REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

A CIBERSEGURANÇA NA PERSPECTIVA DO DIREITO MARÍTIMO E PORTUÁRIO CONSIDERANDO A EVOLUÇÃO TECNOLÓGICA

CYBERSECURITY FROM THE PERSPECTIVE OF MARITIME AND PORT LAW CONSIDERING TECHNOLOGICAL EVOLUTION

Acir Alves Coelho Junior[1]
Larysa Cassatti da Silva[2]

RESUMO: Este estudo analisa a cibersegurança e os desafios para o Direito Marítimo e Portuário considerando a evolução tecnológica. O tema é importante devido ao impacto que a tecnologia apresenta para o campo jurídico destes que desempenham papéis relevantes para o comércio global. Com a crescente digitalização, as operações ficam vulneráveis a ataques cibernéticos, o que afeta a segurança operacional, administrativa e pessoal. A metodologia utilizada será qualitativa, do tipo bibliográfico, sendo dedutivo com natureza descritiva e exploratória. Apesar dos avanços que as legislações deram no que se refere à cibersegurança, ainda há questões que devem ser levadas em consideração, devido à sua importância global. No que se se refere à responsabilidade civil apesar de não ser encontrado com facilidade no ramo do Direito portuário a resposta sobre, e sim no Marítimo, se deduz que ambos possuem responsabilidade objetiva, nos casos que violar as medidas de segurança, deflagrando a proteção de dados do arts. 42 e 44 da LGPD, assim como Convenção Internacional para Salvaguarda da Vida Humana no Mar (SOLAS) que as demais disposições devem obrigatoriamente seguir.

Palavras-chave: cibersegurança; hackers, Direito Marítimo; Direito Portuário.

ABSTRACT: This study deals with cybersecurity and its challenges in Maritime and Port Law considering technological evolution. The topic is important due to the impact that technology has on the legal field, especially with regard to Maritime and Port Law, which plays a relevant role in global trade. With increasing digitalization, operations are vulnerable to cyber-attacks, which affects operational, administrative and personal security. The methodology used wil qualitative, bibliographical, detective with a descriptive and exploratory nature. Despite the great advances that legislation has made regarding cybersecurity, there are still issues that must

[1] Possui graduação em Direito pela Universidade do Planalto Catarinense, Pós Graduação em Direito e Processo do Trabalho pela Universidade Federal de Santa Catarina, especialização em Direito Marítimo, Portuário e Aduaneiro pela Universidade do Vale do Itajaí, MBA em Administração Global pela Universidade Independente. Mestre em Administração pela Universidade do Estado de Santa Catarina, aperfeiçoamento em Ciências Políticas pela *Universidad de La Habana* e aperfeiçoamento em Negócios Internacionais pela *Universidad de Panama*. Doutor em Meio Ambiente. Professor da Universidade da Região de Joinville (UNIVILLE).

[2] Bacharel em Direito pela Universidade da Região de Joinville (UNIVILLE). Áreas de interesse e pesquisa incluem Direito Marítimo, Portuário, Internacional, Aduaneiro e temas relacionados à tecnologia.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

be taken into consideration, due to their global importance. About civil liability, although the answer to this is not easily found in the field of port law, but rather in maritime law, it can be deduced that both have objective liability, in cases where security measures are violated, triggering protection. of data from arts. 42 and 44 of the LGPD, as well as the International Convention for the Safety of Life at Sea (SOLAS), which the other provisions must follow.

Keywords: cybersecurity; hackers; Maritime Law; Port Law.

1 INTRODUÇÃO

O presente trabalho tem como objeto analisar as implicações da cibersegurança advinda dos avanços tecnológicos no Direito Marítimo e Portuário, dada sua relevância no cenário global e econômico. Assim sendo, a escolha do tema foi baseada na análise dos dias atuais e na crescente preocupação com os avanços tecnológicos nestes setores. A indústria 4.0 abrange os meios de proteção de operações, sistemas, gerenciamento de interesses pessoais e econômicos, bem como a apuração da responsabilização civil em caso de incidentes "considerando que um ataque pode alterar a rota de navegação, atingir equipamentos, causar acidentes marítimos e violar dados pessoais" (CAMPOS, 2021, p. 128 - 148). Deste modo, a importância do tema decorre da intersecção e combinações acadêmicas, práticas e sociais, bem como da sua relevância global na economia e do crescente interesse na cibersegurança.

A cibersegurança surgiu da necessidade e da percepção de que a tecnologia crescia de forma exponencial e que a ineficiência de tais questões poderiam afetar em todas as sociedades, assim como o Direito Marítimo e Portuário que é objeto de estudo deste trabalho, já que há necessidade de aprimoramento em questões administrativas, operacional e as demais questões que serão abordadas neste trabalho.

Em decorrência dos riscos políticos e econômicos, a tecnologia se faz presente nestes setores para viabilizar a conectividade, eficiência e o alcance global, na qual facilita a comunicação e o acesso às informações. Segundo Gatto e Albuquerque (2023), "o avanço tecnológico e as transformações digitais permitiram um avanço significativo na forma como os setores marítimo e portuário operam", já Santos e Araújo pontuam que (2023, p. 4), "a internet trouxe inúmeras possibilidades e vantagens, como a facilidade de comunicação, acesso à informação e oportunidades de negócios". Dessa forma, compreender como a cibersegurança funciona em diferentes setores é crucial, uma vez que a cibersegurança não apenas protege a

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

integridade e confidencialidade dos dados, incluindo dados pessoais, como também contribui para a produtividade e crescimento contínuo. Além disso, oferece soluções para otimizar a logística e aumentar a eficiência das operações, aumentando a confiança dos armadores, prestadores de serviços e outros atores envolvidos (GATTO; ALBUQUERQUE, 2023).

Seguindo o mesmo parâmetro, às questões digitais automatizam e incentivam sua adoção e uso, especialmente diante das crescentes ameaças, como os *malwares*, *phishing* e ataques de negação de serviço (DoS), que representam ataques dos *hackers*. Isso, aliado à necessidade de atender às demandas interligadas, que impulsionam a conectividade e a automação para alcançar objetivo como a redução de custos, o cumprimento de metas e a otimização do tempo das atividades Marítimas e Portuárias que facilitam as operações diárias (SOPESP- Sindicato dos Operadores Portuários do Estado de São Paulo, 2019).

Sendo assim, é claro que é necessário estabelecer atividades necessárias para o gerenciamento e controle destes ataques, sobretudo no que diz respeito à responsabilização civil, dada sua alta capacidade de intencionalidade e complexidade, já que "é um aspecto importante para garantir que aqueles que cometem crimes cibernéticos sejam responsabilizados pelos danos causados" (SANTOS; ARAÚJO, 2023, p. 4).

Ademais, no cenário marítimo e portuário, sua relevância é ainda maior devido ao fato de que 90% das mercadorias são transportadas pelo mar, o que demonstra a relevância dos estudos e das regulamentações no âmbito do Direito Marítimo e Portuário (CASTRO, 2021, p. 5 - 6). Dessa forma, esses dados reforçam a necessidade de uma análise mais ampla e multidisciplinar das implicações da cibersegurança nos setores marítimos e portuários, tendo em vista os diversos aspectos técnicos, legais e operacionais envolvidos.

A Revolução Técnico-Científica-Informacional, no século XX, a mercantilização dos produtos, de acordo com Faria (2020), passou a ser informatizada de forma muito rápida na busca da automatização em diversos setores, principalmente no que diz respeito ao setor marítimo-portuário, que está cada vez mais confiando nas novas tecnologias para se tornar competitivo e eficiente na gestão de seus recursos. Isso resulta em um grande volume de dados armazenados e gerados, surgindo assim a necessidade de implementação de Inteligência Artificial (IA) para facilitar as operações. No entanto, a inserção dos meios tecnológicos abre

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

as portas para ataques cibernéticos, uma vez que apresentam um sistema vulnerável, muitas vezes devido a erros dos setores que administram e à falta de regulamentação. Essa falta de regulamentação é devida à dificuldade do legislador em acompanhar os avanços tecnológicos, além da implementação das regulamentações (CF/88, convenções internacionais etc.) e das plataformas como *blockchain* ou *TradeLens*, configuradas para os setores Marítimo e Portuário.

No que se refere à vulnerabilidade e ao foco para a modernização, de acordo com Faria (2020, p. 165 - 187), há uma interconexão que facilita o comprometimento dos sistemas em relação às ciberameaças, como intersecção de comunicações, *malwares*, roubo de identidade, roubo ou manipulação e fuga de informações, mudança de rotas para roubo de cargas, dentre outros. Os ataques podem ocorrer com a simples abertura de um e-mail infectado por *phishing*, e-mail *attachments* (anexos) ou *hyperlink*. Após o término do ataque, os impactos podem ser devastadores: disrupção, ausência de fluxos de informação entre os sistemas de controle do navio, e a base de controle e os sistemas de TI nos portos.

Diante das diversas modulações de ciberataques e dos efeitos que causam para os operadores e responsáveis pelo setor marítimo-portuário, há os altos custos para tentar amenizar os danos causados, seja pela recuperação de dados, seja pela via judicial para a responsabilização civil, além de questões éticas, por podem afetar valores como a privacidade, a propriedade, a liberdade, a saúde ou a vida. Os fornecedores de cibersegurança têm de lidar com desafios éticos associados ao conhecimento dos limites da sua própria atuação: saber até onde devem ir para garantir os propósitos de segurança e integridade das redes, sem contender com os interesses e direitos fundamentais dos vários agentes envolvidos (ANDRADE, 2020).

O texto inicia contextualizando a evolução tecnológica e a segurança cibernética, e o desenvolvimento destes, destacando os desafios e os riscos que o Direito Marítimo e Portuário encontram diante da evolução tecnológica e sua responsabilidade civil, para então adentrar na problemática e a regulamentação, diante a evolução tecnológica, com ataques cibernéticos em busca de uma maior segurança jurídica.

2 A EVOLUÇÃO TECNOLÓGICA E A SEGURANÇA CIBERNÉTICA

Os eventos históricos como a Revolução Industrial, ocorrida em meados do século

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

XIII, que introduziu as máquinas a vapor, influenciaram significativamente a evolução da época, além de ter influenciado em diversos aspectos evolutivos da tecnologia (CAVALCANTE, 2019, p. 01), e posteriormente influenciando na cibersegurança, uma vez que a sociedade está em constante mudança, adequando-se às suas necessidades.

Nesse contexto, a tecnologia já estava presente em diversas sociedades e culturas, mas de maneiras distintas, como na fabricação de ferramentas agrícolas ou na China na medieval, que produzia pólvoras para fins militares, como a fabricação de bombas.

> A tecnologia sempre existiu, desde o início dos tempos ela já estava entre nós, só que em formas diferentes que nós não conseguimos enxergar, nos tempos antigos foi criada a roda, uma forma de inovação, de tecnologia, isso há 3.500 a.C, já na idade média os chineses inventaram a pólvora e os fogos de artifício, no século XVIII, mais precisamente no ano de 1712, Thomas Newcomen desenvolve o motor a vapor (SANTOS; RODRIGUES; SOUZA, 2019, p. 01).

A tecnologia surgiu devido à necessidade do homem de se adaptar à sua época. Os *Homo Erectus*, durante a Era Paleolítica, perceberam que pedras poderiam gerar faíscas ao contato com materiais com capacidade de combustão, o que resultou em uma das maiores revoluções até os dias atuais, a descoberta do fogo, que transformou os instintos de sobrevivência de 1,8 milhões e 300 mil anos atrás em algo tão inovador.

> Entre 1,8 milhões e 300 mil anos atrás, o *Homo Erectus*, um ser com o raciocínio mais evoluído, descobriu que se fizesse fricção entre duas pedras, esfregando uma na outra, ele conseguia produzir uma faísca, que se colocada em algum lugar de fácil combustão, pegaria fogo normalmente (MUSITANO; COLONESE, 2021).

É evidente que, com a evolução da sociedade, há uma constante busca por aprimoramento e mudança em suas criações, assim como ocorreu com a tecnologia, que surgiu para facilitar e incentivar tanto as questões comerciais quanto sociais. Após essas considerações, é possível adentrar na área de estudo do presente trabalho, que se concentra na cibersegurança sob a perspectiva do Direito Marítimo e Portuário, considerando a evolução tecnológica.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

2.1 Visão geral do surgimento da cibernética diante as transformações tecnológicas

O marco da era cibernética, iniciou-se com Bob Thomas em 1971, desafiando toda a ciência computacional, a possibilidade de um *software*[3] se movimentar por meio de rede, sem deixar rastros, recebendo a denominação de primeiro *worm*[4]. Por seguinte, foi estudado por Ray Tomlinson, na tentativa de autor replicar o *worm*, tendo êxito em seu estudo.

Em 1983, foi concedida nos Estados Unidos, quando o *Massachusetts Institute of Technology* (MIT) desenvolveu um sistema e método de comunicação criptografada - a Patente 4,405,89 (LOTUFO, 2020, p. 01). Já em 1986 foi o momento em que tentativas pacíficas de Bob Thomas se tornaram precursoras de uma era obscura para a cibersegurança, de modo que houve ataque pelo alemão Markus, em uma base militar. De acordo com Lotufo (2020, p. 02) "Markus Hess conseguiu hackear um portal em Berkeley e usou essa conexão para acessar a *Arpanet*, conseguindo hackear 400 computadores militares com informações sensíveis, inclusive materiais do Pentágono, com a intenção de vender a informação para a KGB". No entanto, foi uma tentativa frustrada, uma vez que foi detectada pelo astrônomo Clifford Stoll, nomeado sua técnica de *honeypot*.

Não obstante, as demais tentativas em 1988, dois anos após o ataque *hacker* frustrado por Markus Hess, Robert Morris fez sua tentativa, colocando o nome de "*Morris worm*[5]", consistindo em testar a força da internet, assim criando um programa que se propagava. Segundo Lotufo (2020, p. 02) "o pesquisador criou um programa que deveria se propagar pela internet, se infiltrar nos terminais Unix usando um *bug* conhecido e depois se auto replicar nesses ambientes" e a consequência disto foi o reconhecimento em ser a primeira pessoa do mundo ser autuada sob *Computer Fraud and ABuse Act* pelo ataque *Denieal-of-Service (DoS)*.

[3] *Morris worm,* denominação dada pelo Robert Morris em sua tentativa de forçar a internet, ou seja, Morris é em sua homenagem e *worm* significa verme.
[4] *Hardware*, é a parte física do computador, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos que fazem o computador funcionar (DANTAS).
[5] *Software, "*Software é um conjunto de instruções que devem ser seguidas e executadas por um mecanismo, seja ele um computador ou um aparato eletromecânico. É o termo usado para descrever programas, apps, scripts, macros e instruções de código embarcado diretamente (firmware), de modo a ditar o que uma máquina deve fazer" (GOGONI, 2023).

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

Diante desta contextualização, nota-se que um estudo em que não se tinha pretensão de causar algum tipo de incidente, tomou proporção oposta, quando outras pessoas identificaram que tal descoberta seria revolucionária para a ciência da computação, uma vez que as pretensões divergiram para busca de poder e subordinação, pois essa inovação colocaria dados sensíveis em risco, assim fragilizando qualquer sistema existente.

2.2 A transformação digital e a vulnerabilidade dos sistemas

A transformação digital, se modula com a evolução tecnológica, no qual segundo Sleiman (2020, p. 06) "é indiscutível o fato de que ela está relacionada à evolução tecnológica e seu impacto para a sociedade, portanto, na forma de se relacionar, interagir, consumir e de produzir – como produtos digitais, entre outros". Portanto, é importante ressaltar que tal ocorreu em uma época que os padrões de organização eram simples do que se é atualmente, este seria imagináveis compreender como, por exemplo, os homens da caverna conseguiram se desenvolver, pela insuficiência de recursos, em que no século XXI não é o problema. Mas é indiscutível que as transformações que ocorreram em tempos tão distantes, como o do surgimento do fogo, foram cruciais e impactaram para evolução e transformação tecnológica.

Nas palavras de WEISS (2019, p. 1):

> A vida humana tem sido marcada pelas novidades, pelas mudanças, decorrentes de sua inegável inventividade. Hoje nos encontramos e nos relacionamos no mundo virtual. Já não nos reunimos em torno de nogueira ou ao pé do rádio, como faziam nossos antepassados. Nossas fogueiras e rádios agora se chamam redes sociais e tudo sugere que não poderemos nos desvencilhar sem danos.

De praxe, estas transformações continuaram ocorrendo e cada vez mais rápidas, uma vez que vivessem em uma era de transformações digitais e de que modo analítico se caracteriza um sistema concorrencial de mercado, que consiste em transformar e aprimorar suas tecnologias. Deste modo, pode conceituar a Transformação digital, segundo Vial (2019 *apud* FROEHLICH; REINHART; NUNES, 2023, p. 2), é um processo que busca o melhoramento para obtenção de uma maior organização, resultando em melhoras significativas tais como, nas combinações tecnológicas de informações, computação e de conectividade. Portanto, denota-

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

se que se subsidiária na perspectiva da evolução tecnológica, pois a partir do mesmo em que nasceu o entendimento das demais áreas da ciência da computação.

Devido às constantes mudanças, existe a preocupação em relação à vulnerabilidade dos sistemas, que decorrem da busca de adequação às necessidades pessoais e das transformações tecnológicas, as quais estão sujeitos a falhas que ocorrem denominados como *malwares,* sendo *software,* atacam arquivos, ou seja, são contenciosamente maliciosos, subtraindo informações, podendo se dividir em *ransomware,* consistindo em sequestro de dados concordantes ou não.

Deste modo, segundo Tupinambá (2020, p. 29) "temos visto um aumento das proteções lógicas (software) das empresas e, ao mesmo tempo, o crescimento de ataques físicos à infraestrutura e à segurança dos dados corporativos". Existe ainda, os *phishing* ou *phishing scam* 'golpe de pescaria', que em 2020 foi considerado um dos maiores vetor de ataques e fraudes cibernéticos, segundo as palavras de Tupinambá (2020, p. 15) "consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou executar algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios.

É uma técnica de engenharia social, assim como ocorre golpe no cotidiano, como fraude do *WhatsApp* ou fraude de cartão de crédito, em que alguém com conhecimento específico consegue invadir e enganar pessoas sem conhecimento sobre. A mesma situação ocorre em companhias em que há indivíduos qualificados e com acesso a uma ampla gama de inovações, resultando em uma dependência tecnológica dos setores marítimo e portuário segundo (Gatto e Albuquerque, 2023).

Portanto, a tecnologia é um campo muito vasto, na qual os sistemas, mesmo tendo certa complexidade, estão sujeitas a invasões, pois da mesma forma que existem estudiosos da ciência criando *softwares* para integralizar os sistemas de forma pacífica, tentando proteger dados e simplificar o serviço, existem as pretensões maliciosas dos *hackers* que conseguem fraudar e causam danos irreversíveis para grandes, pequenas empresas que buscam preservar seus sistemas.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

3 A SEGURANÇA CIBERNÉTICA NOS SETORES MARÍTIMO E PORTUÁRIO

Para abordar o assunto em questão, é necessário compreender as suas particularidades e as conexões jurídicas. Antes de tudo, é importante salientar que são ramos distintos e autônomos e possuem suas particularidades que os diferenciam, assim como exposto em sua definição, na qual segundo o Nunes (*apud*, WANDERMUREM, 2019) o Direito Marítimo é o conjunto de normas que regulam as relações jurídicas que versam sobre a navegação e do comércio marítimo, fluvial ou lacustre, bem como dos navios a seu serviço e os direitos e obrigações das pessoas que se dediquem ao ramo. Já o "Direito Portuário regula as relações portuárias, como de gestão de contratos, a armazenagem das cargas, a contratação de operadores efetivos ou avulsos, a qualidade das instalações e todas as demais questões envolvendo a administração portuária" (MIRÓ NETO ADVOGADOS).

No entendimento de Castro (2021, p. 6 - 29), assim entra:

> O Direito marítimo irá regular as relações do navio e a partir do navio, disciplinando as atividades que são necessárias para as embarcações efetuarem o transporte pela via aquaviária, e especialmente no que diz respeito à responsabilidade civil. Já o Direito Portuário tem como objetivo regular as atividades que se dão no porto e a partir do porto.

A indústria marítima e portuária movimenta bilhões em operação e distribuição anualmente, o que requer a integração de aspectos tecnológicos para a manutenção destas atividades. Dessa forma, a logística é aplicada ao descarregamento, à administração, ao armazenamento das mercadorias, à identificação de áreas de risco, ao transporte de cargas e operações de pesquisa, conhecidas como *offshore.* Anteposto, necessita-se se conscientizar para que as operações possam ser seguras e eficazes, a ponto em que as possibilidades e benefícios, se dão através da comunicação, que oportunizam negócios, assim como pontua (SANTOS; ARAÚJO, 2023, p. 4).

Entretanto, é necessário observar algumas regras para lidar com os riscos cibernéticos, tais como, seguir diretrizes e as medidas de prevenção, assim como de que "os usuários estejam cientes das boas práticas de uso da internet, como a criação de senhas fortes, evitar clicar em links suspeitos e manter seus dispositivos atualizados como as últimas correções de segurança" (SANTOS; ARAÚJO, 2023, p. 5). Portanto, a conscientização destes métodos e diretrizes, não

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

se faz como meio limitador de uso, mas sim como meio de prevenir e dar atenção a uma questão desafiadora dentro do mercado digital e tecnológico.

De acordo com Duarte (2020, p.3) "são vários desafios de cibersegurança que os portos e as plataformas associadas têm que enfrentar, qualquer que seja o tipo de tecnologia ou sistema de informações usadas nas atividades portuárias". Nesse sentido o tema requer uma abordagem holística para entender as ameaças emergentes, que serão submetidos e trabalhar para que os avanços da segurança cibernética segundo Gatto e Albuquerque (2023) "estejam tão evoluída quanto os hackers, adquirindo uma maturidade capaz de garantir as diretrizes acima de debelar as investidas dos criminosos", ou seja a evolução dos meios de proteção inseridos na cadeia global deve estar estabilizada ao mesmo nível ou um passo à frente dos hackers, pois com a automatização e a digitalização proporcionam eficiência e agilidade, que coincidentemente os ataques, exigindo medidas de segurança robustas e conformidade com as normas e regulamentos nacional e internacional.

Deste modo, a necessidade de se interconectar com a tecnologia devendo implementar medidas de segurança, que diante ao ataque hacker os dados são violados, sendo dos sistemas, comunicação, integridade e confidencialidade dos dados.

Nas palavras de Gatto e Albuquerque (2023):

> Entre os principais tipos de ataques estão: os direcionados, que afetam sistemas de gerenciamento de contêineres e de monitoramento de segurança, por exemplo; ataques de phishing, que envolvem o envio de e-mail fraudulentos; ataques por malware, vírus que danificam ou roubam os dados; e negação de serviço, que torna os sistemas de tráfego inoperantes.

Deste modo, vide a importância de se seguir as diretrizes da IOT (Internet das coisas), IMO (*International Maritime Organization*), GDPR (Regulamento Geral de Proteção de Dados) da União Europeia, LGPD (Lei Geral de Proteção de Dados, que segundo Santos e Araújo (2023, p. 8 *apud* NOLASCO, SILVA, 2022) na busca de conscientização e proteção aos direitos dos usuários e responsabilizar as empresas em caso de violação de dados, por isso que deve ser realizado um investimento para implementação mesmo que seja de custo elevado inicialmente, mas poderá amenizar gastos milionários em caso de ataques cibernéticos.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

3.1 Aspectos da segurança cibernética nos portos

A infraestrutura tecnológica em que emerge a cibersegurança é crítica, mesmo que desempenhe um papel importante na era da digitalização, e tal se faz pelo aumento dos riscos de ataques contra os sistemas, uma vez que, Melo (2020 *apud* SANTOS; ARAÚJO, 2023, p. 7) entende que a rápida evolução das tecnologias digitais também apresenta desafios para a área de cibersegurança, uma vez que os hackers estão constantemente desenvolvendo novas técnicas para explorar vulnerabilidade em sistemas e redes. Dessa forma, a segurança das informações nos sistemas é crucial, uma vez que, de acordo com Vecchia (2019 *apud* SANTOS, 2021, p.10), essa medida tem como objetivo tornar as informações mais seguras, o que requer a implementação *hardware*[6] *e software*[7], tendo como elementos: mecanismo, política e cultura.

Além, da busca de atender as necessidades com segurança das informações houve uma conjuntura de ações que estabeleceram e trouxeram um assunto desconhecido anos atrás para a grande massa tecnológica, pois o simples fato de estar sujeito a ataques cibernéticos podem causar um grande espanto e medo não só para os setores marítimo e portuário, como também para os envolvidos diretamente ao fato, assim dizer que um armador, um agente de TI (Tecnologia da Informação) e os funcionários destas estão conformados que seus dados a qualquer momento podem estar a mercê de criminosos, é um fato inverídico, uma vez que, "a uma insegurança no ciberespaço e os mecanismos de controle e proteção, quais podem ter efeitos devastadores para a dignidade humana, com o potencial de afetar valores como privacidade, a propriedade, a liberdade, a saúde ou mesmo a vida" (ANDRADE *et al. 2020, p. 7).*

> O monitoramento da Infraestrutura de TI das empresas e organizações é essencial para a detecção precoce de possíveis vulnerabilidades e ataques. Isso envolve a implementação de sistemas de monitoramento avançados que possam identificar atividade suspeitas ou anormais nos sistemas e redes. Além disso, é importante contar com equipes especializadas em segurança da informação que possam analisar dados conectados pelo sistema de monitoramento e tomar medidas rápidas para mitigar possíveis ameaças. O monitoramento contínuo permite uma resposta mais eficiente

[6] *Ransomware,* código malicioso que torna inacessível os dados armazenados, geralmente usando criptografia ou bloqueio, o que equivale ao refém, desta forma exigindo-se pagamento para restauração do acesso.
[7] *Spoofing,* dentre os tipos de ataques de hackers que afetam todo o sistema, o mesmo é uma técnica utilizada em que os hackers se passam por outra pessoa ou uma empresa legítima para roubo de dados.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

> aos incidentes de segurança e reduz o impacto dos ataques cibernéticos nas organizações, segundo o entendimento de De Paula *et al.* (2022 *apud* SANTOS; ARAÚJO, 2023, p. 09).

Neste contexto, a cibersegurança não objetiva apenas a proteção e a defesa dos sistemas integrados nestes setores, mas também sob a perspectiva do indivíduo e sua extensão.

3.2 Casos notórios de ataques cibernéticos no Direito Marítimo e Portuário

Os setores marítimos e portuário para o cenário comercial global representam em torno de 80% (oitenta por cento) das mercadorias transportadas por via aquaviária de um país para o outro através das logísticas portuárias, como já mencionado em outros tópicos (CAMPOS, 2021, p. 128).

É indispensável que sejam automatizadas as empresas e as organizações para atender às demandas operacionais destes setores, uma vez que, de acordo com Dias (2019, apud FROEHLICH; REINHART; NUNES, 2023, p. 2), enfrentam a competição comercial e, portanto, a velocidade e a troca de informações são fundamentais para o êxito desses negócios.

A configuração deste ambiente e a necessidade de implementar a tecnologia para atender às demandas e se adequar no mercado competitivo, se não feito conforme a Resolução IMO MSC (Organização Marítima Internacional - Comitê de Segurança Marítima) 428 (98) que nas palavras de Campos (2021, p.130) trata sobre "gestão de riscos cibernéticos no Sistema de Gestão de Segurança (*Maritime Cyber Risk Management in Safety Management System*), com medidas obrigatórias a partir de 1 de janeiro de 2021".

Além desta resolução existem diretrizes e códigos, e não seguir tais parâmetros impostos pode ocasionar problemas irreversíveis às empresas, pessoas e organizações, partindo deste ponto será demonstrado alguns casos notórios de ataques cibernéticos. Assim sendo, para que as medidas funcionem bem, é necessário realizar integração com outras áreas como *compliance*, que defende a implementação de boas práticas em segurança da informação, o que evitaria os problemas mais comuns durante as vistorias.

Segundo Siota (2023):

> *Compliance*, (do inglês *to comply*) em palavras resumidas, significa estar de acordo com determinadas normas ou regulamentos preestabelecidos. Assim sendo, quando

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

> falamos sobre compliance dentro da cibersegurança, estamos nos referindo a seguir um conjunto de boas práticas relacionadas à segurança da informação. Mesmo que o compliance não queira dizer exatamente segurança, certamente a adequação a alguma norma ou regulamento melhora a responsabilidade e a transparência das operações de segurança das empresas. Organizações que não adotam um programa de compliance costumam enfrentar auditorias mais severas e, em muitas situações, acabam por perder boas oportunidades de negócio ou mesmo ter sua reputação manchada.

Portanto, deve-se levar em considerações outras áreas que trabalham para manter a integridade dos sistemas, operações e dados, nas quais impõem medidas para concretização, assim a realização autoavaliação, priorização das lacunas de segurança, estabelecer cronogramas, que ajudarem para atingir as prioridades em questão a segurança, além da realização de monitoramento contínuo. (SIOTA, 2023).

De acordo com Faria (2021, p. 3) "as ameaças são várias, vão desde a intercepção de comunicações, bloqueio de serviço *malware*, roubo de identidade, roubo ou manipulação de dados e fuga de informação entre outras mais relevantes", assim o mais comum acontecer é conhecido como software malicioso que segundo Vecchia (2019 *apud* Santos, 2021, p. 12)" trata-se um malware que bloqueia o acesso a um dispositivo ou realiza a criptografia de arquivos. Para desbloquear decifrar há solicitação de um valor pecuniário à vítima, assim como ocorreu em 2017 com a empresa MAERSK, considerada a maior armadora mundial no transporte de contentores, tal ataque se deu, segundo Farias (2021, p. 2) "por *ransomware*[8] *'NotPetya'*, que já tinha utilizado para atacar a empresa holandesa TNT Express, em julho de 2017". Diante disso, observa-se que é mais comum do que se aparece ocorrerem ataques cibernéticos, uma vez que existe uma maior integralização em logística e serviços tecnológicos, assim em caso que se utilizado os GPS, poderia ocorrer um desvio da programação geográfica, ficando a mercê de ataques piratas ou desvio de carga, partindo desse ponto a análise desse sistema é correlata, pois em 2019, houve mistificação de sinal de GPS em 20 zonas costeiras,

[8] BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

que inclui portos de Shanghai, Fuzhou, Dalian por via de um sistema "*spoofing*[9]", de acordo com Faria (2021, p. 4) "através de estações em terra que podem, aproveitar os sistemas de GPS destinado a melhorar a precisão daquele sistema de posicionamento.

Outro evento relevante para o estudo sobre a cibersegurança foi o ataque contra às torres gêmeas em 11 de setembro de 2001, que emitiu um alerta a IMO (Organização Marítima Internacional) sobre as questões a segurança portuária, na qual implementou o Código Internacional para Proteção de Navios e Instalações Portuárias - ISPS Code que passou a vigorar em 2004, segundo Brasil (2020, *apud* SANTOS, 2021, p. 12-13).

Segundo Souza (2021):

> Mesmo não tendo tanta divulgação em grandes mídias, Tulio cita casos de ataques cibernéticos que impactaram diversas empresas do setor marítimo, trazendo prejuízos financeiros e danos de imagem. Como por exemplo: em 2017, um incidente de segurança relacionado ao ransomware *NotPetya*, que executou um dos maiores ataques cibernéticos da história, impactando também a dinamarquesa MAERSK, maior operadora de navios de contêineres e navios de abastecimento do mundo; em 2018 um ataque cibernético que afetou a empresa Chinesa COSCO Shipping; em 2020, a gigante Francesa de contêineres, CMA CGM SA, foi alvo de um ataque com o ransomware Ragnar Locker; e a própria *Organização Marítima Internacional* (IMO), que também foi vítima de um ataque cibernético sofisticado, que inativou por alguns dias os serviços de Internet da organização.

Dessa forma, ficou demonstrado que as empresas e as organizações estão suscetíveis a ataques, e que é necessário aprimorar e minimizar riscos e prejuízos causados. Assim, serão examinados as diretrizes e as Resoluções após os ataques, bem como a implementação desses sistemas de forma eficiente dentro dos setores.

4 REGULAMENTAÇÃO DO DIREITO MARÍTIMO E PORTUÁRIO NOS CASOS DE VIOLAÇÃO A CIBERSEGURANÇA

É imperativo debater e analisar as regulamentações e as medidas a serem tomadas para minimizar os riscos relacionados à cibersegurança nos setores Marítimo e Portuário, com finalidade de proteger, preservar e confidencialidade destes setores.

[9] IACS, infeções associadas aos cuidados de saúde, contribui para efetivação dos regulamentos e padrões internacionais, facilitando, assim, o comércio marítimo e assegurando sua conformidade com as normas globais. Por estabelecer critérios técnicos, a associação contribui significativamente para a prevenção de acidentes, proteção do meio ambiente e a segurança da vida e da propriedade no mar. (PROPER MARINE).

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

> Contudo, tornou-se essencial para os marítimos não só compreenderem e adotarem estas novas tecnologias como, igualdade uma postura cautelosa e de alerta de em relação a certos acontecimentos e ocorrência que podem correr perigosamente mal num curto espaço de tempo. Vislumbra-se novo estágio da prontidão marítima que necessita de um robusto e bem definido "código" que alargue e concretize um "novo" conceito de segurança marítima em sentido lato que reforce as convenções internacionais e a sua aplicação (FARIA, 2021, p. 01).

A vulnerabilidade do setor marítimo e portuário já mencionado nos tópicos anteriores decorre pois estão inseridos em um meio competitivo. Desta forma, utilizam a tecnologia para atingir a eficiência, e a utilização das mesmas tende ser modernizada, o que pode facilitar as ações criminosas. Portanto, as medidas a serem tomadas devem ser integradas e acompanhadas de uma robusta operação na tentativa de conter os atos ilícitos e disruptivos, das quais as regulamentações nem sempre conseguem atingir de forma eficiente.

> São vários os desafios de cibersegurança que os portos e as plataformas associadas têm que enfrentar, qualquer que seja o tipo de tecnologia ou sistema de informação usados em várias atividades portuárias. As ameaças são várias, vão desde a interceção de comunicações, bloqueio de serviço, malware, roubo de identidade, roubo ou manipulação de dados e fuga de informação, entre outras mais relevantes. Os impactos podem também ser de vária ordem e nefastos, como por exemplo, paralisia total das operações, morte ou lesões nas pessoas, rapto, roubo de cargas e perdas financeiras ou de reputação, que urge evitar a todo o custo. A tradicional segurança marítima terá de ser robustecida com medidas de proteção contra ataques ilícitos e disruptivos e, por outro lado, em sede legal, as condutas ditas " desculpáveis" ou " meramente culposas" das tripulações deverão ter, cada vez, menor aplicação tendo em conta a regulamentação existente (FARIA, 2021, P. 3- 6).

Ao mencionar que a tribulação terá sua culpabilidade reduzida cada vez mais, percebe-se que as regulamentações estão acompanhando a evolução tecnológica, compreendendo a uma vulnerabilidade da cibersegurança. Sendo assim, um desvio de rota, roubo de carga, paralisação do sistema portuário ou qualquer outro meio, pode ser consequência de ataques de hackers, que podem decorrer de falhas decorrentes de falta de proteção e gerenciamento dos sistemas e operações. Em casos de incidentes, a cibersegurança deve estar associada à responsabilização civil, uma vez que a violação não se limita aos setores marítimos e portuários, mas também a terceiros, indivíduo ou meio ambiente, como meio de fazer cumprir com as obrigações e deveres de proteção.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

4.1 A problemática e necessidade de meios regulamentares no âmbito internacional

A problemática em questão aborda a perspectiva em que os legisladores enfrentam dificuldades de acompanhar, em tempo útil, as transformações tecnológicas (ANDRADE *et al. 2020, p. 07)* e das questões econômicas, por conta do alto investimento em adoção tecnológico e organizacionais, além de ser essencial que seja destinado atenção a capacitação aos colaboradores, assim garantindo que todos estejam cientes das melhores práticas de segurança e aptos a reconhecer e responder a ameaças.

A problemática em amenizar as invasões devem de prisma não ser o foco principal, uma vez que, a implementação de medidas de segurança e adoção das diretrizes e regulamentações apesar de ter um custo elevado, a longo prazo poderá amenizar impactos aos operadores, investidores, armadores, aos órgãos governamentais e questões inerentes a Dignidade da Pessoa Humana.

Na perspectiva de Faria (2021, p. 12):

> Não atinge os navios e aos portos de forma direta, mas também indiretamente, pela incidência nas embarcações, sobre as pessoas que estão embarcadas, sobre as plataformas ou infraestrutura no mar e sobre o ambiente marinho, designadamente, através dos acidentes de poluição.

Desta maneira, a interconexão das infraestruturas críticas dos Estados e o aspecto tecnológico na perspectiva de Andrade *et al.* (2020, p.10), motivou a União Europeia adotar de medidas destinadas a assegurar a proteção das redes e infraestruturas, através da Diretiva 2008/ 114/ CE de dezembro de 2018. Apesar das tentativas em regulamentar outras diretrizes com a Diretiva SRI 2016, que foi transportada pela Lei n° 46/2018, não foram plenamente adotadas (ANDRADE *et al. 2020, p. 10).*

A União Europeia em analisar tais conjunturas, lançou o Relatório de Cibersegurança no setor Marítimo, segundo foi um marco para as demais propositura de resoluções, medidas etc., assim como a Resolução MSC. 428 (98) - Gestão de Risco Cibernéticos Marítimos em Sistemas de Gestão de Segurança pela IMO (Organização Marítima Internacional) em 2017 estabelecendo medidas obrigatórias a partir de 1° de janeiro de 2021 (CASTRO, 2021, p.03), em qual advenho em decorrência de um ataque cibernético. Além disso, são variáveis as cadeias regulamentadoras em busca de segurança.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

Ainda Castro (2021, p. 03) explica que:

> As Diretrizes sobre gestão de risco cibernético marítimo (*Guidelines on maritime cyber risk management*, MSC- FAL.1/Circ.3 5 July 2017), 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 controle de risco cibernético sejam incluídos nos Sistemas de Gerenciamento de Segurança existentes. Nesse sentido, a segurança cibernética deverá ser coberta pelo código ISM a partir de 1° de janeiro de 2021.

Apesar das dificuldades enfrentadas pelos legisladores para regulamentar questões relacionadas à cibersegurança nos setores do Direito Marítimo e Portuário, há um esforço concentrado em proteger tais questões, que é possível através da cooperação e integração entre os Estados.

No âmbito internacional a cibersegurança é regulamentada, sobretudo, no âmbito marítimo pelo Código Internacional para o Gerenciamento da Operação Segura de Navios e para a Prevenção da Poluição (ISM *Code*), que foi adotado em 1° de janeiro de 2021, e "desde 1998 é obrigatório, de acordo com o Capítulo IX da Convenção SOLAS (CAMPOS, 2022, p. 03).

Dessa forma, as outras regulamentações estão sujeitas a ela, provendo e buscando um ambiente mais 'sólido', porém o ISM *Code* não se aplica aos portos. O instrumento utilizado para a proteção portuária com relação a cibersegurança denomina-se *International Association of Ports and Harbors* - Associação Internacional de Portos e Instalações portuárias (IAPH), que é uma diretriz que desenvolve meios de mitigar a segurança cibernética, sendo usado como base para Códigos como ISPS (Código Internacional para Proteção de Navios e Instalações Portuárias) que foi desenvolvido em resposta direta a esses ataques e se tornou o "regime de segurança obrigatório abrangente" (2021).

No Brasil, questões relacionadas à cibersegurança estão diretamente relacionadas à proteção de dados, Lei Geral de Proteção de Dados Pessoais (LGPD), n° 13.709, de 14 de agosto de 2018 (CASTRO, 2021, p. 04). E tal lei, diga se passagem, se baseia no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), implica-se sobre os armadores, proprietário da embarcação, agente marítimo que procedem dados pessoais vinculados a União Europeia,

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

independentemente da bandeira do navio e da nacionalidade da tripulação, decorrente de que qualquer questão concernente a tratamentos de dados pessoais situados a União deve ser realizado conforme o imposto (CASTRO, 2021, p. 05).

Disposto ao tratamento dados à LGPD, pode afirmar que sua apreciação e implementação é obrigatório, conexos com finalidade e objetivos, e não cumprimento de tais medidas do dispositivo acarreta responsabilização civil específica pela violação do dever de proteção de dados no que se confere ao âmbito marítimo (CAMPOS, 2021), na qual será considerado uma responsabilidade objetiva.

> No cenário marítimo, não pairam dúvidas de que essas medidas incluem as normas de segurança, com destaque aos Códigos ISM e ISPS, ambos obrigatórios de acordo com as disposições da Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS). A não adoção dessas medidas obrigatórias poderá ensejar a responsabilidade civil objetiva em decorrência do descumprimento do dever de proteção de dados (CAMPOS, 2021).

Deste modo, as pessoas que estão ligadas nos setores marítimo e portuário devem se valer e aplicar tais medidas, uma vez que, implicações legais que serão analisadas ainda dentro deste tópico.

4.2 Medidas de segurança

É relevante discutir a regulamentação, dada a sua amplitude e grau de proteção, para fazer valer o direito. Contudo, há medidas para neutralizar essas questões, que são decorrentes de leis, como a LGPD, resoluções e planos de segurança, etc. Algumas dessas medidas estão presentes na Resolução.428(98), no código ISM, que trata de questões marítimas, além do ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, *InterManager*, WSC e *SYBAss*, que tratam de Diretrizes para a segurança cibernética a bordo de navios, bem como a Recomendação consolidada do IACS sobre resiliência cibernética (Rec. 166), na qual, identificou que "para que os navios fossem resilientes contra incidentes cibernéticos, todas as partes da indústria precisam estar ativamente envolvidas", adotando a partir de análises Requisitos Unificados (UR E26 e UR E27). No que se refere aos portos, ao Relatório de Segurança Cibernética da comunidade portuária da IAPH, e o código ISPS. (IACS - *International Association of Classification Societies*).

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

Observa-se nesse contexto que há diversas medidas de segurança estabelecidas para gerenciamento e proteção dos riscos advindos dos incidentes cibernéticos.

4.2.1 Resolução MSC.428(98) e Código ISM

A Resolução MSC.428(98) demonstra preocupação e a sensibilização em relação às ameaças e as vulnerabilidades apresentadas pelos incidentes cibernéticos. Dessa forma, a Resolução reconhece que os administradores, as sociedades classificadoras, os armadores e os operadores, agentes de navios, fabricantes de equipamentos, prestadores de serviços, portos e instalações portuárias devem se atentar e estar acelerar o processo (RESOLUTION MSC.428(98), 16 jun. 2017).

Ainda no que se refere a Resolução MSC.498(98), há tópicos a serem observados:

> 1- AFIRMA que um sistema de gestão de segurança aprovado deverá levar em conta gestão de riscos cibernéticos de acordo com os objetivos e requisitos funcionais do Código ISM; 2- INCENTIVA os administradores garantir que os riscos cibernéticos sejam adequadamente abordados nos sistemas de gestão de segurança o mais tardar na primeira verificação anual do Documento de Conformidade da empresa após 1° de janeiro de 2021; 3- RECONHECE as preocupações necessárias que podem ser necessárias para preservar a confidencialidade de certos aspectos da gestão de riscos cibernéticos e 4- SOLICITA aos Estados Membros que tragam esta resolução à atenção de todas as partes interessadas.

Dessa forma, as regulamentações devem observar os critérios de gestão de risco, salvaguardando as questões cibernéticas. Sendo assim, o ISM CODE (Código Internacional para o Gerenciamento da Operação Segura de Navios e para a Prevenção da Poluição), adotado pela Resolução A. 741 (18), visa assegurar segurança no mar, tanto em termos de meio ambiente quanto de propriedade. Para isso, deve-se observar com cautela as disposições da Resolução mencionada anteriormente, sendo assim o código faseado, além das documentações necessárias para tal.

Quadro 1: Código ISM (Código Internacional para o Gerenciamento da Operação Segura de Navios e para a Prevenção da Poluição).

Etapa	*Observação*
IMPLEMENTAÇÃO	Objetivos: promover práticas seguras na operação de navio e um ambiente de trabalho; avaliação dos riscos identificados para os navios, pessoas e ambiente e estabelecimento de garantias e aperfeiçoamento das

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

	habilidades no gerenciamento, devendo estar em conformidade com normas e regras obrigatórias e que códigos, diretrizes, etc. devem ser levados em consideração. Aplicação: podem ser aplicadas para todos os navios. Exigências funcionais para um sistema de gerenciamento de segurança: devem as companhias desenvolver e implementar e manter o sistema, observando: política de segurança e proteção ambiental; instruções e procedimentos para assegurar operação segura de navios e proteção do meio ambiente de acordo com as relevantes legislações internacionais e do Estado da bandeira; procedimentos para reportar acidente e não conformidades com as disposições deste código;
POLÍTICA DE SEGURANÇA E PROTEÇÃO AMBIENTAL	A Companhia deve estabelecer uma política de segurança e proteção ambiental a qual descreve como os objetivos estabelecidos no parágrafo 1.2 serão atingidos. A Companhia deve assegurar que a política seja implementada e mantida em todos níveis da organização, tanto com base no navio quanto com base em terra
RESPONSABILIDADE E AUTORIDADE DA COMPANHIA	Se a entidade que é responsável pela operação do navio é outra que não o armador, o armador tem que comunicar o nome completo e detalhes de tal entidade à Administração. A Companhia deve definir e documentar a responsabilidade, autoridade e inter-relação de todo o pessoal que gerencia, executa e verifica o trabalho relacionado e afetando a segurança e prevenção da poluição. A Companhia é responsável por assegurar que recursos adequados e apoio baseado em terra são supridos para capacitar as pessoas ou pessoas designadas para executarem suas funções.
RECURSO PESSOAL	A Companhia deve assegurar que o comandante é apropriadamente qualificado para comando; As instruções que são essenciais para serem ministradas antes da saída para o mar devem ser identificadas, documentadas e dadas. A Companhia deve assegurar que todo o pessoal envolvido no sistema de gerenciamento de segurança da Companhia tenha um entendimento adequado de normas, regras, códigos e diretrizes relevantes. A Companhia deve estabelecer e manter procedimentos para identificar qualquer formação a qual possa ser requerida em apoio do sistema de gerenciamento de segurança e assegurar que tal formação é ministrada para todo o pessoal envolvido. A Companhia deve estabelecer procedimentos pelos quais o pessoal do navio receba informações relevantes sobre o sistema de

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

	gerenciamento de segurança em um idioma de trabalho ou idiomas entendidos por eles. A Companhia deve assegurar que o pessoal do navio é capaz de efetivamente se comunicar na execução de suas obrigações relacionadas ao sistema de gerenciamento de segurança
PRONTIDÃO DE EMERGÊNCIA	A Companhia deve identificar potenciais situações de emergência a bordo, e estabelecer procedimentos para respondê-las. A Companhia deve estabelecer programas de adestramento e exercícios para preparar para ações de emergência. O sistema de gerenciamento de segurança deve incluir medidas assegurando que a organização da Companhia possa responder a qualquer tempo para perigos, acidentes e situações de emergência envolvendo seus navios.
RELATÓRIO E ANÁLISE DE NÃO CONFORMIDADE, ACIDENTES E OCORRÊNCIAS PERIGOSAS	O sistema de gerenciamento de segurança deve incluir procedimentos assegurando que não conformidades, acidentes e situações perigosas são reportados para a Companhia, investigados e analisados com o objetivo de aperfeiçoar a segurança e a prevenção da poluição. A Companhia deve estabelecer procedimentos para implementação de ações corretivas, incluindo medidas destinadas a prevenir a reincidência

Fonte: Elaborado pelos Autores, 2024

4.2.2 IAPH e ISPS

O IAPH (Diretrizes de Segurança Cibernética para Portos e Instalações Portuárias) é uma associação comercial global para portos e instalações portuárias, que buscou observar os impactos aos incidentes cibernéticos e a importância de criar diretrizes capazes de mitigar os incidentes cibernéticos. Para o sucesso da diretriz, foram realizados estudos, na qual contou com a ajuda do Banco Nacional e em cooperação com a IMO, que foram motivados por riscos significativos aos portos, a cooperação de ambos é evidenciado no MSC 103/92 (*Mediterranean Shipping Company* - Companhia de Navegação Mediterrânea) que reconheceu as lacunas das instalações que era apresentada nas orientações anteriores e na MSC 104/7/1, que instrui os operadores sobre as questões cibernéticas, assim concluindo seu trabalho. (SEGINFO- Portal, Podcast e Evento sobre Segurança da Informação, 2021).

Tais questões foram relevantes para o desenvolvimento da questão da cibersegurança, porém não suficientes, assim criando o código ISPS (Código Internacional para Segurança de Navios e Instalações Portuárias), objetivando a detecção das ameaças à instalação portuária,

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

REVISTA DE DIREITO E NEGÓCIOS INTERNACIONAIS DA MARITIME LAW ACADEMY - MLAW
INTERNATIONAL LAW AND BUSINESS REVIEW
Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

estabelecendo estrutura internacional envolvendo a cooperação entre os governos, órgão governamentais, administradores locais e as indústrias portuária e de navegação a fim de detectar ameaças à proteção e tomar medidas preventivas contra incidentes que afetam navios ou instalações portuárias que se utilizam no comércio internacional, ou seja, busca atender e estabelecer regramentos para que todos sigam e amenizem os riscos, assim como estando preparados em caso de incidente nestes setores (ADISSI, 2021).

4.2.3 Procedimentos

De acordo com as medidas de proteção estabelecida pela Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis os procedimentos a serem seguidos para mitigar os problemas pertinentes a proteção incidentes são: a) cadastramento de usuário; b) antivírus, *antispyware* e *firewalls*; c) política de senhas, para a inicialização, *login* na rede, proteção de tela, *logoff* automático. Esses procedimentos, servem para impedir o acesso não autorizado aos sistemas informatizados de gestão, operação e segurança da instalação portuária. Também as medidas objetivam permitir o compartilhamento de informações entre os diversos setores portuárias, de forma segura, mediante: a) mídias removíveis; b) redes sociais; c) armazenamento em nuvem, assim como também para proteção de dados: a) política de *backup*; b) pessoas e c) vedação de instalação de programas não avalizados pelo setor de TI da instalação portuária (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - Comissão Nacional de Segurança Pública nos Portos, Terminais e vias navegáveis, p.24- 25).

Essas medidas lógicas são uma das formas de aumentar a segurança e a eficácia nos cenários, na qual desde o cadastramento até a vedação de instalação de proteção de dados assim como apresentado nas figuras acima, ou seja, com isso só confirma que mesmo havendo a dificuldade de regulamentação por parte dos legisladores, há medidas que buscam amenizar tais ataques.

4.3 Responsabilidade civil e a LGPD no Direito Marítimo e Portuário

Para compreender as questões envolvendo responsabilidade civil no Direito marítimo e portuário, é necessário realizar apontamentos para melhor se entender as questões que dizem

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

respeito à segurança cibernética neste contexto. Sendo assim, é necessário uma análise mais ampla para que assim chegue na questão do trabalho sobre, qual seria a responsabilidade em casos de incidentes cibernéticos nesses setores mencionados.

Segundo Diniz (2023, p.20) "a responsabilidade civil como aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros em razão de ato próprio, imputado, de pessoa por quem responde, ou de fato de coisa, ou animal sob sua guarda ou, ainda, de simples imposição legal". Dessa forma, ao analisar a estrutura descrita acima, é possível notar a dificuldade de se aprofundar ao tema, devido às suas questões pessoais, que estão relacionadas a atos que atingem a moral e o patrimônio.

Diante do entendimento de Diniz (2023, p.11):

> Por repercutir em todas as atividades humanas, tutelando inclusive os direitos da personalidade, múltiplos são os dissídios doutrinários e díspares são os posicionamento dos tribunais, "quanto a definição de seu alcance, à enunciação de seus pressupostos e a sua própria textura", tornando-se um dos árduos e complexos problemas jurídicos e de mais difícil sistematização.

A responsabilidade pode ser subdividida em responsabilidade civil subjetiva, que decorre da ilicitude e a responsabilidade objetiva se fundamenta no risco, ou seja, uma decorre a imposição legal em que não observados o que menciona responde por tal, e a outra é na perspectiva de que mesmo que tenha seguido a legislação aceitou assumir o risco, de causar dano a alguém.

Na perspectiva de Diniz (2023, p.20):

> A regra básica é que a obrigação de indenizar, pela prática de atos ilícitos, advém da culpa. Ter-se-á ato ilícito se a ação contrariar dever geral previsto no ordenamento jurídico, integrando-se na seara da responsabilidade extracontratual (CC, arts. 186 e 927), e se ela não cumprir obrigação assumida, caso em que se configura a responsabilidade contratual (CC, art. 389)53. Mas o dever de reparar pode deslocar-se para aquele que procede de acordo com a lei, hipótese em que se desvincula o ressarcimento do dano da ideia de culpa, deslocando a responsabilidade nela fundada para o risco. P. ex.: arts. 927, parágrafo único, e 931 do Código Civil prevêem casos de responsabilidade por ato lícito;

A responsabilidade subjetiva como regra, mas há divergências doutrinárias sobre responsabilidade civil, assim podendo existir responsabilidade objetiva, mesmo que se tenha seguido os padrões, diretrizes e as regulamentações no contexto cibernético, uma vez que o

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

comportamento atinge não somente os proprietários, mas também aos terceiros que tem relação direta nos setores marítimo e portuário. Em decorrência de tal, se faz necessário abordar a LGPD para contextualizar e visualizar de forma mais clara qual a responsabilidade de ambos, uma vez que, sua implementação é obrigatória.

No que diz respeito à responsabilidade civil no setor marítimo, é perceptível que a responsabilidade civil será objetiva, quando não observados os pressupostos legais que visam minimizar e gerenciar os riscos, ou seja, ficando comprovado a não observância das medidas de segurança será caracterizado como irregular, por não ser observado a legislação, gerando de tal modo responsabilidade civil específica, por descumprimento de dever de proteção de dados (CAMPOS, 2021, p. 4)

De tal modo, os dispositivos da LGPD em seus artigos 42 e 44, abordam sobre tais questões deste modo dispondo o art. 42 da LGPD, que o controlador ou operador, em razão da atividade de tratamento de dados pessoais, causar danos patrimonial, moral, individual ou coletivo, em violação a LGPD, é obrigado a repará-lo, podendo os mesmo responder de forma solidária. Já no artigo 44, parágrafo único, responde pelos danos da violação de segurança, ao deixar de adotar as medidas de segurança previstas no artigo 46 da LGPD, contudo não é algo fixado, e que deve- ser levado sempre em consideração, pois a responsabilidade poderá ser afastada segundo Campos (2021, p.16) quando estiverem consoante o artigo 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 terceiros.

Sendo assim, apesar das dificuldades em regulamentar o cenário da responsabilidade civil, de acordo com as convergências de autores, percebe-se que a legisladores têm desempenhado um trabalho criterioso ao tentar a amenizar os riscos e realizar o gerenciamento no que tange às questões cibernéticas, deste modo, a responsabilidade em que os operadores e administradores têm é objetiva devido seu dever de proteção de dados, conforme previsto no artigo 44, da LGPD ou em outros dispositivos legais mencionados, como os Códigos que

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

regulam os setores marítimos e portuário, ISM e ISPS e também pelo fato da LGPD (CAMPOS, 2021, p.18).

Ao fazer a análise de responsabilidade civil no setor portuário, não se obteve uma resposta clara sobre, em artigos e doutrinas, qual seria a responsabilidade civil concernente à segurança cibernética.

5 CONSIDERAÇÕES FINAIS

Há uma complexidade notável no ciberespaço, dada a velocidade com que suas estruturas se modificam, em comparação com o que se refere à cibersegurança. Isso ocorre porque surge como mecanismo de controle de ataques *hackers*, como o *ransomware*, os *malwares*, dentre outros, o que resulta em uma maior proteção à sociedade, e aos setores marítimo e portuário, que representam a economia global, e, se afetadas podem causar prejuízos irreversíveis, tanto aos administradores, quanto aos terceiros envolvidos, além de prejuízo financeiro.

Dessa forma, considerando o impacto que os ataques podem causar, devido à interconexão que facilita a ruptura dos sistemas, tais falhas podem ser causadas por malwares, roubo de identidade, roubo ou manipulação e fuga de informações, mudança de rotas para roubo de cargas, entre outros. Portanto, é necessário regulamentar e fornecer treinamento aos cooperados sobre o ciberespaço, uma vez que os ataques passam despercebidos de uma operação a outra.

No âmbito internacional, a Convenção Internacional para Salvaguarda da Vida Humana no Mar regula os códigos e as resoluções (Resolução MSC.428(98) e Código ISM, IAPH e ISPS), a qual é obrigatória, uma vez que a não observância do mesmo acarreta responsabilidade objetiva, podendo ser diversas observadas os critérios para configurar responsabilidade. No Brasil, há um esforço em adotar medidas de segurança, como a LGPD, que aumenta a confiança e a credibilidade nas operações portuárias e marítimas, no entanto, é crucial manter um progresso constante no desenvolvimento de novas tecnologias para inibir os ataques cibernéticos.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

Diante do que foi apresentado, conclui-se que os progressos tecnológicos que ocorrem desde a Revolução Técnico-Científico-Informacional, fazem com que a sociedade procure sempre evoluir, e buscar meios que assegurem e protejam a integridade, moral e dados. Sendo assim, a importância em se estudar a cibersegurança, uma vez que protegem e trazem maior confiança para operadores de diversos setores, como o marítimo e o portuário.

As medidas não afastam integralmente os riscos, mas amenizam os riscos decorridos da violação, assim se faz necessário abordar a responsabilidade civil nas áreas marítimo e portuária, apesar de serem ramos distintos e autônomos, ambos terão a responsabilidade civil objetiva quando não observados as medidas prevista a serem seguidas violando tais. No que tange à responsabilidade civil portuária, não foi encontrado nada que tratasse especificamente sobre, mas ao analisar, regulamentações e os dispositivos como dispõem os arts. 42 e 44 da LGPD, assim como Convenção Internacional para Salvaguarda da Vida Humana no Mar (SOLAS), conclui-se que a responsabilidade será mesma do que se tratar da esfera marítima, vinculados o dever de proteção de dados, porém poderá haver outros meios de responsabilização que dependerá de análise de um caso específico.

6 REFERÊNCIAS

ADISSI, Marceu. ISM CODE - Código Internacional para o gerenciamento da operação segura de navios e para prevenção da poluição. **IFPB- Instituto Federal da Paraíba** , Paraíba , 09 abr. 2021. Disponível em: https://www.ifpb.edu.br/cabedelocentro/cursos/epm/acesso-a-informacao/legislacao/normas-internacionais-final/ism-code-codigo-internacional-para-o-gerenciamento-da-operacao-segura-de-navios-e-para-a-prevencao-da-poluicao.pdf/view#:~:text=Outros%20Documentos-,ISM%20CODE%20%2D%20C%C3%B3digo%20Internacional%20para%20o%20Gerenciamento%20da%20Opera%C3%A7%C3%A3o%20Segura,para%20a%20Preven%C3%A7%C3%A3o%20da%20Polui%C3%A7%C3%A3o&text=O%20ISM%20Code%20estabelece%20uma,para%20a%20preven%C3%A7%C3%A3o%20da%20polui%C3%A7%C3%A3o. Acesso em: 05 jun. 2024.

ADISSI, Marceu. ISPS CODE - Código Internacional para proteção de navios e instalações portuárias. **IFPB- Instituto Federal da Paraíba** , Paraíba , 09 abr. 2021. Disponível em: https://www.ifpb.edu.br/cabedelocentro/cursos/epm/acesso-a-informacao/legislacao/normas-internacionais-final/isps-code-codigo-internacional-para-protecao-de-navios-e-instalacoes-portuarias.pdf/view. Acesso em: 08 jun. 2024.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

CASTRO, Osvaldo Agripino Junior. Constitucionalização do direito marítimo e direito marítimo portuário. **Revista de direito e negócios internacionais da marítimo law academy – MLAW International Law and Business Review**, v. 1, n. 1, p. 6- 29, 2021. Disponível em: https://mlawreview.emnuvens.com.br/mlaw/article/view/28/53. Acesso em: 28 out. 2023.

CAMPOS, Ingrid Zanella Andrade.A Resolução de segurança cibernética e a LGPD no direito marítimo. **Estadão**, São Paulo, 08 jan. 2021. Disponível em: https://www.estadao.com.br/politica/blog-do-fausto-macedo/a-resolucao-de-seguranca-cibernetica-e-a-lgpd-no-direito-maritimo/. Acesso em: 20 abr. 2024.

CAMPOS, Ingrid Zanella Andrade. A segurança cibernética no direito marítimo: uma análise do dever de proteção de dados. **Revista Observatório Portuário**, v. 01, n. 2, p. 1- 8, 2022. . Disponível em: https://periodicos.unisanta.br/index.php/rop/article/download/3219/2189#:~:text=Assim%2C%20a%20seguran%C3%A7a%20cibern%C3%A9tica%2C%20no,gest%C3%A3o%20da%20seguran%C3%A7a%20das%20embarca%C3%A7%C3%B5es. Acesso em: 20 abr.. 2024.

CAVALCANTE, Zedequias Vieira; SILVA, Mauro Luis. A importância da revolução industrial no mundo da tecnologia. **Editora Cesumar**. p. 1-6, outubro 2011. Disponível em: https://www.unicesumar.edu.br/epcc-2011/wp-content/uploads/sites/86/2016/07/zedequias_vieira_cavalcante2.pdf. Acesso em: 10 out. 2023.

CENTRO NACIONAL. Cibersegurança Portugal. **Relatório cibersegurança em Portugal: ética e direito**. Lisboa, 2020. Disponível em: https://www.cncs.gov.pt/pt/relatorio-etica-e-direito/.Acesso em: 12 out. 2023.

DANTAS, Tiago. Hardware e software. **Mundo Educação**. Disponível em: https://mundoeducacao.uol.com.br/informatica/hardware-software.htm#:~:text=Hardware%20%C3%A9%20a%20parte%20f%C3%ADsica,algum%20tipo%20de%20processamento%20computacional.Acesso em: 21 ago. 2024.

DINIZ, Maria Helena.**Curso de direito civil brasileiro: Responsabilidade civil**. Biblioteca virtual. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553627765/. Acesso em: 08 jun. 2024.

FARIA, Duarte Lynce de. O impacto da cibersegurança no quadro jurídico regulatório da segurança marítima. **JANUS.NET– e-journal of international relations**,v.11, n. 2, p. 165-186, 2021. ISSN: 1647-7251 Disponível em: https://repositório.ual.pt/bitstream/11144/4636/2/PT-vol11-n2.pdf. Acesso em: 20 nov. 2023.

FROEHLICH, Cristiane; REINHART, Luiza Baggio; NUNES, Moema Pereira. A transformação digital em uma empresa de software de gestão. **Revista Gestão & Conexão**,

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

v.12, n. 3, p. 75-95, 2023.Disponível em: https://periodicos.ufes.br/ppgadm/article/view/40565. Acesso em: 12 out. 2023.

GATTO, Alex; ALBUQUERQUE, Carlos (colab.). Ataques cibernéticos no setor portuário: custos para eliminar riscos são investimento. **Portos e Navios**. Rio de Janeiro. São Paulo, 15 mar. 2023. Disponível em: https://www.portosenavios.com.br/artigos/artigos-de-opiniao/artigo-ataques-ciberneticos-no-setor-portuario-custos-para-eliminar-riscos-sao-investimento. Acesso em: 12 out. 2023.

GOGONI, Ronaldo. O que é spoofing?. **Tecnoblog**. 2023. Disponível em:https://tecnoblog.net/responde/o-que-e-spoofing/. Acesso em: 20 ago. 2024.

HENRIQUES, Antonio; MEDEIROS, João Bosco. **Metodologia Científica da Pesquisa Jurídica**. Biblioteca virtual. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788597011760/epubcfi/6/30[%3Bvnd.vst.idref%3Dbody015]!/4/14/1:318[%C3%A1ri%2Co.]. Acesso em: 20 nov. 2023.

IMO. International Maritime Organization.**Riscos Cibernético Marítimo**. Disponível em: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>. Acesso em: 05 jun. 2024

MILLER, Ruy de Mello. **Incidência tecnológica no direito marítimo. RMM**. São Paulo. Disponível em: https://www.miller.adv.br/single-post/incidencia-tecnologica-no-direito-maritimo5844. Acesso em: 20 out. 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Comissão nacional de segurança pública nos portos, terminais e vias navegáveis. Plano de segurança portuária. Brasil, 2020.

MIRÓ NETO ADVOGADOS. **Como o direito portuário é importante para regulamentar as operações desenvolvidas nos portos brasileiros!**. Curitiba

MUSITANO, Manuela; COLONESE, Paulo. O homem e o fogo. **Invivo- museu da vida fiocruz**, Rio de Janeiro, 29 nov. 2021. Disponível em: https://www.invivo.fiocruz.br/cienciaetecnologia/o-homem-e-o-fogo/#:~:text=Entre%201%2C8%20milh%C3%B5es%20e,f%C3%A1cil%20combust%C3%A3o%2C%20pegaria%20fogo%20normalmente. Acesso em: 25 set. 2023.

PROPER MARINE. O que é IACS (International Association of Classification Societies). Rio de Janeiro.

PINHEIRO, Patricia Peck. (Cord.). **Segurança digital proteção de dados nas empresas**. Biblioteca virtual. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 28 set. 2023.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47

Vol. 4, nº 2, julho a dezembro - 2024. pp 19-47

SANTOS, Bruno Rodrigues *et al*. A evolução da tecnologia: vivendo uma nova era. **Repositório Digital Unicesumar**. p. 1-4,2019.Disponível em: https://rdu.unicesumar.edu.br/handle/123456789/3699. Acesso em: 10 set. 2023.

SANTOS, Eduardo Domanski dos. **Segurança da informação no ambiente portuário**. Monografia (Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI) – Universidade Tecnológica do Paraná, Paraná, 2021. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/29006/1/CT_CEGATI_I_2021_03.pdf. Acesso em: 24 abr. 2024.

SegInfo – Portal, Podcast e Evento sobre segurança da informação. 18 out. 2021.

SEGURANÇA cibernética no setor Marítimo: o futuro está aqui. São Paulo: SOPESP-Sindicato dos Operadores Portuários do Estado de São Paulo, 2019.

SIOTA, Wendel. Compliance e cyber segurança.como começar do jeito certo. **EximiaCo**, Novo Hamburgo, 13 jan. 2023. Disponível em:https://eximia.co/insights/compliance-e-cyber-seguranca-como-comecar-do-jeito-certo/#:~:text=Compliance%2C%20. Acesso em: 20 ago. 2024.

SOUZA, Angélica Silva de; OLIVEIRA, Guilherme Saramango de; ALVES, Lais Hilário. A pesquisa bibliográfica: princípios e fundamentos. **Cadernos da Funcampos**, v.20, n. 43, p. 64-83, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336/1441#:~:text=A%20pesquisa%20bibliogr%C3%A1fica%20%C3%A9%20o,publicados%2C%20para%20apoiar%20o%20trabalho. Acesso em: 26 nov. 2023.

WANDERMUREN, Bruno. Direito marítimo e suas particularidades.**Jusbrasil**,2019. Disponível em:https://www.jusbrasil.com.br/artigos/direito-maritimo-e-suas-peculiaridades/725777973#:~:text=Direito%20Mar%C3%ADtimo%2C%20segundo%20o%20Dicion%C3%A1rio,dedicam%20a%20essa%20esp%C3%A9cie%20de. Acesso em 20 ago. 2024

WEIS, Marcos Cesar. Sociedade sensoriada: a sociedade da transformação digital. 11. ed. Rio de Janeiro: **Editora da FGV**, 2013. 156 p.

RECEBIDO/RECEIVED: 30/10/2024 ACEITO/ACCEPTED: 22/11/2024
Esta obra está licenciada com uma Licença Creative Commons Atribuição-NãoComercial-SemDerivações 4.0 Internacional.
DOI 10.56258/issn.2763-8197.v4n2.p19-47