Cadernos do Programa de Pós-Graduação DIREITO/UFRGS
volume 16 | n. 2 | 2021 | seer.ufrgs.br/ppgdir

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

CYBER SECURITY IN MARITIME LAW: AN ANALYSIS OF DATA PROTECTION DUTY

Ingrid Zanella Andrade Campos*

RESUMO: Considerando que a segurança cibernética no cenário marítimo representa um aspecto relevante para proteção de dados, o objetivo principal deste trabalho é a análise da responsabilidade civil em face do descumprimento do dever de proteção de dados. Para tanto, ratificou-se que, a partir de 1º de janeiro de 2021, deverá haver a adoção da gestão de riscos cibernéticos nos sistemas de gestão de segurança das embarcações. Por fim, demonstrou-se que haverá responsabilidade civil objetiva, quando o tratamento de dados for irregular, quando não se observar a legislação ou não se fornecer a segurança necessária, incluindo a cibernética, conforme Códigos ISM e ISPS.

PALAVRAS-CHAVE: Responsabilidade civil. Direito marítimo. Proteção de dados. Segurança cibernética.

ABSTRACT: *Considering that cyber security in the maritime scenario represents a relevant aspect for data protection, the main objective of this work is the analysis of civil liability in the face of non-compliance with the data protection duty. Therefore, it was ratified that, as of January 1, 2021, there should be the adoption of cyber risk management in the vessels' security management systems. Finally, it was demonstrated that there will be strict civil liability, when the data processing is irregular, when the legislation is not observed or the necessary security is not provided, including cybernetics, according to ISM and ISPS Codes.*

KEYWORDS: *Civil liability. Maritime law. Data protection. Cybersecurity.*

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.

* Doutora e mestre em Direito pela Universidade Federal de Pernambuco (UFPE). Especialista em Liability for Maritime Claims e Law of Marine Insurance, pela International Maritime Law Institute. Professorda da Faculdade Damas da Instrução Cristã. Professora Adjunta da UFPE. Vice-presidente da OAB-PE. Presidente da Comissão de Direito Marítimo, Portuário e do Petróleo da OAB.PE e Secretária geral da Comissão Nacional de Direito Marítimo e Portuário da OAB. Membro da diretoria da Women's International Shipping & Trading Association (WISTA), do Instituto Ibero Americano de Direito Marítimo – IIDM, da Associação Brasileira de Direito Marítimo – ABDM e do Instituto dos Advogados de Pernambuco – IAP. Oficial da Ordem do Mérito Naval – Marinha do Brasil. Sócia titular do escritório Queiroz Cavalcanti Advocacia. E-mail: ingridzanella@qca.adv.br.

A Constituição da República Federativa do Brasil de 1988, através da Emenda Constitucional nº 7, de 15.8.1995 deu nova redação ao parágrafo único, do art. 178 (cento e setenta e oito),[1] que passou a permitir o uso de bandeiras estrangeiras na navegação de cabotagem no Brasil.

Dessa forma o parágrafo único, do supracitado artigo, passou a ter a seguinte redação: "Na ordenação do transporte aquático, a lei estabelecerá as condições em que o transporte de mercadorias na cabotagem e a navegação interior poderão ser feitos por embarcações estrangeiras".

A abertura constitucional à navegação de cabotagem e interior por embarcações estrangeiras foi decorrência da afirmação do Estado democrático de direito, ratificado com a Constituição Federal de 1988, que demarcou a necessidade de uma Constituição Econômica com a extinção de certas restrições ao capital estrangeiro. Desta forma, percebe-se que a intenção da EC nº 7/1995 foi possibilitar a regulação da matéria através de lei ordinária, bem como contribuir para a construção de uma economia mais aberta e competitiva.

No Brasil, atualmente, encontra-se em discussão o programa de estímulo ao transporte marítimo por cabotagem, com objetivo de ampliar a oferta e melhorar a qualidade do transporte marítimo, incentivar a concorrência e a competitividade entre outros. Ainda se destaca o incentivo pela utilização de navios autônomos, bem como de outros sistemas dotados de inteligência artificial, que envolvem uma séria de questões afetas à responsabilidade civil.

Neste 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[2].

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

[1] "Art. 178. A lei disporá sobre a ordenação dos transportes aéreo, aquático e terrestre, devendo, quanto à ordenação do transporte internacional, observar os acordos firmados pela União, atendido o princípio da reciprocidade. Parágrafo único. Na ordenação do transporte aquático, a lei estabelecerá as condições em que o transporte de mercadorias na cabotagem e a navegação interior poderão ser feitos por embarcações estrangeiras".
[2] 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.

um sofisticado ataque cibernético contra os sistemas de TI da organização, o qual conseguiu ultrapassar as robustas medidas de segurança em vigor.[3]

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 ataque cibernético, depois da suíça MSC, da chinesa COSCO Shipping e da dinamarquesa Maersk[4].

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).[5]

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[6]), 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

[3] A IMO foi atingida por um ataque cibernético. *Revista Transporte e Negócios*, Recarei, 01 out. 2020. .Disponível em: https://www.transportesenegocios.pt/imo-alvo-de-ataque-cibernetico/. Acesso em: 04 jan. 2021.
[4] *Ibidem.*
[5] 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 jan. 2021.

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

Gerenciamento de Segurança existentes. Neste sentido, a segurança cibernética deverá ser coberta pelo Código ISM a partir de 1º de janeiro de 2021.[7]

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.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

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).

No cenário marítimo, considerando a navegação de longo curso, interacional, bem como as diversas nacionalidades das embarcações, tripulantes e elementos de conexão no Direito Internacional, importante que ambos os regulamentos sejam considerados, principalmente quando se trata de responsabilidade civil e segurança marítima.

Desta forma, o objeto principal do presente trabalho é analisar a responsabilidade civil pela violação do dever de proteção de dados no cenário marítimo, considerando as medidas de segurança cibernética como obrigatórias.

Em outras palavras, comprovando que caso não sejam adotadas as medidas obrigatórias de segurança cibernética, no âmbito marítimo, poderá ser caracterizado o tratamento de dados como irregular, por não ter sido observada a legislação pertinente, bem como não ter sido fornecida a segurança necessária, gerando responsabilidade civil específica pelo descumprimento dever de proteção de dados.

[7] 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".

Da mesma forma, abordar-se-á 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.

1 BREVES NOTAS SOBRE A PROTEÇÃO DE DADOS NO CENÁRIO MARÍTIMO

Importante esclarecer a quem se aplica o Regulamento Geral de Proteção de Dados da UE (GDPR) no setor marítimo.

Inicialmente, de acordo com o GDPR, qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o regulamento, independentemente de o tratamento em si ser realizado na União.

Igualmente, que o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento não estabelecido na União deverá ser abrangido pelo regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento.

Ainda, que o tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável que não esteja estabelecido na União deverá ser também abrangido pelo regulamento quando esteja relacionado com o controle do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União.

Desta forma, o campo de aplicação territorial do GDPR foi então definido no art. 3º, *vide*:

> 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.
> 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:
> a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

> b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.
> 3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

Considerando o campo de aplicação do GDPR, possível então fazer uma relação específica no que concerne ao setor marítimo. Pode-se concluir que o mencionado regulamento se aplica ao armador, proprietário da embarcação, agente marítimo que processam dados pessoais de pessoas vinculadas à União Europeia ou que estão estabelecidos na União Europeia, independentemente da bandeira do navio e da nacionalidade da tripulação.

Destaca-se que armador é pessoa física ou jurídica que, em seu nome e sob sua responsabilidade, apresta a embarcação com fins comerciais, pondo-a ou não a navegar por sua conta. Por sua vez, tripulante é o aquaviário ou amador que exerce funções, embarcado, na operação da embarcação, toda embarcação e dotada de um número mínimo de tripulantes, chamada de tripulação de segurança. É competência da Autoridade Marítima determinar a tripulação de segurança de cada embarcações.

Ainda, que, no Brasil, a Lei nº 9537/1997, que dispõe sobre a segurança do tráfego aquaviário em águas sob jurisdição nacional, embarcação é qualquer construção, inclusive as plataformas flutuantes e, quando rebocadas, as fixas, sujeita a inscrição na autoridade marítima e suscetível de se locomover na água, por meios próprios ou não, transportando pessoas ou cargas.

Podemos dividir didaticamente a aplicação do GDPR às empresas, considerando o território europeu e os cidadãos europeus, da seguinte forma: (*i*) empresas estabelecidas na União Europeia (UE), que processem dados pessoas, independente de envolver cidadãos europeus, ou seja, inclusive dados de estrangeiros, desde que estema situadas na EU; (*ii*) empresas situadas fora da UE, mas que que processam dados pessoais cidadãos europeus, tripulantes ou passageiros, mesmo em cruzeiros marítimos; (*iii*) empresas, independentemente de estarem situadas em território europeu, mas que ofereçam bens ou serviços a indivíduos na UE ou monitorem seu comportamento.

Por esta razão, não se considera a bandeira ou a nacionalidade do navio e da tripulação. Importante mencionar que o navio é coisa, bem móvel, entretanto de feitio todo especial, pelo

qual merece tratamento mais aprofundado, como instrumento do transporte marítimo, sendo dotado, portanto, de nacionalidade.

De acordo com a Convenção das Nações Unidas sobre o Direito do Mar – CNUDM (Decreto n° 1.530, de 22 de junho de 1995), todo Estado deve estabelecer os requisitos necessários para a atribuição da sua nacionalidade a navios, para o registro de navios no seu território e para o direito de arvorar a sua bandeira. Assim, de acordo com art. 91 da CNUDM, deve haver um elo substancial, um vínculo entre o navio e o Estado de registro.[8]

Como observa Arnaldo Sussekind, as embarcações constituem estabelecimentos móveis, cuja nacionalidade decorre da patente de navegação, comprovada pela respectiva certidão de registro.[9] Logo, o Estado onde se processa o registro da embarcação é detentor da competência para estabelecer os requisitos para concessão de bandeira do país.

A Convenção das Nações Unidas sobre o Direito do Mar, estabelece em seu art. 94, os deveres do Estado de bandeira, constituindo que "1. Todo Estado deve exercer, de modo efetivo, a sua jurisdição e seu controle em questões administrativas, técnicas e sociais sobre navios que arvorem a sua bandeira'.

O Professor Waldemar Ferreira esclarece que o navio tem estado civil, nome, domicílio, nacionalidade, nos seguintes termos:

> Nasce pela sua construcção, como producto do engenho humano. Tem estado civil. Tem nome. É batizado e registrado. Tem domicílio. Carece de passaporte para viajar. Singra os mares. Movimenta riquezas. Põe em contacto os homens de todos os continentes. Vive. Tem nacionalidade, a da sua bandeira. Envelhece, pela sua imprestabilidade, resultante da acção do tempo e do uso, transfigurando-se, às vezes. E chega a morrer, quando não logra vencer o Ímpeto e a fúria dos temporaes. Tem, portanto, individualidade.[10]

Neste sentido, esclarece o Prof. Herculao Inglez, que o navio seria dotado de um sistema de quase personalidade. Explica ainda que o referido atributo é, além disso, uma necessidade lógica do sistema, regulando as relações oriundas da indústria da navegação, e que se baseia no grande princípio da separação do patrimônio de terra e do patrimônio do mar, por extensão do

[8] CAMPOS, Ingrid Zanella Andrade. *Direito Marítimo Sistematizado.* Curitiba, Juruá, 2017, p. 125.
[9] SUSSEKIND, Arnaldo. *Conflitos de leis do trabalho.* Rio de Janeiro: Freitas Bastos, 1979, p. 52.
[10] FERREIRA, Waldemar Martins. *O commercio marítimo e o navio.* São Paulo: Revista dos Tribunais, 1931.

princípio da comandita que, historicamente, se desenvolveu, se é que se não originou, dos usos e costumes do comércio de mar.[11]

Desta forma, cada Estado estabeleceu livremente o critério de concessão de sua nacionalidade à embarcação, seguindo a CDNUM. No Brasil, o critério adotado para a concessão da nacionalidade brasileira é o misto, assim terão o direito de arvorar a bandeira brasileira as embarcações inscritas no Registro de Propriedade Marítima, de propriedade de pessoa física residente e domiciliada no País ou de empresa brasileira; e, sob contrato de afretamento a casco nu, por empresa brasileira de navegação, condicionado à suspensão provisória de bandeira no país de origem. [12]

Por sua vez, no Brasil, a LGPD se aplica a qualquer pessoa, natural ou jurídica, de direito público ou privado, que preencha pelo menos um dos seguintes requisitos: (*i*) tratamento seja realizado no Brasil; (*ii*) oferecem serviços ou mercadoria ao mercado consumidor brasileiro; (*iii*) coletam/tratam dados de pessoas localizadas no Brasil.

Conforme esclarecido, tanto o GDPR como a LGPD possuem aplicação direta aos atores marítimos, objetivando a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2 APLICAÇÃO DA PROTEÇÃO DE DADOS ÀS RELAÇÕES TRABALHISTAS MARÍTIMAS

Como analisado, o GDPR se aplica ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

Nessa senda, o GDPR estabelece, quando trata do contexto laboral, em seu art. 88, que:

> 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do

[11] 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.
[12] CAMPOS, Ingrid Zanella Andrade. *Direito Marítimo Sistematizado.* Curitiba, Juruá, 2017. p. 125.

> trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.[1]

Conforme visto, a LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados. Ainda, quando trata das hipóteses de não aplicação, o art. 4º não menciona as relações trabalhistas, *vide*:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou

De tal modo, da leitura dos dois normativos citados é possível concluir que ambos se aplicam às relações de trabalho. Desta forma, cogente a interpretação que igualmente se aplicam às relações de trabalho no âmbito marítimo.

Esclarece-se que os trabalhadores marítimos constituem o conjunto de pessoas empregadas a serviço do navio e embarcadas mediante um contrato de trabalho. No Brasil de acordo com a Lei nº 9.537/97, que dispõe sobre a segurança do tráfego aquaviário em águas sob jurisdição nacional (LESTA), tripulante é o aquaviário ou amador que exerce funções embarcado na operação da embarcação.

O tripulante deve ser contratado através de uma relação é de emprego, conforme disciplina a LESTA, ao instituir que os aquaviários devem possuir o nível de habilitação estabelecido pela autoridade marítima para o exercício de cargos e funções a bordo das embarcações, e que o embarque e desembarque do tripulante submete-se às regras do seu contrato de trabalho (art. 7^0, parágrafo único). Quanto à relação de vínculo de emprego essa ocorre com o armador da embarcação, que é pessoa física ou jurídica que, em seu nome e sob

sua responsabilidade, apresta a embarcação com fins comerciais, pondo-a ou não a navegar por sua conta[13].

Portanto, não existem dúvidas da incidência do GDPR e da LGPD às relações trabalhistas, inclusive às marítimas, desde que haja a aplicação material e territorial das normas, considerando o campo de aplicação.

3 CONTROLADOR E OPERADOR DE DADOS NO CENÁRIO MARÍTIMO

De acordo com a LGPD, controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; por sua vez, operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

As obrigações e a responsabilidade civil pelo descumprimento do dever de proteção de dados envolvem esses dois personagens, de forma isolada ou solidaria, de acordo com a LGPD.

Controlador, assim, é a pessoa que toma as decisões referentes ao tratamento de dados pessoais, no cenário marítimo, pode ser o proprietário, armador, fretador. O operador, por sua vez, realiza o tratamento de dados pessoais em nome do controlador, ou seja, poderá ser armador, afretador ou agentes marítimos.

A figura do afretador ou fretador está diretamente relacionada a existência de um contrato de afretamento. Desde já se esclarece que o contrato de afretamento é o acordo pelo qual o proprietário (fretador) de um navio se compromete, percebendo em contrapartida o frete, a transportar, ou a possibilitar que o afretador transporte, mercadorias em um determinado navio.[14]

De acordo com Pontes de Miranda no afretamento se atribui o uso e a fruição do navio, por sua vez no contrato de transporte, o transportador tem o dever de transferir bens ou pessoas, de um lugar a outro.[15]

[13] CAMPOS, Ingrid Zanella Andrade. *Direito Marítimo Sistematizado*. Curitiba, Juruá, 2017. p. 281.
[14] CAMPOS, Ingrid Zanella Andrade. *Direito Marítimo Sistematizado*. Curitiba, Juruá, 2017. p. 290.
[15] MIRANDA, Pontes de. *Tratado de direito privado*. Parte especial. Tomo XLV: Direito das obrigações. Rio de Janeiro: Editor Borsoi, 1964. p. 109.

4 DEVER DE PROTEÇÃO DE DADOS E A SEGURANÇA CIBERNÉTICA NO DIREITO MARÍTIMO

De acordo com a LGPD, algumas medidas devem ser adotadas para a efetiva proteção dos dados pessoais. Conforme estabelece o art. 46:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Da mesma forma, o GRPD determina, no art. 32, quando trata de segurança do tratamento de dados, que:

> Artigo 32. Segurança do tratamento:
> 1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
> a) A pseudonimização e a cifragem dos dados pessoais; 4.5.2016 PT Jornal Oficial da União Europeia L 119/51;
> b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
> c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Importante destacar que essas medidas envolvem pessoas, processos e tecnologia. No que se refere à tecnologia, importante acompanhar se as ferramentas são suficientes, se há pontos de melhoria, com atualização e revisão constante. Ainda, se pessoas são o elo mais frágil quando o assunto é segurança, é de suma importância que haja treinamento constante, e que a cultura da empresa seja amplamente divulgada para seus colaboradores.[16]

[16] 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. 83.

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) (IMO, 2017a).

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.[17]

Neste sentido, as Diretrizes para Navios sobre Segurança Cibernética (*The Guidelines On Cyber Security Onboard Ships*)[18], 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;

[17] 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.

[18] 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 dez. 2020.

> 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[19].

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) (IMO 2017a).

5 RESPONSABILIDADE CIVIL PELA VIOLAÇÃO DO DEVER DE PROTEÇÃO DE DADOS, INCLUINDO SEGURANÇA CIBERNÉTICA, NO ÂMBITO MARÍTIMO

O GRPD estabelece o direito de interposição de ação judicial, quando existir violação dos direitos assegurados pelo regulamento, no art. 79, que:

> 1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar reclamação a uma autoridade de controlo, nos termos do artigo 77.o, todos os titulares de dados têm direito à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento.

Por sua vez, a responsabilidade civil é tratada na Seção III do Capítulo VI da LGPD, "Da Responsabilidade e do Ressarcimento de Danos". Nesta senda, é possível se identificar

[19] 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 dez. 2020.

dois campos nítidos de responsabilidade civil, quais sejam: violação à legislação de proteção de dados e deixar de adotar as medidas de segurança estabelecidas na lei, que causem dano.

As referidas hipóteses estão previstas nos arts. 42 e 44, da LGPD. Conforme dispõe o art. 42, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Conforme constitui o artigo, a responsabilidade será do controlador ou do operador, a depender da situação, poderá ser solidária, em face da previsão legal.

Por seu turno, o art. 44, parágrafo único, estabelece que: "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano".

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.

Destaca-se que quando existe uma relação jurídica de consumo, a responsabilidade deve seguir a norma especifica, qual seja o Código de Defesa do Consumidor, conforme dispõe o art. 45, vide: "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

Conforme estabelece a LGPG, a responsabilidade civil poderá ser do controlador, do operador ou solidária (segundo hipóteses legais).

A responsabilidade civil solidária entre o controlador e o operador deverá ocorrer nos casos previstos em lei, quando o operador não seguir as instruções lícitas do controlador, quando descumprir obrigações legais, conforme previsto no art. 42, da seguinte forma:

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

O tratamento de dados será considerado irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado (art. 44, LGPD).

Pela existência do dever geral de segurança imposto no art. 44, as medidas de *compliance*, a comprovação de boas práticas e as certificações são, igualmente, elementos relevantes no âmbito da análise da responsabilidade civil na LGPD[20]. Isso, conforme visto, inclusive no cenário marítimo, em face da adoção obrigatória de padrões e ações considerando a segurança cibernética.

A responsabilidade poderá ser afastada, nas hipóteses de ausência de tratamento de dados, ausência de violação à legislação e no caso de culpa exclusiva do titular, de acordo com o art. 43, da LGPD:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Ressalta-se ainda que não haverá responsabilidade quando os dados forem repassados por exigência legal, hipótese comum inclusive no cenário marítimo[21]. De acordo com a LGPD, o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular ou para o cumprimento de obrigação legal ou regulatória pelo controlador entre outras hipóteses.

Assim, existem exigências legais que dispensam o consentimento da parte, no caso, do tripulante. Entre essas, é possível citar, por exemplo, a obrigação constante na NORMAM 01/DPC, qual seja de os navios repassarem a lista de tripulação à Autoridade Marítima, entre os documentos necessários para a obtenção das certificações de segurança, de acordo com o

[20] 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 dez. 2020.
[21] LGPD. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

Código Internacional para o Gerenciamento de Segurança (Código ISM), adotado pela Organização Marítima Internacional (IMO) pela Resolução A. 741(18).

Importante destacar que há uma discussão atual referente à responsabilidade civil pela violação do dever de proteção de dados.

Como a LGPG eliminou termos como independente de culpa ou atividade risco, parte da doutrina entende pela adoção da responsabilidade civil subjetiva. Neste sentido, cita-se:

> A partir da segunda versão do anteprojeto de lei, ganhou força a opção por um regime de reponsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública e em audiência pública realizada na Câmara dos Deputados, essa escolha foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos antes aventados – "independentemente de culpa" ou "atividade de risco" – que eliminariam a culpa como um dos pressupostos da responsabilidade civil[22].

Rafael Dresch, por sua vez, explica que o art. 42 da LGPD estabelece que o agente de tratamento que, na realização do tratamento de dados pessoais, causar dano a outrem, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Ou seja, segundo o autor:

> Não basta, por conseguinte, o desenvolvimento da atividade de tratamento causadora de um dano para se configurar a responsabilidade civil dos agentes de tratamento, pois essa responsabilidade pode ser atribuída tão-somente quando o tratamento for considerado violador da legislação de proteção aos dados pessoais, ou seja, quando for ilícito. Frente à exigência do ilícito, também resta descartada uma responsabilidade civil objetiva centrada no risco como critério de imputação, seja qual risco for, da atividade, proveito, criado ou profissional[23].

Neste sentido, cita-se:

> Pela existência desse dever geral de segurança imposto no art. 44 citado, as medidas de *compliance*, a comprovação de boas práticas e as certificações são, igualmente, elementos relevantes no âmbito da análise da responsabilidade civil na LGPD. A Autoridade Nacional de Proteção de Dados terá, portanto, um papel destacado ao fixar os níveis de segurança, seja diretamente, através do poder normativo do agente

[22] 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*, Rio de Janeiro, a. 9. n. 3. 2020.

[23] 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 dez. 2020.

> regulador ou, indiretamente, através da possibilidade de delegar essa determinação dos padrões de segurança à autorregulação dos diversos setores do mercado[24].

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 Códigos ISM e ISPS, estar-se-ia diante de uma responsabilidade civil objetiva, ante a ausência de cumprimento do dever legal, descumprimento do dever de proteção de dados.

De tal modo, no âmbito marítimo, tanto o Certificado Internacional de Proteção de Navio, como a certificação através do Documento de Conformidade que atestará o atendimento às exigências do Código ISM, devem considerar aspectos de segurança cibernética.

Dessa forma, a segurança cibernética, como forma de preconizar a segurança de dados, será coberta pelo Código ISM, a partir de 1º de janeiro de 2021, devendo ser parte integrante do sistema de gestão da segurança, inclusive com adoção de planos de contingência.

6 CONCLUSÕES

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.

No Brasil, o tema que ganha especial relevância, com a Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709/2018, que deve ser interpretada em conjunto com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) nº 2016/679, de 27 de abril de 2016.

Conforme restou esclarecido, tanto o GDPR como a LGPD possuem aplicação direta aos atores marítimos, objetivando a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Igualmente, que não existem dúvidas sobre a incidência do GDPR e da LGPD às relações trabalhistas marítimas.

Para que haja a efetiva proteção dos dados, tanto a LGPD como o GDPR estabeleceram algumas medidas que devem ser adotadas. Assim, no âmbito marítimo, destacou-se a Resolução

[24] *Ibidem.*

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, atravpes 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, concluiu-se que, conforme LGPD, 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.

Ressaltou-se ainda que não haverá responsabilidade quando os dados forem repassados por exigência legal, que dispensam o consentimento da parte. Como exemplo, mencionou-se a obrigação constante na NORMAM 01/DPC, qual seja de os navios repassarem a lista de tripulação à Autoridade Marítima, entre os documentos necessários para a obtenção das certificações de segurança, de acordo com o Código ISM.

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

A IMO foi atingida por um ataque cibernético. *Revista Transporte e Negócios*, Recarei, 01 out. 2020. .Disponível em: https://www.transportesenegocios.pt/imo-alvo-de-ataque-cibernetico/. Acesso em: 04 jan. 2021.

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 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*, Rio de Janeiro, 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 dez. 2020.

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

IMO. International Maritime Organization. *Resolução MSC 428* (98)/2017a.

IMO. International Maritime Organization. *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.

SOUZA, Herculano Marcos Inglez de. *Projecto de Código Commercial.* Introdução. v. 1. Rio de Janeiro: Impr. Nacional, 1912. 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 jan. 2021

Submissão: 13/09/2021
Aceito para Publicação: 16/12/2021

DOI: 10.22456/2317-8558.118342