AI AND BIG DATA AT SEA: THEIR POTENTIAL IMPACTS ON SEAFARERS

Khanssa Laqdami [1], **Eslam Ramadan Badry Gad** [2]

1. *Associate Professor of Maritime Labour Law & Policy, ITF Seafarers Trust, World Maritime University, Malmo, Sweden, kl@wmu.se*

2. *Third Lecturer, College of maritime transport & technology Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt, capt_esbadry@aast.edu*

Keywords: AI and Big Data, Impacts, Work at sea, seafarers

1. **ABSTRACT:** With the integration of Artificial Intelligence (AI), Big data, and advanced navigation systems, the shipping industry is revolutionizing in ways that offers advanced maritime safety and security, improvement of energy consumption, maintenance, and efficiency of voyages. This wave of technological advancement brings with it a sense of optimism. At the same time, however, it opens up questions about what these technologies mean in terms of the working conditions and Occupational Safety and Health of Seafarers (OSH). This research paper discusses the increased application of AI and Big Data in the maritime sector, and it explicitly explores their possible application to monitor and surveil seafarers at sea. The paper examines what the potential consequences of deploying such advanced technologies might be in order to oversee and regulate the work of seafarers within an environment where boundaries between work and private life are often blurred. It is in-depth research into the current application of AI in maritime operations with regard to tracking and surveillance, optimization, and safety, therefore giving a proper understanding of the subject. However, despite the fact that there is no documented evidence of AI and big data being used against seafarers, the authors have gone further to discuss how this could be possible, making use of the Voyage Data Recorder (VDR) as an example of collecting data onboard vessels. VDR can be taken as the closest existing technology to AI applied on board ships. Such a tool, as discussed by the authors, can monitor several features of a ship operating at sea: navigation, the performance of the machinery, and human activities. It is this possible use of information against the seafarers themselves in the case of accidents or any other incidents that occur at sea that scares them. Apart from being exciting, there are significant issues around privacy, ownership of data, and perhaps impacting on the rights and responsibilities of the seafarer. This paper contributes to this debate now current with its examination of technology advancements and outcomes in trying to reach balance between technological advance with the well-being and rights of seafarers within this ever-changing automatised Maritime Industry. This is a conversation that needs to be shared among all the stakeholders, from the players in the maritime industry to the policymakers and academics, in order to come up with an evolved consensus on what that future should be.

2. INTRODUCTION

AI and big data are two interrelated technology domains that work in tandem to transform data into meaningful and actionable data. AI is a sub-field of computer science that is trying to build systems

that can do tasks that require human intelligence, such as reasoning, learning, problem-solving, visual understanding, and natural language. Although traditional data processing techniques are classically less purely analysis-driven, AI Systems learn from data; the more input they receive, the more output they can adapt to and perform human-like tasks (Obschonka & Audretsch, 2020). At its core, Big Data and AI are essentially interdependent. Big Data is extremely large datasets that may be managed using traditional data processing tools. This includes the vast sources of structured and unstructured data from various resources, including social media, sensors, and transactions. Conversely, AI is considered to be an intelligent framework that can process this big data and draw insights from it. By using machine learning, neural networks, and deep learning, AI systems find patterns in Big Data, predict outcomes and create new information (Majnarić et al., 2021; Rehman et al., 2019; Wang et al., 2022). AI can carry out complex tasks that usually require human input, meaning that it makes decisions under uncertainty, learns from experience to improve its performance over time, and even generates new data, as in the case of generative AI models. AI is often categorized into broad fields, which can be considered weak AI or strong AI. Weak AI systems are focused on individual tasks—like virtual assistants or recommenders. In contrast, strong AI encompasses the theoretical concept of generalized intelligence that could perform any task a human could. Almost all currently available AI is weak AI that focuses on narrow applications rather than general reasoning capabilities (Demigha, 2020).

The shipping industry, transporting 90% of global trade, is increasingly exploring AI and Big Data in a quest for efficiency, safety, and environmental sustainability (Durlik et al., 2024). Apart from the fuel optimization, predictive maintenance, route planning, and energy management arise other AI applications within the two industries (Arévalo et al., 2024; Geertsma et al., 2017). Moreover, other integration technologies in AI have enhanced efficiency, accuracy, and safety of port operations supported by Abdelsalam & Elnabawi, 2024.

Big Data analytics can investigate large-scale volumes in vessel performance, navigation data, and informed decision-making for logistics optimization, as well as for enhanced energy efficiency and safety. Machine learning, Natural Learning Processing (NLP), and computer vision are also at the core of all other AI technologies applied within this industry to deal with prevailing challenges in their particular contexts. Examples are sophisticated ML algorithms that optimize vessel routing, predict equipment failure, and improve port logistics. NLP uses cases, such as simultaneous translation of maritime communications, bridge the language gap in global operations. AI-powered surveillance systems enhance security at sea by automatically detecting anomalies (Chen et al., 2024; Y. Yang et al., 2023).

Another innovative field of application is the use of autonomous ships. These ships would apply AI-operated systems to handle their functioning with high-order machines learning algorithms and computer vision, enabling cumbersome maritime data to move ahead with little intervention from human resources. Activities in this respect are pioneered by companies such as Rolls-Royce and Kongsberg. Already operational models, like that of the completely electric and autonomous container vessel Yara Birkeland, demonstrate examples of the use of such technology (Fonseca et al. 2021). Such systems combine data from various sensors and radar by satellite communication to make decisions with precision in real-time, without error, making operations safer. Another fast-changing application of AI involves maritime traffic management (Martelli et al., 2021).

Moreover, AI algorithms are being applied to monitor the pattern of vessel movements with the aim of anticipating traffic density and thermally optimizing shipping routes for optimum performance

(Zhang et al., 2022). Such systems can alleviate congestion in busy maritime zones while enhancing operational efficiency and fuel consumption. AI-driven tools are also being implemented to optimize port logistics. AI with predictive analytics would make it easier to automate the scheduling so that cargo is loaded and unloaded faster, reducing the overall time taken for the turnover process. It will reduce operational costs as well. The integration of AI in port operations also fits the current general trend of developing "smart" ports and adopting digital technologies that contribute to better connectivity and productivity (Almeida, 2023). It is seen, upon review, that such technologies have the potential to contribute meaningfully to the attainment of IMO's decarbonization targets. Predictive analytics models, supported by Big Data, are making possible new routes that are more fuel-efficient and hence contribute to the reduction of GHG emissions (Durlik et al., 2024).

Another emerging use of AI in vessel servicing involves AI-driven condition-based prediction and maintenance systems. These depend on data from IoT sensors attached to critical machinery or equipment to predict a failure before it takes place. Such a strategy minimizes downtime, saves money on expensive repairs, and increases the operating life of oceanic systems. In sum, these technologies enable a gradual shift in strategy from reactive to predictive in maintaining facilities, marking a monumental shift in maritime engineering items (Ahmed Murtaza et al., 2024).

However, despite the potential of AI and Big Data in maritime operations to create a more sustainable and efficient industry, the path to realizing these promises includes challenges to overcome. There are still very significant hurdles, including high implementation costs, a complex set of international regulatory frameworks, concerns related to its impact on the well-being of seafarers on board ships, and, most importantly, privacy and security concerns (Lagdami, 2023).

3. ETHICAL IMPLICATIONS OF USING AI AND BIG DATA IN MANAGING SEAFARERS ON BOARD SHIPS

The technological revolution brings unprecedented opportunities for operational efficiency and workforce management. Nevertheless, it simultaneously introduces complex ethical challenges across multiple domains, including potential worker surveillance, occupational safety and health (OSH) risks, and cybersecurity vulnerabilities.

3.1 Potential surveillance of workers

Integrating AI and Big Data in the maritime industry has significantly transformed workforce management. Traditionally, workers' performance has been evaluated through Key Performance Indicators (KPIs) and assessments by Human Resource (HR) departments (Lagdami, 2023). However, analog and digital tools are now employed with technological advancements to monitor work performance, potentially serving as surveillance tools. This shift enhances managers' ability to issue directives, evaluate performance, and decide on promotions or contract execution. This marks a radical change where AI-enabled applications help manage the workforce. Approximately 40% of HR duties globally now use such technologies to capture data about individuals, including sentiments and social media activity, generating "big data" for monitoring efficiency (Moore, 2019). The practice of "People Analytics" involves using big data to assess workers' performance and manage talent, with about 71% of international companies prioritizing this use due to its benefits in addressing business continuity and reputational risks (Moore, 2019, citing Houghton and Green, 2018).

According to a recent study by WMU, seafarers are likely to be targeted for surveillance onboard ships by AI in ways that could go well beyond safety matters (Lagdami, 2023). This practice can be attributed to various factors inherent to the special conditions of working in a maritime environment. Ships are confined spaces for all intents and purposes, and they severely restrict the physical movement and interaction of crew members with the outside world. Crew members live and work in close quarters, complicating interpersonal dynamics. Consequently, ships are more vulnerable to challenges related to protecting the personal data of seafarers (Lagdami, 2023).

Given that life on board merges professional duties with personal time, monitoring seafarers' work schedules and responsibilities might be challenging without touching on their private lives. Effective work management is essential to avoid fatigue that affects performance and safety at sea. However, measures need to be established to protect seafarers from using technologies that might discriminate against them based on their fatigue levels and, indirectly, their performance.

3.2 OSH Risks

AI technologies have enhanced HR roles like human capital management but pose risks to OSH. Tools like "People Analytics" aid recruitment by accessing candidate data and conducting bias-free interviews. However, these tools can lead to structural, physical, and psychosocial risks if not managed ethically. Due to algorithmic decision-making, employees may experience stress from perceived surveillance or fear of job loss. AI systems like Cobots and Chatbots have been integrated into industrial processes, reducing human labor and raising psychosocial concerns about job security. While Cobots can mitigate OSH risks by reducing exposure to hazardous environments, they also introduce risks such as robot/human collisions and security vulnerabilities.

Additionally, AI-driven automation can lead to work overload as employees strive to meet machine-paced demands (Moore, 2019, citing Kaivo-oja, 2015). In addition, a report reveals that collaborative robots (cobots) minimized the OSH risks by reducing workers' exposure to hazardous ergonomic, physical, and chemical environments. On the contrary, another study recognized three main categories of OSH issues that occur during the interaction of humans, cobots, and the environment:

1. *Collision hazards:* unpredictable robot behavior, which can stem from machine learning, may lead to collisions between robots and humans.
2. *Security risks:* The robot is connected to the internet, and this can breach its software integrity, presenting security risks for the system.
3. *Environmental Risks:* Unpredictable human reactions and the gradual deterioration of sensors in unstructured environments can cause environmental risks (Moore, 2019).

AI has enabled the integration of voice recognition and machine vision into chatbots, which raises concerns about unskilled and skilled jobs being taken over by machines through AI, eliminating the need for human workers. If it is not well managed, AI-assisted robots have the potential to stress workers and create anxiety (Lagdami, 2024). It has been observed that the combination can create psychosocial concerns wherever there is a mixture of automation, algorithmic management, and digitalization, especially when workers are expected to keep pace with machines and not the opposite. In some cases, a single worker has to oversee more than one machine, receiving alerts on their own devices such as smartphones or computers. Such an environment can contribute to work exhaustion,

forcing seafarers to work beyond work hours. The pressure on seafarers to adjust to technological changes can push them to technostress, the stress directly related to using new technologies (Lagdami, 2024).

3.3 Cybersecurity Challenges

The integration of AI and Big Data in the maritime industry also increases vulnerability to cybersecurity breaches. In tacting much more seriously into the digital era, cybersecurity breaches have risen, with operational technology attacks leaping as high as 900% in the last 3 years (Akpan et al., 2022). Systems that use interconnected networks, cloud platforms, and real-time data exchange become obvious targets for cyber-attacks (Yang et al., 2019). Different threat actors could use such vulnerabilities to access information to manipulate or disrupt critical operations at sea. For example, a cyber-attack on an AI-powered navigation system can issue a wrong route for vessels, thus putting crews and cargo in hazardous situations. Similarly, a breach in Big Data systems can negatively impact operations at ports or disrupt in global supply chains (Kanellopoulos, 2024; Yang et al., 2019).

Notable incidents have been demonstrated in the outcomes of such breaches, such as the ransomware attack on Maersk, the largest shipping company in the world, in 2017. "The failure of its massive IT system caused disruption in shipping operations across the world, apart from the estimated loss to be $300 million." (Soyer & Tettenborn, 2020; Tabish & Chaur-Luh, 2024). This incident was essentially operational, except for the broader implications on data security; sensitive information on customers and operational data was vulnerable to corruption in the sudden recovery process (Clavijo Mesa et al., 2024; Welburn & Strong, 2022). In a similar example, in 2020, the Mediterranean Shipping Company, MSC, faced a cyber-related incident involving unauthorized access to its customer database (Soyer & Tettenborn, 2020). This breach caused disruptions in container bookings and sensitive data exposure, shaking customers' trust and requiring costly mitigation efforts. Such incidents have brought up the growing demand for solid cybersecurity measures that would help protect sensitive data, including seafarers' personal information, against theft and misuse (Katsikas et al., 2025).

By far, the most concerning impact of such incidents is the leakage of seafarers' personal information, in the era of digitalization onboard ships. Kechagias et al. (2022) identify that, with the increasing use of networked digital tools in everyday operations, seafarers are particularly at risk from hacking incidents. Heering et al. (2021) also indicate that present maritime education and training programs lack a proper element of cybersecurity, rendering seafarers poorly prepared while on the job to identify and neutralize any cyber threats. Such cyber incidents put at risk sensitive information such as medical records, identity details, and financial data. In addition, such information may lead to identity theft, fraud involving financial transactions, and psychological trauma, among other impacts (Symes et al., 2024). Trust between seafarers and their employers is also undermined whenever inadequate steps have been taken to secure information. These incidents could also cause profound reputational harm to the shipping companies, leading to possible legal liabilities, regulatory penalties, and erosion of stakeholder confidence (Karim, 2022) Therefore, cybersecurity risks must be dealt with in robust frameworks through international cooperation to keep sensitive data secure and maritime operations resilient.

4. METHODOLOGY

This study employed a combined approach between literature review and expert interviews. An extensive literature review on the application of AI and Big Data in the maritime sector was performed. The review covers more than fifty-five papers on the current implementations of AI and Big in the maritime sector. It is important to note that there is a significant gap in literature concerning the social aspects of applying AI and Big Data in the maritime industry. Only a few studies address the ethical aspect of the use of AI and, more specifically, the potential surveillance and control of seafarers through AI, as well as the implications of cybersecurity threats to seafarers using their personal data.

In addition, twelve (12) semi structured interviews were conducted with experts from maritime and aviation sectors (for comparative purposes) and technology developers specializing in AI and Big Data applications. These interviews provided valuable insights into practical applications of AI and Big Data in the maritime industry, potential future developments and their implications, challenges, and concerns regarding implementing these technologies, and comparative perspectives from the aviation industry, a more mature, placed-automation industry-aviation.

The authors used a qualitative analysis method to synthesize the information from the literature review and expert interviews. This analysis focused on important themes, trends, and the possible effects of AI and Big Data on seafarers, especially concerning the OSH risks posed by worker surveillance, privacy concerns, and cybersecurity vulnerabilities. This method enables an in-depth understanding of the subject, merging the theoretical knowledge in literature with expertise from industry experts and technology developers. Using a qualitative analysis method, which is appropriate for this subject as not much research work has been done in this regard, gives a more nuanced picture of the interactions between AI/Big Data technologies and seafarers' working conditions through this methodology. They examine four critical areas: technological integration, operational efficiency, seafarer well-being, and ethical considerations. Many of these technologies (AI + Big Data) have the potential to both benefit and threaten seafarers as they get more sophisticated. Although these technologies can potentially improve maritime safety, optimize route planning, and increase operational efficiency, they pose substantial challenges, including heightened vigilance, possible job insecurity, and privacy concerns. Through scrutinizing such advancements and their respective consequences, this paper seeks to participate meaningfully in the discourse, offering a contribution towards the future of the human element, seafarers, in a highly automated and digitized maritime industry. The analysis seek to aid stakeholders in understanding these complex interrelationships by charting the link between technological interventions at sea and various seafarer experiences, showing that a balanced approach is required from the shipping industry to ensure that technological developments do not come at the cost of seafarers' welfare.

5. CASE STUDY USING THE VDR AS AN EXAMPLE

The voyage data recorder (VDR), also commonly referred to as a ship's "black box", is designed to assist in recording some of the critical operation and navigation information during the voyage. The International Maritime Organization (IMO) governs its use in line with the International Convention for the Safety of Life at Sea, commonly referred to as SOLAS 74, providing that VDRs must be fitted on all passenger ships and cargo vessels over 3000 gross tons (Hopcraft et al., 2023). It also records, to maintain the standard required for maritime safety, the vessel's position, speed, bridge audio, and Very High Frequency (VHF) communications. These shall be tested annually for performance under SOLAS

Regulations 18 and 20 (IMO, 2020), which validate the recorded data integrity, recoverability, and protective devices. With recent technological advancements involving the addition of AI in maritime operations, severe legal and ethical challenges arise, especially in balancing seafarers' privacy and data protection to ensure the maritime is safe (Battineni et al., 2024).

To effectively illustrate the significance of the VDR as a central case study in the realms of AI and Big Data, it is vital to highlight its foundational role in the evolution of sophisticated data collection and analysis systems within the maritime industry. Although the VDR itself does not utilize artificial intelligence, it marks a substantial milestone in the quest for thorough data gathering on vessels, serving as a critical steppingstone towards the integration of AI and Big Data solutions.

The VDR systematically records a wide array of data, including navigational details, engine performance metrics, and the activities of crew members aboard the ship. This diverse pool of information offers invaluable insights that can potentially be harnessed through advanced AI algorithms and Big Data analytics. Such integration could significantly enhance maritime operations, improve safety protocols, and streamline crew management practices.

By establishing this connection, we can see how technologies like the VDR lay the groundwork for the development of future AI and Big Data applications in the maritime sector. This transformation not only facilitates better decision-making but also paves the way for more innovative and efficient ways of operating vessels, ultimately leading to a safer and more productive maritime industry.

5.1 Introduction of AI into Maritime Operations and Psychological Stress on Seafarers

Integrating AI into the maritime industry brought fundamental changes into operation, primarily through technologies like VDR. While these tend to improve safety and efficiency at sea, they have also considerably impacted on the psychological well-being of the seafarers concerned. Most seafarers raise concerns about being watched at any one time since these VDR systems are linked to onshore offices. In the words of one seafarer, "*It seems like we are tracked down, not just for the purpose of safety, but control.*" The sense of invasion from monitoring technologies beyond operational necessity is upsetting. The fear is that such perpetual monitoring might destroy a great deal of trust between the seafarers and the company, which is surely bound to have a spillover effect on output and morale. This means there is a dire need to balance operational monitoring with respect for the crew's privacy.

5.2 Privacy Concerns and Lack of Regulation

While VDR data is very important in any maritime safety investigation, regulations have yet to address seafarers' privacy issues (Hopcraft et al., 2023). The guidelines issued by IMO are primarily related to the functionality of the data and recovery post-incident; thus, this leaves a gap in how this data is accessed and used in real-time operations. One interviewee, the CEO of Danelec, a developing technology company based in Denmark, commented, "*The data we collect is important for investigations, but we are aware of the gap in the legislation on how this information is accessed and used, particularly about the crew's privacy.*" Such acknowledgment by a leading VDR manufacturer underlines the need to introduce robust privacy protection. Such lack of clarity in regulation not only puts seafarers in jeopardy of their data falling into misuse but also proves to be a failure to align maritime practices with the modern data protection standards evident in other industries.

It goes without saying that while VDR data is essential in ensuring safety, its management must be critically analyzed so as not to infringe on basic seafarers' rights. A framework that correctly outlines

what to do and what not to do with data would be a great way of soothing these concerns and making life on board much safer and more supportive.

5.3 Ongoing Monitoring and Perception of Surveillance

The integration of AI-enabled VDRs has increased concerns regarding continuous monitoring, with a belief among many crew members that their privacy is compromised. As one mariner working in Danish Flag Ship said, "*Knowing that everything we say or do on the bridge is recorded and could be reviewed later makes it hard to feel at ease during operations*". That reflects a more profound problem, which means that ensuring the safety of the operation is perceived as a mechanism of control. It is not an isolated feeling but indicative of a more significant challenge in balancing technological advances against psychological welfare for the crew. It is intended to make the crew safer and more accountable by monitoring them, but such a system has the unintended consequence of increased workplace stress.

This may have longer-term implications for crew performance and raises questions about the purposes for which data is used and for whom. It would benefit employers if they could reassure seafarers that data is not used punitively or outside its intended purpose and reduce, to some degree, anxiety related to such technologies.

5.4 Impact of Cloud-Connected VDR Systems

Newly introduced cloud-based information VDR systems by companies like Danelec based in Denmark complicate privacy issues. After providing the crucial data virtually when an emergency arises, the system promotes data security to uncomfortable levels. How many seafarers can be monitored? The CEO of Danelec Marine responds, "*Only central data is stored in-cloud - not routine conversations.*" This does not do much to conquer high levels of distrust among seafarers about data being abused. It has pinpointed an essential issue: this kind of transparency means little when the workers fail to believe that the technology is being implemented for their benefit. This would require that the maritime industry lay down protocols and communicate them clearly enough to instill trust. If not, the advantages of a cloud-based system might be buried by the psychological impact such a system has on seafarers, who may consider their every action being tracked.

5.5 Aviation Industry Comparisons

An excellent example of this approach is the aviation industry, in which it is forbidden, under regulation, to allow any punitive usage of information obtained by a Flight Data Recorder (FDR). One interviewee working with Delta Airlines said that "*in aviation, any data provided is first scrubbed to avoid any identification, and analyses are ensured to be "not adversarial to pilots.*" Therefore, using data without punitive outcomes is fully in line with a so-called non-punitive safety culture because it maintains people's protection while being operationally accountable. On the other hand, such protection does not exist within the maritime industry, which in turn leaves seafarers exposed to possible invasion of privacy (Hopcraft et al., 2023).

This disparity underlines the extension of protection similar to that of the maritime industry. Emphasis on anonymity and no individual blame, but rather a focus on systemic improvement, shows

the model that could go a long way in easing anxiety among seafarers and making their work environment more supportive.

5.6 Call for Balance and Technological Adaptation

The above discussion aligns with what seafarers have been demanding: a more balanced approach to implementing advanced technologies. While they acknowledge the safety benefits of AI and VDR systems, they point out their right to privacy and involvement in decision-making. As one Captain who prefers to stay anonymous pointed out, "*We are not against new technologies, but it is important that their introduction respects our privacy and is accompanied by the relevant training to minimize stress*". To assuage these fears now requires serious collaboration between technology developers, shipowners, and seafarers.

From an analytical point of view, one can readily note that technological integration within the shipping sector will prosper only when such psychological effects within the workforce are addressed. Properly training seafarers regarding the use of new technology and involving them in the discussion would reduce the distress caused by implementing such technologies. In addition, regulatory frameworks must be robust and guarantee the privacy of seafarers so that a relationship based on trust and cooperation prevails. Absent these measures, the full potential of such technology as AI and VDR systems may not be realized, which is somewhat ironic because it is the very workforce they purport to support.

6. ANXIETY BECAUSE OF FEARS OF CYBER-ATTACKS AND PRIVACY VIOLATIONS AMONG SEAFARERS

While modern vessels increasingly rely on networked systems and internet connectivity, bringing considerable benefits related to operational efficiency and crew welfare, the downside is the vulnerability to cybersecurity attacks that directly impinge on the privacy of seafarers (Tam & Jones, 2019). The crew often uses the ship's network for personal use, like accessing social media, banking, or communicating with family; thus, their sensitive information may be exposed in a cyberattack. Views from one seafarer were, "*We use the same network to connect with our families and manage personal tasks. The thought of it is terrifying that a breach could expose private pictures or bank information.*" This comment brings forth the growing anxiety amongst the crew members concerning their digital footprint.

From a technical perspective, the interdependence of today's vessels as operational systems, communications networks, and crew access to the internet often overlap, creating an environment where a breach on one level could compromise an entire network. Cyber-attacks, such as ransomware, are considered a significant hazard since attackers access private data or cripple ship operations. For example, a ransomware attack could block crew members from accessing their accounts or expose private conversations and financial information. This is not just a breach of privacy, it also creates an insecure atmosphere in which crew members feel uncertain about their personal information.

This risk is further exacerbated by the fact that some vessels lack adequate cybersecurity controls. Unlike at corporate office buildings, with an ever-watchful IT team monitoring or mitigating

potential threats from malicious actors, a maritime network would not always have the same oversight and controls implemented (Mileski et al., 2018). A representative from a firm offering cybersecurity services for maritime testified, *"Shipboard networks are frequently not as secure as they should be. That puts them at high value for attacks, which would be really destructive not only to operations but also to personal data from crew members."* The threat of cyberattacks adds another layer to seafarers' stress, who now have a further concern, in addition to physical safety, for their digital personal life.

This is not an unreasonable apprehension; actual incidents demonstrate how such risks can always be a reality. The potential loss of personal data, for example, in situations where a vessel might be the target of a cyber hack, will affect the confidence of any seafarer in that ship's system. For the crew members, there is also the possibility of becoming victims of identity theft and financial loss upon data breach. At its worst, the scenario can include blackmail, coercion, and exploitation of information that was strictly private by their attackers. Such a proposition gives tangible meaning to imposing wide-ranging cybersecurity protocols for operation- and person-based data. If shipping companies implement rigorous security measures, segregation, data encryption, and periodic auditing of ships' systems, among other precautions, risks could be diminished. Besides that, training programs should be initiated, which would help seafarers understand various best practices in cybersecurity, including identifying phishing attempts and not giving away personal information. The opinion of one captain about the measures mentioned above is given: *"We need assurance that the networks we rely on are secure. Training and clear policies on cybersecurity would go a long way in easing our concerns."*.

Therefore, international regulatory bodies such as the IMO and ILO must also take proactive roles in this direction. Strict guidelines should be developed that may help safeguard crew privacy against cyber threats. Taking a cue from the aviation sector, where cybersecurity and data privacy are closely regulated, maritime needs to do the same. "*Regulations that focus solely on operational security are not enough.*" said a representative of the shipping industry. We must make personal data security integral to cybersecurity strategies.

In summary, seafarers strongly fear that there could be cybersecurity attacks aimed at personal information. It is about personal and private life; shared ships' networks remain sensitive concerning vulnerability when breaching into the core of the seafarers' private life and personal being. Solutions would involve fighting it from many angles: technological solutions, large-scale training, and clear regulatory frameworks that put operational concerns on an equal footing with the personal security of data. Without these countermeasures, the psychological distress that comes with cyber threats makes a mockery of the gains from technological advancements in the maritime context.

7. DISCUSSION

The integration of AI and Big Data in the maritime industry does bring certain tantalizing opportunities, but there's a whole set of essential challenges. The critical discussion in this chapter will be limited to three specific areas of interest. First is the issue of emerging worker surveillance. Nowadays, technology has developed so much that every employee can be followed in real time, as well as what every single person was doing at a certain moment on the vessels. This would provide maximum flow of work and complete security for any accidents. At the same time, however, some very serious questions concerning privacy and the rights of the workers have come into focus. Second is OSH risks

with the implementation of AI and Big Data technologies. Such technologies may help to identify risks and enhance safety, while at the same time exposing new hazards. For example, reliance on automated systems leads to complacency among workers and unexpected loopholes in safety protocols. Finally, cybersecurity is at risk in this modern age. The more interconnected these systems are with other systems, the graver the consequences of cyberattacks against maritime operations in terms of data breaches, disruption of activities, and unsafe conditions. On the other hand, poor cybersecurity can compromise the integrity of sensitive information and that of maritime operations. These sectors call attention to, put together, an optimal path which takes the best features of AI and Big Data while reducing the perils lying ahead and the difficulties a path may entail.

Applying AI and Big Data to monitoring seafarers adds intensely contentious ethical issues. While these technologies can increase the efficiency of operations, each approach introduces risks to privacy and autonomy. The restricted environment of ships makes it difficult for monitoring systems not to violate the privacy of seafarers — the line between work and personal life has virtually disappeared. People analytics is a rising trend in workforce management — 71% of international companies emphasize using it (McIver et al., 2018). Yet this can massively result in maritime techno-surveillance, harming seafarers' well-being and job satisfaction. However, adopting AI technologies in the maritime sector raises new OSH issues and challenges. While these technologies may minimize exposure to dangerous environments, they also introduce new hazards (Li et al., 2022). Seafarers may face anxiety and work exhaustion due to fear of job loss due to automation and the stress of keeping up with AI-driven systems. Although cobots lower some hazards, they may introduce others, including the risk of humans colliding with machines (Li & Yuen, 2024). Moreover, constantly keeping up with fast-changing technologies can cause technostress — the pressure to adapt to new technologies creates a special kind of stress. Moreover, the growing reliance on artificial intelligence (AI) and extensive data systems in maritime operations also increases the risk of cyber attacks. These interlinked systems are prime targets for cyberattacks. For instance, one of the concerns is operational disruptions, as cyberattacks against AI-assisted navigation systems can be manipulated to re-route ships on the spot, causing danger to crew and cargo. The second big risk relates to data breaches. Hackers who gain access to Big Data systems can wreak havoc not just on port operations but also on global supply chains. This can have huge financial implications, as was the case in the 2017 ransomware attack on Maersk.

In summary, AI and Big Data have a lot of advantages in the maritime industry, but their integration needs to be kept in check with due ethics and safety mechanisms. Future studies should work on structures that will fully capitalize on their benefits while controlling their adverse effects on seafarers and operations. It is ethically degrading to consider that AI and Big Data can be used for tracking what a seafarer does. These technologies will very probably promote operational efficiency, but they are at the same time bringing new threats against privacy and autonomy along with them.

Similarly, new OSH challenges arise from the increasing use of AI technologies all over the value chain of shipping. While these reduce exposure to hazardous environments, they also bring forth other risks. Anxiety and work burnout could be more important for the seafarers who fear losing their jobs to machines, or their workload being increased by needing to compete with the AI systems. Cobots need to balance the minimization of physical risk, in particular when operating with humans, and the minimization of accidents that, in an automated cell, could arise from human interconnectivity. This rush or urgency to adapt to rapidly changing technologies can also lead to technostress, stress created by the use of new technologies.

Furthermore, higher reliance on artificial intelligence and Big Data systems used in maritime operations acts to increase cyber security risks. The interdependencies among such systems make them very attractive for cyberattacks. First of all, the concern is operational disruption-for example, a cyberattack on AI-based navigation routes to take it to a place that could put crew and cargo in danger. Other major threats are data breaches; if Big Data systems can be accessed by somebody else, that may affect not only the operations of ports and global supply chains but also the privacy of seafarers. While AI and Big Data add great value to the maritime enterprise, they would have to be tempered with ethical considerations and safety controls. Further studies should develop frameworks that can optimize the benefits of these technologies but will also lessen their adverse effects on seafarers and maritime operations in the future.

8. CONCLUDING REMARKS

AI and Big Data adoption in the maritime industry are a two-edged sword: on one hand, promising huge strides into efficiencies, safety, and environmental sustainability; but on the other hand, opening complex ethical questions. Applications start from improving routing of vessels through forecasting failures in equipment, streamlining port processes, maintaining autonomous ships, and optimizing complete onboard operations.

On introducing AI and Big Data, there are challenges related to the surveillance of seafarers, OSH issues, cybersecurity threats, and many others. While these are helpful in operational applications in order to reach efficiency in workforce management, AI-enabled use raises an alarm in terms of privacy encroachment and work-life balance continuum between seafarers.

Also, the integration of AI technologies into marine operations can give rise to psychosocial hazards, for instance, stress related to continuous monitoring and job loss due to automation. Ease of operation with collaborative robots-cobots-and chatbots, and reduced exposure to other hazards introduce new hazards: collision, security breach.

The high-tech environment in the sea brings about immediate impact: one of the prominent new concerns gaining attention is something which we have repeatedly warned about-cybersecurity. An increasingly attractive target for cyber-attacks because of the emerging network of interconnectedness, along with systems for the real-time exchange of data, will have hugely destructive effects on the safety of crew and cargo security, with impacts on the global supply chain.

While the maritime sector is rightly exploring these new technologies (AI and Big Data), it must maintain sight of the need to balance progress with the well-being of its seafarers. As a result, continued conversations between key stakeholders in the industry, policymakers, and academics are required to create ethical safeguards, effective cybersecurity protocols, and holistic training. However, only by taking this collaborative approach can the breadth of this innovation be used for the benefit of the maritime sector while also ensuring that the workforce's rights and safety are protected.

9. ACKNOWLEDGMENTS

The authors acknowledge the maritime and aviation experts and technology developers who shared their experiences and perspectives; A special thank you to the CEO of Danlec Company and two

experts from Delta and all captains and mariners who wish to stay anonymous. Their contributions were instrumental to our understanding of the ethical considerations and challenges presented by AI and Big Data in the maritime sector. The fact that they were willing to enter into this kind of conversation has made it clear that the pursuit of technological development needs to be balanced with the interests of the people at sea.

10. REFERENCES

Abdelsalam, H. E. B., & Elnabawi, M. N. (2024). The transformative potential of artificial intelligence in the maritime transport and its impact on the port industry. *Maritime Research and Technology*, *3*(1), 19. https://doi.org/10.21622/MRT.2024.03.1.752

Ahmed Murtaza, A., Saher, A., Hamza Zafar, M., Kumayl Raza Moosavi, S., Faisal Aftab, M., & Sanfilippo, F. (2024). A paradigm shift for predictive maintenance and condition monitoring from Industry 4.0 to Industry 5.0: A systematic review, challenges, and case study. *Results in Engineering*, *24*, 102935. https://doi.org/10.1016/j.rineng.2024.102935

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), 123–138. https://doi.org/10.3390/network2010009

Almeida, F. (2023). Challenges in the Digital Transformation of Ports. *Businesses*, *3*(4), 548–568. https://doi.org/10.3390/businesses3040034

Arévalo, P., Ochoa-Correa, D., & Villa-Ávila, E. (2024). A Systematic Review on the Integration of Artificial Intelligence into Energy Management Systems for Electric Vehicles: Recent Advances and Future Perspectives. *World Electric Vehicle Journal*, *15*(8), 364. https://doi.org/10.3390/wevj15080364

Battineni, G., Chintalapudi, N., Ricci, G., Ruocco, C., & Amenta, F. (2024). Exploring the integration of artificial intelligence (AI) and augmented reality (AR) in maritime medicine. *Artificial Intelligence Review*, *57*(4), 100. https://doi.org/10.1007/s10462-024-10735-0

Chen, X., Ma, D., & Liu, R. W. (2024). Application of Artificial Intelligence in Maritime Transportation. *Journal of Marine Science and Engineering*, *12*(3), 439. https://doi.org/10.3390/jmse12030439

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information*, *15*(11), 710. https://doi.org/10.3390/info15110710

Demigha, S. (2020), The impact of Big Data on AI. 2020 International Conference on Computational Science and Computational Intelligence (CSCI), DOI 10.1109/CSCI51800.2020.00259

Durlik, I., Miller, T., Cembrowska-Lech, D., Krzemińska, A., Złoczowska, E., & Nowak, A. (2023). Navigating the Sea of Data: A Comprehensive Review on Data Analysis in Maritime IoT Applications. *Applied Sciences*, *13*(17), 9742. https://doi.org/10.3390/app13179742

Durlik, I., Miller, T., Kostecka, E., Łobodzińska, A., & Kostecki, T. (2024). Harnessing AI for Sustainable Shipping and Green Ports: Challenges and Opportunities. *Applied Sciences*, *14*(14), 5994. https://doi.org/10.3390/app14145994

Fonseca, T., Lagdami, K, Schröder-Hinrichs, J.U., Assessing innovation in transport: An application of the Technology Adoption (TechAdo) model to Maritime Autonomous Surface Ships (MASS), *Transport Policy, 114 (2021) 182–195.* https://doi.org/10.1016/j.tranpol.2021.09.005

Geertsma, R. D., Negenborn, R. R., Visser, K., & Hopman, J. J. (2017). Design and control of hybrid power and propulsion systems for smart ships: A review of developments. *Applied Energy*, *194*, 30–54. https://doi.org/10.1016/j.apenergy.2017.02.060

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In *Developments in Maritime Technology and Engineering* (pp. 49–61). CRC Press. https://doi.org/10.1201/9781003216582-06

Hopcraft, R., Harish, A. V., Tam, K., & Jones, K. (2023). Raising the Standard of Maritime Voyage Data Recorder Security. *Journal of Marine Science and Engineering*, *11*(2), 267. https://doi.org/10.3390/jmse11020267

IMO. (2020). *SOLAS 2020 : consolidated text of the International Convention for the Safety of Life at Sea, 1974, and its Protocol of 1988 : articles, annexes and certificates* (I. M. Organization, Ed.). International Maritime Organization.

Kanellopoulos, A.-N. (2024). Enhancing Cyber Security and Counterintelligence in the Shipping Industry. *National Security and the Future*, *25*(1), 137–154. https://doi.org/10.37458/nstf.25.1.6

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Marine Policy*, *143*, 105138. https://doi.org/10.1016/j.marpol.2022.105138

Katsikas, S. K., Kavallieratos, G., & Amro, A. (2025). Future Trends in Maritime Cybersecurity. In *Computer and Information Security Handbook* (pp. 1663–1678). Elsevier. https://doi.org/10.1016/B978-0-443-13223-0.00104-1

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*, 100526. https://doi.org/10.1016/j.ijcip.2022.100526

Lagdami, K (2023). Country Report - Australia: AI & Big Data at Sea, Exploring the potential risk of surveillance of seafarers. In: Transport 2040: Impact of Technology on Seafarers - The Future of Work (pp. 102-118). World Maritime University. https://commons.wmu.se/cgi/viewcontent.cgi?article=1091&context=lib_reports

Lagdami, K (2023). Country Report – Denmark: Technostress at Sea – A Case Study of a Danish-Flagged Vessel. In: Transport 2040: Impact of Technology on Seafarers - The Future of Work (pp. 119-142). World Maritime University. https://commons.wmu.se/cgi/viewcontent.cgi?article=1091&context=lib_reports

Lagdami, K. (2024). Technostress and the future of work at sea. In: Tareq Ahram and Waldemar Karwowski (eds) Human Factors in Design, Engineering, and Computing. AHFE (2024) International Conference. AHFE Open Access, vol 159. AHFE International, USA. http://doi.org/10.54941/ahfe1005747

Li, X., Seah, R., Wang, X., & Yuen, K. F. (2022). Investigating the role of sociotechnical factors on seafarers' psychological capital and mental well-being. *Technology in Society*, *71*, 102138. https://doi.org/10.1016/j.techsoc.2022.102138

Li, X., & Yuen, K. F. (2024). A human-centred review on maritime autonomous surfaces ships: impacts, responses, and future directions. *Transport Reviews*, *44*(4), 791–810. https://doi.org/10.1080/01441647.2024.2325453

Lun, Y. H. V., Lai, K., Cheng, T. C. E., & Yang, D. (2023). New Technology Development in the Shipping Industry. In *Shipping and Logistics Management* (pp. 257–279). Springer International Publishing. https://doi.org/10.1007/978-3-031-26090-2_17

Majnarić, L. T., Babič, F., O'Sullivan, S., & Holzinger, A. (2021). AI and Big Data in Healthcare: Towards a More Comprehensive Research Framework for Multimorbidity. *Journal of Clinical Medicine*, *10*(4), 766. https://doi.org/10.3390/jcm10040766

Martelli, M., Virdis, A., Gotta, A., Cassarà, P., & Di Summa, M. (2021). An outlook on the future marine traffic management system for autonomous ships. *IEEE Access*, *9*, 157316–157328.

McIver, D., Lengnick-Hall, M. L., & Lengnick-Hall, C. A. (2018). A strategic approach to workforce analytics: Integrating science and agility. *Business Horizons*, *61*(3), 397–407. https://doi.org/10.1016/j.bushor.2018.01.005

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*, *3*(4), 414–430. https://doi.org/10.1108/MABR-08-2018-0026

Mohd Tahir, M. S., Mustapha, R., Hashim, M. E. A. H., Mohd Razalli, N., & Kleebrung, A. (2024). Merging the Application of Artificial Intelligence Technology in Maritime Industry: A Systematic Literature Review. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 19–34. https://doi.org/10.37934/araset.63.2.1934

Munim, Z. H., Dushenko, M., Jimenez, V. J., Shakil, M. H., & Imset, M. (2020). Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions. *Maritime Policy & Management*, *47*(5), 577–597. https://doi.org/10.1080/03088839.2020.1788731

Obschonka, M., & Audretsch, D. B. (2020). Artificial intelligence and big data in entrepreneurship: a new era has begun. *Small Business Economics*, *55*(3), 529–539. https://doi.org/10.1007/s11187-019-00202-4

Phoebe V. Moore (2019) Artificial Intelligence in the Workplace: What Is at Stake for Workers? In Work in the age of data, BBVA OpenMind Collection, no. 12, p. 93.

Soyer, B., & Tettenborn, A. (Eds.). (2020). *Ship Operations*. Informa Law from Routledge. https://doi.org/10.4324/9781003000754

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the Maritime Sector: A Literature Review. *Journal of Marine Science and Application*. https://doi.org/10.1007/s11804-024-00443-0

Tabish, N., & Chaur-Luh, T. (2024). Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. *IEEE Access*, *12*, 17114–17136. https://doi.org/10.1109/ACCESS.2024.3357082

Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

Ur Rehman, M. H., Yaqoob, I., Salah, K., Imran, M., Jayaraman, P. P., & Perera, C. (2019). The role of big data analytics in the industrial Internet of Things. *Future Generation Computer Systems*, *99*, 247–259. https://doi.org/10.1016/j.future.2019.04.020

Wang, J., Xu, C., Zhang, J., & Zhong, R. (2022). Big data analytics for intelligent manufacturing systems: A review. *Journal of Manufacturing Systems*, *62*, 738–752. https://doi.org/10.1016/j.jmsy.2021.03.005

Welburn, J. W., & Strong, A. M. (2022). Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, *42*(8), 1606–1622. https://doi.org/10.1111/risa.13715

Yang, D., Wu, L., Wang, S., Jia, H., & Li, K. X. (2019). How big data enriches maritime research – a critical review of Automatic Identification System (AIS) data applications. *Transport Reviews*, *39*(6), 755–773. https://doi.org/10.1080/01441647.2019.1649315

Yang, Y., Gai, T., Cao, M., Zhang, Z., Zhang, H., & Wu, J. (2023). Application of Group Decision Making in Shipping Industry 4.0: Bibliometric Analysis, Trends, and Future Directions. *Systems*, *11*(2), 69. https://doi.org/10.3390/systems11020069

Zhang, X., Fu, X., Xiao, Z., Xu, H., & Qin, Z. (2022). Vessel Trajectory Prediction in Maritime Transportation: Current Approaches and Beyond. *IEEE Transactions on Intelligent Transportation Systems*, *23*(11), 19980–19998. https://doi.org/10.1109/TITS.2022.3192574