CHAMBRE ARBITRALE MARITIME DE PARIS

Gazette de la Chambre

Lettre d'information de la Chambre arbitrale maritime de Paris

Comité éditorial : Philippe Delebecque - Claude Goussot - Jean-Yves Thomas - Michel Leparquier

Editeur : Philippe Delebecque

3 numéros par an **(Janvier - Avril - Septembre)** **Numéro 43 - Printemps 2017**

"Res judicata pro veritate habetur"

Cyber-sécurité et Transport maritime

Sébastien Lootgieter
Avocat associé
Cabinet Villeneau Rohart Simon & associés

Il y a quelques semaines, un hebdomadaire à grand tirage titrait : "La nouvelle cyber-guerre mondiale – Le jour où Internet s'arrêtera". Le grand public a désormais conscience que des individus voire un État étranger puissent s'introduire dans un système informatique, en piller les données ou en contrôler le fonctionnement. L'industrie maritime sait qu'elle n'est pas à l'abri de cette menace. En 2011, des malfaiteurs piratairent les systèmes informatiques de plusieurs sociétés opérant sur le port d'Anvers afin de pouvoir contrôler les déplacements de certains containers chargés de marchandise sensible (**https://goo.gl/WbA3CH**). Depuis, les initiatives visant à faire prendre conscience aux compagnies maritimes de l'importance de la cyber-sécurité se sont multipliées, tant de la part de l'industrie que des pouvoirs publics. Dans un tel contexte, il est important de se demander comment le droit appréhendera ce nouveau risque et quelles responsabilités pourraient en découler.

La cyber-conscience

On a coutume d'enseigner que le droit maritime est un droit de commerçants, né de la pratique. Face à l'émergence d'une cyber-criminalité, l'industrie a su réagir en créant une "*soft law*", reprise dans une "*hard law*" constituée par des textes réglementaires d'origine nationale ou internationale.

L'administration française (la Direction des Affaires Maritimes et l'Agence Nationale pour la Sécurité de Systèmes d'Information) vient d'éditer trois guides : "Cyber-sécurité – évaluer et protéger le navire"(**https://goo.gl/OWmf2N**), "Guide des bonnes pratiques de sécurité à bord des navires" (**https://goo.gl/kSprgG** et "Cyber-sécurité – renforcer la protection des systèmes industriels du navire" (**https://goo.gl/yv5EN9**). Ces guides insistent auprès des compagnies maritimes et des équipages sur le respect de "l'hygiène informatique" ou encore sur la mise en place "d'outils de sécurisation" simples destinés à identifier le cyber-risque et en limiter ses conséquences, comme changer périodiquement les mots de passe ou s'assurer de l'étanchéité des réseaux informatiques.

Parallèlement à ces guides, l'arrêté du 23 novembre 1987 relatif à la sécurité des navires a été modifié à la fin de l'année 2016. Désormais il prévoit dans sa division 130 ("Délivrance des titres de sécurité") que l'évaluation de sûreté du navire devra traiter : "des dispositions relatives à la cyber-sécurité du navire". Ainsi l'évaluation de sûreté devra prendre en compte "la cartographie logicielle" et la gestion des "vulnérabilités système".

La prise en compte réglementaire de la cyber-sécurité se retrouvait déjà dans le Code ISPS aux termes duquel les navires devaient faire l'objet d'une évaluation de sûreté portant sur leurs différents éléments dont "les systèmes de réseaux informatiques" (partie B, règle 8.3).

Pourtant, et en dépit de ce texte précurseur, la prise de conscience par les acteurs du monde maritime de la cyber-sécurité est relativement récente. En février 2016, le BIMCO, de concert avec d'autres associations professionnelles, publiait des "*Guidelines on cyber-security on board ships*" (**https://goo.gl/MK25jM**) auxquelles l'OMI a fait référence dans une circulaire de l'OMI prise du 1er juin 2016, intitulée "*Interim guidelines on maritime cyber-security management*" (**https://goo.gl/Bdqpfh**).

Enfin, la Directive européenne 2016/1148 du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux prévoit que les États devront adopter une stratégie nationale en matière de sécurité des réseaux et des systèmes informatiques (**https://goo.gl/3ZZtVc**). Les opérateurs de "services essentiels" devront prendre les mesures "techniques et organisationnelles" nécessaires pour gérer les risques qui menacent la sécurité des réseaux et des systèmes qu'ils utilisent dans leur activité. Les entreprises de transport maritime sont justement considérées comme des entreprises fournissant un service essentiel.

Pour être complet il faut évoquer la position de certaines sociétés de classification, par exemple, la société ABS a publié plusieurs volumes de règles sur l'application des principes de cyber-sécurité aux opérations maritimes et offshore, la prise en compte de la cyber-sécurité pour les industries maritimes et offshore, des notes sur l'intégrité des données, sur la vérification des systèmes de logiciels et également sur certains standards que doivent respecter les fournisseurs de logiciels. ***Suite de l'article Page 2.***

Suite de l'article "Cyber-sécurité et Transport maritime".

La cyber-navigabilité

Le fréteur doit mettre à disposition de l'affréteur un navire en bon état de navigabilité ; le transporteur maritime pourra voir sa responsabilité engagée vis-à-vis des intérêts cargaison s'il n'a pas fait diligence pour mettre son bâtiment en état de navigabilité au départ.

Un navire dont le système informatique ou l'équipage contreviendrait aux exigences évoquées plus haut en matière de cyber-sécurité pourrait-il être considéré comme innavigable ?

A cette question, la doctrine semble avoir répondu de manière positive. Les professeurs P. Bonassies et C. Scapel indiquent ainsi dans la dernière édition de leur traité de droit maritime que : "le problème (…) se posera de plus en plus, de la sécurité informatique (cyber-sécurité) du navire affrété. Un navire dont les systèmes informatiques ne sont pas protégés peut voir sa navigabilité contestée" (p.764). Cette analyse rejoint la conception large de la notion de navigabilité qui prévaut dans la jurisprudence tant arbitrale que judiciaire.

Dans une sentence n° 768 du 31 mars 1990 les arbitres de la Chambre arbitrale maritime de Paris ont jugé que : "entendue dans son sens large, la navigabilité concerne autant la composition de l'équipage que l'état technique du navire". Dans le même sens ils ont jugé dans une sentence n° 950 du 15 octobre 1996 que : "…le fréteur [doit prendre] toutes dispositions pour que ce transport puisse s'exécuter dans les conditions de sécurité absolue s'agissant là de l'obligation de navigabilité entendue au sens large". Il a été jugé à de nombreuses reprises que le navire dont les installations frigorifiques ne fonctionnaient pas, ou même dont le thermomètre était inexact n'était pas navigable.

De même, la défaillance du système informatique, et en particulier la "non-utilisation de l'ordinateur de bord", fut soulevée par l'affréteur à temps d'un porte-conteneurs qui avait perdu une partie de sa marchandise au cours de différentes traversées pour soutenir l'incompétence de l'équipage dans la procédure ayant donné lieu à la sentence n° 1105 du 14 janvier 2005.

Les tribunaux judiciaires semblent même avoir une conception encore plus large comme en témoigne un récent arrêt "*Western Island*" où la Cour d'appel de Paris a considéré au vu d'une charte-partie GENCON qu'un navire n'était pas navigable dès lors que la cargaison, en dépit de sa nature, avait été positionnée à proximité d'une zone de chaleur.

Un équipement informatique déficient, qui ne serait pas équipé d'un "*firewall*" ou d'un antivirus à jour pourrait être traité de la même façon qu'un équipement frigorifique défaillant qui serait incapable de maintenir la chaîne du froid. De même, un logiciel qui serait incapable de positionner de manière satisfaisante les marchandises dans les cales du navire en tenant compte de leur nature, pourrait être pris en compte pour caractériser l'innavigabilité du navire d'autant plus que le défaut d'un ordinateur de bord peut difficilement être considéré comme une cause exonératoire de responsabilité. Dans un arrêt du 1er octobre 1993, le "Ville du Havre", le transporteur soutenait que le dérèglement affectant l'ordinateur de pilotage automatique du navire était assimilable à un vice caché excluant sa responsabilité. Cet argument fut rejeté par la Cour d'appel de Paris.

Les cyber-responsabilités

Le Code pénal punit le responsable d'une attaque dirigée contre des systèmes informatiques. Si dans certaines affaires, les enquêteurs ont pu retrouver la trace du délinquant à l'étranger et si des condamnations ont pu être prononcées par les tribunaux, en pratique l'armateur d'un navire pourra difficilement être indemnisé directement par le responsable d'une cyber-attaque qui entraînerait la perte d'une cargaison, voire celle du navire.

La victime pourrait donc être tentée de se retourner contre le tiers qui, du fait du piratage, a reçu des instructions causant un dommage.

Dans le cas où la banque de l'affréteur recevrait un faux ordre de virement portant sur un fret imaginaire, la "fraude au président" que les anglais appellent la "*friday afternoon fraud*", l'affréteur pourrait rechercher la responsabilité de sa banque. La Cour de cassation a retenu une telle responsabilité dans un arrêt du 18 janvier 2017 rejetant un pourvoi contre une décision du juge de proximité de Lille ayant jugé que la banque devait prouver la négligence de son client victime d'un virement non-autorisé.

La victime pourrait également se retourner contre le prestataire en charge de la mise en place ou de la maintenance du système informatique à bord du navire.

Le prestataire qui livre et entretient le système est débiteur d'une obligation de conseil. Il est garant des vices cachés pouvant affecter le matériel qu'il fournit. Le concepteur d'un progiciel doit livrer un matériel conforme à ce qui était prévu et sans anomalies. Tout comme la présence d'un virus, le risque d'un piratage informatique ne peut être raisonnablement considéré comme un évènement de force majeure imprévisible.

Il n'en demeure pas moins que si la responsabilité du prestataire peut être engagée, il faudra souvent prendre en compte l'éventuelle faute de la victime, comme l'illustre un arrêt rendu en 2014 par la Cour d'appel de Colmar. La victime d'un acte de piratage informatique reprochait à son prestataire de ne pas avoir pu restaurer les données effacées compte tenu d'une absence de sauvegarde intégrale des données présentes sur son serveur. La Cour d'appel a considéré qu'outre les fautes du prestataire, il y avait eu une négligence de la victime, qui n'avait vérifié ni la capacité du système de sauvegarde, ni la bonne réalisation desdites sauvegardes. Du fait de cette combinaison des fautes, la Cour d'appel a considéré que la faute commise par le prestataire informatique était constitutive d'une perte de chance, à savoir celle qu'aurait eue la victime de pouvoir adapter le matériel avant le sinistre. Le prestataire n'a été condamné à indemniser la victime qu'à hauteur du tiers du préjudice subi.