CHAPITRE 16 - Le navire objet d'une attaque cybernétique, étude du risque juridique

Gersende Le Dimna

CHAPTER 16
Le navire objet d'une attaque cybernétique, étude du risque juridique

Gersende LE DIMNA
Enseignante en droit
École Nationale Supérieure Maritime (ENSM), site du Havre
(France)

Abstract: *The Maritime branch is highly dependent upon cyberspace. Approximately 80% of ISeaT1 relies on wireless technology.*

The same percentage is observed for the world's main transport means for goods, maritime transport.

Maritime safety cannot avoid struggling against cybercriminality, which can consist of controlling a ship or pirating navigational instruments. Some of the incurred risks are known, such as collision, grounding, piracy, robbery. Some are not yet known, since IT developments and criminals' ingenuity are continually growing.

If the maritime industry is now aware of its exposure, this consciousness is quite late and there are very few international conventions relating to it.

The following study offers its readers a legal analysis for both civil and criminal law.

Résumé : *Le secteur maritime est extrêmement dépendant du cyber espace : 80 % de la marétique reposent sur la technologie sans fil.*

C'est ce même pourcentage qui est constaté en ce qui concerne le principal mode de transport mondial de marchandises, à savoir le transport maritime.

La lutte contre la cyberdélinquance fait pleinement partie de la sécurité maritime. Elle consiste par exemple en une prise de contrôle d'un navire, ou encore un piratage des instruments de navigation. Certains risques sont identifiés : abordage, pollution, échouement, piraterie, vols ; d'autres pas encore, tellement le développement des systèmes informatiques et l'ingéniosité des délinquants sont grandissants.

Si l'industrie maritime a désormais compris l'exposition qui est la sienne, cette prise de conscience est tardive et les textes internationaux sont encore rares.

L'étude présentée propose au lecteur une analyse des solutions juridiques envisageables en droit civil ou en droit pénal.

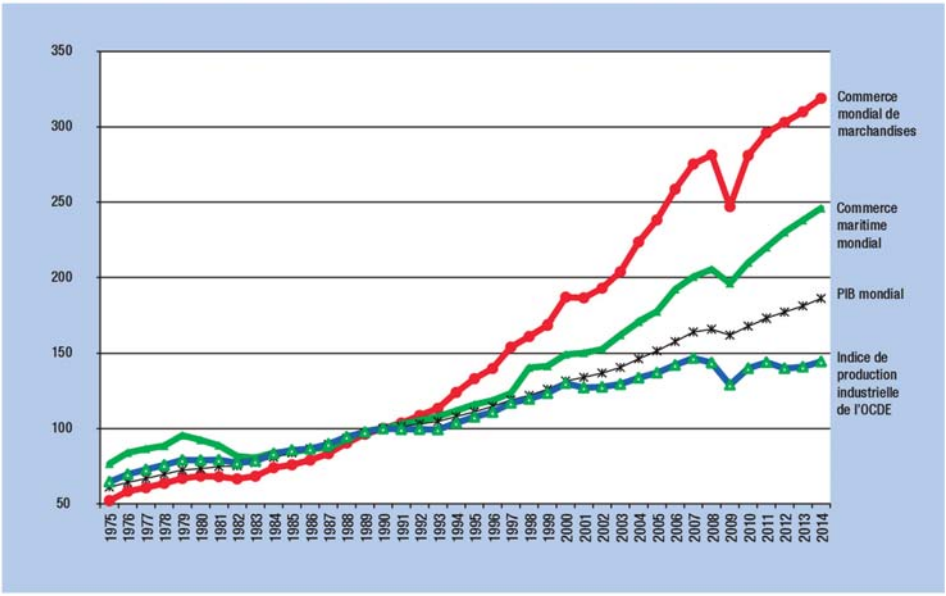




Le transport maritime est à la fois le support et la conséquence de la mondialisation des échanges.

Inutile de revenir sur les chiffres du commerce maritime qui sont connus. Bon gré, mal gré, ce sont de 75 à 90 % des échanges internationaux qui transitent par la mer.

Graphique 1.1 Indice de production industrielle de l'OCDE et indicateurs du PIB mondial, du commerce mondial de marchandises et du commerce maritime mondial, 1975-2014 (1990 = 100)



Source : Graphique établi par le secrétariat de la CNUCED, à partir des sources suivantes : *Principaux indicateurs économiques de l'OCDE*, juin 2015; Département des affaires économiques et sociales de l'ONU, 2015; LINK Global Economic Outlook, juin 2015; CNUCED, diverses éditions de l'Étude sur les transports maritimes; tableau A1a) « Exportations mondiales de marchandises, production et produit intérieur brut 1950-2012 », tableau A1a de l'appendice du rapport de l'OMC (« Statistiques du commerce international 2013 »); et communiqué de presse 739 de l'OMC, 14 avril 2015.

Source : RMT 2015, page 6

Or, le secteur maritime est extrêmement dépendant du cyber espace. Ainsi que le rappelait le livre bleu de la marétique[1] en 2013, « les acteurs du secteur maritime, portuaire et fluvial font face à une concurrence intense et doivent trouver, chacun dans leur métier, des gisements de compétitivité ». Le livre bleu ajoute : « Dans les secteurs des Technologies de l'Information et de la Communication, de nombreuses innovations permettent d'améliorer la circulation de l'information et d'optimiser les chaînes de valeur de plus en plus complexes ».

1) Consultable sur http://fr.slideshare.net/antoinefrancin/livre-bleu-v35

La marétique, c'est-à-dire l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes fluviales et portuaires, repose pour 80% sur la technologie sans fil.

Ces chiffres parlent d'eux-mêmes, le transport maritime est extrêmement dépendant des systèmes informatisés sans fil. La sécurité maritime et plus largement le commerce international sont directement et hautement menacés par la cyber délinquance.

La lutte contre la cyber délinquance fait pleinement partie de la sécurité maritime. Cette dernière se manifeste par exemple par une prise de contrôle d'un navire, ou encore un piratage des instruments de navigation. Certains risques sont facilement identifiés : abordage, pollution, échouement, piraterie, vols ; d'autres pas encore, tellement le développement des systèmes informatiques et l'ingéniosité des délinquants sont grandissants.

Bien qu'ayant compris son exposition, l'industrie maritime est, comparativement aux industries terrestres, très en retard dans la lutte contre la cyber délinquance.

L'OMI a décidé de se saisir du sujet, en impliquant conjointement le Comité de la sécurité maritime et le Comité de simplification des formalités.

Ces initiatives ont abouti à l'adoption, le 1er juin, de directives intérimaires sur la gestion des cyber-risques maritimes[2]. Ces directives ne sont pas juridiquement contraignantes, mais les États sont encouragés à les suivre afin de protéger les transports maritimes des risques particuliers pesant sur eux.

L'Union européenne a pour sa part déjà adopté certaines mesures, dont notamment une directive en date 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[3]. Cette directive insiste sur le caractère déterminant de la lutte pour la sécurité des réseaux, son premier paragraphe annonçant que « les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont *essentielles*[4] aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur ». La cyber délinquance menace, cela est dit très clairement, le marché intérieur de l'Union.

---

2) MSC.1/Circ.1526.

3) Directive (UE) 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.

4) Nous soulignons.

Quelques paragraphes plus loin, le Parlement et le Conseil reconnaissent que : « les moyens existants ne sont pas suffisants pour assurer un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'Union »[5].

Et proposent donc d'adopter une démarche globale au niveau de l'Union, afin de garantir des exigences minimales et communes à l'adresse des « opérateurs de services essentiels et aux fournisseurs de services numériques »[6].

Équivalents aux opérateurs d'importance vitale français[7, 8], les opérateurs de services essentiels sont, au sens de la directive, notamment les banques, les infrastructures de marchés financiers, mais aussi le transport par voie d'eau.

Logiquement, la directive s'adresse à tous les États membres, fixe des obligations relatives à l'adoption de stratégies nationales de sécurité des réseaux et systèmes d'information, et organise des formes de coopérations interétatiques et opérationnelles.

Que des organisations supranationales se saisissent du sujet révèle la première des difficultés liées à la cybersécurité et la cyber délinquance : celles-ci sont par nature internationales. Certes, cela pose des difficultés en termes de lutte opérationnelle, mais avant cela, l'internationalité se heurte aux oppositions qui existent entre ses acceptions domestique et internationale, et, corrélativement, aux problèmes de compétence juridictionnelle. Sur ce point, il est intéressant de relever que la directive du 6 juin pose dans son article 13 la compétence de l'Union pour conclure avec des pays tiers ou des organisations internationales des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération[9].

---

5) ibid. § 5.

6) Ibid. § 6.

7) La directive ne définit pas les opérateurs de services essentiels et ne cite que ces deux services. Elle met à la charge des États membres de définir ces OSE avant le 9 novembre 2018, en tenant compte de 3 critères : l'entité doit fournir un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ; la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et, un incident aurait un effet disruptif important sur la fourniture dudit service (art. 5 § 2). Cette liste devra être réexaminée au moins tous les deux ans (art. 5 § 5).

8) Art. L. 1332-1 C. Déf. : « Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative ». Un arrêté Premier ministre du 2 juin 2006 modifié par un arrêté du 3 juillet 2008 fixe une liste de 12 secteurs d'importance vitale, parmi lesquels figure le transport.

9) Le groupe de coopération est institué par la directive afin de soutenir et faciliter la coopération stratégique

Il n'existe au jour d'aujourd'hui qu'une seule convention internationale en la matière relative à la lutte contre la cybercriminalité, la Convention de Budapest sur la lutte contre la cybercriminalité, signée le 23 novembre 2001 et complétée par un Protocole additionnel en 2003[10], adoptée dans le cadre du Conseil de l'Europe. La Convention est entrée en vigueur assez rapidement, le 1er juillet 2004. Cette rapidité était voulue par les signataires : la Convention prévoyait en effet qu'elle entrerait en vigueur à la condition d'obtenir 5 ratifications – ce qui est relativement peu pour une convention multilatérale – dont au moins 3 États du Conseil de l'Europe. Cette Convention, qui fixe des obligations aux États qui l'ont ratifiée, a, au 1er octobre 2016, été ratifiée par 52 États, dont 10 États non membres du Conseil de l'Europe. L'ouverture de la Convention à des États non membres du Conseil de l'Europe est bien évidemment la bienvenue pour la coopération et la coordination interétatique.

Notons par ailleurs que le système de la Convention a institué un Comité de la Convention sur la cybercriminalité (dit « Comité C-TY ») sur le fondement de l'article 46 § 1 de la Convention afin de représenter les États parties à la Convention de Budapest sur la cybercriminalité. Ce Comité doit être consulté afin de faciliter l'usage et la mise en œuvre de la Convention, l'échange d'informations et l'examen de tout futur amendement à la Convention.

La question de l'adoption de nouveaux instruments juridiques à l'échelle mondiale par le biais de l'ONU semble aujourd'hui être au point mort, faute de consensus sur la nécessité d'un tel instrument entre les États[11].

La deuxième difficulté liée à la cybersécurité des navires réside dans l'incapacité à appréhender tous les risques induits. Certains sont cependant d'ores et déjà connus.

En particulier, le livre blanc sur la cybersécurité des navires publié le 4 janvier 2016 conjointement par le BIMCO, l'ICS, INTERTANKO, INTERCARGO et la Cruise Lines International Association a ainsi identifié 6 failles pour le transport maritime.

Ces failles vont venir cibler les systèmes de bord, c'est-à-dire les systèmes de navigation, les systèmes de contrôle, ou encore les systèmes de communication et de surveillance, et, à travers ces derniers, les documents requis pour le départ et l'arrivée des personnes et des marchandises[12].

---

et l'échange d'informations entre les États membres, renforcer la confiance, et parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

10) Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, signé à Strasbourg le 28 janvier 2003.

11) http://www.un.org/press/fr/2015/soccp365.doc.htm, consulté le 1er octobre 2016.

12) Exigence posée par la norme 2.1 de la Convention visant à faciliter le trafic maritime international, du

Cette liste est pourtant loin d'être exhaustive. Les navires vont continuer à intégrer toujours plus de systèmes informatisés à bord, jusqu'à ce qu'un jour, l'on arrive au point le plus abouti, c'est-à-dire à l'avènement des drones maritimes.

La troisième difficulté consiste en l'identification des menaces cybernétiques, extrêmement variées, qui pèsent sur l'environnement maritime. Le Document présenté par le Canada, les États-Unis, les Îles Marshall, le Japon, le Libéria et la Norvège au Comité pour la Sécurité Maritime et publié par l'OMI en février dernier[13] pointe les menaces suivantes :

- le terrorisme, par idéologie et désir de désorganisation d'un système établi,
- la criminalité organisée, motivée par les gains financiers,
- les hacktivistes, qui par narcissisme, qui par idéologie,
- les travailleurs en place mal intentionnés, par vengeance ou par appât du gain,
- les travailleurs en place innocents, qui n'ont eux, aucune motivation, mais qui peuvent nuire aux systèmes informatisés à leur insu,
- les clients, concurrents et partenaires commerciaux, appâtés par le gain, l'espionnage industriel, ou bien encore, à leur insu,
- enfin, les défaillances techniques et autres incompatibilités des logiciels.

Ajoutons à cette liste les menaces suivantes :

- les *script kiddies* qui sont des néophytes reproduisant et utilisant des infiltrations informatiques mises au point par d'autres. Leur motivation est essentiellement narcissique ;
- les phénomènes naturels, tels que des tremblements de terre, catastrophes naturelles, etc. ;

9 avril 1965 (dite Convention FAL).

13) MSC 96/4/2 du 9 février 2016.

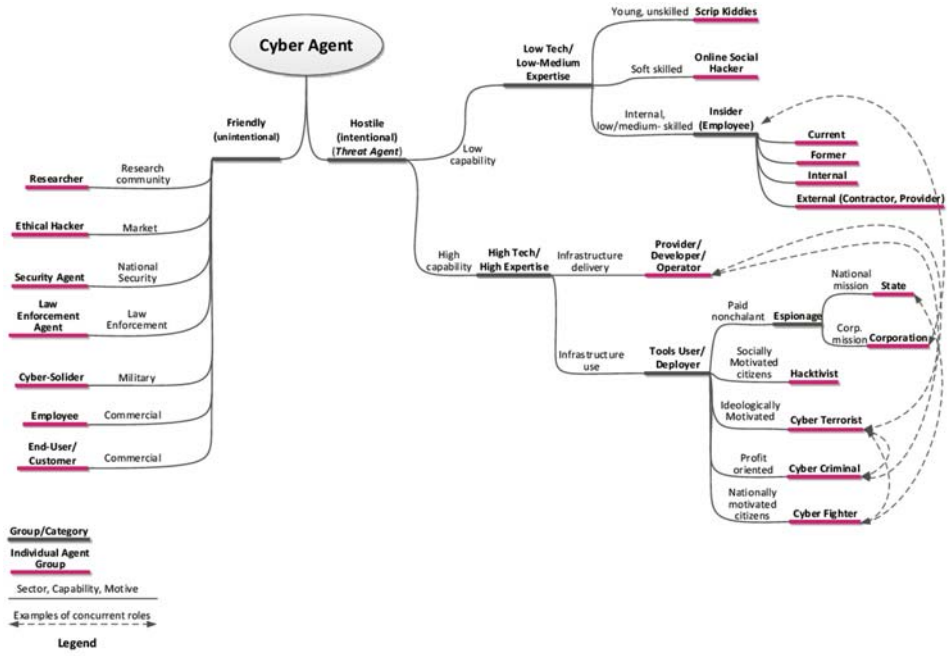


Figure 5: A proactive model as overview of threat agents

Source : Threat Landscape 2015, ENISA

Enfin, notons que ces menaces peuvent prendre des formes très diverses, être indifféremment ciblées ou non ciblées. Parmi les attaques non ciblées, relevons les rançongiciels, le balayage de port, les chevaux de Troie, l'attaque de trou d'eau, et, parmi les attaques ciblées, les DDoS (l'attaque par déni de service distribué) ou l'hameçonnage ciblé.

L'ENISA, dans son dernier rapport sur les principales menaces[14], dresse un tableau assez complet de celles-ci :

14) ENISA Threat Landscape 2015, disponible en téléchargement sur https://www.enisa.europa.eu/publications/etl2015

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
16. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
17. Web-based attacks	↑	2. Web based attacks	↑	→
18. Web application /Injection attacks	↑	3. Web application attacks	↑	→
19. Botnets	↓	4. Botnets	↓	→
20. Denial of service	↑	5. Denial of service	↑	→
21. Spam	↓	6. Physical damage/theft/loss	⊃	↑
22. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
23. Exploit kits	↓	8. Phishing	⊃	↓
24. Data breaches	↑	9. Spam	↓	↓
25. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
26. Insider threat	⊃	11. Data breaches	⊃	↓
27. Information leakage	↑	12. Identity theft	⊃	↑
28. Identity theft/fraud	↑	13. Information leakage	↑	↓
29. Cyber espionage	↑	14. Ransomware	↑	↑
30. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 2: Overview and comparison of Current Threat Landscapes 2014 and 2015

Source : Threat Landscape 2015, ENISA

Nous voyons bien que les risques sont extrêmement variés.

Toute atteinte à ces systèmes engendre un risque très élevé avec des conséquences potentiellement catastrophiques en termes de perte de vies humaines, d'atteinte à l'environnement et aux intérêts économiques non seulement d'entreprises privées mais aussi d'États. Ainsi, objet de la menace, le navire sera à l'origine à la fois de poursuites pénales et de demandes d'indemnisation au civil.

1. Responsabilité pénale

La typologie générale des infractions cybernétiques est importante :

1. les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ; cette catégorie regroupe les accès illégaux (piratage, craquage), l'acquisition illégale de données, l'interception illégale, l'atteinte à l'intégrité des données, les atteintes à l'intégrité du système, etc.
2. les infractions proprement informatiques ;
3. les infractions se rapportant au contenu des informations (ex : pédopornographie, jeux en ligne, etc.) ;
4. les infractions liées aux atteintes à la propriété intellectuelle.

La cyber délinquance maritime est touchée principalement par la première catégorie d'infractions, sans pour autant être épargnée par les autres. En particulier, 4 infractions sont susceptibles d'être retenues contre le cyber délinquant, les 3 premières sont des infractions informatiques, que l'on retrouve aux articles 323-1 à 323-4 du Code pénal, alors que la dernière est une infraction spécifique aux moyens de transports.

A. Infractions relatives aux systèmes de traitement automatisé de données (STAD)

Trois infractions peuvent être envisagées, alors qu'il existe une pluralité de personnes pouvant être poursuivies.

1) Typologie des infractions

Le droit pénal français permet de poursuivre et condamner trois agissements fautifs.

- L'accès ou maintien frauduleux dans un système de traitement automatisé de données

Ils sont réprimés par l'article 323-1 du Code pénal, qui dispose :

> « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende.
>
> Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.
>
> Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère

personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 euros d'amende ».

Le droit pénal étant un droit d'exception, il doit s'entendre strictement. Il faut donc s'entendre sur les termes de l'infraction. En particulier sur la notion de « système de traitement informatisé de données » qui ne reçoit pas de définition juridique, bien que celle-ci fût discutée au Sénat lors des débats parlementaires de la loi Godfrain[15, 16], à l'origine de l'infraction. La doctrine s'entend en général pour retenir que le STAD doit être un ensemble composé d'éléments intégrés dans un système d'une part (par ex. un ordinateur, un logiciel et des données, ou bien un réseau Wi-Fi), et que cet ensemble composé doit avoir pour fonction un traitement automatisé de données, défini comme étant « *l'ensemble des opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'édition de données et, d'une façon générale, leur exploitation* »[17].

Il est intéressant de noter que le texte pénal n'exige pas que ce STAD soit protégé.

L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation. L'autorisation donnée exclut l'infraction. Cette autorisation peut résulter de la loi, du contrat ou de la volonté du « maître du système », grossièrement celui qui détient les droits sur le STAD.

L'infraction sera aussi retenue si l'autorisation de l'accès au système a été détournée à des fins déterminées.

Les modalités de l'accès sont par ailleurs indifférentes.

Le maintien vise quant à lui l'hypothèse où l'accès serait autorisé, mais que les opérations réalisées ne le seraient pas elles-mêmes, ou bien que l'accès aurait été rendu possible fortuitement. C'est le seul maintien qui est sanctionné, la loi n'oblige pas à utiliser le système pour autoriser la condamnation. Ainsi, ne pas mettre fin à sa présence dans le système est sanctionnable.

---

15) Loi nº 88-19 du 5 janvier 1988.

16) La définition suivante avait été adoptée par le Sénat : « tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés ».

17) Arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique. La donnée étant définie comme *« la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement ».*

L'infraction par ailleurs est formelle. Elle n'a donc pas besoin de provoquer un dommage pour être constituée, à la manière d'un empoisonnement qui ne requiert pas que la victime soit malade voire morte.

Enfin, l'infraction est intentionnelle. Il reviendra au ministère public de prouver que celui qui s'est introduit ou maintenu dans le système l'a fait volontairement, alors même qu'il savait que cet accès ou ce maintien étaient interdits.

- L'atteinte à l'intégrité du système

Prévue par l'article 323-1 du C. Pén. comme circonstance aggravante de l'accès ou du maintien frauduleux dans un STAD, l'article 323-2 du Code pénal érige en infraction autonome « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » et la punit de cinq ans d'emprisonnement et de 150 000 euros d'amende.

La peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État.

C'est l'entrave ou le fait de fausser le fonctionnement du STAD qui est sanctionné. Cette infraction vise aussi bien la destruction de fichiers, de programmes, de sauvegardes, que la saturation d'un système.

Ici encore, les termes utilisés par le législateur ne reçoivent pas de définition légale et leur absence nuit à la sécurité juridique. Il pourra s'agir aussi bien d'une simple altération du système, comme de l'impossibilité totale d'utiliser le système, l'atteinte portée peut être intellectuelle ou matérielle. Quant à savoir si l'atteinte doit être un acte positif ou si une simple abstention peut suffire à caractériser l'infraction, il n'existe pas de consensus. La jurisprudence a tranché dans le sens que l'acte devait être positif[18], alors que la doctrine n'est pas unanime.

- L'atteinte à l'intégrité des données

Cette infraction, prévue à l'article 323-3 du C. Pén., punit de 5 ans d'emprisonnement et 75 000 euros d'amende le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient. La peine est portée à sept ans d'emprisonnement et à 300 000 euros d'amende lorsque l'infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État.

18) CA Poitiers, 20 janvier 1998.

L'article regroupe donc deux types d'actes sous la même qualification : l'introduction de données et leur suppression, mais écarte la copie de son champ d'application[19].

La première consiste à incorporer des caractères informatiques nouveaux sur un support du système[20].

Le caractère intentionnel de l'infraction est incontestable. Mais l'introduction de données, en plus d'être intentionnelle, doit être frauduleuse, c'est-à-dire que l'auteur doit avoir la conscience et la volonté de causer un préjudice à autrui. La preuve en est parfois malaisée, et ne pourra donc pas être retenue contre les travailleurs en place innocents qui ont altéré le STAD en introduisant par exemple une clé USB infectée par un virus ou qui auraient téléchargé un logiciel lui-même atteint d'un virus nuisible au système d'exploitation.

C'est cette infraction par exemple qui a été retenue contre Jérôme Kerviel par la Cour d'appel de Paris puis par la Cour de Cassation[21].

La suppression ou la modification de données ne présente pas de difficultés spécifiques. Il faut comprendre ces termes dans leur acception commune : il s'agit de l'effacement ou de changements apportés à l'état des données existantes sans en modifier la nature. L'infraction est constituée notamment lorsqu'un virus a été introduit dans un STAD.

2) Auteurs possibles

L'auteur peut être une personne physique, un « pirate » qui agit seul. Il peut agir en bande organisée, en « groupe ». Il doit y avoir alors une entente entre plusieurs personnes, concrétisée par un ou plusieurs faits matériels ayant pour finalité de commettre des atteintes à un STAD.

L'auteur peut également être une personne morale. Ainsi, le fournisseur d'accès[22] peut se rendre coupable de ces infractions lorsqu'il est à l'origine de la demande de transmission litigieuse, sélectionne le destinataire ou sélectionne ou modifie les contenus faisant l'objet des transmissions[23].

---

19) La copie n'en est pas moins sanctionnée pénalement. Cf. art. L. 335-3 CPI (copie de logiciels).

20) R. Gassin, *Informatique (Fraude informatique)*, Répertoire pénal Dalloz, 1989.

21) Paris, 24 octobre 2012, et Crim., 19 mars 2004, nº 12-87.416.

22) Défini comme étant celui *« dont l'activité est d'offrir un accès à des services de communication au public » (L. 21 juin 2004, art. 6, I, 1).*

23) Art. 32-3-3 Code des postes et communications électroniques : « *Toute personne assurant une activité de transmission de contenus sur un réseau de communications électroniques ou de fourniture d'accès à un réseau de communications électroniques ne peut voir sa responsabilité civile ou pénale engagée à*

La responsabilité pénale du fournisseur d'hébergement[24] va aussi pouvoir être retenue si la preuve est rapportée qu'il a eu connaissance de l'activité ou de l'information illicite, et qu'il n'a pas fait cesser cette activité ou retirer cette information illicite[25].

La tentative, caractérisée par un commencement d'exécution et l'absence de désistement volontaire, est punissable des mêmes peines que si l'infraction avait été consommée[26].

Le complice, c'est-à-dire celui qui a apporté une aide à l'auteur sans pour autant que son action ait été déterminante dans la consommation de l'infraction, est également punissable des mêmes peines que l'auteur de l'infraction.

Notons cette décision rendue récemment par la chambre correctionnelle du TGI d'Annecy le 4 décembre 2015, qui a condamné un administrateur système pour accès et maintien frauduleux dans un système de traitement automatisé de données (STAD) ainsi qu'atteinte au secret des correspondances parce qu'il avait abusé de ses privilèges pour accéder à des répertoires informatiques à des fins autres que professionnelles, puis communiqué les documents trouvés à une inspectrice du travail. L'inspectrice du travail, qui avait diffusé largement ces documents, a été condamnée pour recel de courriers électroniques et pour atteinte au secret professionnel.

B. Le détournement de navire

Classé parmi les atteintes aux libertés de la personne, le détournement de navire est défini par l'article 224-6 du Code pénal comme étant « *le fait de s'emparer ou de prendre le contrôle par violence ou menace de violence d'un aéronef, d'un navire ou de tout autre moyen de transport à bord desquels des personnes ont pris place, ainsi que d'une plate-forme fixe située sur le plateau continental* ». L'infraction est punie de 20 ans de réclusion criminelle (et est donc passible de la Cour d'assises), sachant que la peine peut être assortie d'une période de sûreté allant jusqu'à la moitié de la

---

raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission. »

24) L'hébergeur est une « *personne physique ou morale qui assure, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services* » *(L. 21 juin 2004, art. 6. I, 2).*

25) L'éditeur est défini comme étant « *la personne qui détermine les contenus qui doivent être mis à la disposition du public sur le service qu'il a créé ou dont il a la charge* » TGI Paris, 3 juin 2008.

26) Pour la jurisprudence, le commencement d'exécution peut être soit un acte « *tendant directement à l'infraction avec l'intention de la commettre* » *(Cass. crim., 5 juill. 1951)*, soit un acte « *ayant pour conséquence directe et immédiate de consommer le crime, celui-ci étant entré dans la période d'exécution* » *(Cass. crim., 25 oct. 1962)*, soit enfin un acte qui tend « *directement et immédiatement à la réalisation de l'infraction projetée* » *(Cass. crim., 19 juin 1979).*

peine, voire, par décision spéciale, des deux tiers de la peine. La peine est portée à trente ans de réclusion criminelle si elle est commise en bande organisée, ou à la réclusion criminelle à perpétuité si le détournement s'accompagne de tortures ou d'actes de barbarie ou s'il en est résulté la mort d'une ou de plusieurs personnes.

Contrairement à la formulation issue de l'ancien Code pénal, l'article 224-6 aujourd'hui ne requiert pas que l'auteur du détournement se trouve à bord du navire détourné. L'article est donc pleinement applicable aux cas de cyber-attaques.

S'agissant d'une infraction intentionnelle, la preuve de la volonté coupable de l'auteur doit donc être rapportée.

L'infraction vise les navires et les plates-formes fixes situées sur le plateau continental également, mais impose que des personnes y aient pris place, ce qui exclut donc les drones maritimes.

Enfin, pour que l'infraction soit constituée, l'agent doit « s'emparer » ou « prendre le contrôle » du navire ou de la plate-forme (1er élément), par violence ou menace de violences (2è élément). Les deux éléments sont cumulatifs, bien que les propositions à l'intérieur de chaque élément soient alternatives. Ainsi, pour que l'infraction soit consommée, l'agent pourra procéder soit à une appréhension directe en prenant lui-même la direction de l'engin, soit à une appréhension indirecte par l'intermédiaire de tiers comme les personnels de bord, techniques ou commerciaux (distinction entre « s'emparer » et « prendre le contrôle »), à la condition que cet acte soit accompagné de violence ou de menaces de violences contre les victimes ou leurs proches.

L'on peut se poser la question si la seule prise de contrôle ou le fait de s'emparer d'un navire peut être assimilée à de la violence. La réponse est certainement positive, les tribunaux reconnaissent constamment que la violence puisse être physique, certes, mais également psychique.

C. L'applicabilité de la loi française ?

La complexité du problème provient notamment du fait qu'aussi bien le droit maritime que les infractions informatiques sont largement empreints d'internationalisation. Or, tous ces récents développements ne sont valables que pour le seul droit français. À quelles conditions celui-ci est-il applicable ?

Le Code pénal, récemment modifié par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, nous renseigne.

Il prévoit en effet, art. 113-2 :

> « *La loi pénale française est applicable aux infractions commises sur le territoire de la République.*
>
> *L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ».

Au sens de cet article, le territoire est composé du sol terrestre et s'étend sur sa partie maritime jusqu'à la bordure extérieure des eaux territoriales (12 milles), sauf en ce qui concerne le détournement de plates-formes fixes pour lesquelles l'infraction sera constituée alors même qu'elles se situent sur le plateau continental.

La loi pénale ne distingue pas ici selon que le navire arbore un pavillon français ou étranger. Or, l'avis contentieux du Conseil d'État du 28 novembre 1806, suivi par la Convention de Montego Bay du 10 décembre 1982, accordent à l'État du pavillon la compétence pénale lorsque l'infraction est restreinte au bord. Cela ne nous semble pas contradictoire. En effet, le Conseil d'État et la CMB réservent la compétence à l'État côtier dans certaines situations, à savoir lorsque les conséquences de l'infraction s'étendent jusqu'à l'État côtier, lorsque l'infraction est de nature à porter atteinte à la paix du pays ou bien à l'ordre dans la mer territoriale, en cas de trafics illicites de stupéfiants ou de produits psychotropes (pour la seule CMB), lorsque l'assistance des autorités locales est demandée par le capitaine du navire, ou par un représentant diplomatique du navire, ou encore lorsque l'infraction cause un trouble à l'ordre public. Le détournement correspond au moins aux deux premières situations, et certainement à la dernière. La France pourra donc établir sa compétence à l'égard du navire étranger détourné dans ses eaux territoriales. La Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime[27] prévoit par ailleurs cette même compétence au profit de l'État côtier.

Concernant les navires français, la situation est bien plus claire. En effet, selon l'article 113-3 du Code pénal, « *La loi pénale française est applicable aux infractions commises à bord des navires battant un pavillon français, ou à l'encontre de tels navires*[28] *ou des personnes se trouvant à bord, en quelque lieu qu'ils se trouvent. Elle est seule applicable aux infractions commises à bord des navires de la marine nationale, ou à l'encontre de tels navires ou des personnes se trouvant à bord, en quelque lieu qu'ils se trouvent.* »

Et si le doute subsistait encore, la loi du 3 juin 2016[29] est venue créer l'article 113-2-1 du Code pénal selon lequel « *Tout crime ou tout délit réalisé au moyen d'un réseau*

---

27) Signée à Rome le 10 mars 1988 et entrée en vigueur en France le 1er février 1992.

28) L. nº 2011-525 du 17 mai 2011, art. 87-II-1.

29) L. nº 2016-731 du 3 juin 2016, art. 28 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République ». C'est-à-dire que désormais, en matière de cyberdélinquance, le droit pénal français pourra être appliqué quel(s) que soi(en)t le(s) lieu(x) où se trouvera(ont) l'agent et la victime de l'infraction, pourvu que la victime, personne physique ou morale, réside sur le territoire de la République. Ici, il ne s'agit que de résidence et non de nationalité ! Ce qui élargit grandement le champ de compétence territoriale de la loi française.

2. Responsabilité civile

Contrairement à la responsabilité pénale qui vise à punir l'agent, et qui est exercée par l'État au bénéfice de la société, la responsabilité civile consiste à établir les mécanismes de réparation envers ceux qui ont subi un dommage.

Elle trouve sa source dans deux fondements : la responsabilité civile contractuelle, là où il existe un contrat, et la responsabilité civile délictuelle, là où il n'en existe pas.

A. La responsabilité civile délictuelle

Il s'agit ici d'identifier quels sont ceux qui ne sont pas liés contractuellement avec l'armateur, entendu au sens de l'article L. 5511-1 du Code des transports, c'est-à-dire « *toute personne pour le compte de laquelle le navire est armé. (…) le propriétaire du navire, ou tout autre opérateur auquel le propriétaire a confié la responsabilité de l'exploitation du navire, indépendamment du fait que d'autres employeurs ou entités s'acquittent en son nom de certaines tâches* ».

Deux possibilités éventuelles : le sous-traitant et l'auteur de l'infraction.

1) Les sous-traitants

La sous-traitance est organisée par la loi n° 75-1334 du 31 décembre 1975, qui la définit comme « *l'opération par laquelle un entrepreneur confie par un sous-traité, et sous sa responsabilité, à une autre personne appelée sous-traitant l'exécution de tout ou partie du contrat d'entreprise ou d'une partie du marché public conclu avec le maître de l'ouvrage* »[30].

30) Loi nº 75-1334 du 31 décembre 1975 relative à la sous-traitance, art. 1, telle que modifiée par l'ordonnance nº 2010-1307 du 28 octobre 2010.

Pour que l'on puisse reconnaître la qualité de sous-traitant à un prestataire, le contrat qu'il conclut avec le maître d'œuvre doit être qualifié de contrat d'entreprise[31] et faire suite à un autre contrat d'entreprise conclu entre le maître d'œuvre et le maître de l'ouvrage.

Le sous-traitant en effet n'a pas personnellement contracté avec les intérêts du navire. Il est le cocontractant du constructeur, ou du fournisseur de service. Depuis un arrêt d'Assemblée Plénière en date du 12 juillet 1991, la jurisprudence judiciaire considère que l'action d'un tiers à un contrat dans le cadre d'un groupe de contrat était nécessairement délictuelle[32]. Le fondement délictuel vient par ailleurs d'être également retenu par le Conseil d'État dans un arrêt du 7 décembre 2015, Commune de Bihorel[33], mais à la condition que l'action soit fondée sur la violation des règles de l'art ou la méconnaissance de dispositions textuelles, et non sur l'inexécution du contrat de sous-traitance.

La question de la sous-traitance présente une acuité particulière dans le cadre de la construction navale.

Il existe en effet deux types de contrat de construction navale. Le premier, le contrat de construction à forfait, est celui où l'armateur traite avec un professionnel de la construction navale : pour un prix déterminé, le chantier s'engage à construire le navire et à le livrer après achèvement. Il s'analyse comme un contrat de vente à livrer, et la loi du 31 décembre 1975 ne peut donc s'appliquer.

Le second type de contrat, est appelé contrat à l'économie. Dans ce contrat, l'armateur construit lui-même le navire. Certes, il fait appel à différents prestataires, mais il doit conserver la direction générale de la construction. La sous-traitance s'applique ici.

Ainsi, pour reconnaître la responsabilité du sous-traitant, le maître de l'ouvrage devra rapporter la preuve de la faute du sous-traitant, d'un dommage, et du lien de causalité entre la faute et le dommage. Il est même envisageable que la responsabilité du sous-traitant soit engagée envers les tiers absolus ayant subi un préjudice trouvant sa cause dans la prestation défectueuse du sous-traitant[34].

---

31) Il y a contrat d'entreprise lorsqu'une personne dénommée entrepreneur s'oblige, moyennant rémunération, à accomplir de manière indépendante un travail d'ordre matériel ou intellectuel à la demande et au profit d'une autre personne que l'on dénomme client ou maître de l'ouvrage.

32) Cass. ass. plén., 12 juillet 1991, nº 90-13602.

33) CE, 7 déc. 2015, nº 380419, Commune de Bihorel.

34) Civ. 3e, 30 juin 1998, nº 96-13039.

- L'auteur de l'attaque cybernétique

L'auteur de l'attaque cybernétique peut-il être reconnu responsable civilement des dommages causés à l'armateur ? Certainement, oui.

Cette responsabilité est la responsabilité de droit commun, celle des désormais articles 1240s du Code civil, selon lesquels « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* ». Voici posé le principe général de responsabilité. Le Code civil ajoute que l'on est responsable non seulement de son propre fait, mais également des choses et des biens que l'on a sous sa garde.

La responsabilité du fait personnel, bien sûr, cela s'entend facilement. En écrasant les données d'un STAD, l'agent a causé un dommage. Sa responsabilité sera retenue selon le schéma classique de la responsabilité civile délictuelle : celui qui a subi un dommage devra rapporter la preuve du fait fautif, du dommage, et du lien de causalité entre le fait et le dommage. Le supposé responsable pourra alors s'exonérer de sa responsabilité s'il rapporte la preuve d'un cas de force majeure ou du fait d'un tiers embrassant les caractères de la force majeure, à savoir un fait imprévisible, irrésistible et extérieur aux parties.

Peut-on envisager une action qui serait fondée sur la responsabilité du fait des personnes que l'on a sous sa garde (ex. : commettant / préposé de l'article 1242 al. 5 du Code civil) ou la responsabilité générale du fait des choses (article 1242 al. 1 C. civ.) ? L'exemple serait celui de la clé USB de l'agent maritime infectée par un virus que le second capitaine viendrait introduire dans l'un des ordinateurs du bord ?

On retrouve ici les principes généraux des mécanismes de responsabilité : la responsabilité civile pourra être retenue contre le gardien de la chose qui a provoqué le dommage, c'est-à-dire contre celui qui a le triple pouvoir d'usage, de direction et de contrôle, en distinguant bien évidemment le gardien de la structure du gardien du comportement. Dans le cas présent, la responsabilité recherchée ne serait peut-être pas celle du second capitaine qui aura introduit la clé, envisagé éventuellement comme le gardien de la structure, mais celle de l'agent, gardien du comportement, le vice étant inhérent à la chose, la clé USB.

L'armateur, s'appuyant sur le principe dégagé par l'arrêt Lamoricière, devra alors rechercher la responsabilité du commettant de l'agent, le cas échéant, sur le fondement de l'article 1242 al. 5 C. civ[35]. Mais si l'agent savait que la clé était infectée, les choses

35) L'arrêt Lamoricière du 19 juin 1951 indique en effet que le préposé ne peut être le gardien de la chose. Le responsable est donc nécessairement le commettant.

sont susceptibles d'être différentes. En effet, puisque les atteintes aux STAD sont des infractions intentionnelles, la jurisprudence Cousin[36] pourra s'appliquer et les recours contre le préposé seront possibles puisque le fait dommageable est constitutif d'une infraction !

B. La responsabilité civile contractuelle

Ayant un spectre plus large que la responsabilité civile délictuelle, elle vise deux catégories principales de cocontractants : les « cyber-contractants », c'est-à-dire les fournisseurs de matériels et services informatiques d'une part, et les partenaires commerciaux, tels que le port et les services portuaires, le fréteur, et ceux qui ont fait que le navire a pu être livré, à savoir le constructeur, le vendeur, ou les sociétés de classification.

- Les « cyber-contractants »

Ici, il s'agira des fournisseurs d'accès, des gestionnaires de satellites et des fournisseurs du matériel informatique embarqué.

Fournisseur d'accès et fournisseur de matériel informatique embarqué sont des professionnels, débiteurs d'obligations traditionnelles de renseignement et de conseil mais également d'une obligation de mise en garde. Cette obligation est une obligation renforcée de conseil, et consiste à attirer l'attention sur le caractère dangereux du produit ou les éventuelles défaillances. Or, ne pas attirer l'attention sur la possible corruptibilité du système constitue sans aucun doute une violation de cette obligation de mise en garde susceptible d'engager leur responsabilité contractuelle. Leur responsabilité pourra cependant être atténuée si l'armateur lui-même n'a pas satisfait à son obligation de coopération, qui l'oblige notamment à fournir à son fournisseur toutes les informations utiles au bon fonctionnement du matériel ou du service.

Le vendeur du matériel informatique est de plus tenu, à moins d'une stipulation contractuelle contraire, à la garantie des vices cachés envers son acheteur. Le vice pour pouvoir être invoqué, doit exister au moment de la vente, être caché des parties, et doit rendre la chose impropre à l'usage auquel on la destine. Il est garanti pendant une période de deux ans à compter de la découverte du vice.

La question de la responsabilité des sociétés gestionnaires de satellites mérite également d'être posée. En effet, une attaque ciblée sur un satellite de communication pourra affecter les systèmes de bord de la même façon que si l'attaque était dirigée contre le navire lui-même. Il ne nous a pas été donné la possibilité d'avoir accès à un

36) Plén. 14 décembre 2001, nº 00-82.066.

contrat, mais sans régime spécial, c'est ici encore le droit commun qui trouvera à s'appliquer. Le gestionnaire de satellite pourra être appelé en garantie par le fournisseur d'accès sur le fondement contractuel. Le fournisseur d'accès devra alors rapporter la preuve de l'inexécution du contrat, dans les limites fixées par le contrat lui-même relatives aux aménagements de responsabilité. L'on sait depuis les arrêts Chronopost[37], que les aménagements de responsabilité sont permis, à condition toutefois que d'une part le cocontractant en ait eu connaissance et que d'autre part ces aménagements ne privent pas le contrat de sa cause. La récente réforme du Code civil a maintenu cette solution, bien qu'ayant supprimé la cause, en prévoyant dans un nouvel article 1170 que « *Toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite* ».

- Les partenaires commerciaux de l'armateur

Vis-à-vis du fréteur en premier lieu, la question qui se pose est celle de la navigabilité du navire. L'obligation de mettre le navire en état de navigabilité incombe à tous les fréteurs, quelle que soit la charte-partie. Cette obligation est une obligation essentielle du fréteur.

La navigabilité s'entend aussi bien d'un point de vue nautique que commercial. Or, si l'on conçoit aisément qu'une défaillance des systèmes de bord tels que la propulsion remette en question la navigabilité nautique, la question reste ouverte si les défaillances concernent l'AIS, simple aide à la navigation.

Quoi qu'il en soit, ce sera à l'affréteur d'apporter la preuve de l'innavigabilité du navire du fait de l'exposition aux risques cybernétiques s'il souhaite faire jouer une éventuelle *cancelling clause* ou une clause de *off-hire* prévues au contrat, voire demander la résolution judiciaire de la charte-partie.

D'autre part, l'obligation de maintenir le navire en état de navigabilité n'incombe au fréteur coque-nue qu'au moment de la présentation du navire, contrairement au fréteur au voyage pour lequel l'obligation lui incombe tout au long de la charte-partie. Le non-maintien par l'affréteur coque-nue de cette obligation aurait les mêmes conséquences : *cancelling clause* ou résolution judiciaire, avec éventuellement le versement d'indemnités au fréteur qui permettraient de réparer d'une part les dommages causés par les attaques informatiques et éventuellement le manque à gagner dû au chômage du navire.

L'armateur pourra aussi aller rechercher la garantie du chantier de construction.

37) Cass. Com. 22 oct. 1996, nº 93-18632.

Qu'il s'agisse d'un contrat dit au forfait ou à l'économie, le constructeur répond de l'aptitude du navire à prendre la mer. Le constructeur est débiteur d'une obligation de délivrance conforme : la chose livrée doit être conforme à celle qui a été promise, aucune qualité promise ne doit faire défaut. Cette obligation de délivrance conforme se prescrit par deux ans, mais elle n'est opposable qu'au vendeur professionnel qui contracte avec un consommateur.

Le constructeur de navire est également responsable au titre de la responsabilité des produits défectueux : il devra indemniser les tiers qui ont subi un dommage suite à un défaut de son produit[38], soit sur leur personne, soit sur leurs biens. Cette responsabilité étant de plein droit, le constructeur ne pourra s'exonérer de sa responsabilité qu'en apportant la preuve d'une utilisation anormale du navire, ou bien que ces dommages ont été la conséquence d'une réglementation administrative, ou encore que l'état des connaissances scientifiques et techniques, au moment où il a mis le produit en circulation, n'a pas permis de déceler l'existence du défaut, c'est-à-dire des risques de développement. Ainsi, le constructeur devra garantir les dommages provoqués par la présence à bord de matériels informatiques qui ne présentent pas les garanties attendues relativement aux risques de prise de contrôle à distance, certes, mais également tout équipement informatique indispensable pour maintenir la navigabilité du navire.

Enfin, aux mêmes conditions de fond que le fournisseur de matériel informatique, le constructeur de navire est tenu de la garantie des vices cachés de son navire, mais la garantie doit être demandée dans le délai d'un an cette fois-ci après la découverte du vice.

38) Le produit étant défini comme « *tout bien meuble, même s'il est incorporé dans un immeuble, y compris les produits du sol, de l'élevage, de la chasse et de la pêche. L'électricité est considérée comme un produit* ». Art. 1245-2 C. civ.