A SEGURANÇA CIBERNÉTICA NO DIREITO MARÍTIMO: UMA ANÁLISE DO DEVER DE PROTEÇÃO DE DADOS

Ingrid Zanella Andrade Campos

Vice-presidente da OAB-PE. Presidente da Comissão Nacional Direito Marítimo e Portuário do Conselho Federal da OAB. Doutora e mestre em Direito pela Universidade Federal de Pernambuco (UFPE). Professora efetiva da UFPE. Juíza suplente do Tribunal Marítimo. Advogada. Ingridzanella@qca.adv.br.

I. INTRODUÇÃO

O Brasil é um país maritimamente privilegiado, conta com uma costa de 8,5 (oito vírgula cinco) mil quilômetros navegáveis, em que o transporte marítimo responde, atualmente, por mais de 80% (oitenta por cento) do comércio mundial de mercadorias e se constitui como fator imprescindível na globalização. O transporte aquaviário se consubstancia, então, como um fator fundamental na economia mundial, além de estar inteiramente ligado a questões ambientais e sociais.

Em um cenário de estímulo à navegação, medidas de segurança devem ser adotadas, considerando a proteção de dados pessoais e a segurança cibernética. De acordo com o Relatório sobre o prejuízo de um vazamento de dados, da IBM Security, em 2020 o prejuízo foi estimado em US$ 3,86 milhões. Ainda, 80% das organizações afetadas declararam que as informações de identificação pessoal do cliente foram comprometidas [1].

Em 2020, 2 de outubro, a Organização Marítima Internacional (IMO) sofreu um ataque cibernético. A IMO manifestou, em comunicado, que a interrupção do serviço foi causada por um sofisticado ataque cibernético contra os sistemas de TI da organização, o qual conseguiu ultrapassar as robustas medidas de segurança em vigor.[2]

Na mesma semana, a CMA CGM GROUP foi hackeada, o ataque afetou os servidores periféricos. O grupo foi a quarta maior companhia de navegação a sofrer um

[1] IBM Security. **Relatório sobre o prejuízo de um vazamento de dados, 2020**. Disponível em <Cost of a Data Breach Report 2020 | IBM>. Acesso em 20 de dez. 2020.
[2] Revista Transporte e negócios. **A IMO foi atingida por um ataque cibernético. Disponível em**: <IMO alvo de ataque cibernético - Transportes & Negócios (transportesenegocios.pt)>. Acesso em Acesso em 04 de jan. 2021.

ataque cibernético, depois da suíça MSC, da chinesa COSCO Shipping e da dinamarquesa Maersk.[3]

A segurança cibernética no cenário marítimo representa um aspecto relevante relacionado com à segurança da navegação. A ameaça de ataques cibernéticos no transporte marítimo é, inclusive, um dos sete tópicos do Cybersecurity Trends 2020 da TÜV Rheinland (The 2020 Study on the State of Industrial Security).[4]

Os riscos dos ataques cibernéticos envolvem além de elevado prejuízo financeiro, ameaças à segurança, meio ambiente e pessoas a bordo. Considerando que um ataque pode alterar a rota de navegação, atingir equipamentos, causar acidentes marítimos e violar dados pessoas.

Desta forma, em 2017, a Organização Marítima Internacional (IMO) publicou a Resolução MSC.428 (98), que trata da gestão de riscos cibernéticos no Sistema de Gestão de Segurança (*Maritime Cyber Risk Management in Safety Management Systems*), com medidas obrigatórias a partir de 1º de janeiro de 2021. Ainda, Diretrizes sobre gestão de risco cibernético marítimo (*Guidelines on maritime cyber risk management*, MSC-FAL.1/Circ.3 5 July 2017[5]), reconhecendo que o sistema de gestão de segurança deve levar em consideração a gestão de risco cibernético de acordo com os objetivos e requisitos do Código Internacional da Gestão da Segurança (ISM).

De acordo com a Resolução IMO MSC 428 (98), os Estados devem garantir que os procedimentos para o controle de riscos cibernéticos sejam incluídos nos Sistemas de Gerenciamento de Segurança existentes. Neste sentido, a segurança cibernética deverá ser coberta pelo Código ISM a partir de 1º de janeiro de 2021.[6]

---

[3] Revista Transporte e negócios. **A IMO foi atingida por um ataque cibernético. Disponível em**: <IMO alvo de ataque cibernético - Transportes & Negócios (transportesenegocios.pt)>. Acesso em Acesso em 04 de jan. 2021.

[4] TÜV Rheinland. **The 2020 Study on the State of Industrial Security**. Disponível em: <https://www.tuv.com/landingpage/en/functional-safety-meets-cybersecurity/main-navigation/securing-today-safer-tomorrow/?wt_mc=Website.tuv-com.no-interface.&wt_mc=Advertising.Print.no-interface.CW19_X00_FSCS.shortcut.&cpid=CW19_X00_FSCS_PT>. Acesso em 04 de jan. 2021.

[5] IMO. **Guidelines on maritime cyber risk management**, MSC-FAL.1/Circ.3 5 July 2017.

[6] IMO. Resolução MSC 428 (98). "AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code; 2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;".

Considerando as diversas relações jurídicas que se desenvolvem em torno do navio, o debate em torno da segurança cibernética está diretamente relacionado à proteção de dados, que ganha especial relevância, no Brasil, com a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709, de 14 de agosto de 2018.

Do mesmo modo, destaca-se o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) nº 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Desta forma, o objeto principal do presente trabalho é abordar a problemática subjacente à identificação de formas de garantir a eficiência da proteção de dados e da responsabilidade civil no direito marítimo, visando a uma maior segurança jurídica, inclusive diante da possibilidade de abertura do mercado de cabotagem a embarcações estrangeiras, bem como com o ingresso de navios autônomos.

II. A SEGURANÇA CIBERNÉTICA NO DIREITO MARÍTIMO

No que concerne à segurança no âmbito marítimo, destaca-se o Código Internacional da Gestão da Segurança (ISM). Desde 1998, o Código ISM é obrigatório, conforme Capítulo IX, da Convenção Internacional para a Salvaguarda da Vida Humana no Mar, 1974 (SOLAS). Ao mesmo tempo, o Código Internacional para a Proteção de Navios e Instalações Portuárias (ISPS), que entrou em vigor em julho de 2004, com a inserção da Resolução 2, no Capítulo XI-2 anexo à SOLAS.

O Brasil ratificou e promulgou a Convenção Internacional para Salvaguarda da Vida Humana no Mar (SOLAS) por meio do Decreto nº 87.186/1982, portanto deve dar cumprimento ao estabelecido nos Códigos ISM e ISPS, para a certificação internacional de seus portos e navios.

O Código ISPS, Parte A (requisitos obrigatórios), constitui obrigações ao navio e ao terminal, estabelecendo no item 3, que se aplica a navios de carga, incluindo embarcações de alta velocidade, de arqueação bruta a partir de 500 e instalações portuárias que servem tais navios em viagens internacionais. Ainda, o Código ISPS, Parte B, contém diretrizes que devem ser levadas em consideração ao se implementar as disposições de proteção contidas na Parte A.

As obrigações do Código ISPS incluem quesitos referentes a carga e ao navio, na Parte A, item 7. Conforme estabelece o item 8, Parte A, o navio é obrigado a realizar uma avaliação de proteção, que é parte integral e essencial do processo de elaboração e atualização do plano de proteção do navio. Conforme recomendado pela Parte B, parágrafo 8.3.5 do Código ISPS, a referida avaliação deve abordar sistemas de rádio e telecomunicações, incluindo sistemas e redes de computadores.

Em seguida, no item 9, o Código ISPS trata do Plano de Proteção do Navio, que deverá ser mantido a bordo da embarcação ("9.1. Todo navio deverá ter a bordo um plano de proteção do navio aprovado pela Administração".). No item 10, encontram-se os registros das atividades incluídas no plano de proteção do navio que devem ser mantidos a bordo, inclusive em formato eletrônico, no idioma de trabalho do navio (inglês, francês ou espanhol), entre as quais destaca-se: treinamentos, simulações e exercícios; ameaças de proteção e incidentes de proteção; violações de proteção; alterações no nível de proteção; comunicações relativas diretamente à proteção do navio, tais como ameaças específicas ao navio ou às instalações portuárias nas quais o navio esteja ou tenha estado; incluindo testes do sistema de alarme de proteção do navio.

Ainda, o navio deverá portar o Certificado Internacional de Proteção de Navio, com validade de até 5 anos. Inicialmente ratifica-se que se tratando de uma norma internacional, da qual o Brasil é parte, a documentação mencionada supra deverá estar a bordo do navio, de fácil acesso, caso venha a ser solicitada pela Autoridade Portuária.

De acordo com o Capítulo IX, Regra 2, da Convenção SOLAS, o Código ISM se aplica a:

1. navios de passageiros, inclusive embarcações de passageiros de alta velocidade, não mais tarde que 1o de julho de 1998;
2. petroleiros, navios de produtos químicos, navios transportadores de gás, graneleiros e embarcações de transporte de carga de alta velocidade, de arqueação bruta igual 500 ou mais, não mais tarde que 1o de julho de 1998; e
3. outros navios de carga e unidades móveis de perfuração marítima com arqueação bruta igual 500 ou mais, não mais tarde que1o de julho de 2002.

A certificação ocorre através de uma verificação inicial, bem de verificações periódicas, com a emissão do Documento de Conformidade, que atestará o atendimento às exigências do Código ISM, incluindo medidas de segurança cibernética, conforme estabelece a Resolução MSC 428 (98).

De acordo com o *National Institute of Standards and Technology* (NIST) - Órgão do Departamento de Comércio dos Estados Unidos, para estabelecer ou aprimorar o programa de risco cibernético, há uma estrutura com diretrizes sobre a segurança cibernética. A estrutura (*framework*) é baseada em cinco conjuntos de temas, pilares ou "domínios" de ações que estruturam a gestão de risco cibernético: identificar, proteger, detectar, responder e recuperar.[7]

Neste sentido, as Diretrizes para Navios sobre Segurança Cibernética (*The Guidelines On Cyber Security Onboard Ships*)[8], indicam que o gerenciamento de riscos cibernéticos deve:

1. Identificar as funções e responsabilidades dos usuários, pessoal-chave e gestão em terra e a bordo;
2. Identificar os sistemas, ativos, dados e capacidades que, se interrompidos, podem representar riscos para o navio operações e segurança;
3. Implementar medidas técnicas e procedimentais para proteger contra um incidente cibernético e garantir continuidade das operações;
4. Implementar atividades para se preparar e responder a incidentes cibernéticos.
5. Estabelecer planos de contingência.

Assim, é preciso estabelecer medidas efetivas de proteção de dados, inclusive considerando a segurança cibernética. É importante identificar como gerenciar a segurança cibernética a bordo e delegar responsabilidades para o comandante, os oficiais responsáveis e, quando apropriado, o oficial de segurança da empresa. [9]

Conforme visto, os personagens marítimos podem mudar de acordo com os contratos utilizados. Todavia, destaca-se que o detentor do Documento de Conformidade é, em última instância, responsável por garantir a gestão de cyber riscos a bordo.

Assim, a partir de 1º de janeiro de 2021, as verificações de segurança, de acordo com Código ISM, devem incluir as medidas de segurança cibernética, conforme estabelece a Resolução MSC 428 (98).

---

[7] CANTO DE LIMA, Ana Paula Moraes. **Aspectos Gerais sobre a Lei Geral de Proteção de Dados que as empresas precisam saber**. In: LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. LGPD -Lei Geral de Proteção de Dados: sua empresa está pronta? São Paulo: Literare Books International, 2020. p. 82.

[8] BIMCO. **The Guidelines On Cyber Security Onboard Ships.** BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF e WORLD SHIPPING COUNCIL. Disponível em: <guidelines-on-cyber-security-onboard-ships-min.pdf (ics-shipping.org)>. Acesso em 30 de dez. 2020.

[9] BIMCO. **The Guidelines On Cyber Security Onboard Ships.** BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF e WORLD SHIPPING COUNCIL. Disponível em: <guidelines-on-cyber-security-onboard-ships-min.pdf (ics-shipping.org)>. Acesso em 30 de dez. 2020.

Essas obrigações devem considerar, conforme visto, no âmbito marítimo, a incorporação adequada nos manuais e procedimentos de segurança da embarcação, conforme Códigos ISM e ISPS, considerado a segurança cibernética. A ausência de adoção dessas medidas obrigatórias, podem ensejar a responsabilidade civil específica pelo não cumprimento do dever de proteção de dados.

III. CONCLUSÃO

Considerando as diversas relações jurídicas que se desenvolvem em torno do navio, o debate em torno da segurança cibernética está diretamente relacionado à efetiva proteção de dados e promoção de segurança contra riscos cibernéticos.

Assim, no âmbito marítimo, destacou-se a Resolução IMO MSC.428 (98), que trata da gestão de riscos cibernéticos no sistema de gestão de segurança das embarcações, com medidas obrigatórias a partir de 1º de janeiro de 2021.

Em seguida, os Códigos ISM e ISPS foram analisados, por serem obrigatórios, conforme Convenção Internacional para a Salvaguarda da Vida Humana no Mar, 1974 (SOLAS).

De acordo com o Código ISM deverá haver uma certificação do navio, através de vistorias iniciais e periódicas, com a emissão do Documento de Conformidade que atestará o atendimento às exigências do referido Código, incluindo que a segurança cibernética, a partir de 1º de janeiro de 2021.

No que concerne à responsabilidade civil, conclui-se que quando o tratamento de dados for irregular, por não se observar a legislação ou não se fornecer a segurança necessária, haverá a responsabilidade civil objetiva.

Entre a legislação que deve ser observada, conforme corroborado, no âmbito marítimo, há a segurança cibernética, de acordo com os Códigos ISM e ISPS. Assim, a ausência de adoção dessas medidas obrigatórias, podem ensejar a responsabilidade civil objetiva específica pelo não cumprimento do dever de proteção de dados.

Portanto, quando houver um ilícito, ou seja, o tratamento irregular de dados, deixando de observar a legislação, conforme hipóteses previstas no art. 44 da LGPD ou em outros diplomas legais, como os Códigos ISM e ISPS, estar-se-ia diante de uma responsabilidade civil objetiva, ante a ausência de cumprimento do dever legal de proteção de dados.

Assim, a segurança cibernética, no âmbito marítimo, deve ser reconhecida como um pilar obrigatório, como forma de preconizar a segurança de dados, a partir de 1º de janeiro de 2021, devendo ser parte integrante do sistema de gestão da segurança das embarcações.

REFERÊNCIAS

BIMCO. **The Guidelines On Cyber Security Onboard Ships.** BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF e WORLD SHIPPING COUNCIL. Disponível em: <guidelines-on-cyber-security-onboard-ships-min.pdf (ics-shipping.org)>. Acesso em 30 de dez. 2020.

BIONI, Bruno; DIAS, Daniel. **Responsabilidade civil na proteção de dados pessoais**: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Revista civilistica.com. a. 9. n. 3. 2020.

CAMPOS, Ingrid Zanella Andrade. **Direito Marítimo Sistematizado**. Curitiba, Juruá, 2017.

CANTO DE LIMA, Ana Paula Moraes. **Aspectos Gerais sobre a Lei Geral de Proteção de Dados que as empresas precisam saber**. In: LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. LGPD -Lei Geral de Proteção de Dados: sua empresa está pronta? São Paulo: Literare Books International, 2020.

DRESCH, Rafael. **A especial responsabilidade civil na Lei Geral de Proteção de Dados**. Migalhas de responsabilidade civil. Disponível em: < A especial responsabilidade civil na Lei Geral de Proteção de Dados - Migalhas (uol.com.br)>. Acesso em 20 de dez. 2020.

FERREIRA, Waldemar Martins. **O commercio marítimo e o navio**. São Paulo: Revista dos Tribunais, 1931.

IMO. **Resolução MSC 428** (98)/2017.

IMO. Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3 5 July 2017.

IBM Security. **Relatório sobre o prejuízo de um vazamento de dados, 2020**. Disponível em <Cost of a Data Breach Report 2020 | IBM>. Acesso em 20 de dez. 2020.

MIRANDA, Pontes de. Tratado de direito privado. Parte especial. Tomo XLV: Direito das obrigações. Rio de Janeiro: Editor Borsoi, 1964.

Revista Transporte e negócios. **A IMO foi atingida por um ataque cibernético. Disponível em**: <IMO alvo de ataque cibernético - Transportes & Negócios (transportesenegocios.pt)>. Acesso em Acesso em 04 de jan. 2021.

SOUZA, Herculano Marcos Inglez de. **Projecto de Código Commercial**. Introdução. Rio de Janeiro: Impr. Nacional, 1912. v. 1. p. 79. Disponível em: http://www.stf.jus.br/bibliotecadigital/ObrasSelecionadas/42626/pdf/42626.pdf. Acesso em: 14 set. 2019.

SUSSEKIND, Arnaldo. **Conflitos de leis do trabalho**. Rio de Janeiro: Freitas Bastos, 1979.

TÜV Rheinland. **The 2020 Study on the State of Industrial Security**. Disponível em: <https://www.tuv.com/landingpage/en/functional-safety-meets-cybersecurity/main-navigation/securing-today-safer-tomorrow/?wt_mc=Website.tuv-com.no-interface.&wt_mc=Advertising.Print.no-interface.CW19_X00_FSCS.shortcut.&cpid=CW19_X00_FSCS_PT>. Acesso em 04 de jan. 2021.