L'assurance du risque Cyber

Réflexions sur l'article 5 de la loi LOPMI

La loi N°2023-22 d'orientation et de programmation du ministère de l'intérieur du 24 janvier 2023 qui contient quelques dispositions sur le risque cyber a introduit un nouvel article dans le code des assurances au N°L.12-10-1[1] qui est entré en vigueur le 24 avril 2023.

PIERRE MINOR,
Avocat associé,
Coat Haut de Sigy de Roux Minor,
membre du HCJP

La suppression du mot rançon

Les rédacteurs de cette nouvelle disposition se sont sensiblement éloignés de la rédaction initialement proposée dans le projet de loi[2]. Cette nouvelle disposition qui peut surprendre à plus d'un titre prévoit en effet que le versement de toute somme au titre d'un contrat d'assurance visant à indemniser les personnes morales et les personnes physiques dans le cadre de leurs activités professionnelles des pertes et dommages causés par une cyber attaque, et plus largement par une atteinte à un système de traitement automatisé de données, est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 72 heures après la connaissance de l'atteinte par la victime.

L'article 5[3] du projet de loi avait initialement pour objectif d'encadrer les clauses de remboursement des rançongiciels par les assurances, en conditionnant ce remboursement au dépôt rapide d'une plainte par la victime, au plus tard 48h après le paiement de la rançon, afin, pour reprendre l'exposé des motifs du projet, d'améliorer l'information des forces de sécurité et de l'autorité judiciaire et de « casser » le modèle de rentabilité des cyber attaquants.

Cette rédaction initiale présentait d'un point de vue juridique plusieurs avantages. Elle confirmait tout d'abord expressément la licéité des clauses des contrats d'assurance qui prévoient l'indemnisation des rançons payées par les victimes de cyber attaques. Elle qualifiait ensuite justement ces demandes de rançons, d'extorsion, telle que prévue par l'article L312-1 du code pénal permettant de rappeler que celui qui paye la rançon est avant tout une victime. Elle subordonnait enfin le versement de l'indemnisation du paiement d'une rançon par les assureurs au dépôt de plainte par la victime auprès des autorités compétentes au plus tard 48 heures après le paiement de la rançon et non pas 72 heures après la connaissance de l'atteinte à un système de traitement automatisé de données comme c'est le cas désormais.

Pour les parlementaires le mot « rançon » devait être supprimé du texte de loi car d'aucun aurait pu y voir un encouragement à ces pratiques criminelles. En procédant de la sorte le législateur enlevait à cet article sa portée initiale qui était de créer un cadre juridique pour l'indemnisation des rançons pourtant nécessaire au développement d'un marché de l'assurance du risque cyber.

Un champ d'application large

Désormais le champ d'application de l'article L12-10-1 du code des assurances est extrêmement large puisqu'il conditionne le paiement de toute somme au titre d'un contrat d'assurance couvrant les dommages résultant d'une atteinte à un système de traitement automatisé de

données[4] à un dépôt de plainte auprès des autorités compétentes. La nouvelle rédaction inclut incontestablement les contrats d'assurance couvrant les conséquences des risques cyber et l'indemnisation des rançons mais cette indemnisation n'est plus visée expressément et l'on pourrait s'interroger sur le lien entre le dépôt de plainte et l'indemnisation des autres pertes et dommages causées par une atteinte à un système automatisé de données comme les pertes d'exploitation ou celles liées au coût de la restauration d'un système informatique.

L'interrogation se justifie également dans la mesure où l'indemnisation des rançons n'est pas systématiquement prévue dans tous les contrats d'assurance couvrant les conséquences des risques cyber. Le lien entre le dépôt de plainte et le contrat d'assurance qui ne contient pas une telle disposition interroge alors d'autant plus.

Le dépôt de plainte en cas d'attaque cyber se justifie pleinement pour l'information des forces de sécurité et de l'autorité judiciaire comme indiqué ci-dessus. Il faisait d'ailleurs partie des recommandations formulées par le Haut Comité Juridique de la Place Financière de Paris (HCJP) dans son rapport sur l'assurabilité des risques cyber du 28 janvier 2022[5]. Mais cette recommandation était formulée en lien avec l'assurance des rançons, l'information des forces de sécurité et des autorités judiciaires paraissant impérative en cas de demande et de paiement de rançons et d'indemnisation par l'assurance de ce paiement.

On peut penser que l'approche large désormais retenue par le législateur a notamment pour objectif de permettre aux autorités publiques de disposer de plus de données sur le nombre d'attaques cyber.

Cet objectif aurait alors pu être atteint d'une autre manière en rendant obligatoire de façon générale le dépôt de plainte dans le cadre de toute attaque cyber sans lien avec la mise en œuvre d'une police d'assurance. L'obligation aurait alors concerné toutes les victimes.

Il n'est pas certain que l'objectif d'encourager les dépôts de plainte soit ainsi atteint puisque l'obligation ne vise que certaines victimes qui bénéficient d'un contrat d'assurance et n'a pour conséquence que de permettre l'indemnisation au titre d'un tel contrat . Aucune autre sanction n'est prévue en cas d'absence de dépôt de plainte que la seule paralysie du contrat d'assurance.

On notera enfin que si le champ d'application de la nouvelle loi est très large, il ne concerne pas toutes les situations car les demandes de paiement des rançons ne résultent pas toujours d'une attaque par ransomware. Elles peuvent également être faites sous la menace d'une divulgation de données confidentielles ou de données préjudiciables à l'entreprise

La volonté de masquer le mot « rançon » a finalement bouleversé l'économie du texte d'origine en le privant de ses qualités intrinsèques.

Des points de vigilance pour les entreprises

Les entreprises devront désormais être particulièrement vigilantes car le champ d'application du nouveau texte est très large. Sont visées par le nouveau texte toutes les pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnées aux articles 323-1 à 323-3-1 du code pénal, ce qui recouvre des situations extrêmement différentes n'incluant pas systématiquement une demande de rançon ou une perte ou une altération de données.

Sont ainsi concernées le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données, le fait d'entraver ou de fausser le fonctionnement d'un tel système, d'y introduire frauduleusement des données ou d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient. Ceci peut concerner des situations très diverses, comme celle par exemple d'une cyber attaque entrainant le cryptage des données ou leur vol, accompagnée ou

1/ « Art. L. 12-10-1.-Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.

« Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle. »

2/ Projet de loi n°5185 d'orientation et de programmation du ministère de l'intérieur

3/ Art. L. 12 10 1. – Le versement d'une somme en application d'une clause assurantielle visant à couvrir le paiement d'une rançon par l'assuré dans le cadre d'une extorsion prévue à l'article 312-1 du code pénal, lorsqu'elle est commise au moyen d'une atteinte à un système de traitement automatisé de données prévue aux articles 323-1 à 323-3-1 du même code, est subordonné à la justification du dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard 48 heures après le paiement de cette rançon. »

4/ Tel que visé par les articles 323-1 à 323-3-1 du Code pénal

5/ Voir pages 36 à 38

non d'une demande de rançon, mais également l'hypothèse de la reproduction ou du transfert (parfois à soi-même) sans autorisation, de données de l'entreprise par un salarié ou un tiers.

Toutes ces situations devront désormais entrainer le dépôt d'une plainte par la victime auprès des autorités compétentes dans le délai de 72h après la connaissance de l'atteinte par la victime sauf à perdre tout droit à indemnisation au titre de la police d'assurance souscrite.

Ce délai de 72h devra donc être un point d'attention particulièrement important pour les entreprises qui devront l'inclure dans leurs procédures internes de gestion de crises cyber de façon à ne pas l'oublier dans un contexte où le premier réflexe n'est peut-être pas de penser à l'assurance surtout si les pertes ou les dommages ne sont pas immédiatement apparents.

Le point de départ de ce délai de 72H sera inévitablement source de contentieux. Le texte initial envisageait un délai de 48h commençant à courir à partir de la date de paiement de la rançon, point de départ aisément vérifiable. A ce critère objectif le législateur a préféré s'appuyer sur la connaissance par la victime de l'atteinte à un système de traitement automatisé de données. La question de la détermination de la date se posera avec acuité en particulier pour les personnes morales et les grands groupes. Que devra-ton retenir ? La date où les services informatiques ont connaissance avec certitude de l'atteinte au système de traitement automatisé de données ou celle où la direction générale dispose de cette information ? Quelle date retenir pour l'incident informatique qui se révèle après enquête être ultérieurement une atteinte ?

Les entreprises seront donc bien avisées de documenter le déroulement des incidents informatiques et la prise de connaissance de l'atteinte au système et de sa date. C'est à partir de cette date que le délai commencera à courir que des pertes ou dommages aient été identifiés ou non.

La nécessité de documenter la prise de connaissance de l'atteinte par l'entreprise

s'impose en particulier à l'égard de la compagnie d'assurance qui se fera dans un premier temps juge du respect du délai de 72h. La fourniture d'éléments objectifs aisément vérifiables devrait ainsi limiter les risques de contentieux sur le point de départ du délai.

Il appartiendra aux entreprises de faire preuve également de dextérité pour articuler correctement dans le temps la saisine de leur compagnie d'assurance au titre de la police souscrite et le dépôt de plainte. La police d'assurance pourra peut-être faire l'objet d'une mise en œuvre pour des incidents informatiques qui se révèleront ultérieurement être des atteintes visées par les articles 323-1 et suivants du Code pénal. Le dépôt de plainte ne devra donc pas être oublié et s'inscrire dans le délai de 72H après la connaissance de l'atteinte par l'entreprise victime.

Cette disposition pourrait toutefois être considérée comme protectrice des entreprises car leur permettant de diligenter les enquêtes nécessaires pour s'assurer de la réalité de l'atteinte visée par les dispositions du code pénal précité. C'est à partir du moment où la connaissance de la victime est certaine que le délai commence à courir. Devraient ainsi être évités les multiples dépôts de plainte effectués par prudence mais pour des incidents qui se révèlent être mineurs et qui ne rentrent pas finalement dans les

hypothèses visées par les dispositions des articles 323-1 et suivants du code pénal. Mais la détermination du point de départ du délai fera sans aucun doute l'objet de nombreuses contestations et il apparait vraisemblable que certaines entreprises préfèreront déposer plainte dès qu'une suspicion d'une atteinte existe pour ne pas prendre le risque de perdre leur droit à indemnisation au titre de leur police d'assurance.

On rappellera pour mémoire qu'un autre délai de 72h devra être géré par l'entreprise dans le contexte d'une atteinte à l'un de ses systèmes de traitement automatisé de données C'est celui contenu dans l'article 33[6] du RGPD[7] qui impose la notification à l'autorité de contrôle compétente de la violation de données à caractère personnel dans un délai de 72H. Le point de départ de ce délai est la date à laquelle l'entreprise a connaissance de cette violation de données personnelles date qui ne correspondra pas toujours avec la date prévue au nouvel article L.12-10-1 du code des assurances qui est la date de prise de connaissance par l'entreprise d'une atteinte à un système de traitement automatisé de données.

L'assurabilité du cyber rançonnage

La loi n'a donc pas atteint l'objectif, souhaité par beaucoup et notamment par les compagnies d'assurance, de voir affirmer expressément la possibilité au plan juridique de couvrir par l'assurance le risque de cyber rançonnage des entreprises. Cependant les débats parlementaires attestent de la volonté du législateur de traiter cette question sans écarter l'assurabilité et il ne semble pas contestable que le « versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données »[8] puisse inclure le remboursement des cyber-rançons qu'aucune disposition n'interdit par ailleurs.

La couverture de ce risque par les assurances apparait donc aujourd'hui possible en raison non seulement de la nouvelle loi mais également dans la mesure où elle ne contrevient pas à une règle de droit comme l'a démontré le rapport précité du HCJP.

On rappellera qu'au regard du droit pénal[9] et s'agissant de la situation de l'entreprise victime, le paiement de la rançon n'est pas en soi une infraction pénale car le paiement est effectué sous la contrainte. « Il s'analyse en une extorsion puisqu'elle vise à obtenir une remise de fonds sous la contrainte ce qui correspond au délit prévu par l'article 312-1 du Code Pénal. Il n'apparait donc pas possible de reprocher pénalement un paiement fait sous une contrainte constitutive d'une infraction pénale, la société payeuse étant la victime de cette infraction »[10].

Il convient également de rappeler l'article 122-7 du Code pénal qui exclut la responsabilité pénale de 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.

S'agissant de l'entreprise d'assurance, prévoir le remboursement d'une cyber-rançon au profit de l'entreprise victime d'un cyber chantage devrait être également considéré comme licite, le paiement de la rançon ne constituant pas une infraction. La couverture d'assurance n'a en effet ni un objet ni une cause illicite. Elle est comparable comme le précise le rapport du HCJP « à une assurance couvrant le risque de vol ou de destruction »[11].

Une limite à ce principe pourrait toutefois se trouver dans l'infraction de financement du terrorisme prévue par l'article 421-2-2 du Code pénal dans l'hypothèse où la cyber-rançon serait demandée par un groupe terroriste. L'infraction étant caractérisée par la connaissance que les fonds remis sont « destinés à être utilisés, en tout ou en partie, en vue de commettre (un acte de terrorisme) »[12] l'entreprise victime qui paye une cyber-rançon pourrait être poursuivie de ce chef si elle avait connaissance du fait que la demande de cyber-rançon émanait d'un groupe terroriste. Il convient de noter que la contrainte exonératoire de responsabilité pénale prévue à l'article

6/ En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

7/ 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)

8/ Article 5 de la loi

9/ Rapport du HCJP pages 23 et suivantes

10/ Rapport du HCJP page 23

11/ Rapport du HCJP page 24

12/ Article 421-2-2 du Code pénal

122-2 du Code Pénal pourrait néanmoins trouver à s'appliquer dans certains cas[13] à condition que l'entreprise victime ait agi sous l'empire « d'une force ou d'une contrainte à laquelle elle n'a pu résister ».

La question se pose également pour l'assureur qui pourrait être considéré comme complice et accusé de financement indirect du terrorisme dans l'hypothèse notamment où il a connaissance, en amont du règlement de la rançon, que celle-ci va alimenter un réseau terroriste. La fongibilité entre le paiement de l'indemnité par l'assureur et le paiement de la rançon par l'entreprise[14] est alors susceptible d'exposer l'assureur dans ce cas à une accusation de complicité.

Cependant si l'information que la demande de rançon émane d'un groupe terroriste parvient à l'assureur après le paiement de la rançon, la qualification de financement du terrorisme au titre de l'article 421-2-2 du code pénal ne devrait pas pouvoir être retenue, le paiement de l'indemnisation effectué par l'assureur va demeurer entre les mains de l'assuré et intervient après le paiement de la rançon. Dans cette hypothèse il n'y a aucune fongibilité entre les deux paiements.

Il convient de rappeler également que le respect des régimes de sanctions prononcées par les autorités internationales, européennes et nationales et des mesures de gel des avoirs destinées notamment à lutter contre le terrorisme s'impose également aux assureurs.

Sous réserve du respect de ces règles destinées à lutter contre le terrorisme et son financement, l'assurance des rançons ne se heurte à aucune interdiction en droit français, le paiement de la rançon par l'assuré ne constituant pas en lui-même une activité illicite ou pénalement condamnable[15].

La contrariété à l'ordre public du code civil semble aussi exclue même s'il pouvait être tentant de considérer, par un raccourci, que les assureurs en remboursant les rançons aux victimes contreviennent à l'ordre public ou aux bonnes mœurs car ces remboursements encourageraient indirectement les cybercriminels à poursuivre leurs attaques et donc à commettre de nouvelles infractions.

Enfin on mentionnera qu'au regard du droit des assurances le principe que l'assureur ne répond pas des pertes et dommages provenant d'une faute intentionnelle ou dolosive de l'assuré[16] n'a pas vocation à s'appliquer dans le cas de l'indemnisation d'une rançon, l'assuré est dans ce cas une victime et les pertes et dommages qu'il subit ne relève ni d'une faute intentionnelle ou dolosive de sa part.

L'occasion de confirmer expressément la licéité de l'assurance des rançons a donc été manquée et d'aucuns le regretteront car comme le rapport du HCJP le précisait[17] « ce n'est 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. »

D'autres opportunités de clarification se présenteront peut-être dans l'avenir car toutes les recommandations du HCJP figurant dans le rapport sur l'assurabilité des risques cyber n'ont pas été mises en œuvre à ce jour. Parmi celles-ci figurait une demande de clarification des textes nationaux et européens applicables aux obligations LCB-FT des assureurs en matière de remboursement de cyber rançon 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. On pourrait également citer la demande de clarification de l'article L121-8 du Code des assurances pour voir intégrer dans le concept de guerre les attaques cyber perpétrées par les États[18]. ■

13/ Article 122-2 du Code pénal.

14/ Rapport du HCJP page 24

15/ « l'assurance d'un risque pénal est illicite en tant que telle et 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 » L. Mayaux « Assurance et ordre public : à la recherche d'un critère » RGDA 2008, N°3 cité dans le rapport précité du HCJP page 21.

16/ Article L113-1 du Code des assurances

17/ Rapport du HCJP page 32

18/ Rapport du HCJP pages 48 et suivantes.