TRANSPORTE MARÍTIMO, TERRORISMO E SEGURO[1]

(https://doi.org/10.47907/livro/2022/02/cap05)

Alexandre de Soveral Martins*

Sumário: 1. Introdução. 2. Terrorismo. 3. Há mar e mar, há risco e risco. 4. Umas vezes há cobertura, outras não. 5. Observações finais

Palavras-chave: seguro marítimo; terrorismo; transporte marítimo

Summary: Introduction. 2. Terrorism. 3. There is sea and sea, there is risk and risk. 4. Sometimes there is hedge, sometimes not. 5. Final remarks

Keywords: maritime insurance; terrorismo; maritime carriage

1. Introdução

Os atos de terrorismo são objeto de grande cobertura pelos meios de comunicação social. As condições em que são praticados tornam-nos difíceis de prever. Tanto mais que, por razões de segurança, muita informação que lhes diz respeito não é divulgada[2]. E isso, só por si, já

* Professor Associado, Univ Coimbra, IJ, FDUC.

[1] Neste texto são retomadas algumas reflexões que foram objeto da nossa conferência sobre o tema proferida em 15 de julho de 2021 no âmbito do projeto «The New Maritime Silk Road: Navigation and Security in the Technological Era» do CUSMAT-Centro Universitario di Studi Marittimi e dei Trasporti da Università di Macerata (Itália). O estudo foi atualizado com referências ao direito nacional (Lei 46/2018, de 13 de agosto) e à proposta de nova Diretiva para substituir a Diretiva NIS (*Network and Information Security Directive*, ou Diretiva SRI – Segurança das Redes e da Informação), que veio estabelecer "medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno" (artigo 1.º, n.º 1). Foram igualmente tidas em conta várias novas referências bibliográficas e cláusulas-modelo anteriormente não identificadas.

[2] Sobre essa escassez de informação, v. Jeffrey Thomas, «Terrorism Insurance: Issues of Policy, Regulation and Coverage», *New Appleman on Insurance*, Newark: Lexis Nexis (April 2008), 37-69, 348.

tem consequências negativas para a atividade das seguradoras. Estas gostam de lidar com grandes números para poderem encontrar probabilidades e, assim, calcular o prémio do seguro[3]. São esses grandes números que ajudam a identificar o risco, mas, felizmente, os ataques terroristas não são frequentes. Contudo, sem informação credível os prémios corretos do ponto de vista atuarial são difíceis de encontrar. Quando não é possível calcular probabilidades[4], as seguradoras vão resistir a cobrir o risco. O problema estende-se à disponibilização de resseguro[5].

E, no entanto, os ataques terroristas podem gerar danos avultados que se estendem para lá das fronteiras de um país. O perigo de utilização de armas de destruição maciça por organizações terroristas existe. Os próprios navios podem ser usados para causar danos em portos ou em canais de navegação[6]. Quando se interrompe a navegação em certas linhas, podem ser causados efeitos económicos negativos em muitas partes do globo.

Por outro lado, organizações terroristas podem tentar adquirir empresas de navegação marítima para transportar armas e/ou os seus membros, bem como para usar o navio ou a mercadoria para o ataque que pretendem realizar[7].

Atualmente, os ciberataques podem ter os navios e as empresas de navegação como alvo. Sobretudo à medida que avançamos para a utilização de documentos de transporte eletrónicos e de navios

---

[3] V., quanto à relação entre a lei dos grandes números, o terrorismo e o seguro, Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», in José Manuel Aroso Linhares / Maria João Antunes, coord., *Terrorismo. Legislação comentada. Textos doutrinais,* Coimbra: Instituto Jurídico, 2019, 363-405, a p. 364.

[4] Jeffrey Thomas, «Terrorism Insurance: Issues of Policy, Regulation and Coverage», 39.

[5] Lembrando isso mesmo quanto ao ciberrisco, Bariş Soyer, «Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems», in Proshanto K. Mukherjee / Maximo Q. Mejia Jr ./ Jingjing Xu, ed., *Maritime Law in Motion*, Cham: Springer, 2020, 627-642, 631.

[6] À semelhança, aliás, da utilização de veículos automóveis: sobre isto, Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», 377 e ss., lembrando a questão da cobertura pelo seguro obrigatório de responsabilidade civil automóvel.

[7] V., quanto a essa possibilidade, Michael McNicholas, *Maritime Security: An Introduction*, Oxford: Elsevier, 2016, 265

autónomos[8]. Ataques *ransomware*, *hacking* de sistemas de portos para apropriação de carga, introdução de *malware* que afeta o sistema ECDIS (*Electronic Chart Diplay and Informations System*) ou o sistema AIS (*Automatic Identification System*), localização de contentores com carga interessante, furto de dados, *spoofing* de sistemas GPS[9], são algumas das muitas possibilidades que a tecnologia já abriu[10].

Há locais no Mundo que são considerados perigosos para ataques por meios mais «tradicionais»[11]. O Corno de África, o Sudeste Asiático e, em especial, os Estreitos de Malaca e o Golfo da Guiné são zonas em que os riscos aumentam. Os prémios de seguro aumentam se o navio vai circular por zonas de alto risco ou áreas de risco acrescido percecionado.

Muitas vezes, os contratos de seguro vão incluir as cláusulas *Navigation Limits*[12], que limitam a atuação do navio a certas áreas[13]. O chamado UBI – *Usage Based Insurance* também procurará controlar a localização do navio ou do contentor. A *Internet of Things* (IoT) pode ajudar a controlar o movimento da carga. Sensores de localização e

---

[8] V. Simon Cooper, «Cyber Risk, Liabilities and Insurance in the Marine Sector», in Bariş Soyer/Andrew Tettenborn, ed., *Maritime Liabilities in a Global and Regional Context*, Oxon/New York: Routledge, 2019, 103-117.

[9] Dando conta de ataques a sistemas de GPS de navios no Mar Negro durante os conflitos entre a Ucrânia e a Rússia de 2017, Bariş Soyer, «Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems», 628, nt. 5.

[10] Simon Cooper, «Cyber Risk, Liabilities and Insurance in the Marine Sector», 104 ss., Glenn Wright, *Unmanned and Autonomous Ships. An Overview of* MASS, Oxon/New York: Routledge, 2020, 133 s. Sobre o ciberrisco em geral, p. ex., Elisabete Ramos, «Cyber-risk, D&O Insurance and Directors' Protection», in César García Novoa/Diana Santiago Iglesias, dir., *4ª Revolución Industrial: Impacto de la automatización y la inteligencia artificial en la sociedad y la economia digital*, Cizur Menor: Aranzadi , 2018, 185-202.

[11] Darren Calley / Karen Hulme / David Ong, «New Marine Security Threats», in David Atard, gen. ed., *The* IMLI *Manual on International Maritime Law*, vol. III, Oxford: Oxford University Press, 2016, 511-540, 519.

[12] Sublinhando o «predomínio de los modelos contractuales de inspiración anglosajona» no seguro marítimo, Ignacio López Bustarad, «El riesgo en el seguro marítimo», in José Luíx García-Pita y Lastres / Maria Rocío Quintáns Eiras / Angélica Díaz de la Rosa, dir., *El derecho marítimo de los nuevos tempos*, Cizur Menor: Aranzadi, 2018, 1123-1143, 1124.

[13] Michael Davey / James Davey / Oliver Caplin, *Miller's Marine War Risks*, 4th. ed., Oxon/New York: Routledge, 2020, 212, recordando as *Navigation Limitations for Hull War, Strikes, Terrorism and Related Perils Endorsement* (JW2005/001A).

sistemas de informação geográfica estão a tornar-se habituais e muito úteis[14]. Mas a globalização também permitirá realizar ataques em qualquer mar ou oceano.

2. Terrorismo

As definições de terrorismo variaram ao longo dos anos. Na Convenção para a prevenção e punição do terrorismo, de 1937, os atos de terrorismo eram os que fossem dirigidos contra um Estado e com o objetivo ou planeados para criar uma situação de terror na mente de pessoas em particular, ou num grupo de pessoas ou no público em geral.

Mais recentemente, a Diretiva 2017/541, de 15 de março de 2017, apresenta uma lista de atos dolosos que serão terroristas se forem praticados com um dos seguintes objetivos: intimidar gravemente uma população; compelir de forma indevida os poderes públicos ou uma organização internacional a praticarem ou a absterem-se de praticar um ato; desestabilizar gravemente ou destruir as estruturas políticas, constitucionais, económicas ou sociais fundamentais de um país ou de uma organização internacional.

Certo é que o terrorismo não é uma atuação criminosa como as outras. A pirataria e o roubo têm subjacentes motivações privadas. Os terroristas têm outras coisas em mente. Mas leis diferentes dão também diferentes definições de terrorismo[15], e a distinção entre terrorismo e risco de guerra nem sempre é fácil.

Uma da mais importantes cláusulas-modelo para o transporte marítimo de mercadorias é a *Termination of Transit Clause (Terrorism) 2009* do *Joint Cargo Committee* da *Lloyd's Market Association*. Esta cláusula define o terrorismo como sendo «an act of any person acting on behalf of, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of any government whether or not legally constituted or any

---

[14] Simon Cooper, «Insurance and artificial intelligence», in Bariş Soyer/Andrew Tettenborn, ed., *New Technologies, Artificial Intelligence and Shipping Law in the 21st Century*, Oxon/New York: Routledge, 2020, 178-190, 182.

[15] V. «Definition of Terrorism by Country in oecd Countries», <https://www.oecd.org/daf/fin/insurance/terrorism-risk-insurance-programmes.htm>.

person acting from a political, ideological or religious motive». Estão, assim, incluídas as atuações de lobos solitários[16].

A definição de terrorismo que seja aplicável vai estabelecer o perímetro da cobertura. Se a lei aplicável ao contrato de seguro contiver a sua própria definição, podem surgir conflitos entre ambas[17].

3. Há mar e mar, há risco e risco

A importância económica do transporte marítimo torna-o um alvo apetecível e as cadeias logísticas não são invioláveis. Um contentor pode viajar de comboio, em cima de um camião, no convés de um navio, passar por dois ou mais portos e por vários terminais de contentores[18]. Muitas pessoas estarão envolvidas. A cadeia logística já foi considerada uma rede ou uma empresa conjunta[19].

Um ataque terrorista num elo dessa cadeia pode provocar danos a bens de muitas pessoas para além do transportador e do interessado na mercadoria. Pessoas feridas ou os herdeiros de quem perdeu a vida, mas também proprietários ou utilizadores de bens danificados estarão entre os muitos que procurarão ser indemnizados depois do ataque. Por

---

[16] Sobre estes, António Miguel Veiga, «Radicalização e "lobos solitários" no contexto da denominada "luta contra o terrorismo"», in José Manuel Aroso Linhares / Maria João Antunes, coord., *Terrorismo. Legislação comentada. Textos doutrinais,* 67 4-484.

[17] V., para uma comparação entre a definição das *2009 Cargo Clauses* e a da *Terrorism Act* 2000, Jonathan Gilman *et al., Arnould: Law of Marine Insurance and Average*, 20th ed., London: Thomson Reuters, 2021, 1310. O crime de terrorismo está descrito no art. 4.º da L 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo), que também caracteriza os crimes de organizações terroristas e de outras organizações terroristas nos seus arts. 2.º e 3.º, respetivamente. O tipo de crime terrorismo pressupõe uma certa intenção: «prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral». Para um comentário, v. José Manuel Aroso Linhares / Maria João Antunes, coord., *Terrorismo. Legislação comentada. Textos doutrinais*.

[18] V., p. ex., Caroline Foster, «Counter-Terrorism and the Security of Shipping in South East Asia», in Natali Klein / Joanna Mossop / Donald Rothwell, ed., *Maritime Security. International Law and Policy. Perspectives from Australia and New Zealand*, Oxon / New York: Routledge, 2010, 138-154, 140.

[19] Carlo Corcione, *Third Party Protection in Shipping*, Oxon / New York: Routledge, 2020, 3.

sua vez, o segurado pode ser o dono, fretador ou afretador do navio, o proprietário das mercadorias a bordo, outra seguradora, beneficiários de garantias sobre as mercadorias ou sobre o navio, os acionistas da transportadora, etc., etc.[20]. Se a mercadoria estava parada num armazém de um porto qualquer, o ataque que a danifique obrigará a verificar cuidadosamente se o seguro marítimo cobre danos causados a mercadorias que não estão em trânsito[21].

Haverá, muitas vezes, dificuldades em estabelecer nexos causais. Quem se sinta lesado procurará estabelecer laços causais entre o ataque e consequências muito remotas. Pense-se, designadamente, em perdas de chance, em quebras de faturação, em interrupções na laboração de um estabelecimento. Por exemplo, se um petroleiro é atacado e o petróleo derramado impede o funcionamento de instalações turísticas. Quando um navio afunda, pode não ser fácil descobrir o que causou o fogo ou a explosão a bordo[22].

Será, em regra, difícil obter indemnizações de terroristas ou das respetivas organizações[23]. Muitas vezes, a transportadora ou o proprietário das mercadorias, que foi lesado com o ataque, pode também surgir como demandado em ações intentadas por outros lesados que considerem que os primeiros não foram suficientemente diligentes na adoção de medidas de prevenção ou mitigação[24].

Os proprietários ou fretadores do navio, os seus empregados, os operadores portuários, as autoridades portuárias, etc., podem ser demandadas tendo em vista obter uma indemnização. Se um ciberataque tem lugar e é bem sucedido, pode ter sido porque houve medidas de segurança que não foram adotadas ou porque os consultores que tinham sido contratados não identificaram todos os riscos e não souberam informar sobre quais poderiam ser os eventos causadores de danos.

---

[20] Susan Hodges, *Cases and Materials on Marine Insurance Law*, London / Sydney: Cavendish, 1999, 46 ss.

[21] John Dunt, *Marine Cargo Insurance*, 2nd. ed., Oxon / New York: Routledge, 2016, 250.

[22] Michael Davey / James Davey / Oliver Caplin, *Miller's Marine War Risks*, 4th. ed., Oxon / New York: Routledge, 2020, 251.

[23] V. Michael Greenberg *et al., Maritime Terrorism. Risk and Liability*, Santa Monica: Rand, 2006, xxii. Entre nós, Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», 402.

[24] Michael Greenberg *et al., Maritime Terrorism: Risk and Liability*, 68.

O transportador pode vir a ser considerado responsável porque não controlou quem subiu a bordo ou porque não adotou medidas de segurança contra ciberataques. O respeito pelo *International Ship and Port Facility Code* (ISPS Code), incluído atualmente na Convenção Solas, poderá ajudar a manter os navios e a carga em segurança.

A IMO (*International Maritime Organisation*) tem *Guidelines on Maritime Cyber Risk Management* (Orientações sobre Gestão do Ciberrisco) que estão a ganhar considerável importância porque há quem comece a sustentar que o Código ISM (*International Safety Management Code*), também incluído na Convenção SOLAS, deve ser lido em conformidade com as mesmas[25], bem como o dever de revelar informações antes da celebração do contrato de seguro[26].

A BIMCO (*Baltic and International Maritime Council*), a *Chamber of Shipping of America*, a *Digital Containership Association*, a INTERCARGO (*International Association of Dry Cargo Shipowners*), a InterManager, a INTERTANKO (*International Association of Independent Tanker Owners*), a ICS (*International Chamber of Shipping*), IUMI (*International Union of Maritime Insurance*), a OCIMF (*Oil Companies International Marine Forum*), a Sybass (*Superyacht Builders Association*) e a WSC (*World Shipping Council*) adotaram umas orientações sobre a cibersegurança a bordo de navios (*Guidelines on Cyber Security Onboard Ships*), e os EUA têm o NIST *Framework* (NIST – *National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity*). A ISO e a *International Electrotechnical Commission* adotaram a regra 27001 sobre tecnologias da informação (Standard on Information technologies). Os controlos do Estado do porto (*Port State controls*) terão de começar a dar mais atenção à gestão do risco cibernético quando verificam se o navio respeita as exigências relativas a sistemas de gestão de segurança[27]. O mesmo se pode dizer quanto aos Planos de

---

[25] Simon Cooper, «Cyber Risk, Liabilities and Insurance in the Marine Sector», 108.

[26] Simon Cooper, «Cyber Risk, Liabilities and Insurance in the Marine Sector», 113 s.

[27] Simon Cooper, «Cyber Risk, Liabilities and Insurance in the Marine Sector», 108. O *Port State control* tem sido considerada a 'last "safety net"', para além das Convenções Internacionais da IMO, as Convenções da OIT, o controlo pelo Estado de bandeira, as sociedades de classificação de navios e as seguradoras (v. *ibid.*, 91 e ss. V. também Steven Jones, «Implications and Effects of Maritime Security on the Operation and Management of Merchant Vessels», in Rupert Herbert-Burns / Sam

Segurança dos Navios (*Ship Security Plans*, ou SSPs[28]). Entretanto, surgiu a Diretiva 2016/1148 «relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União» (Diretiva NIS – *Network and Information Security* – ou Diretiva SRI – Segurança das Redes e da Informação), que veio estabelecer "medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno" (artigo 1.º, n.º 1). Esta Diretiva foi transposta pela Lei n.º 46/2018, de 13 de agosto, mas já se iniciou o processo que visa a substituição daquela por uma nova Diretiva para, designadamente, reduzir os níveis de cibercriminalidade e de terrorismo[29]. A Diretiva NIS estabelece "requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais" (artigo 1.º, n.º 2, alínea d); v. também o artigo 2.º, n.º 1, alínea c), da Lei n.º 46/2018), estando incluídas na lista de operadores de serviços essenciais certas companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e mercadorias, certas entidades gestoras dos portos e entidades que gerem obras e equipamento existente dentro dos portos, bem como certos operadores de serviços de tráfego marítimo, desde que cumpram os critérios previstos no artigo 5.º, n.º 2. Tudo isto, naturalmente, acabará por ter reflexos também no que se entenderá por negligência[30].

Bateman / Peter Lehr, ed., *Lloyd's* MIU *Handbook of Maritime Security*, Boca Raton / London / New York: CRC Press, p. 87-116, p. 99 e s. Para um comentário à Diretiva 2009/16/CE relativa à inspeção de navios pelo Estado do porto (reformulação) ou port State control Directive (recast), Michael Pimm, «Commentary on Directive 2009/16/EC of The European Parliament and of the Council of 23 April 2009 on Port State Control», in Henning Jessen /Michael Jürgen Werner, ed., EU *Maritime Transport Law*, München / Oxford / Baden-Baden: Beck / Hart / Nomos, 2016, 856-901, mas sem ter em conta alterações posteriores.

[28] Sobre os SSPs, Steven Jones, «Implications and Effects of Maritime Security on the Operation and Management of Merchant Vessels», 95.

[29] V. a Proposta de Diretiva do Parlamento Europeu e do Conselho «relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 COM(2020) 823 final, p. 8. V. também o Parecer do Comité Económico e Social Europeu sobre a Proposta (2021/C 286/28) e o Relatório sobre a proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 (relator: Bart Groothuis).

[30] Michael Greenberg *et al., Maritime Terrorism: Risk and Liability*, 72.

4. Umas vezes há cobertura, outras não

Antes do 11 de setembro de 2001, a cobertura relativamente a atos de terrorismo estava muitas vezes incluída nas apólices sem que fosse exigido qualquer acréscimo no valor a pagar às seguradoras[31]. Aparentemente, aquela não daria especial atenção ao risco de terrorismo[32].

Depois do trágico atentado às Torres Gémeas, o mercado começou a excluir a cobertura daquele risco. As resseguradoras e os P&I Clubs tiveram aí um papel muito relevante[33]. O comportamento era compreensível, pois aquele ataque teve consequências em praticamente todos os ramos de seguro. Houve quem escrevesse que, até àquele dia, as seguradoras nunca tinham imaginado que um ataque pudesse gerar perdas tão avultadas. Em Portugal, o art. 45.º, 2, do Regime permite que o contrato de seguro exclua a cobertura, designadamente, dos riscos derivados de terrorismo[34]. Na Espanha, o art. 418 da *Ley de Navegación Marítima* exclui da cobertura do seguro marítimo o risco de terrorismo, embora a norma não pareça ser imperativa[35].

Entretanto, várias tentativas foram levadas a cabo para procurar que o mercado funcionasse novamente. As escolhas, porém, têm sido muito diferentes de país para país.

Nos EUA, a lei TRIA (*Terrorism Risk Insurance Act*), de 2002, criou o *Terrorism Risk Insurance Plan*, que atualmente se estenderá *pelo menos até 31.12.2027*. Este programa permitirá o pagamento de reembolsos às seguradoras que cubram o risco de terrorismo e participem no plano se determinadas condições forem preenchidas. O programa TRIP abrange alguns transportes marítimos.

O programa Pool Re, no Reino Unido, já não abrange o seguro marítimo. Na Rússia, o RATIP (*Russian Anti-Terrorism Insurance Pool*) tem

---

31 Baird WEBEL, «Terrorism Risk Insurance Legislation in 2007: Issue Summary and Side-By-Side», in Miguel PALACIOS, ed., *Terrorism Insurance*, Nova Science Publishers, 2007, 1-18, 2.

32 Jeffrey THOMAS, «Terrorism Insurance: Issues of Policy, Regulation and Coverage», *New Appleman on Insurance*, 37.

33 Baird WEBEL, «Terrorism Risk Insurance Legislation in 2007: Issue Summary and Side-By-Side», 1.

34 Sobre esse art. 45.º, 2, p. ex., Filipe de Albuquerque MATOS, «A cobertura de actos terroristas pelos seguros», 372.

35 Nesse sentido, Ignacio LÓPEZ BUSTARAD, «El riesgo en el seguro marítimo», 1142.

um papel de resseguradora, abrangendo o seguro de carga, mas não o de navios. Na Alemanha, há uma seguradora chamada *Extremus Versicherungs*-AG que cobre o risco de terrorismo, mas tem apoio governamental[36]. Na França, o GAREAT (*Gestion de l'Assurance et de la Réassurance des Risques, Attentats et Actes de Terrorisme*) funciona como uma *pool* que fornece aos seus membros co-seguro, mas a responsabilidade do transportador marítimo não é abrangida[37]. Os exemplos poderiam repetir-se.

Uma das cláusulas muito usadas na prática seguradora é a *Institute Cargo Clauses (A)*. Esta continua a excluir a cobertura por perda, dano ou despesas causadas por qualquer ato de terrorismo ou por qualquer pessoa agindo por um motivo político, ideológico ou religioso. A *Strikes Exclusion Clause* também afasta a cobertura quanto a «loss damage liability or expense caused by […] 24.2. any terrorist or any person acting from a political motive»[38].

No entanto, a *Institute Strikes Clauses (Cargo)* dá cobertura a «loss or damage» causado por qualquer ato de terrorismo («any act of terrorism») (Clause 1.2)[39], e por qualquer pessoa atuando por um motivo político, ideológico ou religioso («any person acting from a political, ideological or religious motive»), embora com as limitações que resultam da *Transit Clause* (Clause 5)[40]. Cobertura por «loss or damage» causados ao navio é conferida pela Institute War and Strikes Clauses (1.5 and 1.6).

---

36 Baird WEBEL, «Terrorism Risk Insurance: Issue Analysis and Legislation», 21.

37 A França conta ainda com o *Fonds de Garantie des Victimes des actes de Terrorismo et d'autres Infractions* para indemnizar vítimas de ataques terroristas relativamente a «dommages corporels»: v. art. 9 da *Loi 86-1020*, de 9 de setembro de 1986, já alterada. De acordo com a página do Fundo (https://www.fondsdegarantie.fr/fgti/fonctionnement/), o mesmo não recebe financiamento do Estado francês.

38 Sobre esta, v. Jonathan GILMAN *et al., Arnould: Law of Marine Insurance and Average*, 1308 s., dando igualmente atenção à *Malicious Acts Exclusion* e aos problemas de interpretação associados.

39 Para uma análise da Clause 1.2. com a redação que tinha na altura, N. Geoffrey HUDSON / Tim MADGE / Keith STURGES, *Marine Insurance Clauses*, 5th ed., Oxon / New York: Routledge, 2012, 351 s.; e D. ROSE, *Marine Insurance: Law and Practice*, 2nd ed., Oxon / New York: Routledge, 2013, 372 s.

40 V. John DUNT, *Marine Cargo Insurance*, 2nd. ed., Oxon/New York: Routledge, 2016, 246. Michael DAVEY / James DAVEY / Oliver CAPLIN, *Miller's Marine War Risks*, 264, consideram que a *Institute Strikes Clause (Cargo)* não cobre «pure economic loss to which an industrial dispute may give rise» nem «physical loss or damage to the cargo due to delays».

Parece ser rara a cobertura relativamente a ataques NCBR (*Nuclear, Chemical, Biological and Radiological*[41], encontrando-se uma exclusão do *Institute Cargo Clauses* (A) (Clause 4.7) com o seguinte teor: «[In no case shall this insurance cover] loss damage or expense directly or indirectly caused by or arising from the use of any weapon or device employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter». Redações semelhantes encontram-se na *Institute Strikes Clauses (Cargo)* (Clause 3.9) e na *Institute War and Strikes Clauses* (Clause 3.8)[42]. Os ciberataques também não parecem cobertos quando se opte pela *Joint Cargo Committee Cyber Exclusion and Write-Back Clause* (CL437) ou pela *Cyber Attack Exclusion Clause* (CL 380)[43].

Danos causados por poluição marítima resultante de um ataque terrorista poderão eventualmente estar cobertos. Os P&I *Clubs* estarão a comprovar que «cover is in place under the Civil Liability Conventions for damage resulting from acts of terrorism […] subject to the requirement that the shipowner has war risks cover on standard terms with a separate limit for P&I liabilities»[44]. A Convenção CLC (Convenção Internacional sobre Responsabilidade Civil pelos Prejuízos Devidos à Poluição por Hidrocarbonetos, de 1992, já alterada), exige que os proprietários de navios com certa capacidade cubram a sua

---

[41] Jeffrey THOMAS, «Terrorism Insurance: Issues of Policy, Regulation and Coverage», 54.

[42] Sobre o tema, John DUNT, «English Law and Practice», in John DUNT, ed., *International Cargo Insurance*, Oxon/New York: Routledge, 2012, 84, Stephen RIBLE, «United States Law and Practice», in John DUNT, ed., *International Cargo Insurance*, 230 s.; Francesco SICCARDI, «Italian Law and Practice», in John DUNT, ed., *International Cargo Insurance*, 292; e Joachim BARTELS, «German Law and Practice», in John DUNT, ed., *International Cargo Insurance*, 346.

[43] Para uma análise desta última, Baris SOYER, «Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems», 636 ss., dando conta das alterações à mesma pelo mercado londrino, que tem vindo a adotar a CL 380 Hull amended, e chamando a atenção para a importância de se negociarem *write-backs*. Sobre os seguros cibernéticos à medida (Taylor made cyber insurance), Elisabete RAMOS, «Corporate governance and cyber governance. How to govern the future?», in Maria Miguel CARVALHO / Sónia MOREIRA, ed., *E.Tec Yearbook. Governance and Technology*, Braga: School of Law – University of Minho, 2021, 157-178, 173 ss.

[44] Måns JACOBSSON, «Liability and Compensation for Ship-Source Pollution», in David ATARD, gen. ed., *The* IMLI *Manual on International Maritime Law*, vol. III, Oxford: Oxford University Press, 2016, 305.

responsabilidade através de seguro ou outra garantia financeira[45]. No entanto, o art. III.2[46] estabelece que o proprietário não será responsável se provar que o prejuízo por poluição resulta «na totalidade, de um facto deliberadamente praticado ou omitido por terceiro com a intenção de causar um prejuízo«» e isso «appears to cover acts of terrorism»[47].

Muitas são as alternativas que, em abstrato, poderão estar disponíveis para lidar com a falta de cobertura ou com a cobertura demasiado cara ou escassa. A imposição às seguradoras do dever de fornecer essa cobertura, o apoio público a seguradoras que forneçam a cobertura, a criação de incentivos fiscais, o recurso a fundos[48], as *cat bonds*[49], as *pools* ou o co-seguro[50] são possibilidades que merecem atenção, tendo cada uma as suas vantagens e riscos[51]. A intervenção pública, por exemplo, pode retirar estímulos à iniciativa privada[52].

---

[45] Art. VII, 1. Não é a única Convenção a estabelecer a obrigatoriedade de seguro. A Diretiva 2009/20/CE relativa ao seguro dos proprietários de navios em matéria de créditos marítimos obriga os Estados-Membros a exigir que «os proprietários de navios que arvorem a sua bandeira subscrevam um seguro que cubra esses navios» (v. a transposição no DL 50/2021, de 2 de março).

[46] A Convenção CLC é complementada pela Convenção FIPOL (Convenção Internacional para o Estabelecimento de um Fundo Internacional para Compensação pelos Prejuízos Devidos à Poluição por Hidrocarbonetos, de 1992) e pelo Protocolo de 2003 à Convenção FIPOL.

[47] Måns Jacobsson, «Liability and Compensation for Ship-Source Pollution», 300.

[48] Sobre a oportunidade de fundos públicos autónomos, considerando-a uma «alternativa credível», Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», 399 e ss.

[49] V., p. ex., Andrew Gerrish, «Terror CaTs: TRIA's Failure to Encourage a Private Market for Terrorism Insurance and How General Securitization of Terrorism Risk May Be a Viable Alternative», 1856; Adam Alvarez, *Hedging Hurricanes. A Concise Guide to Reinsurance, Catastrophe Bonds, and Insurance-Linked Funds*, 2nd. ed., Alvarez & Associates, 2017, 28.

[50] Sobre o co-seguro marítimo e a distinção entre aquele e as *pools*, Javier Vercher Moll, «El coaseguro marítimo», in José Luís García-Pita y Lastres / Maria Rocío Quintáns Eiras / Angélica Díaz de la Rosa, ed., *El derecho marítimo de los nuevos tempos*, Cizur Menor: Aranzadi, 2018, 1333-1343, 1340.

[51] Considerando que o resseguro e o retrosseguro «não constituem técnicas eficazes para a cobertura da extensa e muito dispendiosa danosidade provocada pelos ataques terroristas», Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», 393.

[52] Vittorio Afferni, «Le coperture antiterrorism: problematiche e possibili soluzioni», in *Assicurazioni* 3-4 (2001) 267-279, 272.

5. Observações finais

As consequências dos ataques terroristas facilmente se estendem por vários países. A limitação de coberturas a riscos nacionais ou a exclusão de cobertura no que diz espeito a ataques no mar poderão tornar difícil a obtenção de indemnizações por parte de lesados. À semelhança do que já foi alcançado noutros âmbitos, a existência de uma convenção internacional que permitisse criar um fundo que suportaria o pagamento de indemnizações quando não houvesse cobertura por um contrato de seguro poderia ser a solução mais prática. Há, porém, que evitar que o seguro permita financiar os próprios terroristas e as suas organizações[53].

De qualquer modo, o caminho a seguir deve ter em conta que as escolhas feitas podem criar incentivos para não se avançar no sentido da prevenção ou mitigação do risco. O conflito entre uma Cultura de Segurança (*Security Culture*) e uma Cultura de Cumprimento (*Compliance Culture*)[54] está aí e pode ter consequências nos tribunais, tornando fundamental um trabalho de antecipação e planeamento.

---

[53] Alertando para isso mesmo, Filipe de Albuquerque Matos, «A cobertura de actos terroristas pelos seguros», 385 e ss.

[54] V. Wayne Talley, *Maritime Safety, Security and Piracy*, London: Informa Law, 2008, 84.