations de LCB-FT sont tenues de déclarer au service Tracfin les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme. Elles s'abstiennent d'effectuer toute opération portant sur ces sommes jusqu'à ce qu'elles aient fait la déclaration à Tracfin. Elles ne peuvent alors procéder à la réalisation de l'opération que si Tracfin n'a pas notifié d'opposition ou si, au terme du délai ouvert par la notification de l'opposition, aucune décision du président du tribunal judiciaire de Paris n'est parvenue à la personne assujettie.

Il convient, à ce stade de préciser, que les articles du CMF précités n'ont pas été écrits en tenant compte des particularités liées au remboursement des cyber-rançons et les règles actuelles ne sont

[32] *Il s'agit des infractions suivantes :*
- complicité d'accès et maintien frauduleux dans un système de traitement automatisé de données (STAD) articles 121-6, 121-7, 323-1, 323-5, 323-7 CP,
- complicité d'introduction frauduleuse de données dans un STAD articles 121-6, 121-7 323-3 alinéa 1, 323-5 CP,
- complicité de modification frauduleuse de données contenues dans un STAD, complicité d'entrave au fonctionnement d'un STAD articles 121-6, 121-7, 323-2, 323-5, 323-7 CP,
- complicité d'extorsion en bande organisée articles 121-6, 121-7, 131-26-2, 132-71, 312-6 alinéa 1, 312-1 alinéa 1, 312-13, 312-14 CP,
- association de malfaiteurs en vue de commettre un ou plusieurs crimes ou délits punis de 5 ans au moins, articles 450-1, 450-3 et 450-5 CP.

pas forcément claires notamment vis-à-vis des opérations de « *vigilance renforcée* » qui seraient à effectuer par les assureurs.

Il convient toutefois de mentionner que dans les Lignes Directrices conjointes TRACFIN-ACPR sur les obligations de déclaration et d'information à TRACFIN[33], les deux autorités détaillent les critères liés à des typologies de financement du terrorisme ; parmi ceux-ci figurent le paiement des rançons à la suite d'un enlèvement ou d'un vol de données personnelles et l'utilisation d'instruments de monnaie électronique.

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 comme mentionné ci-dessus[34] ; lorsqu'une déclaration s'impose, les assureurs ne peuvent procéder au remboursement de la rançon qu'à la condition que Tracfin n'a pas notifié d'opposition[35] à ce paiement. 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. Ainsi, la France met en œuvre divers régimes de sanctions à but de lutte contre le terrorisme ainsi que d'autres régimes dont un régime de sanction pour lutter contre les cyberattaques qui menacent l'Union ou ses États membres[36].

La mise en œuvre des mesures de gel est une obligation de résultat à la charge des organismes financiers dont le non-respect peut faire l'objet de sanctions pénales. Il convient de relever qu'il existe

[33] *Voir point 99.*

[34] *Ces règles s'imposent également aux assurés dès lors qu'ils sont eux même assujettis aux obligations de LCBFT (cf. L561-2 CMF).*

[35] *À cet égard, dans son rapport d'activité 2019, TRACFIN mentionne qu'elle a été saisie par le signalement d'un Prestataire de Services sur Actifs Numériques-PSAN mentionnant une acquisition de 5.35 bitcoins (soit 50 000€) d'un dirigeant d'entreprise pour le paiement d'un ransomware.*

[36] *Voir le registre des gels : personnes et entités sanctionnées : https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/tout-savoir-sur-les-personnes-et-entites-sanctionnees.*

une vraie difficulté d'effectuer en pratique cette identification, les pirates passant par des adresses mails étanches rendant la traçabilité très compliquée. Les assureurs et leurs experts tentent par les moyens techniques dont ils disposent de vérifier les liens et affiliations (*via* les *chain analysis*) entre adresses IP de paiement et les attaquants. Un travail est également effectué sur les failles exploitées et les modes opératoires des attaquants qui peut permettre dans certains cas de remonter vers des groupes d'ores et déjà identifiés.

Compte tenu de ces difficultés pratiques d'identification il existe toujours un risque juridique pour les assureurs étant donné l'obligation de résultat imposée par les textes.

Aussi, avant tout remboursement de rançon l'assureur doit s'efforcer de procéder à l'aide des éléments d'identification obtenus d'identifier l'attaquant et vérifier, s'il n'est pas désigné par une mesure de gel des avoirs. Si cela était le cas, l'assureur est tenu de le déclarer « *dans les plus brefs délais* » à la DG Trésor.[37]
Tout remboursement par l'assureur d'une rançon payée à l'une des personnes ou entités gelées/sanctionnées au niveau national, européen ou international est prohibé.

2.1.3 - Aperçu de la situation à l'étranger[38]

Il est intéressant d'examiner la situation à l'étranger de façon à la mettre en perspective avec la règlementation française.

De plus il est à noter que certaines législations, essentiellement la législation américaine, ont une portée extraterritoriale et doivent être prises en compte par les assureurs dans le cadre de la mise en œuvre de leurs procédures de compliance.

2.1.3.1 - États-Unis (voir également Annexes 5 et 6)

À la suite du nombre grandissant de cyberattaques par ransomware dont sont victimes depuis quelques mois les entreprises américaines[39], la cybersécurité et plus spécifiquement les attaques

---

*[37] Voir art. L562-4 CMF et R562-3 + Lignes Directrices conjointes de la Direction Générale du Trésor et de l'ACPR sur la mise en œuvre des mesures de gel des avoirs, document de nature explicative, version mise à jour au 16 juin 2021 ; il est vrai que l'assureur ne paye pas directement la rançon aux attaquants et qu'à ce titre, si le remboursement se fait auprès d'une entité non désignée, les assureurs n'auraient pas à faire de déclaration à la DGT. Il convient toutefois de relever que les Lignes Directrices visent également les fonds ou ressources économiques qui sont « mis **indirectement** à la disposition » d'une personne ou entité désignée. Selon les Lignes Directrices, l'interdiction de mise à disposition indirecte « vise notamment le cas de l'organisme financier qui sait que les fonds ou ressources économiques bénéficient in fine à la personne ou l'entité désignée. » Voir point 2.1.3.4*

[38] Un certain nombre d'informations contenues dans la présente partie ne sont pas officielles mais sont issues d'échanges intervenus dans le cadre de discussions informelles avec les associations nationales d'assureurs.

[39] Le géant de la viande JBS, le gestionnaire d'oléoducs Colonial Pipeline, une compagnie de ferries du Massachusetts, des collectivités locales et des hôpitaux américains, la société américaine Kaseya…

par ransomwares, font aujourd'hui l'objet d'une attention particulière des autorités américaines au plus haut niveau.

De manière générale, **bien que non interdits**, le paiement par les victimes et le remboursement par les assureurs des rançons sont **découragés** par les autorités américaines lesquelles incitent parallèlement à l'adoption de politiques visant à réduire le risque d'attaques cyber.

En revanche, le paiement d'une rançon devient **illicite** s'il viole la réglementation OFAC (*Office of Foreign Assets Control*, Agence du Département du Trésor américain). En effet, depuis octobre 2020, les organismes, et notamment les établissements financiers qui facilitent le paiement de rançons réclamées par les cybercriminels, pourraient se voir sanctionner par l'OFAC.

Le 01 octobre 2020, l'OFAC a publié un « avis » alertant sur les risques de sanctions liées au paiement de rançons auprès d'entités criminelles identifiées par les autorités américaines. Jugeant que de nombreuses entreprises sont en capacité de payer la rançon grâce à l'assurance qu'elles ont souscrite, l'OFAC a alerté sur les risques de sanctions civiles et pénales encourues par les institutions facilitant le paiement d'une rançon, dans l'hypothèse où celui-ci est effectué auprès d'une entité sanctionnée. Se fondant sur deux lois centrales dans le régime de sanctions américain que sont l'*International Emergency Economic Powers Act* (IEEPA) et le *Trading with the Enemy Act* (TWEA), l'OFAC a pu émettre l'interdiction formelle de contribuer financièrement ou de fournir des fonds à des personnes ayant des liens avec des activités cybercriminelles (« *blocked list persons* ») :

- les « *sanctioned jurisdictions* » et leur gouvernement (Crimée, Cuba, Iran, Corée du Nord et Syrie),
- toute personne résidant dans l'un de ces États,
- toute personne figurant sur la liste « SDN » (*Specially Designated Nationals and Blocked persons*),
- toute personne détenue à 50% ou plus par l'une des personnes figurant ci-dessus.

Toute violation de la règlementation OFAC expose le contrevenant à une amende civile qui peut être éventuellement suivie de poursuites pénales (dans le cas où il est prouvé que la personne ayant payé la rançon savait que le paiement était effectué auprès de « *Sanctioned Persons* » et donc illégal).

S'agissant de la territorialité de la réglementation OFAC sont concernés les :

- citoyens US quel que soit leur lieu de résidence,
- résidents permanents US, toute personne vivant aux US,
- entités de droit US ainsi que leurs filiales situées hors US,
- entités de droit EU ayant une filiale aux US.

En ce qui concerne la question de l'assurabilité des rançons à proprement parler, la réglementation OFAC précitée interdit formellement « *la facilitation* » du paiement de rançon par toute personne si le paiement de rançon à des cyber-attaquants va à l'encontre de la réglementation OFAC (*ie* : si le paiement est effectué auprès d'une entité sanctionnée) ; sont visées comme facilitateurs les entreprises d'assurance : "*Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, **cyber insurance firms**, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.*"

Toute personne (y compris les assureurs[40]) intervenant dans la chaîne de paiement d'un ransomware pourrait être reconnue civilement et pénalement responsable en tant que « *facilitateur* » si le paiement est effectué auprès d'une « *sanctioned person* ».

L'amende civile peut être infligée, y compris dans les cas où le facilitateur ne savait pas ou n'avait pas de raison de savoir qu'il effectuait une transaction avec une « *sanctioned person* ».

Lorsque l'OFAC évalue la sanction applicable au payeur de la rançon ou au facilitateur, il prend en compte :

- la mise en place d'un programme de conformité fondé sur le risque afin de réduire le risque de violation de la réglementation OFAC,
- le rapport qu'il établit de sa propre initiative à l'attention des forces de l'ordre sur l'attaque,
- la manière dont ce payeur/facilitateur a coopéré avec les forces de l'ordre.

À ce jour, il n'y a pas eu d'actions pénales ou civiles américaines, que ce soit par l'OFAC ou une autre agence américaine, contre les victimes d'attaques par ransomware ou leurs banques ou assureurs en rapport avec la réalisation, le traitement ou l'indemnisation d'un paiement par ransomware.

Cet avis de l'OFAC a été mis à jour le 21 septembre 2021. En plus de rappeler le risque de sanction en cas de « *facilitation* » de paiement de rançon, l'OFAC insiste sur la nécessité pour tous les acteurs économiques de se doter d'un programme de conformité visant à atténuer l'exposition au risque de sanction[41] et liste les agences gouvernementales à contacter par toute personne impliquée dans une demande de rançon à la suite d'une cyberattaque.

Hormis ces avis importants de l'OFAC, il est intéressant de relever diverses initiatives au niveau américain qui illustrent la manière dont le sujet des ransomware est abordé par les autorités américaines (voir Annexe 5).

---

[40] Que ce dernier soit américain ou non dès lors que la rançon est payée auprès d'une entité sanctionnée.

[41] À cet égard, l'OFAC a publié un guide d'aide à la mise en place d'un tel programme : https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

Compte tenu de la portée souvent extraterritoriale des lois américaines, la décision par l'assureur de rembourser une rançon ne pourra être prise qu'après vérification que cette rançon n'a pas bénéficié à l'une des entités « *sanctionnées* » par les autorités américaines et respecte de manière générale les obligations réglementaires mises à la charge des institutions financières par les autorités américaines et en particulier, dans certains cas, l'obligation d'information[42] des autorités en cas d'attaque par ransomware.

2.1.3.2 - Situation dans les autres pays du monde (voir Annexe 4 pour le détail)

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.

L'on peut également relever qu'aux Pays-Bas la question de l'assurabilité des rançons à la suite d'une cyberattaque fait l'objet d'un débat au niveau politique, non tranché à ce jour.

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

2.2.1 - Arguments en faveur de l'interdiction

Les arguments récemment développés en faveur d'une telle interdiction par diverses instances, groupes de travail, parlementaires voire certains assureurs, se concentrent principalement autour

[42] *Voir FinCen Advisory du 01/10/2021 : Suspicious Activity Reporting-SAR.*

des axes[43] suivants :

• le paiement des rançons et leur remboursement potentiel par les assureurs nourrit un écosystème criminel et par cela augmente le risque d'attaque ; cet effet d'amplification est particulièrement élevé dans le domaine cyber.

• Bien que les assureurs et les assurés tendent à garder confidentielle l'existence des couvertures « rançon », cette 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, selon les propos tenus par le parquet de Paris lors de l'audition devant le Sénat, « *les français payent* ».[44]

• 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 car elles se croient « protégées » (principe du « risque moral »).

• En tout état de cause, payer la rançon ne garantit aucunement la restauration des données, d'une part parce qu'il n'y a aucune garantie que les Cyber malfaiteurs remplissent leurs « promesses » (communication de la clé de déchiffrement, non publication des données piratées etc…) et d'autre part parce que les fichiers modifiés par les ransomware ont de fortes chances d'être corrompus[45]. Par ailleurs 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 (qui cède au chantage s'expose à nouveau…).

---

[43] *Dans son rapport en date du 10 juin 2021 précité, le Sénat insiste également sur le risque de solvabilité que font peser les « cyber risques » sur les assureurs, en particulier :*

- du fait de l'existence de « silent cover » dans de nombreux contrats qui peuvent conduire les assureurs à prendre en charges des dommages liés à une attaque cyber par le biais de contrats non spécifique (contrat dommage, RC exploitation, Fraude malveillance etc…), et

- de l'absence de stabilisation du marché et de l'existence de risques systémiques importants.

Mais cet argument n'est pas spécifique à la couverture des rançons cyber. Il concerne l'assurance des risques cyber en son ensemble et la nécessité pour les assureurs d'identifier de manière autonome les « cyber risques », de l'exclure des contrats traditionnels et de mettre en en place les mesures nécessaires pour maitriser et limiter leurs risques par le biais d'études actuarielles, de leur politique de souscription et des choix effectués par chacun au niveau des garanties offertes à leur clients comme pour tout autre type d'assurance. Le fait que le marché des « cyber risques » soit un marché émergent, en tout cas en Europe (même si le marché américain est plus mature) justifie une surveillance accrue et éventuellement, pourquoi pas, pour certains évènements, la mise en place de système de transfert de tout ou partie du risque à l'État par un mécanisme de type GAREAT mais il ne saurait, en soi, justifier une interdiction quelconque. Au niveau des assureurs Français et comme l'a indiqué la FFA (tel que relevé dans le Sénat dans son rapport précité) un travail précis de l'exposition de leur portefeuille au risque cyber a d'ores et déjà été effectué pour identifier leurs expositions au « silent cover » afin de les supprimer, de permettre une tarification du risque cyber au juste prix ainsi qu'une meilleure maîtrise des cumuls potentiels.

[44] *« Cyberattaques : les assureurs étrillés sur le paiement des rançons » Argus de l'Assurance 20 avril 2021. Si le nombre d'attaques cyber a explosé depuis 2020, les chiffres réels par pays sont loin d'être fiables mais la France ne semble pas payer « plus » que d'autres pays tels les USA ou l'Allemagne. Voir sur ce point le rapport d'Hiscox « Cyber Readiness 2020 » précité. Ce point a été confirmé par l'ANSSI lors des auditions organisées par le HCJP.*

[45] *Source « Attaques par rançongiciels, tous concernés comment anticiper et réagir en cas d'incident ? » ANSSI août 2021.*

• La possibilité de remboursement des cyber-rançons par les assureurs augmente le risque de violation du régime des sanctions/lutte contre le financement du terrorisme.

• Les difficultés d'identifier les cyberattaquants constituent un obstacle à l'application des mesures LCB-FT et gel des avoirs auxquelles sont soumis les assujettis.

En résumé, pour les partisans d'une telle interdiction, interdire le remboursement des rançons par les assureurs inciterait les entreprises à ne pas céder aux demandes de paiement rançon et à mieux se protéger contre le risque cyber ce qui conduirait nécessairement à une diminution des attaques de ce type et une baisse de la cybercriminalité et du financement du terrorisme.

2.2.2 - Arguments en faveur de l'assurabilité[46]

• Dans les cas extrêmes de mise en danger de la survie de l'entreprise ou de la continuité d'activités essentielles pour le fonctionnement de l'économie ou de la société, 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[47]. Par ailleurs, si l'entreprise ne peut financer cette rançon la paralysie de son système d'exploitation peut générer des pertes d'exploitation ou des dommages en termes de responsabilité civile très importants et mettre en danger la survie de l'entreprise.

• Comme déjà relevé 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 » ou autres demandes de cyber-rançons.

• 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 :

- d'une part parce que des solutions préférables au paiement de la rançon sont trouvées grâce à l'accompagnement technique de l'assurance (accompagnement de gestion de crise, accompagnement par des experts informatiques etc...),

- d'autre part parce qu'il existe des mesures pour inciter les assurés victimes à opter pour ces autres solutions (franchises et/ou des découverts obligatoires plus ou moins élevés en fonction du niveau de protection de l'assuré).

• En outre une telle interdiction rendrait nécessairement moins attractifs les contrats d'assurance cyber proposés aux entreprises sur le marché, d'où un moindre encouragement pour ces dernières

[46] *Pour les incidences juridiques négatives que pourrait avoir une interdiction unilatérale par la France sur les entreprises et le marché français de l'assurance, se reporter au point 2.3.1 ci-dessous.*

[47] *À cet égard il n'a jamais été reproché aux assureurs de participer à un « écosystème » criminel dans le cadre des assurances de vol ou fraude en affirmant que l'existence de ces couvertures encouragerait les voleurs/fraudeurs.*

à adopter les bonnes pratiques en matière de protection contre la cybercriminalité. Si les conditions de souscription sont trop complexes et les couvertures réduites les PME ne souscriront pas.

• Contrairement à l'affirmation selon laquelle la possibilité d'obtenir le remboursement d'une rançon par l'assureur en cas d'attaque cyber n'« *inciterait* » pas les entreprises à prendre les mesures de protection adaptées[48]. **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[49] mais également sur la mise en place effective de ces mesures**. À ce jour, et à notre connaissance, l'ensemble des opérateurs sur le marché exigent de leurs assurés qu'ils aient mis en place certaines mesures de sécurité (mesures qui ont été renforcées depuis quelques années du fait de l'évolution de la sinistralité) pour pouvoir bénéficier des garanties d'assurance cyber. La plupart des contrats proposent d'ailleurs l'intervention de sociétés spécialisées en la matière pour aider les assurés à auditer leurs installations afin d'identifier les risques spécifiques à l'entreprise et mettre en place les mesures nécessaires.

• On rappellera que les assureurs couvrent les conséquences du vol pour les victimes même si le vol est pénalement répréhensible. Les assureurs n'ont jamais été accusés d'être à l'origine du développement des vols parce qu'ils indemnisent les victimes de ces infractions. Au contraire, les assureurs ont participé et participent toujours activement au développement de tout un écosystème de prévention et de protection des acteurs économiques contre le vol (prise en compte des moyens de prévention pour lutter contre tous les types de vols, de véhicules, d'habitations, industriels, en cours de transport…).

• De même, les assureurs estiment qu'ils « n'encouragent » pas les assurés à régler les rançons comme cela a pu être dit. Ayant parfaitement conscience des risques pris en cas de paiement de la rançon (risque que l'assuré soit à nouveau victime d'une demande de rançon et donc d'un nouveau sinistre pour l'assureur ; risque de non-récupération de données ; risques de corruption des données récupérées etc…), 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 de mettre fin ni aux demandes de rançon, ni à la cybercriminalité en général, ni de réduire les coûts pour la société ; pire, cela conduirait à pénaliser certaines entreprises ou collectivités victimes des cybercriminels et

[48] *Voir le rapport du Senat précité page 131.*

[49] *L'introduction par les assureurs d'exclusions du risque cyber dans les contrats d'assurance classiques (RC générale, dommages, fraude...) a fait prendre conscience aux entreprises de l'importance du risque cyber et de la nécessité de prendre des mesures de protection et de souscrire une assurance autonome.*

qui pourraient se retrouver ainsi en grande difficulté financière faute de pouvoir faire porter tout ou partie de leurs pertes sur l'assurance[50].

2.3 - Problématique européenne

La possibilité d'interdire ou de limiter l'assurance du paiement d'une rançon à la suite d'une cyber-attaque par ransomware doit être appréhendée à l'aune du marché européen dans lequel évoluent les entreprises d'assurance françaises et les assurés victimes de ransomware.

En effet, 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 et pourrait d'autre part contrevenir au principe européen de libre circulation des services (2.3.1).

Par ailleurs, 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 (ci-après EM) qui pourraient, elles, continuer à bénéficier d'une couverture d'assurance leur permettant d'être garanties contre le risque de ransomware.

Se pose donc la question de la possibilité pour l'UE d'adopter un texte contraignant, qui interdise ou limite l'assurabilité du risque de paiement des rançons en cas d'attaque par ransomware, eu égard aux principes de subsidiarité et de proportionnalité qui régissent l'exercice des compétences de l'Union européenne (2.3.2).

2.3.1 - La portée d'une interdiction nationale de l'assurabilité du risque de paiement des rançons en cas d'attaque par ransomware

Juridiquement (voir analyse détaillée en Annexe 7), bien que l'on ne puisse préjuger de l'interprétation souveraine du Traité et du droit dérivé par la CJUE, seule compétente en dernier ressort pour juger de la légalité d'une mesure nationale d'intérêt général ou d'ordre public, il semble

[50] *On ajoutera qu'aux États Unis tant le FBI que les services de renseignements sont opposés à l'interdiction pure et simple pour les assureurs de prendre en charge les cyber-rançons. La collaboration entre assurés (qui ont l'obligation de coopérer avec les autorités pour pouvoir bénéficier des garanties), les entreprises de cybersécurité et les forces de l'ordre permettent régulièrement à ces dernières de remonter et de démanteler des filières de cybercriminels en utilisant les informations qui leurs sont fournis par les assurés et leur expert en sécurité en cas d'attaque et ce en particulier semble-t-il grâce en particulier aux informations sur les adresses IP utilisés. La mise en place d'une telle collaboration par l'intermédiaire d'équipes de force de sécurité et de magistrat dédiées telles que proposée par le Sénat dans son rapport précité pourrait être utilement envisagée.*

qu'une interdiction légale[51] d'assurer le risque rançon pourrait satisfaire aux critères[52] développés par les institutions communautaires.

Ainsi, l'interdiction française d'assurer ce type de risque devrait pouvoir s'imposer aux assureurs qui exerceraient leur activité en France par voie de LPS ou de LE y compris dans les situations où la loi applicable au contrat d'assurance n'est pas la loi française.

Mais il existe toujours un risque de sanction pour entrave à la libre circulation des services et à l'exercice de la LPS et de LE.

Par ailleurs et surtout, une interdiction purement 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 et ne résoudrait pas le problème de la distorsion de concurrence entre entreprises victimes selon qu'elles sont établies dans un EM qui autorise ou non l'assurabilité du risque de ransomware.

Il convient dès lors d'envisager la possibilité d'une interdiction édictée par un texte européen.

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

L'existence ne serait-ce que potentielle d'une restriction à la libre circulation des services, conduit à s'interroger sur la faisabilité d'une harmonisation européenne de la question de l'assurabilité du risque de paiement des rançons en cas d'attaque par ransomware.

La question est celle de savoir si l'Union européenne serait compétente pour imposer aux États membres d'interdire l'assurabilité des rançons par un acte de droit dérivé (pour une analyse détaillée, voir Annexe 7).

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 et

---

[51] S'agissant de la forme de la disposition française qui interdirait de couvrir le risque de rançon en cas de cyberattaque, il semble que seule une disposition légale ou réglementaire puisse valablement « porter » une telle interdiction et constituer une règle d'intérêt général qui puisse s'imposer aux opérateurs en LPS ou en LE ; un code de conduite professionnel approuvé par l'ACPR ou une recommandation ACPR édictant une interdiction ne sont pas juridiquement envisageables.

[52] Les critères sont les suivants :
- relever d'un domaine non harmonisé,
- ne pas faire double emploi avec la règle du pays d'origine,
- poursuivre un objectif d'intérêt général,
- être non discriminatoire,
- être objectivement nécessaire,
- être proportionnée à l'objectif poursuivi.

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. À cet égard, la révision de la Directive Solvabilité II pourrait constituer un véhicule législatif *ad hoc*.

Toutefois, eu égard aux recommandations formulées par le groupe de travail ci-après et 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, proposer un texte européen interdisant l'assurabilité des rançons n'est pas souhaité par les auteurs du présent rapport. Il convient de noter également qu'aucun État membre n'a, à ce jour, adopté un texte législatif pour interdire l'assurance du risque de rançon. Le souci de protection des entreprises et de façon plus générale de toute victime potentielle de cyberattaques semble l'emporter.

2.4 - Recommandations du groupe de travail HCJP sur la question du remboursement par les assureurs des rançons versées par les victimes de cyberattaques

Dès lors que les dispositifs français et internationaux visant à lutter contre le blanchiment et le financement du terrorisme sont respectés, compte tenu du besoin des victimes de se garantir contre le risque de ransomware et du marché européen dans lequel évoluent les entreprises d'assurance et les victimes, interdire l'assurabilité du remboursement des rançons en cas de cyberattaque n'est pas préconisé.

Toutefois, compte tenu du risque sans cesse grandissant, d'attaques par ransomware et de l'objectif général de lutte contre la cybercriminalité, que partagent les membres du groupe de travail, les axes d'amélioration suivants pourraient être envisagés.

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

i. Imposer et faciliter les dépôts de plainte[53]. D'un point de vue pratique, ce dépôt de plainte devrait pouvoir être fait en ligne sur un site dédié (voir proposition ci-dessous).

ii. Renforcer/centraliser les dispositifs publics de cyber protection en moyens humains et financiers et améliorer la coordination entre les différentes autorités publiques compétentes[54].

[53] *Selon Marc Boget, Général de division, commandant de la gendarmerie dans le cyberespace, les victimes d'attaques cyber ne déposent plainte que dans un cas sur 270, cf. déclarations au congrès des agents généraux de la Nouvelle-Aquitaine 13 septembre 2021.*

[54] *Il ressort des auditions réalisées dans le cadre de l'élaboration de ce rapport que le cadre actuel des autorités publiques impliquées dans le traitement des cyberattaque et de la cybersécurité en général paraît dispersé : cybermalveillance.gouv, l'ANSSI, l'Office central contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction contre la cybercriminalité (SDLC), la Gendarmerie nationale : le centre d'action contre les criminalités numériques (C3N) du Service central du renseignement criminel (SCRC) et la Préfecture de police de Paris, (DCRI)...*

• Élaborer au niveau national un cadre clair, accessible et commun à tous les opérateurs (publics, privés, quelle que soit leur taille) pour les assister et les aider à répondre aux attaques par ransomware ; à l'instar de ce qui a été mis en place aux US, instaurer une autorité publique unique/centralisatrice[55] dotée de pouvoirs et de moyens suffisants qui puisse être contactée en ligne, afin de :

- abriter la procédure de dépôt de plainte obligatoire mentionnée ci-dessus ;

- 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. À cet égard, cette autorité unique/centralisatrice pourrait communiquer une liste des rançongiciels et leurs variants identifiés ou fortement soupçonnés d'être liés à une organisation terroriste ; cette liste permettrait aux assureurs de refuser le remboursement de la rançon lorsque le rançongiciel utilisé ou son variant y sont mentionnés. Pour plus d'efficacité cette liste pourrait être commune à l'ensemble des États membres et publiée par une autorité unique européenne ;

- 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. À cet égard, pourrait être mise en place une collaboration entre assureurs et autorités judiciaire et policière pour encadrer au mieux le paiement de rançons (communication des adresses IP de paiement, de toute information utile à l'instruction de l'affaire par les autorités publiques…).

• Compte tenu du marché européen dans lequel évoluent les opérateurs (assureurs et victimes) l'élaboration d'un cadre européen renforcerait l'efficacité du dispositif d'aide aux victimes et aux assureurs et pourrait permettre un échange d'informations à un niveau plus global.[56]

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 ; les demandes de couvertures d'assurance contre les risques cyber ou les rançons ne doivent pas apparaître.

---

[55] *Par exemple l'ANSSI.*

[56] *Voir à cet égard les conclusions du Conseil européen sur le projet d'élaboration d'un cadre européen de gestion des crises en matière de cybersécurité via la mise en place d'une Unité conjointe de Cyber sécurité + cadre européen de coopération (CSIRT Network) mis en place dans le cadre de la Directive NIS (pour les opérateurs essentiels et importants) précitée et dans le cadre du futur Règlement DORA pour les acteurs dans le domaine des services financiers - Création d'un Hub européen de reporting d'incident cyber majeur.*

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 qui s'imposent tant aux assurés qu'aux assureurs,

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

• en matière d'indemnisation :

- conditionner la mise en jeu de la garantie rançon à un dépôt de plainte de la part des assurés victimes et à l'information d'un dispositif public compétent (voir ci-dessus)[57],

- 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*[58] qui suivent le paiement de la rançon en cryptoactifs par l'assuré afin d'améliorer les chances d'identifier les cyberattaquants,

- agir avec prudence[59] lorsque l'assureur conseille un intermédiaire qui peut assister l'assuré dans la négociation de la rançon et ne conseiller que des entreprises sérieuses et disposant d'une bonne réputation[60],

- s'abstenir, par prudence, de garantir les rançons payées en cryptoactifs qui ne gardent pas l'historique des transactions[61] et ne peuvent donc permettre la traçabilité du paiement ;

---

[57] Voir également dans ce sens la proposition du rapport d'octobre 2021 sur la cyber-assurance de la députée V. Faure-Mutian :
« Plus globalement, il convient d'inscrire dans le Code des assurances la subordination de l'activation des garanties de cyber-assurance à un dépôt de plainte auprès des services compétents. »

[58] Grâce à la traçabilité, inscrite dans le principe de la blockchain, qui enregistre instantanément chaque information échangée, il peut être possible déterminer à qui appartiennent les adresses anonymes où arrivent les bitcoins (compte en ligne).

[59] Eu égard au risque de qualification d'infractions pénales susceptibles d'être retenues à l'égard des intermédiaires mentionné plus haut au point 2.1.2.1.

[60] À cet égard, voir le label ExpertCyber mis en place par Cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillancegouvfr-lance-son-label-expertcyber ; ce label est destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Dans le cadre le cadre de sa mission d'assistance, le dispositif cybermalveillance.gouv, a pour objectif de mettre en relation des particuliers, des entreprises et des collectivités avec un réseau de professionnels en sécurité numérique pour les assister en cas de problème nécessitant une intervention technique.

[61] Ces monnaies n'étant pas rattachables à un établissement bancaire il est impossible d'investiguer le compte crédité.

• 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. Il s'agit que les assurés soient informés du fait, qu'à la suite des diligences accomplies conformément à la réglementation en vigueur liée à la lutte contre le blanchiment et le financement du terrorisme et à l'application des mesures de gel des avoirs, le remboursement de la rançon par l'assureur pourrait être refusé.

2.4.2 - Mesures 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 ; à cet égard, la législation devrait amener les assureurs à consulter, avant tout remboursement de rançon, la liste précitée des rançongiciels et leurs variants identifiés ou fortement soupçonnés d'être liés à une organisation terroriste.

ii. Agir au niveau européen pour un renforcement harmonisé de la cyber robustesse des entreprises afin d'aboutir à un écosystème sécurisé (voir Annexe 8 pour une analyse détaillée).

La mise en place par toutes les entreprises, y compris les TPE-PME et les personnes publiques d'une véritable politique de gestion du risque informatique portée par un responsable et approuvée au plus haut niveau de l'entreprise est une étape capitale dans la lutte contre les attaques informatiques par ransomwares.

À cet égard, pourrait être adopté au niveau européen un texte trans-sectoriel[62] visant à renforcer la cybersécurité de l'ensemble des opérateurs qui pourrait s'inspirer du cadre législatif européen mis en place par la Directive NIS[63] (*Network and information Security*) ou par le futur Règlement européen *Digital Operational Resilience Act* (DORA) applicable au service financier ; une approche proportionnelle pour moduler l'application des règles de sécurité en fonction des risques présentés par l'opérateur (« *risk based approach* ») devrait évidemment guider l'action du législateur.[64]

---

[62] *À noter que dans le programme de travail 2022 de la Commission européenne, publié le 19/10/2021, est annoncée une initiative législative visant à renforcer la cyber-résilience des opérateurs EU.*

[63] *Voir Directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Une nouvelle directive NIS 2 fait actuellement l'objet du processus législatif européen (cf. Briefing EU legislation in Progress, December 2021).*

[64] *Le renforcement parallèle et déjà initié de la cybersécurité des entreprises d'assurance constitue également une étape importante dans la sécurisation de l'écosystème ; s'agissant du sujet particulier des ransomware, il peut être en effet de l'intérêt des hackers de diriger leurs attaques vers des entreprises d'assurance afin d'avoir accès au détail des couvertures de chaque assuré. L'objectif étant d'orienter les futures attaques vers des entreprises assurées contre les ransomware facilitant ainsi le paiement de la rançon au bénéfice du pirate.*

Une cyber notation[65] des différents acteurs économiques quelle que soit leur taille, par une agence européenne souveraine pourrait compléter le dispositif et garantir la conformité de ces acteurs aux exigences de cybersécurité qui leur seront imposées par ce texte européen. Il s'agit d'informer les parties prenantes du niveau de maturité cyber de ces acteurs tout en maintenant un niveau de confidentialité élevée de la cyber notation.

Mais au-delà du niveau européen, le sujet devrait être traité à l'échelle internationale, compte tenu du caractère mondial du risque cyber.

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 (de pair-à-pair ou en « *peer-to-peer* ». C'est le principal risque lié aux crypto-actifs consistant en la possibilité de transférer des crypto-actis sans l'intervention d'un intermédiaire assujetti à la LCB-FT. Ces cypto-actifs sont souvent mentionnés dans le langage courant par le vocable « crypto-monnaies ».

Selon la définition de l'Autorité des Marchés Financiers (AMF), les « crypto-monnaies », plutôt appelées « crypto-actifs », sont des actifs numériques virtuels qui reposent sur la technologie de la *blockchain* (chaine de bloc) à travers un registre décentralisé et un protocole informatique crypté. Un crypto-actif n'est pas une monnaie. Sa valeur se détermine uniquement en fonction de l'offre et de la demande.

Les crypto-actifs ne reposent pas sur un tiers de confiance, comme une banque centrale pour une monnaie. Il existerait à ce jour plus de 15 000 (site de référence *CoinMarketcap*) crypto-actifs. Les plus connus sont le *bitcoin*, le *ripple*, l'*ether*, le *litecoin*, le *nem* et le *dash*.

Alors que les prestataires de services sur crypto-actifs font l'objet d'un encadrement en matière de 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 ; les crypto-actifs permettent aux cybercriminels de recevoir et de conserver leurs fonds sans intervention d'entités réglementées, sans limite et avec des frais réduits.

D'où l'idée d'œuvrer à une régulation de ces échanges.

---

[65] *En ce sens, voir la démarche exposée par « Preparing for cyber insurance », publiée par Ferma https://www.ferma.eu/advocacy/preparing-for-cyber-insurance/ + le rapport « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance », Philippe Cotelle, Philippe Wolf, Bénédicte Suzan » : « aux États-Unis, la SEC propose aux entreprises privées, depuis le mois de février 2018, un cadre formel pour informer les investisseurs du niveau de maturité cyber de l'organisation et de remontée d'information concernant les attaques cyber dont elle a été victime ».*

À noter que dans son Rapport à l'attention du Gouvernement, mentionné plus haut, l'IST (*American Institute for Security and Technology*) propose une règlementation des échanges en crypto-actifs : "*The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.*"

À cet égard, dans le cadre de sa stratégie sur la finance numérique, la Commission européenne a publié en septembre 2020 une proposition de Règlement sur les crypto-actifs visant à doter l'Europe d'un cadre harmonisé et global pour les crypto-actifs.

Parallèlement et plus récemment[66], 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. L'idée est de garantir une « *traçabilité totale des transactions de cryptomonnaies, telles que le bitcoin, et de prévenir et de détecter leur utilisation éventuelle à des fins de blanchiment de capitaux ou de financement du terrorisme* », indique la Commission européenne. Ainsi la proposition de règlement sur les informations accompagnant les transferts de fonds et de certains crypto-actifs inclut les transferts de crypto-actifs entre prestataires de services ainsi que les transferts en provenance ou à destination de portefeuilles non hébergés par un prestataire. Les prestataires de services sur crypto-actifs devront ainsi recueillir et transmettre des informations sur les donneurs d'ordre et les bénéficiaires des transferts.

Ces initiatives devraient permettre à terme une régulation accrue et harmonisée du marché des crypto-actifs, et de réduire les risques liés à cette catégorie d'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 avec la diffusion de guides pédagogiques tels que le guide ANSSI sur la « C*ybersécurité pour les TPE/PME en 12 questions* » , le kit de sensibilisation aux risques numériques publié par cybermalveillance.gouv.fr

[66] *Notons qu'au niveau national, le législateur a imposé d'une part une réglementation fiscale[66] et a d'autre part contraint les prestataires de services sur actifs numériques (PSAN) de s'enregistrer auprès de l'Autorité des marchés financiers (AMF) ; cette obligation concerne toutes les plateformes proposant l'achat et la vente de crypto-actifs, mais aussi leur conservation si elles sont basées en France ou destinent leurs services aux investisseurs français. En 2020, une ordonnance[66], prise dans le cadre de la loi PACTE a soumis aux obligations posées par le Code monétaire et financier en matière de LCB-FT les activités d'échanges d'actifs numériques contre d'autres actifs numériques (échanges dits « crypto-to-crypto ») et les plateformes de négociation d'actifs numérique. Cette ordonnance est venue compléter le cadre juridique issu de la loi PACTE qui avait déjà inclus dans le champ des entités assujetties à la LCB-FT les prestataires de services d'échanges entre actifs numériques et monnaie ayant cours légal (échanges dits « crypto-to-fiat ») et les services de conservation d'actifs numériques pour le compte de tiers. Cette ordonnance a été complétée par le décret n° 2021-387 du 02 avril 2021 relatif à la lutte contre l'anonymat des actifs virtuels et renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme ; ce décret renforce le dispositif de lutte contre le détournement d'actifs numériques à des fins criminelles.*

ou encore le guide FFA « *Anticiper et minimiser l'impact d'un cyber risque* ». Par ailleurs, la loi pour la croissance et la transformation des entreprises (PACTE) de 2019, a prévu de substituer aux différents réseaux de Centres de Formalités des Entreprises un guichet unique électronique qui sera la seule interface pour les formalités d'entreprise quelles que soient leur activité et leur structure juridique. **Un module de sensibilisation aux risques cyber devrait être intégré dans ce processus de création d'entreprise.**

ii. Réaffirmer les actions des entreprises d'assurance en matière de sensibilisation aux risques cyber auprès des entreprises (membres de cybermalveillance.gouv.fr, actions avec la gendarmerie nationale…).[67]

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

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.

Par conséquent dans une démarche de traitement assurantiel de ce risque composite, il apparait nécessaire de voir comment, dans un contexte français, le risque de guerre est abordé en droit des assurances (**3.1**), et quels sont les éléments de droit international (**3.2**) qui permettraient de mieux appréhender la notion de cyberguerre et de la rattacher à l'acte de guerre.

Cette courte analyse ne prétend pas à l'exhaustivité compte tenu de la multiplicité des questions soulevées par le sujet, et non encore résolues par les États et les organisations internationales.

Elle permet néanmoins de considérer que des attaques cyber assimilables à des actes de guerre sont une réalité admise en droit international, et qu'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 (**3.3**).

[67] *À cet égard, la gendarmerie nationale, la Fédération Française de l'Assurance (FFA, aujourd'hui France Assureurs) et AGEA (Fédération nationale des syndicats d'agents généraux d'assurance) ont signé le mardi 28 septembre 2021 un partenariat inédit pour former et sensibiliser les agents généraux d'assurance au risque cyber.*

3.1 - Le risque de guerre en droit des assurances

La guerre en matière d'assurance terrestre est dans cette zone de risque systémique dont l'ampleur est de nature à rendre inassurables les dommages subis par les personnes assurées du fait de tels évènements. À cet égard se trouve certainement en droit français[68] le fondement du régime légal de la présomption d'exclusion fixé à l'article L121-8 du Code 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 cette exclusion de l'article L121-8 du Code des assurances établie dans les termes suivants : « *L'assureur ne répond pas, sauf convention contraire, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires. Lorsque ces risques ne sont pas couverts par le contrat, l'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère ; il appartient à l'assureur de prouver que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires* ».

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 (infrastructures civiles) à l'occasion d'une attaque cyber d'origine étatique. Il s'agit bien sûr ici d'une inassurabilité technique en raison de l'impossibilité d'apprécier un tel risque et de le tarifer au moment de la souscription, et non pas d'une inassurabilité d'ordre public.

Cependant par rapport à la notion de guerre étrangère de l'article L121-8 du Code des assurances, la principale difficulté va tenir au lien qui pourra être fait entre ces deux notions.

Tout d'abord on relèvera que cette exclusion n'est susceptible de s'appliquer que quand elle est stipulée dans le contrat d'assurance, ce qui est le cas de l'essentiel des contrats du marché français en assurance de dommages aux biens et de responsabilité. Elle a été introduite en droit des assurances par la loi du 13 juillet 1930 dans un environnement où le concept de guerre étrangère était entendu selon une acception juridique classique différente de celle actuelle, marquée par les évolutions des conflits entre États et les évolutions du droit international public.

Néanmoins indépendamment de ces évolutions la revue de la jurisprudence relative à cette exclusion telle qu'elle est faite par la Doctrine permet de dégager quelques orientations, quoique cantonnées à la période entre 1945 et 1948, et en relation avec le conflit mondial de 1939-1945.

---

[68] *L'examen de la situation de six pays européens (Pays Bas, Danemark, Suède, Allemagne, Tchéquie, Roumanie) permet de relever une prohibition légale de l'assurance des risques de conflit armé, ou de guerre aux Pays Bas et au Danemark, sans que cette exclusion au vu de son interprétation soit de nature à inclure une attaque cyber. Les législations des quatre autres pays ne prévoient pas de dispositions légales relatives à des exclusions du risque de guerre.*

La Cour de cassation a ainsi pu définir dans deux arrêts de principe que le fait de guerre visé par l'exclusion correspond aux opérations militaires que sont les combats, bombardements, explosions, destructions ordonnées par les autorités militaires, ainsi qu'à tout fait qui se rattache étroitement aux opérations de guerre étrangère, sans qu'il soit besoin que le fait de guerre soit la cause unique ou directe du sinistre, au point d'y inclure les dommages d'incendie en raison de la destruction des moyens de secours qui en ont empêché la lutte (Cass. civ. 24 et 25 juillet 1945, Cie d'assurance Rhin et Moselle c. Lapel et Ane – Mutuelle de Rouen C. Bufacoux : D.1945, p.277, note P.L.P).

D'autres décisions rendues entre 1945 et 1948 sont encore relevées par la Doctrine, et qui jugent que la loi ne limite pas l'exclusion à la bataille, aux risques du combat, à l'action violente des troupes au temps et au lieu du sinistre (Cass. civ. 18 mars 1946 : RGAT 1946, p. 300. – Cass. civ. 9 décembre 1947 : RGAT 1948, p. 137).

La Doctrine déduit de cette jurisprudence que la Cour de cassation fait preuve de souplesse dans la définition du fait de guerre et dans l'appréciation du lien de causalité qui doit le rattacher au dommage.

Sur la particularité de la présomption légale d'exclusion de l'article L121-8 du Code des assurances qui met à la charge de l'assuré la démonstration que le sinistre trouve son origine dans un fait autre que le fait de guerre étrangère la jurisprudence a une appréciation assez peu contraignante pour l'assuré, lequel ne se trouve pas obligé d'établir précisément l'évènement qui a causé le sinistre mais l'absence de lien de causalité entre ce sinistre et un fait de guerre étrangère, et ce même si l'origine exacte du sinistre est inconnue (Cass. soc., 28 juin 1946 : RGAT 1947, p. 159. – Cass. civ., 23 juillet 1946 : RGAT 1947, p. 171).

De tout évidence le caractère daté de cette jurisprudence rend délicat d'en dégager des enseignements pour mesurer aujourd'hui la portée de l'exclusion légale en cas de cyberguerre, même s'il n'est pas indifférent que la Cour ait pu avoir à l'époque une lecture ouverte des faits de guerre à l'origine des dommages.

En outre la notion clef nous intéressant est d'avantage celle de guerre étrangère, sur la qualification de laquelle la jurisprudence française n'a pas eu à se positionner (à l'exception de la Cour d'appel de Saigon qui avait jugé en 1946 que l'état de guerre persistait en Indochine avec le Japon tant que le législateur français n'y avait pas mis légalement fin. On était donc là dans une approche très formaliste de la guerre, c'est-à-dire celle d'un conflit ouvert et déclaré entre la France et un autre État).

Au-delà de ces arrêts anciens attachés à l'article L121-8 du Code des assurances, un éclairage complémentaire utile peut passer par le rappel de la façon dont la jurisprudence actuelle fait une interprétation stricte, sinon étroite des exclusions légales (cf. exclusion de la faute intentionnelle – Article L113-1 du Code des assurances).

La question se pose donc de ce que pourrait être une interprétation stricte de la notion de guerre étrangère si l'exclusion était invoquée par un assureur lors d'une attaque cyber, et selon quelles conditions il pourrait être reconnu que cette attaque présente les caractères d'une guerre étrangère.

Si cette exclusion devait être appliquée au regard du droit français dont l'article 35 de la Constitution du 4 octobre 1958 dispose dans son premier alinéa que « *La déclaration de guerre est autorisée par le Parlement* », on serait sur une exigence de formalisme assez éloignée d'une cyberguerre, outre qu'on rappellera que depuis 1939 il n'y a pas eu de déclaration de guerre de l'État français.

La révision constitutionnelle du 3 juillet 2008 a ajouté trois alinéas à cet article 35 et introduit une nouvelle catégorie qui est celle d'une « *intervention des forces armées* » à l'étranger impliquant d'informer le Parlement, ce qui contribue à un effacement de la guerre comme catégorie ou institution juridique exclusive, au profit d'autres notions.

Pareille évolution est intéressante et doit inciter à ne pas enfermer le raisonnement sur la portée de l'exclusion dans une définition ancienne et limitée de la guerre étrangère dont l'effectivité serait subordonnée à un acte formel de déclaration.

Certains éléments du droit international public vont aussi dans ce sens et ouvrent la voie pour y accueillir la cyberguerre (voir 3.2. ci-après).

Au-delà de l'assurance terrestre, il convient de relever que les contrats d'assurance notamment maritimes relevant du titre VII, livre premier du Code des assurances (articles L171-1 à L176-5) ne sont pas soumis au régime de présomption de l'exclusion de l'article L121-8 du Code des assurances, mais à celui de l'article L172-16 avec une approche du marché qui accorde la garantie selon des conditions bien particulières : indemnisation des seuls dommages matériels, garantie en périls dénommés, exclusions spécifiques, prise en compte de zones géographiques à risques aggravés, résiliation à bref délai de la police, etc.

3.2 - Éléments du droit international public

Certains éléments du droit international sont intéressants pour la problématique soumise au groupe de travail en ce qu'ils ouvrent sur une signification large de la notion de guerre, associée à celle de conflit armé et qui est susceptible d'inclure les attaques cyber, le tout échappant au formalisme classique d'une déclaration de guerre.

En droit international public on ne trouve pas véritablement de définition de la guerre en tant que telle, et depuis plusieurs décennies on observe en parallèle l'émergence de nouveaux concepts.

Ainsi les Conventions de Genève de 1949 relative au droit international humanitaire par un article 2 commun aux quatre Conventions spécifient les conditions de leur application « *en cas de*

guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes, même si l'état de guerre n'est pas reconnu par l'une d'elles ».

Cette notion de conflit armé entre États est présentée comme centrale dans les commentaires de 2020[69] attachés aux Conventions en ce qu'elle permet l'application de ces instruments quand bien même il n'y aurait pas une guerre déclarée entre les États belligérants et une reconnaissance de cette situation entre eux.

Une telle approche en droit international est intéressante pour notre problématique car elle ouvre sur une signification large de la notion de guerre, laquelle associée à celle de conflit armé échappe au formalisme classique d'une déclaration de guerre qui pourrait donc ne pas être le préalable nécessaire à la qualification de cyberguerre en cas d'attaque cyber.

Sur ce point les commentaires de 2020 autour de l'article 2 commun des Conventions de Genève et de la notion de conflit armé international posent la question d'opérations cyber pouvant donner lieu à un conflit armé international.

La réponse apportée est claire dans l'hypothèse d'actions cyber menées par un État contre un autre, parallèlement à des opérations militaires plus classiques ou pour soutenir celles-ci, il ne fait aucun doute qu'une telle situation constituerait un conflit armé international. Il en serait de même si ces actions cyber constituant des actes isolés étaient exclusives de toute autre opération militaire plus classique, mais qu'elles entrainaient des destructions de biens civils ou militaires équivalentes.

En revanche la réponse est plus ouverte dans l'hypothèse d'attaques cyber avec des effets qui seraient moins dévastateurs pour les infrastructures civiles ou militaires dont le fonctionnement serait simplement perturbé. Les critères d'intensité, et de seuil de nuisance toléré seraient à prendre en compte, mais selon les auteurs il reste aux États à clarifier en droit si de telles opérations cyber pourraient être vues comme des actions armées constitutives de conflits armés soumises aux Conventions de Genève.

En tout état de cause en n'écartant pas d'emblée une possible qualification de conflit armé international y compris pour cette dernière hypothèse, c'est donc bien le spectre le plus large des attaques cyber perpétrées par un État, et ce quels qu'en soient les effets, qu'il parait possible de retenir.

À ce titre les Conventions de Genève sont donc un éclairage utile pour une meilleure compréhension de ce que peut être sur le plan juridique une cyberguerre, à l'aune de la notion de conflit international

[69] *Les commentaires aux Conventions de Genève de 1949 ont pour objectif de préciser la compréhension des règles de ces conventions. Ils ont été rédigés pour la première fois en 1952. Cette actualisation de 2020 donne une lecture plus moderne des Conventions qui tient compte de l'évolution des conflits et de la pratique du droit s'y rapportant.*

entendu comme l'engagement par un État d'actions hostiles militaires contre un autre État quelles qu'en soient les modalités.

À l'inverse les Conventions de la Haye de 1899 et de 1907[70] qui restent sur une notion de guerre déclarée semblent inopérantes pour contribuer en droit à la définition de cette méthode de guerre contemporaine que constitue la cyberguerre.

Pour sa part la Charte des Nations Unies est construite sur un régime qui rend les guerres d'agression illicites et ne permet l'usage du recours à la force contre un autre État que s'il est autorisé en vertu d'un mandat du Conseil de sécurité des Nations Unies.

Il n'a pas été relevé au cours des années écoulées de décisions des Nations Unies en application de la Charte constatant un recours à la force illégitime de la part d'un État à la suite d'une attaque cyber, ou dans ce même contexte autorisant en réaction un État à user de la force conformément à son droit de légitime défense. Cependant des analyses convergentes admettent que l'interdiction du recours à la force et de la légitime défense des États visées aux articles 2 et 51 de la Charte des Nations Unies s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées et dont une opération cyber ne peut être exclue[71].

En ce qui concerne l'identification des auteurs d'une telle opération cyber et leur origine étatique ou non, le point est important et complexe mais pas insoluble si on considère qu'il n'existe pas d'obligation en droit international pour un État de prouver publiquement l'imputabilité d'un acte illicite dont il est victime à un autre État. Et s'agissant d'actes qui ne seraient pas menés par les États eux-mêmes au travers de leurs propres organes, le droit international dégage des critères de contrôle effectif ou de contrôle global[72] de la part d'un État à destination d'acteurs non étatiques permettant de lui imputer les opérations en cause.

Sur un terrain plus factuel les attaques cyber imputées à des États ces dernières années sont : l'attaque NotPetya (juin 2017) attribuée à l'État Russe, et celle du Sony Hack (novembre 2014) attribuée à l'État de Corée du nord. L'imputation pour l'attaque NotPetya notamment a été documentée par les agences de renseignement des États victimes comme les USA et le Royaume Uni.

---

[70] Convention (III) de la Haye (1907), article 1 : Les Puissances contractantes reconnaissent que les hostilités entre elles ne doivent pas commencer sans un avertissement préalable et non équivoque, qui aura, soit la forme d'une déclaration de guerre motivée, soit celle d'un ultimatum avec déclaration de guerre conditionnelle. Voir également article 2 de la Convention (II) de la Haye (1899).

[71] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Ouvrage de référence constitué de règles et commentaires mais sans valeur juridique contraignante pour les États, réalisé par des experts dans le cadre de l'OTAN (CCDCOE) – Edition 2017.

[72] Pour un contrôle effectif : approche de la Cour Internationale de Justice et de la Commission du Droit International (ONU). Pour un contrôle global: approche TPYI.

L'attaque NotPetya a eu la particularité de par l'ampleur des dommages occasionnés et le grand nombre d'entreprises touchées d'exposer les assureurs dont certains ont pu opposer les exclusions conventionnelles des actes de guerre telles que stipulées dans les polices anglo-saxonnes. Si certains commentaires vont en l'espèce dans le sens de la caractérisation d'un acte de guerre avec des chances pour les assureurs de voir l'exclusion admise[73], la *Lloyd's Market Association* a néanmoins d'ores et déjà publié des nouveaux modèles de clauses d'exclusions propres à la cyberguerre[74], et une première décision d'un tribunal américain a récemment considéré qu'une clause traditionnelle d'exclusion de la guerre ne s'appliquait pas à la cyberattaque NotPetya de 2017[75].

Ces quelques éléments d'analyse permettent de caractériser un environnement international avec des situations intermédiaires qui ne sont ni la paix, ni la guerre, mais où le conflit armé entre États ne cesse pas pour autant d'exister avec des recours à la force dont les moyens peuvent passer par des attaques cyber.

3.3 - Recommandations du groupe de travail HCJP

Entre un droit des assurances français dont l'exclusion légale des risques de guerre étrangère n'avait pas été pensée pour des attaques cyber perpétrées par des États, et des relations internationales où le formalisme de la déclaration de guerre est de plus en plus rare, *a fortiori* par rapport à des attaques cyber, il y a l'opportunité d'une clarification des limites de l'assurabilité en raison de l'ampleur des dommages susceptibles d'être générés par un acte de cyberguerre.

Cette clarification devrait entrainer une modification de l'article L121-8 du Code des assurances.

L'objectif serait d'inscrire l'exclusion dans la contemporanéité du droit et des relations internationales, en ajoutant au concept de guerre étrangère, celui de conflit armé international. Une définition de la notion de guerre étrangère devrait compléter l'article L121-8 pour une claire compréhension de la part des assurés. Elle serait rédigée selon une acception large incluant le 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 qui conditionnerait l'exclusion ne devant pas, à la différence de l'état de guerre étrangère dans son acception classique, être déterminé par une déclaration

[73] *NotPetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks - Katherine S. Wan - Washington Law Review Volume 95 Number 3 – 10.01.2020.*

[74] *https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.asp.*

[75] *Superior Court of New Jersey, 6 December 2021, Merck & Co. Inc., and International Indemnity Ltd v. Ace American Insurance Company, et al.*

formelle, ou une attribution publique mais par une appréciation de faits et de critères propres à un conflit armé entre États dont les moyens de guerre seraient menés en partie ou exclusivement au travers d'opérations cyber.

Sur cette base la rédaction modifiée de l'article L121-8 du Code des assurances avec l'insertion d'un troisième alinéa définissant la guerre étrangère pourra s'établir comme suit :

L'assureur ne répond pas, sauf convention contraire, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires.

Lorsque ces risques ne sont pas couverts par le contrat, l'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère ; il appartient à l'assureur de prouver que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires.

Est considérée comme une guerre étrangère, au sens du présent article, y compris en l'absence de déclaration formelle de guerre ou d'attribution publique, tout conflit armé international impliquant un État, ou une, ou plusieurs personnes agissant sous le contrôle ou au service des intérêts de cet État, y compris en cas de mise en œuvre d'armes ou de moyens cybernétiques.

Il est entendu que cette modification n'aurait pas vocation à réduire le champ de l'obligation d'assurance fixé à l'article L126-2 du Code des assurances en cas d'attentats ou d'actes de terrorisme dès lors que les faits concernés relèveraient d'une telle qualification pénale.

En l'absence de modifications de l'exclusion légale une autre voie serait la stipulation d'une exclusion conventionnelle établie par l'assureur mais qui ne serait pas sans poser des difficultés de rédaction au regard de l'exigence de son caractère formel et limité (article L113-1 du Code des assurances) faisant ainsi peser une certaine insécurité juridique sur le dispositif tant à l'égard de l'assureur, qu'à l'égard des assurés confrontés à des rédactions variables entre assureurs. Cette voie purement conventionnelle n'est donc pas recommandée d'autant que l'article L121-8 laisse la place à la liberté contractuelle pour une éventuelle couverture.

ANNEXE 1

Liste des membres du groupe de travail

ANNEXE 1

LISTE DES MEMBRES DU GROUPE DE TRAVAIL

« L'assurabilité des riques cyber »

PRÉSIDENT :

- **Pierre Minor,** Président du groupe de travail, Ancien Directeur Juridique du Crédit Agricole, Avocat associé, Coat Haut de Sigy de Roux Minor AARPI

MEMBRES :

- **Charlotte Ast,** Direction Générale du Trésor, Adjointe au Chef du bureau Finance durable, droit des sociétés, comptabilité et gouvernance des entreprises
- **Paul Berger de Gallardo,** Avocat, Cabinet Gide Loyrette Nouel
- **Marie Betolaud,** Responsable Juridique, France Assureurs (Fédération Française de l'Assurance)
- **Hélène Boissan,** Directrice Juridique, AIG Europe SA (France)
- **Mariette Bormann,** Directrice du Pôle juridique, fiscal, distribution et conformité de la Fédération Française de l'Assurance
- **Helen Browne,** Group General Counsel AXA Group
- **Stéphanie Cabossioras,** Directrice Adjointe des affaires juridiques, Autorité des Marchés Financiers
- **Patricia Choquet,** Conseiller expert contentieux régulation, Autorité des Marchés Financiers
- **Bruno Contamin,** Contrôleur des assurances, Autorité de Contrôle Prudentiel et de Résolution
- **Christophe Delcamp,** Directeur Adjoint des assurances de dommages et responsabilité, France Assureurs (Fédération Française de l'Assurance)
- **Patrick Degiovanni,** Directeur Général Adjoint, Pacifica
- **Pierre Dupont,** Responsable Juridique du Pôle Assurance IARD, Direction Juridique AXA France
- **Pauline Facon,** Adjointe au Chef du Pôle affaire internationales, coordination européenne et enjeux technologiques, Direction Générale du Trésor
- **Gérard Gardella,** Secrétaire Général du HCJP, Ancien Directeur Juridique groupe Société Générale
- **Richard Gueldre,** Avocat associé, Cabinet Gide Loyrette Nouel
- **Luc Grynbaum,** Professeur agrégé des Facultés de droit, Université de Paris, Chef du département Droit Économie Gestion de l'Université Sorbonne, Abu Dhabi

- **Elodie Lainé,** Juriste, Autorité de Contrôle Prudentiel et de Résolution
- **Mylene Larbi,** Adjointe au Chef de bureau des entreprises et intermédiaires d'assurance, Direction Générale du Trésor
- **Fouad Larhrib,** Adjoint au Chef de bureau des produits et marchés d'assurance, Direction Générale du Trésor
- **Stéphane Lucard,** Responsable Juridique et Conformité de Pacifica (Crédit Agricole Assurances)
- **Bernard Mettetal,** Avocat Of Counsel, HMN, Partners
- **Francesco Martucci,** Professeur agrégé des Facultés de droit, Université de Panthéon, Assas Paris II
- **Alice Navarro,** Magistrate, Conseillère Juridique du Directeur Général du Trésor
- **Marie Aude Noury,** Avocat au Barreau de Paris
- **Anne Marie Papeix,** Responsable RC médicale, RC entreprise et Environnement, France Assureurs (Fédération Française de l'Assurance)
- **Sophie Parisot,** Responsable Souscription Cyber & Responsabilité Professionnelle AIG Europe SA
- **Eléonora Sorribes,** Avocat associé, HMN, Partners
- **Jean Paul Thomas,** Responsable Département assurance transports, France Assureurs (Fédération Française de l'Assurance)
- **Francis Vicari,** Directeur Juridique Groupe par intérim, Crédit Agricole SA
- **Maxime Vroman,** Responsable Sinistres Risques Financiers AIG Europe SA (France)
- **Laure Zicry,** Head of Cyber Western Europe, Willis Towers Watson

ANNEXE 2

Liste des personnes auditionnées

ANNEXE 2
LISTE DES PERSONNES AUDITIONNÉES
« L'assurabilité des riques cyber »

- **Jamie Boucher,** Partner Skadden, Arps, Slate, Meagher & Flom
- **Didier Rebut,** Professeur, Université de Panthéon Assas (Paris II)
- **Grégoire Lundi,** ANSSI
- **Fabien Caparros,** Chef d'état-major de la sous-direction Stratégie ANSSI
- **Hugo Zylberberg,** ANSSI
- **Alexandre Nardone,** Directeur Général, Inquest

ANNEXE 3

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

ANNEXE 3

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016,

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Article 58 - Pouvoirs

(…)

2. Chaque autorité de contrôle dispose du pouvoir d'adopter toutes les **mesures correctrices** suivantes :

a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ;

b) rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement ;

c) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement ;

d) ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ;

e) ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel ;

f) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;

g) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19 ;

h) retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;

i) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas ;

j) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;

b) le fait que la violation a été commise délibérément ou par négligence ;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

g) les catégories de données à caractère personnel concernées par la violation ;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

3. Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43 ;

b) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43 ;

c) les obligations incombant à l'organisme chargé du suivi des Codes de conduite en vertu de l'article 41, paragraphe 4.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 ;

b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 ;

c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49 ;

d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX ;

e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

7. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58, paragraphe 2, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

8. L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

9. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le présent article peut être appliqué de telle sorte que l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le 25 mai 2018 et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.

Article 84

Sanctions

1. Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

2. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du paragraphe 1 au plus tard le 25 mai 2018 et, sans tarder, toute modification ultérieure les concernant.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(Sanctions « administratives »)

Article 20

I - Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées

sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi.

II - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible **de faire l'objet d'une mise en conformité**, prononcer à son égard une mise en demeure, dans le délai qu'il fixe :

1° de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;

2° de mettre les opérations de traitement en conformité avec les dispositions applicables ;

3° à l'exception des traitements qui intéressent la sûreté de l'État ou la défense, de communiquer à la personne concernée une violation de données à caractère personnel ;

4° de rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement de ces données.

Dans le cas prévu au 4° du présent II, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.

Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d'extrême urgence.

Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.

Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.

III - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, **saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes** :

1° un rappel à l'ordre ;

2° une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte ;

3° à l'exception des traitements qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'État, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même règlement ou de la présente loi ;

4° le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;

5° à l'exception des traitements qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'État, la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;

6° la suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;

7° à l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

Le projet de mesure est, le cas échéant, soumis aux autres autorités de contrôle concernées selon les modalités définies à l'article 60 du même règlement.

Article 21

I - Lorsque le non-respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er de la présente loi et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte, qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'État, adopter l'une des mesures suivantes :

1° l'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'État ;

2° la limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'État ;

3° la suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant ;

4° la suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ;

5° la suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 66 de la présente loi ;

6° l'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans le cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte ;

7° un rappel à l'ordre ;

8° l'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'État. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

II - En cas de circonstances exceptionnelles prévues au 1 de l'article 66 du règlement (UE) 2016/679 du 27 avril 2016, lorsque la formation restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres autorités de contrôle concernées, le comité européen de la protection des données mentionné à l'article 68 du même règlement et la Commission européenne.

Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement (UE) 2016/679 du 27 avril 2016.

III - Pour les traitements relevant du règlement (UE) 2016/679 du 27 avril 2016, lorsqu'une autorité de contrôle compétente en application du même règlement n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 dudit règlement.

IV. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction

compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.

Article 22

Les mesures prévues au III de l'article 20 et aux 1° à 7° du I de l'article 21 de la présente loi sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable de traitement ou à son sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris les agents des services de la commission.

La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne, aux frais des personnes sanctionnées.

Sans préjudice des obligations d'information qui incombent au responsable de traitement ou à son sous-traitant en application de l'article 34 du règlement (UE) 2016/679 du 27 avril 2016, la formation restreinte peut ordonner que ce responsable ou ce sous-traitant informe individuellement, à ses frais, chacune des personnes concernées de la violation relevée des dispositions de la présente loi ou du règlement précité ainsi que, le cas échéant, de la mesure prononcée.

Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce.

L'astreinte est liquidée par la formation restreinte, qui en fixe le montant définitif.

Les sanctions pécuniaires et les astreintes sont recouvrées comme les créances de l'État étrangères à l'impôt et au domaine.

Article 23

Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou celles de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la commission, qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 20 à 22, le retrait de l'agrément qui a été délivré à cet organisme.

NOTA : Conformément à l'article 29 de l'ordonnance n° 2018-1125 du 12 décembre 2018, ces dispositions entrent en vigueur en même temps que le décret modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction résultant de la présente ordonnance, et au plus tard le 1er juin 2019.

(Pour mémoire : sanctions pénales)

Article 40

Les infractions aux dispositions de la présente loi sont prévues par la section 5 du chapitre VI du titre II du livre II du Code pénal.

Article 41

Le procureur de la République avise le président de la Commission nationale de l'informatique et des libertés de toutes les poursuites relatives aux infractions prévues par la section 5 du chapitre VI du titre II du livre II du Code pénal et, le cas échéant, des suites qui leur sont données. Il l'informe de la date et de l'objet de l'audience de jugement par lettre recommandée adressée au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

ANNEXE 4

Situation dans les autres pays du monde

SITUATION DANS LES AUTRES PAYS DU MONDE

a) Canada

L'assurance rançon ainsi que le paiement des rançons sont licites. Toutefois, les autorités policières (dont la Gendarmerie Royale du Canada) conseillent de ne pas payer les rançons, sauf dans certaines circonstances, par exemple quand les entreprises n'ont pas de plan de sauvegarde de leurs données. La victime qui paie une rançon doit notifier ce paiement à la police.

b) Nouvelle Zélande

L'assurance rançon est permise ; selon la fédération des assureurs ICNZ, la couverture de rançon est une solution de « dernière chance » pour les assureurs qui encouragent plutôt la prévention.

Le CERT NZ, un organisme du Ministère du Commerce, de l'Innovation et de l'Emploi en Nouvelle-Zélande, recommande également de ne pas payer les rançons, étant donné que cela ne garantit pas le retour des données. Le gouvernement suit la politique de non-paiement des rançons. Il ne semble pas y avoir de débat sur la licéité des paiements de rançons actuellement.

c) Australie

Le paiement des rançons est possible mais l'*Australian Cyber Security Centre* (ACSC), un organisme du Gouvernement australien, recommande de ne pas payer les rançons.

Le 21 juin 2021 un parlementaire a proposé d'imposer des obligations de *reporting* en cas de ransomware aux organisations dont le CA excède $10 millions et qui envisagent de payer des rançons avec des sanctions d'un montant maximum de $222,000, en cas de non-respect de ces obligations.

d) Brésil

Le Gouvernement brésilien interdit la couverture ou l'indemnisation pour les demandes de rançon à la suite d'un kidnapping mais ne semble pas s'être prononcé sur l'assurabilité des rançons cyber.

e) Luxembourg

Il n'existe pas d'interdiction de l'assurance rançon et aucune recommandation n'a été émise à ce sujet par le régulateur luxembourgeois.

La problématique de paiement des rançons, qu'il s'agisse de celles versées par la victime en cas de kidnapping ou dans d'autres cas comme en matière de cyber criminalité n'est pas en débat au Luxembourg et les polices K&R existent depuis fort longtemps. Cette couverture est aujourd'hui offerte en cas de cyberattaque également. La garantie permettant le remboursement de la victime en

cas de cyberattaque n'est pas perçue comme encourageant les actes illégaux immoraux ou contraire à l'ordre public. Un débat existe cependant sur le point de savoir si le remboursement de la rançon par l'assureur doit être en soi traité comme nécessitant une déclaration de soupçon dans le cadre des mesures de lutte contre le terrorisme/lutte contre le blanchiment.

f) Japon

Il n'existe pas de restriction explicite concernant le remboursement des rançons à la suite d'une attaque cyber. Toutefois, ces paiements peuvent, au cas par cas, être considérés comme allant à l'encontre de l'ordre public. Toutes les polices cyber n'offrent pas la couverture du remboursement des rançons.

g) Royaume-Uni

L'assurance rançon est licite à l'exception des cas de financement du terrorisme.
Selon la position officielle du gouvernement il convient d'éviter au maximum de payer les demandes de rançons. Au Royaume-Uni, le *National Cyber Security Center* (un organisme gouvernemental) a mis à jour en mars 2021 son guide « *Mitigating Ransomware and Malware Attacks* » en décourageant indirectement le paiement des rançons et en encourageant la mise en place de stratégie « *defense-in-depth* ». Ainsi, le paiement des rançons demeure possible tant que la rançon ne finance pas le terrorisme.
L'association des assureurs britanniques ABI (*Association of British Insurers*) défend l'assurabilité du paiement de la rançon au sein des polices cyber mais les assureurs encouragent ou conditionnent la garantie à la mise en place de mesures de prévention pour éviter les attaques cyber et en limiter les effets.

h) Allemagne

La Circulaire Bafin 3/1998 « *Guidelines on the provision of ransom insurance* » adoptée en 1998 par l'autorité de contrôle allemande a posé les conditions de la validité des couvertures kidnapping et rançon ; a ainsi été imposée aux assureurs et assurés, l'obligation de confidentialité quant à l'existence de la police mais également en cas de sinistre, l'obligation pour les parties en cas de demande de rançon, d'informer les autorités et de collaborer avec les services de police.

S'agissant des rançons exigées à la suite d'attaques cyber, en 2017, la BaFin a spécifiquement autorisé la couverture du risque de ransomware au sein d'une police cyber dès lors que :

- l'assurance est proposée dans le cadre plus large d'une police d'assurance contre les risques cyber ; elle ne peut être proposée séparément ;

- le travail d'enquête de la police ne doit pas être entravé ;

- lorsqu'une attaque a lieu et que l'assureur couvre le paiement de la rançon, très peu de personnes sont autorisées à détenir des informations ;

Selon le GDV (association allemande des assureurs), si l'assurance cyber couvre les ransomwares (ce n'est pas toujours le cas), les assureurs ont le devoir de proposer à l'assuré un support technique en cas d'attaque par ransomware qui est à privilégier avant tout paiement de rançon qui ne peut intervenir qu'en dernier ressort.

Les mêmes principes s'appliquent en Autriche.

i) République Tchèque

Il n'existe pas d'interdiction légale de l'assurance rançon. Les conditions de garantie dépendent de la politique de souscription de chaque assureur. Selon les informations obtenues de l'association des assureurs tchèques, la plupart de ses membres ne proposent pas encore ce type de produit.

j) Pays-Bas

Le paiement des rançons et la couverture d'assurance ne sont pas interdits, mais découragés par le gouvernement néerlandais.

Par ailleurs, toutes les cyber-assurances ne couvrent pas le paiement de la rançon. Tous les assureurs qui proposent cette garantie, prévoient clairement que le paiement d'une rançon ne doit intervenir qu'en dernier recours et que la couverture n'est accordée que si l'assuré a pris les mesures préventives exigées, notamment en matière de cybersécurité. Des Députés et le Ministre de la Justice ont récemment soulevé la question de l'assurabilité des rançons. En 2020, le Ministre de la Justice, M. Grapperhaus a déclaré dans une lettre adressée au parlement : « *Payer les rançons encouragera les activités criminelles. De plus, la police s'attend à ce que le paiement de la rançon conduise à davantage d'attaques de rançongiciels ; je préfère que l'assureur ne paie pas pour la rançon qui se retrouve entre les mains de criminels, mais plutôt pour le préjudice subi par l'assuré du fait du non-paiement de cette rançon* ». Au cours des discussions, il a été par ailleurs souligné que les entreprises disposant d'une cyber-assurance sont généralement bien mieux préparées et protégées, ce qui minimise les effets possibles d'une attaque.

Très récemment la police néerlandaise a lancé une plateforme destinée à éviter le paiement des rançons suite à une cyberattaque ; les services de police estimant que ce paiement ne permet pas toujours à l'entreprise de récupérer ses données et de régler le problème.

k) Belgique

Il n'existe pas d'interdiction d'assurer le risque de ransomware, sous réserve du respect des mesures du régime des sanctions internationales et la lutte contre le terrorisme.

l) Grèce

Il n'existe pas d'interdiction d'assurer le risque de ransomware ; il s'agit d'un petit marché en cours de développement qui ne fait pas aujourd'hui l'objet de discussions au niveau politique.

m) Irlande

Il n'existe pas d'interdiction légale d'assurer le risque de ransomware, ni de « guidance » visant à imposer aux assureurs des conditions de couverture spécifiques pour ce risque ; le Gouvernement irlandais insiste plus sur le cyber résilience des acteurs et sur le rôle des assureurs dans le développement de bonnes pratiques pour lutter contre les cybers attaques et leurs effets.

n) Italie

Il n'existe pas d'interdiction d'assurer le risque de *ransomware*, sous réserve du respect des mesures du régime des sanctions internationales et la lutte contre le terrorisme ; le marché offre des couvertures cyber pour les frais de récupération de données, pour les pertes d'exploitations ainsi qu'en cas de versement d'une rançon qui ne peut être réalisé qu'avec l'accord de l'assureur et sous certaines conditions (information préalable des autorités de polices/obligation de confidentialité quant à l'existence de la police d'assurance...).

o) Pays nordiques

Il n'existe pas d'interdiction d'assurer le risque de ransomware. Le sujet fait aujourd'hui débat dans le monde académique essentiellement au regard de l'application des règles interdisant le financement du terrorisme/le blanchiment d'argent.

p) Portugal

Il n'existe pas d'interdiction d'assurer le risque de ransomware. Au Portugal le montant de la rançon ou les pertes financière suite à une cyber attaque sont en général couverts par le biais des contrats "Fraude".

q) Espagne

Il n'existe pas d'interdiction d'assurer le risque de ransomware. À ce jour le débat n'est pas ouvert au niveau politique. La plupart des assureurs offrent des polices cyber incluant le remboursement de la rançon sous réserve de l'application des sanctions internationales mentionnées dans le rapport de l'OCDE de 2020 mettant en exergue le risque de financement du terrorisme.

ANNEXE 5

Initiatives américaines ransomware

INITIATIVES AMÉRICAINES RANSOMWARE

Le 1er octobre 2021 : le *Financial Crimes Enforcement Network* (“*FinCEN*”) - émanation du Département du Trésor américain, avec son “*Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*” (the “*FINCEN Advisory*”) a alerté sur les risques et sur les obligations de reporting à la charge des entités financières en ce qui concerne le paiement des *ransomware*. Les institutions devront donc également tenir compte de cet avis et des obligations réglementaires qu’il contient en cas de paiement et/ou de remboursement de rançons.

Le 4 février 2021, le FBI[76] a mis en garde contre le paiement d’une rançon qui ne garantit pas d’une part, la récupération des données et d’autre part peut encourager les cybercriminels.

Également le 4 février 2021, le département des services financiers de l’État de New-York[77] a recommandé de ne pas verser de rançon et note que « l*es paiements de rançon alimentent le cercle vicieux des logiciels de rançon, car les cybercriminels les utilisent pour financer des attaques de plus en plus fréquentes et sophistiquées* ».

03 avril 2021 : les autorités américaines ont mis en place une Task-Force au sein du Ministère de la Justice, censée développer une stratégie pour mieux lutter contre les pirates se servant des ransomwares et exigeant que toutes les informations liées aux enquêtes sur les ransomwares soient désormais centralisées au sein de cette « *Task force* ».

29 avril 2021 : publication par l’IST (*Institute for Security and Technology*) d’un rapport de quarante-huit recommandations à l’attention du gouvernement américain dans le but de combattre les acteurs cybercriminels et le ransomware. L’interdiction du paiement des rançons n’a pas été recommandée au regard des nombreux défis liés à une telle interdiction.

Pour limiter les conséquences des ransomwares, ce groupe de travail propose quarante-huit recommandations organisées en quatre objectifs. Parmi ces quarante-huit recommandations, ils identifient cinq actions plus fondamentales et urgentes :

- prévenir les attaques grâce à la mise en place d’une stratégie nationale et internationale répressive contre les acteurs du cybercrime et les nations qui les abritent ;

---

[76] *Le document est accessible à l’adresse suivante : https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet.*

[77] *La recommandation est accessible à l’adresse suivante : https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02.*

- mener une campagne anti-ransomware soutenue et agressive à l'échelle de l'ensemble des institutions publiques américaines sous l'égide de la Maison Blanche qui implique la mise en place :

  - une *Task Force* inter-agences dirigée par le *National Security Council* en coordination avec l'autorité US de cybersécurité,

  - une *Task Force* commune sur les ransomwares au sein du Gouvernement américain,

  - un *Hub* collaboratif sur les ransomwares regroupant et dirigé par le secteur privé ;

- financer par le gouvernement des fonds destinés à répondre aux attaques par ransomware ; obliger les organisations à déclarer les paiements de rançon et exiger de ces organisations qu'elles envisagent des alternatives avant tout paiement de rançon (dernier ressort) ;

- mener un effort coordonné au niveau international pour élaborer un cadre clair, accessible et commun pour aider les organisations à répondre aux attaques par ransomwares. Pour certains secteurs critiques et manquant de ressources, des mesures incitatives d'ordre financier pourraient être proposées afin que ces derniers puissent également respecter ce nouveau cadre ;

- réguler le marché des crypto-actifs qui favorise la cybercriminalité et plus particulièrement les ransomwares ; les gouvernements devraient exiger que les échanges de crypto-monnaies, les crypto kiosks et les *trading desks over-the-counter* (OTC) se conforment aux lois existantes, y compris les lois sur la connaissance du client (KYC), la lutte contre le blanchiment d'argent (AML) et la lutte contre le financement du terrorisme (CFT).

12 mai 2021 : « *Executive Order de la Maison Blanche* » dont l'objectif est d'améliorer les capacités de cyberdéfense des États-Unis, afin de lutter efficacement contre les cyber campagnes malveillantes et qui oblige les agences fédérales américaines à adopter un certain nombre de contrôles de sécurité et de bonnes pratiques, notamment la mise en œuvre de « *politiques de confiance zéro* » et l'adoption du cadre du *National Institute of Standards and Technology* (NIST).

03 Juin 2021 : le Département de la Justice américain a accordé aux investigations sur les attaques par ransomwares une priorité similaire à celle du terrorisme ; selon une note interne adressée aux Bureaux des procureurs américains dans tout le pays, les informations relatives aux enquêtes sur les ransomwares menées sur le terrain doivent être coordonnées de manière centralisée au sein de la *Task Force* créée en avril 2021 et mentionnée ci-dessus.

Les ministères américains de la Justice et de Sécurité intérieure ont récemment mis en place un **site internet pour les victimes des attaques de ransomware** afin de rassembler toutes les informations, en cas d'attaque mais aussi en matière de prévention, sur une même plateforme.

22 juin 2021 : le Secrétaire d'État américain Mayorkas a publié un communiqué dans lequel il se félicite de la création d'un **groupe de travail EU-US sur la lutte contre le ransomware**. Le groupe de travail aidera à renforcer la coopération transatlantique pour faire face plus efficacement aux ransomwares, en particulier avec des mesures de prévention et de respect des lois. Le communiqué conjoint UE-US précise que les mesures de prévention seront axées sur la protection des réseaux ainsi que sur le risque de payer les criminels responsables. Aucune mention relative à l'assurance n'est à relever. À ce jour il semble que le groupe de travail n'ait pas encore été lancé.

1er juillet 2021 : la fédération américaine des assureurs (*American Property Casualty Insurance Association* - APCIA) a publié des principes directeurs sur l'extorsion cyber/ransomware.
L'APCIA estime que, sous réserve des sanctions applicables et autres lois, les assureurs doivent être autorisés à fournir une couverture prévoyant le remboursement des rançons en cas de cyber extorsion. La fédération précise que ce principe est conforme à l'approche adoptée de longue date sur la question parallèle des couvertures "*kidpnap & ransom*" qui sont autorisées par les régulateurs tant que ces paiements ne violent pas les lois sur les sanctions. La fédération alerte également sur les conséquences d'une interdiction comme la moindre résilience économique des entreprises victimes de ransomware.

Août 2021 : création du *Joint Cyber Defense Collaborative* (JCDC) par la *Cybersecurity and Infrastructure Security Agency* (CISA) chargé de l'élaboration des plans de cyberdéfense de la nation.

12 août 2021 : l'association américaine des superviseurs d'assurance *National Association of Insurance Commissioners* (NAIC) a décidé de créer, d'ici la fin de l'année, un comité permanent sur la cybersécurité afin de surveiller les développements dans ce domaine et notamment sur les ransomwares (communiqué).

ANNEXE 6

Ransomware – U.S. Economic Sanctions and Other Regulatory Considerations

RANSOMWARE - U.S. ECONOMIC SANCTIONS AND OTHER REGULATORY CONSIDERATIONS

By Jamie Boucher, Jim Perry, and Vartan Shadarevian, Skadden, Arps, Slate, Meagher & Flom LLP.
This article has been prepared by Skadden, Arps, Slate, Meagher & Flom LLP for educational and informational purposes only and is not intended and should not be construed as legal advice.

Introduction

In recent years, the world has seen an alarming increase in ransomware attacks. Globally, attempted ransomware attacks reported in the first half of 2021 increased by 151% over the same period in 2020, including the high-profile attack in May 2021 on the U.S. Colonial Pipeline.[78] With the continued COVID-19 pandemic, remote work, and an increased reliance on corporate IT systems, this trend is likely to continue. Ransomware incidents can severely impact business processes and leave organizations without the data or systems they need to run their operations. Faced with a ransomware attack, a company may be tempted to make a ransomware payment in hopes of recovering access to its data or systems. However, making ransomware payments can carry legal risk. While ransomware payments are not generally prohibited under U.S. law, ransomware payments may violate economic sanctions enforced by the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) or may implicate other U.S. laws and regulations, including those related to anti-money laundering (AML) reporting. Companies, and their banks and insurers, should familiarize themselves with these laws and regulations well before an attack occurs and consider them carefully when deciding whether to make a ransomware payment.
This article provides a brief overview of the ransomware threat, discusses how a ransomware payment may violate OFAC sanctions or implicate other U.S. regulations, including AML reporting obligations, and describes steps companies can take to mitigate these risks.

How ransomware works

Ransomware is a form of malware designed to encrypt files on a device, rendering those files and the systems that rely on them unusable. In a ransomware attack, a computer may become locked, or the data on it might be stolen, deleted or encrypted. Malicious actors demand a ransom in exchange for decryption or access to these systems or files. More recently, attackers have also stolen data and threatened to release publicly sensitive information if not paid. Ransomware has become more sophisticated in recent years, with attackers working together to launch more complex attacks and using "fileless" ransomware, through which malicious code is written directly to a computer's memory.[79]

[78] *SONICWALL, MID-YEAR UPDATE: 2021 SONICWALL CYBER THREAT REPORT (July 29, 2021).*

[79] *See CrowdStrike, How "Fileless" Ransomware Works, https://www.crowdstrike.com/resources/infographics/how-fileless-ransomware-works/, (last visited September 17, 2021).*

Victims can be of any size, but attackers are increasingly targeting larger enterprises and demanding higher ransoms as a result. The attack on the U.S. Colonial Pipeline is a notable recent example of such a demand. The Colonial Pipeline supplies roughly half of the fuel consumed by the U.S. East Coast. Company operations were shut down temporarily in May 2021 after the company's computer system was broken into by a group known as "DarkSide." In response, Colonial Pipeline paid a roughly $5 million (about 75 bitcoin) ransom to bring their computers back online.[80] Ultimately, the U.S. Department of Justice recovered most of the funds. [81]

OFAC sanctions and their relevance to ransomware

While a company hit with a ransomware attack may be tempted to pay its attackers, it should be wary that ransomware payments may violate OFAC sanctions. OFAC sanctions apply to U.S. Persons[82] and to activities occurring within U.S. territory.[83] Non-U.S. Persons may be subject to OFAC sanctions even if they are not physically present in the United States if, for instance, they conduct business in or process transactions through the United States, or they cause a U.S. Person to violate OFAC sanctions. For this reason, many non-U.S. companies comply with OFAC sanctions on a voluntary basis even if their conduct would not otherwise have a U.S. nexus.

OFAC sanctions generally prohibit transactions that involve a comprehensively sanctioned jurisdiction (at present these are the Crimea region of Ukraine, Cuba, Iran, North Korea, and Syria). Almost all commercial activity is prohibited with individuals or companies within, or the government of, a comprehensively sanctioned jurisdiction. OFAC sanctions also prohibit U.S. Persons from dealing with any person on OFAC's List of Specially Designated Nationals and Blocked Persons (the SDN List)[84], or any person owned, directly or indirectly, in aggregate, 50% or more by one or more persons on the SDN List.[85] The SDN List includes, for instance, designated terrorists, narcotics traffickers, and weapons of mass destruction proliferators. The SDN List also includes persons designated by OFAC for their involvement in cyber-related activities. For instance, OFAC recently designated SUEX OTC, S.R.O, a cryptocurrency exchange, for its role in facilitating

[80] *Michael Schwirtz & Nicole Perlroth, Darkside, Blamed for Gas Pipeline Attack, Says It Is Shutting Down, N.Y. TIMES, (May 14, 2021).*

[81] *Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.*

[82] *A U.S. Person is any U.S. citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States. See, e.g., 31 C.F.R. § 560.314.*

[83] *See, e.g., 31 C.F.R. § 560.204.*

[84] *See OFAC, Specially Designated Nationals and Blocked Persons, https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (last visited September 20, 2021).*

[85] *OFAC, Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked, U.S. DEP'T OF THE TREASURY (August 13, 2014).*

financial transactions for ransomware actors.[86] This was the first such designation by OFAC of cryptocurrency exchange under its cyber-related authorities. The assets of any person on the SDN List that come into the control or possession of U.S. Persons must be blocked (*i.e.*, frozen) and cannot be transferred without authorization from OFAC.[87]

OFAC sanctions also prohibit the "facilitation" by any person, wherever located, of any payment prohibited by OFAC sanctions.[88] Facilitation could involve the processing by a bank or indemnification by an insurer of a ransomware payment prohibited by OFAC sanctions. In such a case, a U.S. nexus could arise because the victim is a U.S. Person or any part of the payment occurred in the United States or involved a U.S. Person. Non-U.S. companies, including financial institutions, are prohibited from facilitating a ransomware payment by a U.S. Person to a sanctioned person, such as a person on the SDN List. OFAC may determine that a non-U.S. company facilitated a prohibited ransomware payment even by a non-U.S. Person, if, for example, a leg of the payment was in U.S. dollars or a U.S. Person was involved in negotiating the payment.[89]

Any person in the chain of a ransomware payment could be held both civilly or criminally liable for facilitating a payment involving a sanctioned person. OFAC may impose civil penalties for violations based on "strict liability," which means that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a prohibited transaction. Therefore, even inadvertent violations of OFAC sanctions can lead to civil penalties.

The penalties for violating sanctions can be severe. Currently, penalties under the International Emergency Economics Powers Act (IEEPA)[90], the main statutory authority for OFAC sanctions, can be as much as $311,562 per violation or twice the amount of the transaction (or transactions) that is the basis of the violation, whichever is greater.[91] Criminal violations require knowledge, or reason

---

[86] *Press Release, U.S. Dep't of the Treasury, Treasury Takes Robust Actions to Counter Ransomware (September 21, 2021), https://home.treasury.gov/news/press-releases/jy0364.*

[87] *Title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC.*

[88] *See, e.g., 31 C.F.R. § 560.208.*

[89] *U.S. sanctions do not attach to the U.S. dollar per se. However, any involvement of a U.S. financial institution in a transaction confers OFAC jurisdiction over the transaction. U.S. dollar transactions often involve a U.S. financial institution in the clearing or settlement of the transaction.*

[90] *The authority of the U.S. President to impose and enforce sanctions is derived from two main statutory sources, the IEEPA (50 U.S.C. § 1701 et seq.) and the Trading with the Enemy Act of 1917, as amended, as well as various other statutes, including, but not limited to, the National Emergencies Act (50 U.S.C. § 1601 et seq.) and the United Nations Participation Act (22 U.S.C. § 287c),and certain statutes which direct the President to impose sanctions on specific countries or entities in specific circumstances in furtherance of U.S. foreign policy objectives.*

[91] *50 U.S.C. § 1705(b). The maximum under civil penalty under IEEPA is adjusted each year pursuant to the Federal Penalties Inflation Adjustment Act. See, e.g., Inflation Adjustment of Civil Monetary Penalties, 86 Fed. Reg. 14534 (March 17, 2021).*

to know, that the ransomware payment is illegal, but can be harsher, with monetary penalties of up to $1,000,000 per violation and the potential for up to twenty years' imprisonment.[92]

It should be noted that OFAC sanctions are highly complex, encompass over thirty different programs, and change frequently.[93] Any person contemplating a ransomware payment should consult counsel in determining whether the payment may be prohibited under OFAC sanctions.

The OFAC ransomware advisory

In response to ever-increasing ransomware attacks against or involving U.S. Persons, OFAC, on October 1, 2020, released its "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments", and updated this guidance on September 21, 2021 (the OFAC Advisory).[94] While the OFAC Advisory did not change U.S. law as it pertains to ransomware payments, it served to alert ransomware victims and their advisors, banks, and insurers of the potential OFAC sanctions risks regarding facilitating ransomware payments.

The OFAC Advisory strongly discourages ransomware payments, highlights the risks to those facilitating such payments, and encourages actors to strengthen defensive and resilience measures to prevent and protect against ransomware attacks.[95] OFAC encourages financial institutions and other companies, including those involved in facilitating potential ransomware payments, to have a risk-based compliance program that considers the risks of making ransomware payments to sanctioned persons.[96] Although a U.S. Person may seek a license from OFAC to engage in an otherwise prohibited ransomware payment, the advisory notes that OFAC will treat such applications with a presumption of denial.[97]

To the extent that a person makes or facilitates a ransomware payment that is later determined to have a sanctions nexus, in determining what enforcement response is appropriate, OFAC will consider a number of factors. These factors include whether a company had a risk-based compliance

---

[92] *50 U.S.C. § 1705(b). For more information regarding OFAC's enforcement of U.S. economic sanctions, see OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appx. A.*

[93] *A complete list of OFAC sanctions programs can be found at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.*

[94] *OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, U.S. DEP'T OF THE TREASURY (September 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [hereinafter OFAC Advisory].*

[95] *See OFAC Advisory, supra note 17, at 1.*

[96] *OFAC Advisory, supra note 17, at 4.*

[97] *Id., at 5.*

program, took steps prior to the attack to improve cyber-security practices to reduce the risk of ransomware extortion, made a self-initiated, timely, and complete report of the ransomware attack to law enforcement or other appropriate U.S. government agencies, and cooperated fully and timely with law enforcement during and after the attack.[98] Although not specifically stated in the OFAC Advisory, victims and any party facilitating a ransomware payment should conduct rigorous diligence to determine, to the extent possible, that the attacker is not a sanctioned person (this includes parties acting on behalf of a comprehensively sanctioned jurisdiction). While taking these mitigating steps cannot guarantee that OFAC will not bring an enforcement action, the OFAC Advisory indicates that taking these steps, particularly the complete and timely self-reporting of an attack, makes it more likely that OFAC will resolve an apparent violation involving a ransomware attack with a non-public response, such as a no action letter or a cautionary letter, rather than pursuing a civil monetary penalty.[99]

The OFAC Advisory notes that OFAC will continue to impose sanctions on actors that materially assist, sponsor, or provide financial, material, or technological support to malicious cyber activities, including ransomware attacks.[100] In a further sign of OFAC's focus on ransomware, OFAC issued, on October 15, 2021, a brochure to promote sanctions compliance in the virtual currency industry, highlighting the use of virtual currencies in making ransomware payments.[101] In light of these developments, companies should stay abreast of changes in OFAC regulations and any new designations.

Recent AML-related guidance

U.S. regulators other than OFAC have also issued guidance in recent years regarding the risk of ransomware, including by providing guidance to regulated companies on how to mitigate the risk of a ransomware attack. Notably, in October 2020, the U.S. Department of the Treasury's Financial Crime Enforcement Network (FinCEN) released its "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," and updated this guidance on November 8, 2021 (the FinCEN Advisory).[102] FinCEN is generally responsible for administering the various U.S. AML

[98] *Id., at 4-5. OFAC will consider a self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as the U.S. Cybersecurity & Infrastructure Security Agency or the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure to OFAC. OFAC Advisory, supra note 17, at 5.*

[99] *Id., at 5.*

[100] *Id., at 3.*

[101] *OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry, U.S. DEP'T OF THE TREASURY (October 15, 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.*

[102] *FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, U.S. DEP'T OF THE TREASURY (November 8, 2021), https://www.fincen.gov/sites/default/files/2021-11/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf [hereinafter FinCEN Advisory].*

laws and for enforcing the obligations banks and other financial institutions have under these laws. These laws and regulations create civil and criminal penalties for money laundering, and impose significant compliance requirements to detect and report money laundering.

The FinCEN Advisory warns of the risks to and potential reporting obligations of financial institutions related to ransomware payments. FinCEN notes that processing a ransomware payment is a multi-step process that involves at least one depository institution and one or more money services business (MSBs). MSBs include businesses that transmit value from one place to another, including transmitting virtual currency such as bitcoin.[103] FinCEN noted that, depending on their activities, entities like digital forensics and incident response companies, who may facilitate a ransomware payment, may be an MSB subject to AML laws.[104]

The FinCEN Advisory reminds U.S. financial institutions, including banks and MSBs, of their obligation to file Suspicious Activity Reports (SARs), including SARs regarding ransomware payments. A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to $5,000 (or, with one exception, $2,000 for MSBs) or more in funds or other assets and involves illegal activity.[105]

Financial institutions should determine if filing a SAR is required or appropriate when dealing with a ransomware incident, whether by processing a ransomware payment on behalf of a victim or third party, or if the financial institution is itself a victim of a ransomware attack. To assist financial institutions in this regard, FinCEN identified certain red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.[106]

To help companies stay abreast of the ransomware threat, FinCEN released a report in October 2021 containing analysis of ransomware trends in Bank Secrecy Act reporting filed between January 2021 and June 2021. The report found that the average amount of reported ransomware transactions per month in first six months of 2021 was approximately $100 million, identified sixty eight different variants of ransomware in the reported data, and described typical ransomware money laundering typologies.[107]

---

[103] *For the complete regulatory definition of MSB, see 31 C.F.R. 1010.100(ff).*

[104] *FinCEN Advisory, supra note 25, at 3-4.*

[105] *Id., at 8-9.*

[106] *Id., at 7.*

[107] *FinCEN, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, U.S. DEP'T OF THE TREASURY (Oct. 15, 2021).*

Other recent U.S. government guidance

In addition to OFAC and FinCEN, in recent years, numerous U.S. government agencies have provided guidance related to the ransomware threat, underscoring a U.S. "whole-of-government" approach to the problem. The White House[108], U.S. Cybersecurity & Infrastructure Security Agency (CISA)[109], Securities and Exchange Commission (SEC)[110], Federal Bureau of Investigation (FBI)[111], Federal Financial Institutions Examination Council[112], and the Conference of State Bank Supervisors[113], among others, have published guidance to companies and financial institutions on how to prepare for and prevent potential ransomware attacks.

As with the OFAC and FinCEN advisories, these documents generally do not create new regulatory obligations but provide guidance for companies and financial institutions on how to protect against ransomware attacks. Even in the absence of specific legal obligations related to ransomware, the failure by U.S. financial institutions to take reasonable precautions to protect against ransomware and other malware attacks could expose them to regulatory actions, including for "safety and soundness" violations. The SEC has also noted that victims of ransomware attacks may be subject to economic losses that may trigger public disclosure obligations. Moreover, companies should keep in mind that malware attacks, including ransomware events, may create risks for insider trading.[114]

Consideration for organizations facing possible ransomware threats

The OFAC and FinCEN advisories make clear that ransomware payments can involve legal risks to victims and their banks and insurers. These risks could increase in coming years given the focus

[108] *See Memorandum from Anne Neuberger, Deputy Assistant to the President and Deputy Nat'l Sec. Advisor for Cyber and Emerging Techn., to Corporate Executives and Business Leaders (June 2, 2021), https://s3.documentcloud.org/documents/20796933/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware17.pdf.*

[109] *See, e.g., CISA & Multi-State Information Sharing & Analysis Center, Ransomware Guide (September 30, 2020) (providing a resource for organizations to prevent, respond, and resolve cyber incidents). In January 2021, CISA unveiled the "Reduce the Risk of Ransomware Campaign" to raise awareness and instigate actions to combat this ongoing and evolving ransomware threat. See CISA, CISA Launches Campaign to Reduce the Risk of Ransomware (February 16, 2021).*

[110] *SEC, "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," February 26, 2018 (discussing the potential economic impacts to public companies, including from ransomware attacks, that may trigger disclosure obligations); SEC, "Cybersecurity: Ransomware Alert," (July 10, 2020) (warning of the increasing sophistication of ransomware attacks and advising financial services participants to monitor U.S. government ransomware alerts).*

[111] *See, e.g., FBI Internet Crime Compliance Center (IC3) & National Cyber Investigative Joint Task Force, Ransomware, What It Is & What To Do About It (February 4, 2021).*

[112] *Federal Financial Institutions Examination Council, Joint Statement, Cyber Attacks Involving Extortion (March 3, 2015).*

[113] *In October 2020, the CSBS, the Bankers Electronic Crimes Task Force and the U.S. Secret Service, issued a ransomware self-assessment tool for banks. See Conference of State Bank Supervisors, State Regulators Issue Ransomware Mitigation Tool (October 13, 2020).*

[114] *SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (February 26, 2018).*

by the U.S. government on the ransomware problem. To the extent that companies such as bank insurers are viewed as encouraging bad actors by backstopping ransomware payments, regulators could increase the legal requirements around ransomware policies. While it remains unlikely, regulators may move to prohibit ransomware payments altogether.

In the first instance, organizations should take steps to protect their information by putting in place adequate safeguards to reduce the risk of an attack. Companies should maintain offline, encrypted backups of their data and should regularly test those backups. Backup procedures should be conducted on a regular basis to ensure backups are current. Organizations should consider using third parties to test the security of their systems.

Organizations should create, maintain, and follow a cyber incident response plan and associated communications plan that includes response and notification procedures in the event of a ransomware incident. Companies should ensure that their policies are clear as to whether, and under what circumstances, they will pay, process, facilitate, or insure a ransomware payment. Insurers should ensure that their policies are clear as to whether, and under what circumstances, ransomware events will be covered, and that insured entities have adequate safeguards to reduce the risk of an attack. Banks should evaluate the risks of processing payments related to ransomware and ensure they have procedures in place to detect and report ransomware payments.

The decision to make a ransomware payment should be made carefully, with acknowledgement and acceptance of risks and in concert with various stakeholders. The FBI, OFAC, and other U.S. agencies have pointed out that paying the ransom demanded by the perpetrator of a ransomware attack does not guarantee that a victim's files will be recovered.[115] Payment could also encourage further attacks. In deciding as to whether a payment should be made, individuals and companies should consider various factors. These include whether the payment is legal under relevant laws and regulations, the availability of back-up data, the timeline for restoration of affected operations, and independent validation as to whether the attacker's decryption keys will work. Companies should consider the relative costs of paying a ransom versus restoring data and any reputational considerations that making the payment might pose. In weighing its options, a company should consider the advice of legal counsel, law enforcement, cyber insurance carriers, and security experts.

To the extent that a ransomware payment is made, all parties should take steps to ensure that the recipient is not a sanctioned person and that the victim has communicated and cooperated with law enforcement. Where necessary, a SAR should be filed. Finally, companies should stay abreast of regulatory developments in the U.S. and elsewhere, particularly if high-profile ransomware attacks like that against the Colonial Pipeline continue.

[115] *See, e.g., OFAC Advisory, supra note 17, at 3.*

ANNEXE 7

Analyse de la problématique européenne

ANALYSE DE LA PROBLÉMATIQUE EUROPÉENNE

Rappel sur le passeport européen

Dans le cadre du marché unique européen, et en application du système de la licence unique, un assureur bénéficiant d'un agrément octroyé dans son pays d'origine peut exercer son activité sur l'ensemble des territoires des États membres de l'Espace Économique Européen (ci-après dénommé « EEE ») *via* la Libre Prestation de Service (LPS) ou le Libre Établissement (LE).

Ces règles, issues de différentes directives européennes, ont été transposées en droit français au sein du Titre VI du Livre III du Code des assurances.

Le principe du passeport européen est donc effectif s'agissant du marché de l'assurance, les entreprises exerçant dans ce cadre restant soumises au contrôle de leurs autorités d'origine selon le principe dit du « *Home Country Control* ».

Si l'entreprise d'assurance est par principe soumise à la loi de son pays d'origine (État membre-EM où il a été agréé), il n'en va pas de même pour la loi applicable au contrat d'assurance qu'il entend proposer.

I - Les règles de conflits de lois applicables au contrat d'assurance et le risque d'entrave au passeport européen

En application des règles de conflit de lois prévues par la Directive Solvabilité II et le Règlement Rome I[116], transposées en France au niveau des art. L181-1 à L183-2 et L310-4 CA, la plupart des contrats d'assurance destinés à couvrir les risques des entreprises dont l'établissement est situé en France, sont régis par la loi française à l'exclusion de toute autre, quand bien même ces risques seraient couverts par une entreprise étrangère agissant en France par voie de LPS ou de LE.

Dès lors, un assureur étranger agissant en France *via* le passeport européen qui souhaiterait couvrir le risque de ransomware d'une entreprise située en France, serait confronté à l'interdiction française et ne pourrait donc couvrir ce risque.

L'art. L181-1 prévoit toutefois des cas où ce n'est pas la loi française qui s'applique au contrat d'assurance mais celle d'un autre EM[117].

---

[116] *Voir https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32008R0593&from=FR*

[117] *Par exemple pour les grands risques, les parties ont le libre choix de la loi applicable...L181-1-5° ; à noter que la transposition française de Rome I a favorisé l'application de la loi française puisqu'elle n'a pas repris les dispositions de l'art. 7.2 de Rome I qui précise que : « À défaut de choix par les parties de la loi applicable, le contrat d'assurance est régi par la loi du pays où l'assureur a sa résidence habituelle. »*

Mais l'art. L181-3 CA précise que quelle que soit la loi applicable au contrat d'assurance, ce choix ne peut « *faire obstacle aux dispositions d'ordre public de la loi française* ».

L'ordre public est une composante de l'intérêt général ; il s'agit de « *l'ensemble des exigences fondamentales considérées comme essentielles au fonctionnement des services publics et au maintien de la sécurité ou de la moralité* ».[118]

Par ailleurs, les règles d'intérêt général françaises viennent également tempérer l'application d'une autre loi que la loi française.

L'article 180 de la directive dite Solvabilité II énonce en effet que :

« *Ni l'État membre où le risque est situé ni l'État membre de l'engagement ne peuvent empêcher le preneur d'assurance de conclure un contrat avec une entreprise d'assurance agréée dans les conditions énoncées à l'article 14 [la licence unique], pour autant que la conclusion de ce contrat ne soit pas en opposition avec les dispositions juridiques protégeant l'intérêt général dans l'État membre où le risque est situé ou dans l'État membre de l'engagement.* »

En application de l'art. L362-4 CA, un décret en Conseil d'État aurait dû préciser les obligations auxquelles sont astreintes pour des raisons d'intérêt général les entreprises étrangères agissant en France par voie de LPS ou de LE ; à notre connaissance ce décret n'est jamais paru.

Pour pouvoir être imposée à un assureur étranger exerçant en France son activité par voie de LPS ou de LE (quelle que soit la loi applicable au contrat), l'interdiction de l'assurabilité des rançons doit pouvoir être qualifiée de mesure d'intérêt général ou d'ordre public telles que définies par la jurisprudence de la Cour de Justice de l'Union Européenne (ci-après dénommée « CJUE ») et par la Commission européenne (CE).

Si tel n'était pas le cas cette interdiction pourrait être qualifiée d'entrave à l'exercice de la LPS ou de la LE en France et sanctionnée par les institutions européennes compétentes.[119]

Dans une Communication Interprétative de la CE, « *Liberté de prestation de services et intérêt général dans le secteur des assurances (2000/C 43/03)* », celle-ci a souligné qu'une disposition nationale devait nécessairement satisfaire à certaines conditions cumulatives qui permettent de

[118] *Voir définition du lexique juridique G. Cornu.*

[119] *L'hypothèse est bien connue et renvoie notamment à l'une des jurisprudences de principe Alpine Investments à propose de l'interdiction de proposer des services financiers par téléphone. CJCE 10 mai 1995 Alpine Investments BV, C-384/93, ECLI :EU :C :1995 :126.*

justifier l'entrave à l'exercice de la LPS. La règle doit ainsi :

- relever d'un domaine non harmonisé,

- ne pas faire double emploi avec la règle du pays d'origine,[120]

- poursuivre un objectif d'intérêt général,[121]

- être non discriminatoire : elle ne doit pas être imposée par l'État membre à des entreprises agrées dans un autre État sans qu'elle ne l'applique à ses propres entreprises d'assurances,

- être objectivement nécessaire : à ce sujet, la CE souligne que cette condition permet notamment de vérifier si l'objectif poursuivi ne relève pas de la protection du marché national,

- être proportionnée à l'objectif poursuivi : il s'agit ici de démontrer que l'interdiction d'assurer le risque de ransomware a pour objectif de mettre fin aux cyber attaques et au financement du crime organisé.

Du côté de la CJUE, il est de jurisprudence constante qu'une restriction peut être admise si elle est justifiée par une raison impérieuse d'intérêt général et qu'elle respecte le principe de proportionnalité, en ce sens qu'elle doit être propre à garantir la réalisation de l'objectif qu'elle poursuit et ne pas aller au-delà de ce qui est nécessaire pour l'atteindre.

Toute la question sera donc d'envisager l'interdiction d'assurer le risque de ransomware à l'aune de l'objectif poursuivi : la lutte contre le financement du crime organisé. Il pourrait être jugé qu'interdire l'assurabilité des rançons est disproportionné par rapport à l'objectif poursuivi car dans les faits cette interdiction ne mettra pas fin aux attaques par ransomware et que cet objectif aurait pu être atteint différemment.

L'appréciation de la proportionnalité des règles envisagées dépendrait naturellement de leur contenu, s'agissant notamment des conditions d'assurabilité du ransomware, avec la nécessaire comparaison avec d'autres mécanismes qui pourraient être utilisés afin de poursuivre les mêmes objectifs de sauvegarde de l'ordre public et de lutte contre le financement du terrorisme. Il est vrai que la Cour de justice apprécie avec minutie les régimes nationaux d'interdiction auxquels peuvent être préférés des régimes d'autorisation préalable, voire déclaratoires. À cet égard, la circonstance que d'autres États membres n'interdisent pas la proposition d'un tel service n'est pas en soi un

[120] *A priori aucun État membre n'a encore rendu illégale l'assurabilité du ransomware.*

[121] *Parmi les motifs d'intérêt général pouvant constituer comme une raison impérieuse, figurent l'ordre public et la sécurité publique ; il revient à l'État d'identifier de la façon la plus détaillée la raison d'intérêt général en cause. Par exemple, la Cour de justice a admis comme motif d'intérêt général « l'évitement du risque d'impunité des personnes ayant commis une infraction qui s'inscrit dans le cadre de la prévention de la criminalité et de la lutte contre ce phénomène » CJUE, Gde ch.,6 septembre 2016, Petruhhin, C-182/15, ECLI :EU:C:2016:630 ; CJUE, Gde ch., 10 avril 2018, Romano Pisciotti, C-191/16, ECLI:EU:C:2018:222. Ces arrêts n'ont pas été rendus concernant les services mais la solution vaut mutatis mutandis.*

élément dirimant à ce que la France prohibe une telle offre. En effet, la jurisprudence laisse une marge d'appréciation aux États membres pour protéger l'ordre public et la sécurité publique. Toutefois, la Cour de justice apprécie, au titre de la proportionnalité, les sanctions éventuellement prévues. Si, là encore, la marge d'appréciation joue, elle est sensible à la nature de la sanction, privilégiant parfois celle qui s'avère administrative, à celle qui est pénale, sans toutefois que le caractère pénal ne soit nécessairement vecteur de disproportion. Ainsi, l'imposition de sanctions, y compris de nature pénale, peut être considérée comme nécessaire afin de garantir le respect effectif d'une réglementation nationale, à condition toutefois que la nature et le montant de la sanction imposée soient dans chaque cas d'espèce proportionnés à la gravité de l'infraction qu'elle vise à sanctionner[122].

II - L'exercice par l'UE de sa compétence vis-à-vis d'un texte européen visant à interdire l'assurabilité des rançons en cas de cyber attaque

L'existence ne serait-ce que potentielle d'une restriction à la libre circulation des services, article 56 TFUE essentiellement, article 49 TFUE dans une moindre mesure, conduit à s'interroger sur la faisabilité d'une harmonisation européenne de la question de l'assurabilité du risque de paiement des rançons en cas d'attaque par ransomware.

La question est celle de savoir si l'Union européenne serait compétente pour imposer aux États membres d'interdire l'assurabilité des rançons par un acte de droit dérivé. Dans la mesure où est en cause l'activité des assurances, on se situe dans le domaine des services. Autrement dit, l'éventuelle législation de l'Union relève du domaine du marché intérieur[123] qui constitue une compétence partagée de l'Union.

Dès lors, l'article 53, paragraphe 1, TFUE (marché intérieur), combiné avec l'article 62 TFUE, peut constituer une base juridique adaptée pour l'édiction d'un acte de droit dérivé et, plus précisément, d'une directive. Dans cette hypothèse ; l'acte de droit dérivé imposerait aux États membres de mettre en place les contrôles adéquats et de déterminer le régime de sanctions applicable aux violations des dispositions nationales prises en application de la directive. Les États membres doivent alors prendre toutes les mesures nécessaires pour assurer l'application de ces sanctions lesquelles doivent être effectives, proportionnées et dissuasives.

En droit, la compatibilité avec le Traité de la disposition d'un acte de droit dérivé interdisant l'assurabilité des rançons peut se poser. L'article 53 TFUE permet au législateur de l'Union d'arrêter les directives permettant la coordination des dispositions législatives, réglementaires et administratives

[122] *CJUE, Edgard Jan De Clercq, C-315/13, précité.*

[123] *Le terrain de l'art. 83 TFUE (espace de liberté, de sécurité, de justice) paraît moins adapté.*

des États membres concernant l'accès des activités de services et l'exercice de celle-ci. Il constitue la *lex specialis* de l'article 114 TFUE, *lex generalis* du marché intérieur, qui permet l'adoption par la procédure législative ordinaire de mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres qui ont pour objet l'établissement et le fonctionnement du marché intérieur. Les mesures visées par l'article 114, paragraphe 1, TFUE doivent, d'une part, comporter des mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres et, d'autre part, avoir « *objectivement et effectivement (…) pour objectif d'améliorer les conditions de l'établissement et du fonctionnement du marché intérieur* » . Par l'expression « *mesures relatives au rapprochement* », l'article 114 TFUE, a conféré au législateur, « *en fonction du contexte général et des circonstances spécifiques de la matière à harmoniser, une marge d'appréciation quant à la technique de rapprochement la plus appropriée afin d'aboutir au résultat souhaité, notamment dans des domaines qui se caractérisent par des particularités techniques complexes* »[125]. Dès lors, la notion de « *mesures relatives au rapprochement* » doit être interprétée comme englobant le pouvoir du législateur de l'Union de prescrire les mesures relatives à un produit ou à une catégorie de produits déterminés[126]. Il paraît cependant délicat d'envisager qu'une disposition de droit dérivé puisse concerner l'interdiction de ce type de couverture dans la mesure où il n'existe pas à ce jour une disparité législative ou réglementaire entre les États membres.

À cet égard, la jurisprudence apporte deux séries de précisions. D'une part, si la simple constatation de disparités entre les réglementations nationales ne suffit pas pour justifier le recours à l'article 114 TFUE[127], il en va, en revanche, différemment en cas de divergences entre les dispositions législatives, réglementaires ou administratives des États membres qui sont de nature à entraver les libertés fondamentales et à avoir ainsi une incidence directe sur le fonctionnement du marché intérieur[128]. **Il faudrait donc établir concrètement de quelle manière l'interdiction de l'assurabilité des rançons a une incidence directe sur le fonctionnement du marché intérieur**. D'autre part, dans la mesure où il s'agirait d'interdire cette assurabilité, la preuve de l'incidence directe doit être particulièrement circonstanciée. Il convient dans le cas de l'interdiction d'un produit comme l'assurabilité des rançons, d'établir la proportionnalité d'une mesure visant une prohibition générale en ce que celle-ci n'est pas prima facie de nature à favoriser le marché intérieur. Toutefois, la Cour de justice n'exclut pas que, de façon accessoire à un acte visant une activité transfrontalière, certaines modalités de cette activité soient interdites au titre du marché intérieur[129].

---

[124] *CJCE, GC, 6 décembre 2005, Royaume-Uni c/ Parlement européen et Conseil, C-66/04, ECLI:EU:C:2005:743.*

[125] *Ibid. ; CJUE, GC, 22 janvier 2014, Royaume-Uni c/ Parlement et Conseil, C-270/12, ECLI:EU:C:2014:18.*

[126] *Ibid.*

[127] *CJCE, 5 octobre 2000, Allemagne c/ Parlement et Conseil, C-376/98, ECLI:EU:C:2000:544.*

[128] *CJCE, 11 juin 1991, Commission c/ Conseil, dit « dioxyde de titane », C-300/89, ECLI:EU:C:1991:244 ; CJCE, GC, 14 décembre 2004, Arnold André, C-434/02, ECLI:EU:C:2004:800 ; CJUE, 8 juin 2010, Vodafone e.a., C-58/08, ECLI:EU:C:2010:321.*

[129] *CJCE, Allemagne c/ Parlement et Conseil, C-376/98, précité.*

En tout état de cause, dans l'hypothèse où une telle directive serait adoptée, il conviendrait d'apprécier la teneur de la disposition concernée et le degré d'harmonisation que celle-ci promeut. En effet, la Cour de justice considère qu'une harmonisation complète ne saurait être présumée en l'absence d'une volonté clairement exprimée en ce sens par le législateur de l'Union[130]. De surcroît, il est admis que, même dans une matière harmonisée de façon non exhaustive, les autorités nationales peuvent conserver une marge de manœuvre dès lors que la directive le prévoit. Pour des motifs d'intérêt général, pouvant recouvrir les raisons impérieuses précédemment invoquées, l'État d'accueil peut s'opposer à la conclusion de certains contrats[131].

Afin de satisfaire l'exigence de proportionnalité, il faudrait que la Commission établisse dans sa proposition qu'une telle interdiction soit de nature à permettre le fonctionnement du marché intérieur. Il semble difficile que la Commission se saisisse de la seule question de l'assurabilité des rançons pour proposer un acte législatif. Ce serait tout au plus dans un texte plus général qu'une disposition viendrait réglementer cette question.[132]

En effet, si l'on se place sur le terrain de l'opportunité, il parait peu probable que le législateur de l'Union adopte un acte de droit dérivé spécifiquement consacré à l'interdiction d'un type de prestations, ici l'assurabilité des rançons. En revanche, si un acte de nature plus générale venait à être adopté ou amendé, une disposition pourrait être consacrée à cette question.

[130] *CJCE, Gde ch., 7 septembre 2004, Commission c/ République française, C-347/02, ECLI:EU:C:2004:486 ; Commission c/ Grand-Duché de Luxembourg, C-346/02, ECLI:EU:C:2004:485.*

[131] *CJUE, 27 avril 2017, Onix Asigurari SA, C-559/15, ECLI:EU:C:2017:316.*

[132] *Par exemple la Directive Solvabilité 2 qui fait actuellement l'objet d'une révision au niveau européen...*

ANNEXE 8

Renforcer la cybersécurité de l'ensemble des opérateurs

RENFORCER LA CYBERSECURITÉ DE L'ENSEMBLE DES OPÉRATEURS

Les entreprises qualifiées d'opérateurs d'importance vitale (OIV) ainsi que celles qui sont qualifiées d'OSE sont protégées de manière satisfaisante à l'échelle européenne et nationale, par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En revanche, les TPE et PME qui ne sont pas identifiées comme d'importance vitale, essentielles ou importantes ne sont pas assez bien cyber protégées par ce dispositif public.

La Directive NIS 1 (*Network and Information System Security*) adoptée en 2016 a constitué la première étape d'une action de l'UE pour garantir un niveau élevé et harmonisé pour les réseaux et Systèmes d'Information de l'UE ; elle a permis notamment de faire émerger en Europe la catégorie des Opérateurs de Services Essentiels (OSE), acteurs « *essentiels* » au fonctionnement de l'économie et de la société. En France ce dispositif de cybersécurité vient compléter celui des Opérateurs d'Importance Vitale (OIV) introduit par la loi de programmation militaire de 2013. La transposition de la Directive NIS1 en France a donné lieu à l'adoption d'un corps de règles détaillées et exigeantes[133] destinées à renforcer la cyber résilience des opérateurs qualifiés d'OSE. Cette Directive fait aujourd'hui l'objet d'une révision[134] dont l'objectif est notamment d'élargir la liste des entités (essentielles et importantes) devant se doter de manière obligatoire d'un niveau de sécurité approprié. On ne peut que saluer cet objectif qui aboutira à terme à une augmentation du niveau général de la cyber robustesse des opérateurs.

Un texte visant à renforcer la cybersécurité de l'ensemble des opérateurs pourrait s'inspirer du cadre législatif européen mis en place par la Directive NIS mentionnée ci-dessus et par le futur Règlement européen Digital Operational Resilience Act (DORA) applicable au service financier ; une approche proportionnelle pour moduler l'application des règles de sécurité en fonction des risques présentés par l'opérateur (« *risk based approach* ») devrait évidemment guider l'action du législateur.

Le renforcement parallèle et déjà initié de la cybersécurité des entreprises d'assurance constitue également une étape importante dans la sécurisation de l'écosystème ; s'agissant du sujet particulier des ransomwares, il peut être en effet de l'intérêt des hackers de diriger leurs attaques vers des entreprises d'assurance afin d'avoir accès au détail des couvertures de chaque assuré. L'objectif étant d'orienter les futures attaques vers des entreprises assurées contre les ransomwares facilitant ainsi le paiement de la rançon au bénéfice du pirate.

---

[133] *Voir Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, Arrêtés des 13/06/2018, 01/08/2018 et 14/09/2018.*

[134] *Voir proposition de Directive relative aux mesures visant à instaurer un haut niveau de cyber sécurité au sein de l'Union : https://www.senat.fr/europe/textes_europeens/COM_2020_823.pdf*

Dans ces conditions, le renforcement de la cyber résilience des assureurs tel que proposé par le législateur européen avec DORA est également une étape importante dans la lutte contre les cyber attaques.

À cet égard, notons que les contrôleurs et législateurs européens et nationaux ont déjà entrepris de doter les entreprises d'assurance de règles de gouvernance et de gestion du risque informatique[135].

Ces textes, plus particulièrement le Règlement DORA et ses textes d'application (Normes Techniques Règlementation) devraient, sans nul doute, renforcer la cyber résilience de l'ensemble du secteur et limiter le nombre d'attaques par ransomwares dont pourraient être victimes les assureurs.

Une fois que ce cadre européen, renforçant la cyber sécurité des opérateurs aura été adopté et appliqué à l'ensemble des opérateurs, un système de notation garanti par une agence européenne cyber-souveraine ou de certification pourrait parachever le dispositif et garantir que l'opérateur répond aux normes de gouvernance et de sécurité en matière de risque informatique telles que définies par les textes législatifs.

À noter également que dans le cadre de la stratégie européenne en matière de cybersécurité, deux initiatives européennes ont vu le jour en juin 2021 :

- dans sa recommandation C (2021) 4520 du 23 juin 2021, la Commission européenne a proposé la création d'une « *Joint Cyber Unit* » afin de garantir une réaction coordonnée de l'Union en cas d'incidents ou de crise de cybersécurité majeure ; l'idée étant d'améliorer les échanges de bonnes pratiques , d'assurer une connaissance de la situation partagée et de garantir une réponse coordonnée en cas d'incidents ou de crise de cybersécurité majeurs ;

---

[135] Ont ainsi été adoptés les textes suivants :

- la transposition en droit français de la Directive Network Information Security (NIS) intervenue en 2018 et ayant abouti, pour certains assureurs, à la désignation en tant qu'OSE qui les oblige à respecter 23 règles en matière de cybersécurité,

- la publication en 2020 par l'EIOPA de ses Lignes Directrices sur la sous-traitance à des fournisseurs de cloud,

- la publication en 2020 par l'EIOPA de ses Lignes Directrices relatives à la sécurité et à la gouvernance des technologies de l'information et de la communication (TIC),

- le projet de Directive visant à réviser la Directive NIS précitée, publié en décembre 2020,

- la publication en 2020 par l'ACPR d'un document « Analyses et Synthèses » consacré aux réponses des organismes d'assurance à un questionnaire portant sur la gestion des systèmes d'information (SI) et de leur sécurité (SSI). Dans ce document, l'ACPR soulève des points d'attention à l'égard des assureurs en matière de gestion des risques liés aux systèmes d'information et leur sécurité,

- la publication en septembre 2020 par la Commission européenne de la proposition de Règlement sur la résilience digitale opérationnelle dans le domaine des services financiers-plus couramment dénommée DORA (Digital Operational Resilience Act),

- le guide publié par l'ANSSI en janvier 2021 qui vient compléter le dispositif réglementaire applicable aux Opérateurs de Services Essentiels en ce qui concerne la protection des systèmes d'information essentiels,

- la publication en juillet 2021 de la notice ACPR relative aux modalités de mise en œuvre des orientations/Lignes Directrices de l'EIOPA (citées plus haut) relatives à la sécurité et à la gouvernance des technologies de l'information et de la communication (TIC).

- le Règlement 2021/887 du 20 mai 2021 a établi un Centre de compétence européen pour l'industrie et la recherche en matière cybersécurité dont la mission est de renforcer les capacités européennes et de « *booster* » la recherche et la compétitivité européenne en matière de cybersécurité.