Les risques cybernétiques dans le domaine des transports

Actualité législative publié le **16/10/2019**, vu **2625 fois**, Auteur : Droit de la sécurité informatique

En juin 2011, plusieurs employés et agents du port d'Anvers reçoivent un email a priori anodin. Une pièce est jointe à cet email.

1. En juin 2011, plusieurs employés et agents du port d'Anvers reçoivent un email a priori anodin. Une pièce est jointe à cet email. Cette pièce jointe contient en fait un « *cheval de Troie* », un logiciel malveillant qui va faire entrer dans l'ordinateur un parasite à l'insu de son utilisateur. Ce parasite va permettre à des malfaiteurs situés à plusieurs centaines de kilomètres, aux Pays Bas, d'accéder aux mots de passe utilisés pour pouvoir récupérer et tracer les conteneurs sur les quais du port. Avec ce mot de passe, les pirates vont alors pouvoir suivre le déplacement de certains conteneurs sensibles où, en plus d'une cargaison régulière, on trouve de la drogue ou d'autres marchandises de contrebande.

Cette intrusion informatique sera découverte, mais les malfaiteurs ne vont pas en rester là. Ils vont entrer par effraction dans les locaux d'une société opérant sur le port et installer sur son matériel électrique des appareils espions qui vont permettre de prendre le contrôle à distance des ordinateurs. Les trafiquants vont pouvoir suivre les conteneurs, les positionner à leur guise dans des lieux et à des moments voulus pour permettre à des complices de les récupérer sans être inquiétés, jusqu'à un coup de filet des polices belges et néerlandaise en juin 2013 (2) .

2. La même année, un universitaire américain, Todd Humphrey, de l'université du Texas, après être arrivé à prendre le contrôle d'un drone, a pris le contrôle d'un yacht de luxe le *White Rose of Drachs* en utilisant un simple ordinateur portable et un appareil permettant de brouiller le GPS du navire (3) .

3. La fraude maritime est aussi ancienne que la navigation ; les faux connaissements, les fausses cargaisons, les faux navires, et les escroqueries en tout genre ne sont pas neufs. Mais les deux exemples que nous venons d'évoquer se caractérisent par l'utilisation d'un moyen nouveau. Il y a eu prise de contrôle d'un système informatique par l'intermédiaire d'internet, d'ordinateurs, d'emails... par toutes ces techniques qui se sont généralisés et ont pris de plus en plus de place depuis de la fin des années 1990. C'est ce qu'on appelle vulgairement la cybernétique, la science du contrôle. Cette cybernétique va donner naissance à de nouveaux risques. Existent-ils en matière de transport ? Sont-ils pris en compte par le droit positif et par l'industrie maritime ? Enfin, à quelles responsabilités peuvent-ils donner lieu ? Nous allons successivement nous pencher sur ces diverses questions.

I. - LA CYBERSECURITÉ, NOUVEL ENJEU DE LA SÉCURITÉ MARITIME ?

4. Dans son ouvrage « *Long-Cours* » le commandant Pierre Estur expliquait que sur la passerelle à côté du commandant, du lieutenant, du timonier, il y avait une table sur laquelle se trouvait « *la carte appropriée du secteur, et tout près, la règle..., le compas à pointe sèche, crayons, gommes...* » (4) . Certes l'électronique est déjà au service de la navigation, mais si le navigateur par satellite se développe, certains systèmes ont une fiabilité beaucoup plus réduite (5) . C'était il

y a trente ans, depuis les choses ont bien changées.

5. Il suffit désormais d'aller sur la passerelle d'un navire ou le centre de contrôle d'un port pour s'apercevoir que l'utilisation de l'informatique et des systèmes d'information est de plus en plus présente. Le Système d'Identification Automatique, *AIS*, permet de connaître instantanément l'identité, le statut et la position d'un navire. Comme sur les voitures, les navires sont équipés d'un GPS. L'utilisation d'un système de visualisation des cartes, l'*ECDIS* (Electronic Chart Display and Information System) se généralise également. Les mécanismes de propulsion du navire peuvent également être gérés de manière informatique.

6. La généralisation de l'informatique ne se limite pas au navire. Les marchandises font aussi l'objet d'un traitement informatique. Des ports français utilisent par exemple le *Cargo Community System AP+* qui va permettre, grâce à une connexion internet ou un réseau dédié, de pouvoir gérer de manière dématérialisée les flux de marchandises, les procédures administratives et commerciales (6) . Tous ces systèmes sont-ils fiables ? Une réponse positive semble difficile à adopter.

7. Prenons par exemple le cas de l'AIS. Il fournit des données facilement accessibles. Elles peuvent permettre à des pirates de retracer la route d'un navire. Certains navires coupent volontairement leur AIS. Il est même possible de le truquer ou de le pirater.

En décembre 2012 au moins trois navires iraniens immatriculés en Tanzanie ont trafiqué leurs AIS prenant les identités de navires syriens (7) . De même, il y a quelques années une société informatique parvenait à établir des signaux AIS artificiels montrant un navire américain naviguant vers la Corée du Nord, ou encore déplaçant en l'espace quelques secondes un remorqueur de sa position initiale à un autre endroit situé à plusieurs milles nautiques. On sait enfin que certains opérateurs, en particulier lorsqu'ils sont dans des zones sensibles, vont délibérément changer le nom de leur navire, de manière à dissuader toute personne qui voudrait éventuellement les attaquer.

8. Si des armateurs peuvent eux-mêmes contourner l'AIS, des cybers pirates pourraient faire de même, pour satisfaire leurs propres fins.

Un autre facteur de développement de la cybersécurité en matière maritime, et en particulier en matière de transport, c'est la généralisation dans les échanges du connaissement électronique. On sait que ce type document est depuis de nombreuses années présenté comme le futur de l'industrie maritime. Pour l'instant ces prévisions n'ont pas été couronnées de succès mais les règles de Rotterdam contiennent des dispositions qui visent les documents électroniques de transport. Elles prévoient que la marchandise peut voyager sous un document électronique de transport à conditions qu'il soit nécessaire de mettre en place des procédures pour en conserver l'intégrité.

9. Nous sommes face à une industrie qui est de plus en plus informatisée et connectée, mais il y a un manque de conscience de la réalité du cyberisque chez les opérateurs maritimes. Dans un article paru en mai 2014 à la suite d'une étude du cabinet KMG, un journaliste du *Lloyd's List* a fait remarquer que la cyber sécurité à bord des navires de commerces et dans les principaux ports avait 10 à 20 ans de retard par rapport aux systèmes des ordinateurs terrestres, laissant ainsi une porte ouverte à une échelle de menaces de plus en plus importantes (8) .

10. Les menaces sont variées. Le vol d'informations sensibles ; l'intrusion dans un système pour le contrôler ; l'hameçonnage (ce que les anglais appellent le « *phishing* ») avec lequel des pirates vont soutirer à leur victime des renseignements personnels en faisant croire qu'elle s'adresse à une banque ou une administration ; la diffusion de fausses informations sur une société ; le détournement de fonds ; la demande de rançon qui peut par exemple se produire après qu'un pirate ait bloqué le système informatique d'une entreprise ; l'éventuelle attaque contre un navire

n’est pas à exclure. Il y a enfin le trafic et la contrebande.

12. Ces menaces sont variées et leurs auteurs peuvent être de différentes origines. Il y a les Etats étrangers (9) ; on sait que les Etats Unis reprochent souvent à la Chine d’être derrière des cyberattaques. Il y a des activistes/pirates (10) qui s’érigent comme gardiens de principes qu’ils croient immuables. Il y a aussi des criminels, comme nous l’avons vu à Anvers, ou enfin des concurrents qui pourraient par exemple pirater des systèmes internet pour essayer d’obtenir des informations confidentielles.

II. - LE RISQUE CYBERNÉTIQUE ET LE DROIT POSITIF

13. En 2014, le Canada déposait à l’OMI une proposition pour le développement de lignes directrices sur la cybersécurité dans le monde maritime (11) . Ce document rappelle les différents exemples de risques cybernétiques, identifie les mesures à prendre pour faire progresser la sécurité, décrit les différents systèmes utilisés dans le monde maritime, leur vulnérabilité et les moyens pour en prévenir les risques. Le but était alors d’établir un guide des bonnes pratiques comme il peut en exister à l’égard de la piraterie. Il semble cependant que l’OMI ait finalement laissé à des organisations non -gouvernementales le soin de régler cette question (12) .

14. Aux Etats Unis, la cyber sécurité est traitée depuis plusieurs années par les pouvoirs publics qui sont sans doute plus sensibilisés à ce type de problème depuis les attentats du 11 septembre 2001. Le FISMA (*Federal Information Security Management Act*) de 2002 impose aux différentes entités fédérales de prendre des mesures spécifiques pour limiter les risques liés à la cybersécurité (13) . En février 2013, une ordonnance 13636 était prise par le Président sur la cybersécurité dans les infrastructures critiques, cette notion incluant les ports maritimes (14) . En juin 2015, les gardes-côtes des Etats Unis établissaient un document déterminant la stratégie à adopter en matière de risque cybernétique (15) . Ils sont en train d’établir des lignes directrices visant à répondre à certaines questions de l’industrie, en particulier sur la manière de protéger et limiter les risques liés à la cybersécurité.

15. La France n’est pas à la traîne. La réglementation sur la sûreté maritime évoque expressément la cybersécurité. Une note technique du 25 février 2015 relative à la certification de sûreté des navires battant pavillon français décrit la cybersécurité dans son paragraphe 3.5 comme un « *élément périphérique* » participant à la sûreté globale du navire au même titre que la mise en œuvre d’une citadelle et d’une équipe de protection privée destinées à lutter contre les pirates somaliens (16) .

III. - LA REPONSE DE L’INDUSTRIE : L’EXEMPLE DE L’ASSURANCE

16. L’industrie maritime n’est pas restée insensible au risque cybernétique.

En avril 2015 un groupe de travail était mis en place entre la BIMCO, l’International Chamber of Shipping, Intercargo et Intertanko, pour développer des lignes directrices sur la cybersécurité (17) . Mais c’est surtout dans le monde de l’assurance que la question s’est posée.

Lors du Rendez-vous de l’assurance transport organisé par le CESAM en mai 2015, Patrick de la Morinerie directeur d’AXA Corporate Solutions identifiait le « *Cyber* » comme une menace spécifique auquel les assureurs devront faire face et qui est comparable à la piraterie (18) . Le risque cybernétique a également animé les discussions de l’Association internationale des assureurs maritimes (IUMI) à Berlin en septembre 2015. On peut enfin évoquer un rapport très récent sur le risque cybernétique établi par le comité commun de l’assurance corps du Lloyd’s (19) .

17. Quand une entreprise est victime d’un sinistre quelle qu’il soit, c’est vers son assureur qu’elle se tourne. Les choses ne sont pas différentes lorsque ce sinistre a été causé par une attaque

cybernétique.

18. La société Word Fuel Services Inc («WFS») recevait un appel d'offre de l'administration des Etats-Unis pour la fourniture d'une quantité importante de gasoil. World Fuel Services a présenté une offre qui a été acceptée, le montant de l'opération s'élevant à 17.000.000 USD. Pour trouver le combustible, WFS contactait différents fournisseurs et adressait ensuite sa facture à l'administration. En fait, ce fournisseur avait été victime d'une fraude. L'administration américaine n'était pas au courant de cette opération qui ne correspondait à aucun appel d'offre officiel. WFS s'est retournée contre son assureur pour réclamer l'indemnisation du préjudice subi. L'assureur s'y est opposé et engageait une procédure devant le Tribunal fédéral de New York afin de faire constater qu'il n'avait pas à couvrir ce sinistre. La procédure est actuellement en cours (20) . On peut aussi évoquer une autre procédure judiciaire aux Etats Unis entre Sony et son assureur Zurich à propos du piratage de données du réseau de la Playstation en avril 2011. Les pirates avaient réussi à voler des données personnelles d'environ 77.000 comptes de clients de Sony, la forçant ainsi à fermer son réseau pendant presque un mois. Sony a dû faire face à plusieurs actions de la part des consommateurs et s'est retourné contre son assureur afin que celui-ci prenne en charge les frais de défense, mais également d'indemnisation qui pourraient lui être réclamés. Le Tribunal de New York a jugé que la couverture responsabilité civile de Sony ne pouvait couvrir ce sinistre. L'affaire a depuis été transigée (21) .

19. L'assurance a très tôt pris en compte les dommages pouvant être liés à un risque cybernétique d'abord pour les exclure de la couverture des risques ordinaires.

En décembre 2002, la FFSA établissait une première clause d'exclusion des risques chimiques, biologiques, biochimiques, électromagnétiques et cybernétiques qui était en fait l'adaptation en langue française de clauses déjà diffusées par le marché britannique (clause 356A et clause 365). Ces clauses prévoyaient une exclusion des pertes et dommages résultant directement ou indirectement de l'utilisation ou l'exploitation, dans l'intention de nuire, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, virus informatique ou transmission de données, ou tout autre système électronique.

20. En novembre 2013, une nouvelle circulaire 07/2004 de la FFSA transmettait une nouvelle clause au marché de Londres, la clause 380, prévoyant une exclusion des dommages causés par une cyberattaque. Cette exclusion a encore été reprise en janvier 2012 avec une clause additionnelle à la police française d'assurance maritime sur corps de navire qui stipule : « *sont exclus les pertes et dommages, recours de tiers ou dépenses résultant directement ou indirectement de l'utilisation ou de l'exploitation, avec l'intention de causer des dommages, de tout ordinateur ou équipement informatique, programme ou logiciel informatique, programme malveillant, virus informatique ou processus informatique, ou tout autre système électronique* »

21. Cette exclusion se retrouve dans la couverture des P&I Clubs. Certains vont reprendre mot à mot la clause 380. Il faut également prendre en compte dans les règles des P&I Club les clauses spécifiques sur le connaissement électronique qui excluent la couverture dans le cas où le mécanisme électronique permettant d'utiliser les documents n'a pas été approuvé préalablement par le club de protection.

22. Néanmoins le risque cybernétique étant de plus en plus important, les assureurs essaient de mettre en place des nouveaux produits d'assurance.

Souscrire un tel risque n'est cependant pas facile. Il faudrait des compétences techniques et le souscripteur devrait systématiquement se rapprocher du directeur informatique de la société. Plusieurs questions de posent en particulier sur les obligations qui vont être la charge de l'assuré mais également sur l'étendue de la couverture d'assurance. Souvent les assureurs vont couvrir les frais d'expertise technique, les pertes indirectes qui pourraient être liées au piratage, les frais de justice, les frais de notification à la clientèle, les frais de surveillance de données, les frais de

restauration d'image ou encore les frais d'extorsion.

23. Ce n'est pas tout, quelles données vont être protégées ? Uniquement celles en France ou celles qui sont à l'étranger ? La couverture doit-elle jouer si l'assuré est lié indirectement par l'intermédiaire d'un de ses employés à la fraude ou encore si l'action à des impacts matériels sur l'entreprise ? Dans quel délai le sinistre doit-il être déclaré ? Les produits d'assurance qui peuvent exister évoluent très rapidement mais le marché cherche encore ses marques.

24. Une récente affaire aux Etats Unis illustre la difficulté de l'assurance du cyberisque. En 2013, une organisation gérant des hôpitaux en Californie a été victime d'une attaque informatique, qui a entraîné le vol de plusieurs milliers de dossiers médicaux. Ce vol a été facilité par le fait que les dossiers étaient stockés sur un système informatique accessible par Internet sans mécanisme de sécurité ni cryptage. L'assureur de la clinique a engagé une action devant un Tribunal fédéral à Los Angeles en soutenant qu'il n'était pas obligé de couvrir au motif qu'il y aurait eu dans la police une clause d'exclusion car l'assuré n'avait pas recouru à des « *pratiques de sécurité minimum* » (« *Minimum Required Practices* »). La clinique aurait dû régulièrement maintenir des mécanismes de sécurité sur son système, et en ne le faisant pas elle s'est exposée à ce risque de vol (22) . Le 2 juillet 2015, le tribunal se déclarait incompétent car l'assureur n'avait pas respecté les termes de la clause de médiation prévue par la police (23) . La définition du standard minimum reste ouverte. Serait-elle la même pour une clinique que pour un armateur, pour un port, ou pour un navire ?

IV. - CYBERSECURITÉ ET RESPONSABILITÉS

25. Il y tout d'abord la responsabilité du pirate. Celui-ci supporte une responsabilité pénale qui est prévue aux articles 323-1 et suivants du Code pénal qui sanctionnent le fait d'accéder, de se maintenir frauduleusement, d'entraver, ou de fausser le fonctionnement de tout ou partie d'un système de traitement automatisé de données. Cet article a récemment été appliqué dans un arrêt de la Chambre Criminelle qui a rejeté le pourvoir fait par le prévenu qui s'était introduit sur le site extranet de l'Agence de sécurité sanitaire de l'alimentation et a téléchargé des données qu'il avait fixées sur différents supports et diffusées à des tiers (24) . Le Tribunal de correctionnel d'Amiens a récemment condamné un pirate qui avait développé un virus informatique qui avait infecté près de 25.000 téléphones (25) .

26. A cette responsabilité pénale s'ajoute une responsabilité civile. Mais il reste que la mise en jeu de la responsabilité du pirate est assez hypothétique compte tenu de la difficulté de retrouver le responsable de l'attaque, surtout s'il est à l'étranger.

27. La victime peut-elle également être responsable ? La réponse est positive. La responsabilité de la victime pourrait être envisagée à l'égard de ses cocontractants mais également à l'égard des tiers sur le fondement de l'article 1382, la faute pouvant être constituée par l'absence de protection du système informatique, ou sur le fondement de l'article 1384. Le risque de piratage informatique pourrait difficilement être considéré comme un cas de force majeure, irrésistible, extérieur aux parties et surtout imprévisible (26) .

28. En matière maritime on pourrait même se demander si une cyberattaque ne pourrait pas affecter la navigabilité d'un navire. La navigabilité doit être entendue de manière large puisqu'elle couvre non seulement la composition de l'équipage mais également l'état technique du navire (27) . Par exemple on s'est récemment demandé si la présence de gardes armés à bord d'un navire pouvait avoir des conséquences sur sa navigabilité. La même question pourrait se poser à l'égard de la sécurité informatique. Une cyberattaque pourrait aussi avoir des conséquences sur le caractère sûr ou non d'un port si elle expose le navire à un danger qui ne pourrait pas être surmonté par une bonne pratique maritime.

29. Enfin se pose le problème de la responsabilité du prestataire informatique qui est débiteur d'une obligation de conseil et de moyen. Par analogie on peut évoquer la jurisprudence rendue en matière de piratage de systèmes téléphoniques où des clients ont constaté sur leurs factures qu'il y avait des appels passés à destination de pays exotiques. Les tribunaux ont reconnu la responsabilité du prestataire qui n'avait pas attiré l'attention du client sur la nécessité d'avoir un mot de passe et de sécuriser son réseau. Dans un arrêt *SARL Design & Solution c. Waterlot Bernard Equipements Téléphonique* du 16 avril 2015, la Cour d'appel de Poitiers a retenu la responsabilité du prestataire qui n'avait pas donné de conseil sur les différentes fonctions du poste à son client qui n'était pas un professionnel en matière de téléphonie. Le client a été indemnisé car il avait perdu une chance de pouvoir bénéficier d'une protection plus efficace dès l'installation de son système de communication.

30. Dans un arrêt du 25 mars 2014, *Les Films de la Croisade v. Nerim*, la Cour d'appel de Versailles a condamné le responsable de la maintenance du système de télécommunication (28) . La responsabilité de l'installateur a été exclue car il n'y avait aucune défaillance du matériel. Au contraire le responsable de la maintenance n'avait pas respecté ses obligations d'information et de conseil, et n'avait pas informé le client sur les risques de piratages ou encore, sur la nécessité de mettre à jour ses logiciels ou de changer les codes.

31. On peut enfin évoquer la jurisprudence rendue dans ce qu'on a coutume d'appeler la « *fraude au président* » qui va souvent commencer par un piratage et un email frauduleux censé émaner du responsable d'une entreprise. Par un jugement du 30 octobre 2014, le Tribunal de commerce de Paris a reconnu la responsabilité d'une banque qui avait émis un virement sur le fondement d'instructions frauduleuses, en retenant un manque de vigilance face à un ordre de virement d'un montant inhabituel, à destination d'un compte inhabituel (29) .

(1)

Texte d'une allocution prononcée dans le cadre du programme du XXII^{ème} colloque de la « Journée Ripert » organisé par l'Association Française du Droit Maritime (AFDM), Paris 29 juin 2015.

(2)

Comment Anvers a été piraté et s'en est sorti, www.lalibre.be, 23 octobre 2013 ; *How hackers attacked the Port of Antwerp,* Tradewinds, 1er août 2014 ; *Hackers deployed to facilitate drugs smuggling*, Europol Public Information, juin 2013.

(3)

Spoofing a Superyacht at Sea, news.utexas.edu, 30 juillet 2013.

(4)

P. Estur, *Long-Cours - Navires et Marins,* Pen-Duick, Versailles, 1987, p. 94.

(5)

Ibid., p. 96/97.

(6)

Voir par exemple à Rouen : «*AP+ est le système d'information qui généralise l'application de règles de gestion pour le traitement en temps réel des opérations import, export et transbordement de toutes les marchandises passant par la place portuaire rouennaise. En agrégeant les données sur les mouvements et les changements de statut de la marchandise, AP+ assure la traçabilité en temps réel de l'ensemble de la chaîne logistique* » (www.uprouen.org).

(7)

Exclusive : Iran shipping signals conceal Syria ship movements, www.reuters.com, 6 décembre 2012.

(8)

« *Cyber security on board merchant vessels and at major ports is 10 to 20 years behind the curve compared with office-based computer systems, leaving them wide open to an ever-increasing range of threats, according to the director of information protection at advisory firm KPMG* », Lloyd's List, 6 mai 2014.

(9)

Sophisticated scams highlight growing cyber risk to shipping, Tradewinds, 10 octobre 2014 :» *Marine shipping providers were also the target of so-called spear-phishing campaigns by China's People's Liberation Army. Such attacks use spoof e-mails targeted at a single company to secure access to confidential data... Foreign governments regularly probe computer networks of the US Defense Department, and logistics providers, including ship operators, are a prime target. That is because in the event of major conflict, military resupply networks are expected to be a front-line target of cyber warfare, according to the Senate report.*»

(10)

On parle de « *hacktivists* », mot formé de «hacker» et «activistes».

(11)

Ensuring security in and facilitating international trade - measures toward enhancing maritime cybersecurity, OMI, I:\FAL\39\7.doc.

(12)

Cf. *supra.*, para 16.

(13)

44 USC § 3541 et s.

(14)

Executive Order - Improving Critical Infrastructure Cybersecurity, accessible sur le site www.whitehouse.gov.

(15)

US Coast Guard, *Cyber Strategy,* Juin 2015, Washington (https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf).

(16)

Note technique du 25 février 2015 relative à la certification de sûreté d'un navire battant pavillon français (guide à destination des armateurs de navire sous pavillon français), B. O. Développement Durable n^{o} 5 du 25 mars 2015.

(17)

*Cyber solution ? A consortium of international shipping associations is drawing up guidelines to tackle cyber security issues faced by the industry,*www.Tradewindsnews.com, 16 avril 2015.

(18)

P. de La Morinerie, *Assurance maritime et transports, les enjeux actuels*, www.cesam.org.

(19)

Cyber Risk - A Joint Hull Committee paper in conjunction with Stephenson Harwood, septembre 2015 ; *Cyber attack on shipping 'foreseeable'*, Lloyd's List, 3 septembre 2015.

(20)

AGCS Marine Insurance Company v. World Fuel Services, Inc. et al., SDNY, N° 1 :14-cv-05902 ; *WFS In Court Over $18M Bunker Scam Claim*, www.shipandbunker.com, 13 octobre 2014.

(21)

N.Y. Court : Zurich not obligated to defend Sony units in data breach litigation, www.insurancejournal.com, 17 mars 2014.

(22)

Columbia Casualty Company v. Cottage Health System, C.D.Cal., n° . CV 5-03432.

(23)

*Insurer's Failure To Mediate Kills Its $4M Data Breach Claims,*www.law360.com, 20 juillet 2015.

(24)

Cass. crim., 20 mai 2015, n° 14-81.336 ; *Maintien frauduleux dans un fichier et vol de données : l'occasion peut faire le larron*, Dalloz actualités, 5 juin 2015.

(25)

Le hacker picard de 20 ans condamné à 6 mois ferme, www.linformaticien.com, 9 novembre 2012.

(26)

Cass. com. 25 novembre 1997, *D.* 1999.16 : «*le risque de contamination par virus était un risque connu dans le domaine informatique ayant suscité une abondante littérature ainsi que la mise au point de logiciel de détection et de suppression des virus et d'une véritable stratégie de défense à l'égard de ces risques d'invasion*».

(27)

CAMP sentence n° 768, 31 mars 1990, *DMF* 1991. 118 : « *Entendue dans son sens large, la navigabilité concerne autant la composition de l'équipage que l'état technique du navire* ».

(28)

Versailles, 25 mars 2014, n° 12/07079.

(29)

Les banques en première ligne face à la « fraude au président », www.lesechos.fr, 29 janvier 2015 ; Trib. com. Paris, *SAS Etna Industries c. CIC*, 30 octobre 2014, RG : 2013075398