AUTONOMOUS SHIPPING AND SMART PORTS IN INDIA: LEGAL CHALLENGES, REGULATORY READINESS AND GLOBAL BENCHMARKS

Ananta Kar, Kavita Shinde, Gurupreet Singh Sandhu, Ashok Raja, Vajaradeep Koshika*

Abstract

The rapid rise of Maritime Autonomous Surface Ships and smart-port technologies is reshaping global maritime operations, requiring matching legal and regulatory changes. While many leading maritime nations update their frameworks, India's readiness for autonomous shipping and smart ports remains underexplored. This study assesses India's legal and regulatory capacity for autonomous vessels and smart ports, comparing it to international benchmarks. Using a qualitative doctrinal and comparative approach, it examines key Indian laws—Merchant Shipping Act, Inland Vessels Act, and port rules—alongside global treaties like UNCLOS, SOLAS, COLREGs, and STCW. Secondary empirical data from the Logistics Performance Index, liner shipping connectivity, and port connectivity metrics compare India's performance to top global leaders.

The study identifies major regulatory gaps in India, stemming from human-centric legal assumptions, inadequate liability rules for algorithm-driven operations, and the absence of maritime-specific cybersecurity and data governance frameworks. Empirical comparisons show that India lags behind leading hubs—Singapore, Japan, and China—in logistics efficiency, liner shipping connectivity, and port integration metrics, hindering smart-port development and higher vessel autonomy. In comparison, the EU and Singapore have adopted integrated regulatory frameworks combining autonomous shipping rules, cybersecurity requirements, and data governance.

* Scholar, IIT Madras; ms25a208@smail.iitm.ac.in

In conclusion, India requires comprehensive legal reforms, including MASS-specific regulations, updated liability frameworks, mandatory cybersecurity protocols for ports, and structured data governance rules. Aligning these reforms with international standards will enhance regulatory certainty, operational reliability, and competitiveness in the evolving digital maritime sector.

Keywords: Maritime Autonomous Surface Ships (MASS); Smart Ports; Maritime Law; Regulatory Readiness; Cybersecurity and Data Governance; India

1. Introduction

The global maritime sector is undergoing a major technological shift, like containerization. Advances in automation, AI, sensors, cyber-physical systems, and digital platforms are transforming vessel navigation, operations, and port management (Watson et al., 2017). Maritime Autonomous Surface Ships reduce human roles in navigation and tasks, while smart ports use IoT, digital twins, 5G, automation, and data platforms to optimize operations. These promise greater efficiency, safety, sustainability, and resilience.

The IMO classifies MASS into four degrees of autonomy, from decision-support systems to fully unmanned vessels. Its Regulatory Scoping Exercise identified gaps in SOLAS, STCW, COLREGs, and UNCLOS, which assume human masters, crew, and lookouts. The EU, Japan, Norway, and Singapore advance via pilots, trials, and sandboxes (Lee et al., 2024).

India's long coastline, major ports, and ambitions position it well. Programs like Sagarmala, Maritime India Vision 2030, and port digitalization show commitment. Ports such as Jawaharlal Nehru Port Authority, Visakhapatnam, and Cochin have digital systems and smart features. The Inland Waterways Authority of India issued draft guidelines for autonomous inland vessels (Domenighini, 2024).

However, India faces major legal and regulatory challenges. The Merchant Shipping Act, Major Port Authorities Act, and Inland Vessels Act assume manned vessels and traditional ports. Terms like “master,” “seafarer,” “competent person,” and “proper lookout” create uncertainties for autonomous operations. Cybersecurity rules improve but lack maritime focus and global alignment, like the EU’s NIS2 Directive. Port data lacks rules for ownership, sharing, and interoperability (Li et al., 2024).

Globally, leaders create rules for automation risks. The EU integrates MASS research, GDPR/Data Act, and NIS Directives. Norway runs MASS trials; Singapore builds cyber-resilient ports (Lee et al., 2024). India should adopt these.

Current research lacks assessment of India's legal readiness vs. global standards (Lee et al., 2024). Studies focus on global conventions, liability, and safety; few check Indian laws for MASS and smart ports. Legal issues in cybersecurity and data governance are underexplored. This study fills the gap by analyzing legal, regulatory, and governance challenges for autonomous shipping and smart ports in India, compared to international standards.

1.1 Research Objectives

The study pursues four core objectives:

1. To assess the sufficiency of India’s current maritime legislation in regulating Maritime Autonomous Surface Ships.
2. To investigate liability, insurance, and accountability issues arising from autonomous vessel operations in Indian waters.
3. To review the regulatory readiness of Indian smart ports regarding cybersecurity, data management, and digital infrastructure.
4. To compare India’s legal and regulatory framework with international benchmarks and recommend specific reforms for alignment and future preparedness.

1.2 Research Questions

To achieve these objectives, the study addresses the following research questions:

1. **RQ1**: What degree of adequacy do India’s existing maritime laws provide for regulating MASS operations within evolving autonomous shipping paradigms?
2. **RQ2**: In what ways should liability be allocated for collisions, system malfunctions, and cyber-related incidents involving autonomous vessels in Indian waters?
3. **RQ3**: To what extent are Indian smart ports equipped for cybersecurity, data governance, and regulatory compliance in managing autonomous and digital maritime activities?

4. **RQ4**: How does India's regulatory framework stack up against international standards, and what legal reforms are needed to achieve alignment with global best practices?

1.3 Significance of Study

India aims to become a leading global maritime hub, making strong legal preparation essential. Autonomous vessels and smart ports bring new safety risks, cybersecurity threats, liability uncertainties, and governance challenges. Stakeholders- including insurers, shipowners, port operators, regulators, and policymakers- need clear legal guidelines for future operations. This study's comparative legal analysis enriches maritime law scholarship (Lee et al., 2024), guides policymaking, and strengthens India's ability to adopt emerging technologies.

2. Literature Review

Maritime Autonomous Surface Ships and rapid digital changes in ports have sparked growing interest among researchers, regulators, and industry experts. This literature review summarizes global and Indian studies on autonomous shipping, port digitalization, liability, data governance, cybersecurity, and regulations. It uses legal analyses, regulatory reviews, technical studies, and reports from the reference document. The review covers four sections linked to the research objectives: legal and regulatory challenges for MASS; liability and insurance; smart port governance, data management, and cybersecurity; and international benchmarks for India's readiness.

2.1 Autonomous Shipping: Concepts, Definitions, and Regulatory Gaps

Scholars agree that autonomous shipping greatly changes maritime operations. It challenges basic principles of international maritime law. The IMO defines four levels of autonomy: from ships with automated processes but human pilots onboard, to fully autonomous vessels with no humans aboard. These levels are widely used in research and regulations to spot regulatory gaps (Corsi et al., 2025).

Scholars agree that autonomous shipping greatly changes maritime operations. It challenges basic principles of international maritime law. The IMO defines four levels of autonomy: from ships with automated processes but human pilots onboard, to fully autonomous vessels with no

humans aboard. These levels are widely used in research and regulations to spot regulatory gaps (Corsi et al., 2025).

Numerous scholars argue that major international conventions—UNCLOS, SOLAS, MARPOL, COLREGs, and STCW—were designed for crewed vessels, assuming onboard human presence, decision-making, and expertise. Legal analyses highlight ambiguities in terms like “master,” “crew,” “seafarer,” and “proper lookout.” For example, COLREG Rule 5 requires a “proper lookout by sight and hearing,” which clashes with sensor- or AI-based systems on autonomous ships (Lee et al., 2024). SOLAS and STCW also mandate crewing and certifications are incompatible with unmanned operations.

Without onboard crew, existing flag state jurisdiction and the "genuine link" principal face questions, especially with remote control centers abroad. This demands rethinking "command" and "control" to assign responsibilities to remote operators and AI systems. The IMO is addressing these gaps with a goal-based, non-mandatory MASS Code for autonomous vessels' safety and operations.

Reviews from the European Maritime Safety Agency and journals like *Marine Policy* and *Research in Marine Sciences* suggest that Maritime Autonomous Surface Ships may need changes to current rules, new interpretations of provisions, or entirely new legal frameworks. Experts like Chircop argue that existing regulations lack flexibility for uncrewed ships unless key terms are redefined (Luchenko et al., 2023).

The IMO’s Regulatory Scoping Exercise identified many treaty provisions that block MASS operations, need clarification, or have gaps—especially defining “master,” “crew,” and “responsible person” (Kim et al., 2022).

Current rules also lack guidance on remote operation centers and remote operators’ qualifications. This requires shifting duties and liabilities from onboard crew to shore-based teams and automated systems. Such changes are vital for clear accountability and safe navigation in automated shipping (Corsi et al., 2025).

In India, research on autonomous shipping is limited but growing, noting similar regulatory gaps. The Merchant Shipping Act 1958 focuses on human roles in safety, seaworthiness, navigation, and liability. Recent Indian studies examine if MASS fit existing laws or need changes and new rules (Lee et al., 2024). The Inland Waterways Authority’s draft rules for autonomous vessels are a start but incomplete and limited to inland waters. This reveals a major

gap for MASS in international and coastal waters (Kim et al., 2022). India's laws, built for traditional ships, must adapt to autonomous tech needs. Scholars propose fixes: robotic ships need closed legal gaps for broad use, or MASS can operate under current rules for testing where not explicitly barred (Luchenko et al., 2023).

2.2 Liability, Insurance, and Accountability in Autonomous Operations

Liability is one of the trickiest and most debated issues in autonomous shipping research. Global studies list many possible responsible parties—such as shipowners, operators, software developers, hardware makers, connectivity providers, and remote-control staff—which makes assigning blame harder (Ringbom et al., 2020).

The literature identifies several models:

- Conventional fault-based liability regimes rooted in maritime tort principles
- Strict liability approaches to streamline fault attribution without onboard human operators
- Product and software liability regimes, particularly for AI-driven decision-making processes
- Hybrid models apportioning responsibility across multiple stakeholders

Research shows that longstanding COLREGs collision liability rules need reevaluation for algorithm-driven decisions. P&I Clubs and firms like Norton Rose Fulbright note gaps in "good seamanship," which do not easily apply to AI systems (Kim et al., 2022). This challenges traditional ideas like prudent navigation and human error, requiring new ways to assess and assign faults in autonomous maritime incidents.

Cybersecurity risks add further challenges to autonomous shipping operations. Cyberattacks on MASS could cause collisions, grounding, or cargo damage. However, current marine insurance lacks clear coverage definitions. Cyber exclusions in standard hull and P&I policies create uncertainty, requiring tailored insurance changes for autonomous vessels (Durmaz, 2024). Moreover, without global legal frameworks for allocating cyber risks in autonomous maritime operations, this uncertainty worsens, challenging insurers and operators.

In India, maritime accident liability relies on human negligence. No legal definitions exist for remote operators or AI decisions, complicating disputes. The Major Port Authorities Act and

Merchant Shipping Act ignore cyber incidents and autonomous failures, leaving gaps that scholars urge to fix. This calls for shifting from fault-based liability—which struggles without human error—to strict liability. Proponents argue it simplifies victim compensation when proving AI fault is hard and costly (Domenighini, 2024).

2.3 Smart Ports: Governance, Data Regulation, and Cybersecurity

Academic and policy literature defines a "smart port" as a digital, automated, and connected port system to improve efficiency, safety, and sustainability. It uses technologies like digital twins, IoT, sensors, automated cranes, autonomous vehicles, and data platforms. Studies highlight the need for regulations to protect operations, secure data, and ensure fair practices, including rules for data ownership, access, and use from smart ports and autonomous vessels (Alamoush & Ölçer, 2025).

2.3.1 Data Governance

International academic literature highlights the increasing importance of port data in digital maritime operations (Alamoush & Ölçer, 2025). The EU's GDPR and Data Act provide strong frameworks for data ownership, access rights, privacy, and interoperability. In contrast, many developing countries, including India, lack specific port data governance regimes (Alamoush & Ölçer, 2025). Without clear standards, challenges remain in sharing AIS data, terminal operations data, customs information, and third-party platform access.

A key concern is port data monopolization, where private terminal operators or digital platforms could dominate essential operational information, harming transparency and competition. Regulatory mechanisms are needed to ensure fair data access and prevent anti-competitive practices in smart ports.

2.3.2 Cybersecurity Challenges

Smart ports are key infrastructure vulnerable to cyberattacks. Reports from ENISA, Stormshield, and IMO highlight rising cyber incidents in port management systems, terminal operating systems, and vessel-to-shore communications.

The EU's NIS2 Directive requires cybersecurity risk management, incident reporting, and supply chain security for ports. The U.S. Coast Guard has strict cybersecurity guidelines.

In India, ports are advancing digitally via Port Community Systems, but cybersecurity rules remain fragmented. The Indian Ports Act, Merchant Shipping Act, and IT Act lack specific

mandates for maritime systems. Studies note the gap between digitalization and legal safeguards (Alamoush & Ölçer, 2025). This rules gap blocks safe adoption of autonomous and smart port tech, needing urgent reforms.

2.4 Global Benchmarks and International Comparative Frameworks

Extant academic literature consistently highlights the vanguard regulatory and operational leadership of jurisdictions including the European Union, Singapore, Norway, and Japan. These regions have conducted Maritime Autonomous Surface Ships trials, promulgated regulatory guidelines, and developed robust frameworks for cybersecurity and data governance. For example, the EU's holistic strategy—encompassing the NIS2 Directive and deliberations on sector-specific cybersecurity regulations—demonstrates a forward-looking commitment to securing essential port infrastructure and data (Alahmadi et al., 2021). Likewise, Singapore, a premier maritime hub, has proactively advanced and deployed initiatives for smart port evolution and autonomous vessel assimilation, prioritizing rigorous regulatory sandboxes and public-private partnerships to safely validate and optimize emerging technologies (Alamoush & Ölçer, 2025).

2.4.1 European Union (EU)

The EU strategy includes MASS research via EMSA, cybersecurity through the NIS2 Directive, and data rules via the GDPR and Data Act. Leading ports like Rotterdam, Hamburg, and Antwerp drive global smart-port innovations (Heikkilä et al., 2022). Their framework prioritizes:

- Compulsory cybersecurity
- Data interoperability
- Platform neutrality
- Strong environmental and safety rules

These set benchmarks for emerging economies like India.

2.4.2 Norway and Japan

Norway's Yara Birkeland project and Japan's autonomous shipping programs provide key lessons for MASS implementation. These countries offer advanced trial regulations, safety

measures, and technical standards. Their experiences stress the need for flexible rules that adapt to fast tech changes, ensure safety, and promote innovation (Ahmed et al., 2024). Australia has also shown strong progress in new technologies, despite starting late (Transport 2040: Automation, Technology, Employment - The Future of Work, 2019). These examples urge developing countries like Malaysia to create national plans with pilots, sandboxes, and partnerships for autonomous maritime tech.

2.4.3 Singapore

Singapore leads in cybersecurity for port operations and digital governance. The Maritime and Port Authority has issued cybersecurity advisories, smart-port data standards, and digital port management guidelines (Alamoush & Ölçer, 2025). This approach mitigates cyber threats, secures data flow for its global hub status, and promotes interoperability for autonomous vessels and smart ports. Strong cybersecurity and data interoperability are essential for Maritime Autonomous Surface Ships adoption (Corsi et al., 2025).

2.4.4 India in the Global Context

In contrast, India's regulatory framework is still developing. It has draft rules for autonomous vessels on inland waterways and smart port projects but lacks full legal support. Scholars suggest a blended model drawing from:

- IMO guidelines on Maritime Autonomous Surface Ships
- EU cybersecurity and data governance rules
- Singapore's digital port principles

This would speed up readiness for autonomous operations, close regulatory gaps, build investor trust, and support advanced tech infrastructure. Success depends on local tech development and strong governance (Mohanty, 2024). Collaboration with neighbors like Singapore—via shared protocols—would accelerate progress (Sani & Suhrab, 2025). It is key to harmonize rules and integrate tech across regions (Turner et al., 2024). Global teamwork is needed to address varying tech adoption levels and avoid fragmentation (Andrei & Scarlat, 2024).

3. Methodology

This study employs a qualitative doctrinal and comparative legal methodology with secondary data analysis. The doctrinal method reviews laws, treaties, and doctrines for manned ships and adapts them to autonomous technologies. Comparatively, it assesses India's readiness against leaders like the EU, Norway, Japan, and Singapore in MASS trials, cybersecurity, data governance, and digital ports, identifying best practices and gaps (Alamoush & Ölçer, 2025).

Secondary sources include IMO documents, Indian policies, reports (EMSA, IDB Smart Port Manual, ENISA/Stormshield), academic works, and data on ports, cyber incidents, digital maturity, and MASS trials (Corsi et al., 2025; Earthy, 2023; Mohanty, 2024).

The analysis has three stages:

1. Doctrinal review of legal gaps between autonomous and manned operations.
2. Comparison of India's cybersecurity, data, liability, and standards with global leaders.
3. Secondary data review of port digitalization, cyber risks, and tech performance.

Validity relies on primary sources, doctrinal methods, and triangulation. Limitations: scarce case law, emerging Indian scholarship, inconsistent data, and rapid tech changes (Andrei & Scarlat, 2024; Earthy, 2023; Mohanty, 2024). This provides a strong basis to evaluate India's preparedness and recommend reforms.

4. Data Analysis and Discussion

The empirical assessment employs descriptive statistics and visual benchmarking to compare logistics performance across the selected economies and to identify areas where India diverges from global best practices.

4.1 Empirical Data Analysis (LPI 2023 Benchmarking)

This section presents a benchmarking analysis of India’s smart-port and logistics readiness using the 2023 Logistics Performance Index (LPI) scores compared with Singapore, Japan, and China.

4.1.1 Descriptive Statistics

Economy	LPI Overa	Infrastructure Score	Tracking &	Logistics Competence Score	Timeliness Score	International	Customs Score

	ll Score		Tracing Score			Shipments Score	
Singapore	4.3	4.6	4.4	4.4	4.3	4	4.2
Japan	3.9	4.2	4	4.1	4	3.3	3.9
China	3.7	4	3.8	3.8	3.7	3.6	3.3
India	3.4	3.2	3.4	3.5	3.6	3.5	3

Table 1: LPI 2023 indicator scores (selected economies)

Table 1 shows Singapore leading all LPI scores, followed by Japan and China. India has the lowest scores overall, with the biggest gaps in infrastructure and customs. These limit smart-port readiness due to poor capacity and efficiency.

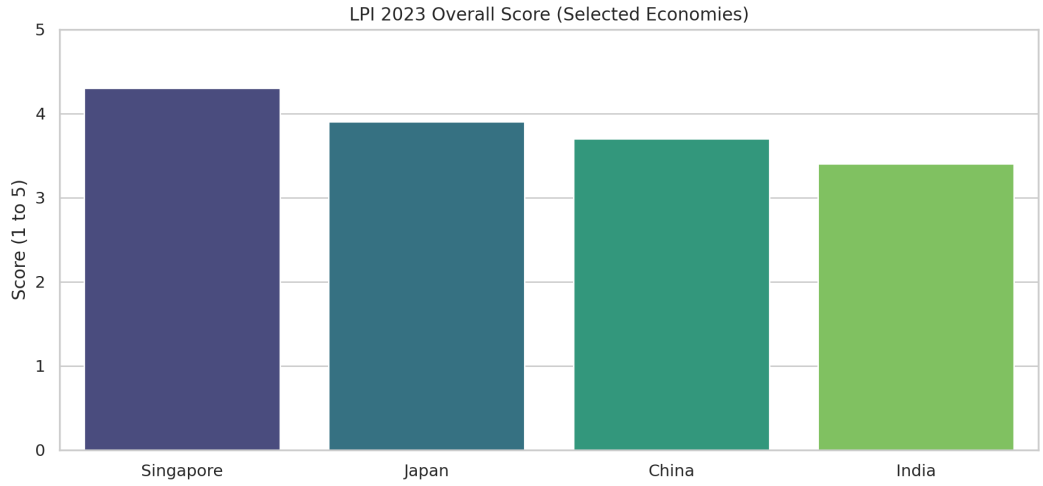

Figure 1: Indicator score profile heatmap (2023)

Figure 1 shows the rankings from Table 1. It confirms Singapore's strong leadership and India's weaker position. The chart highlights the large performance gap India must close to match global logistics and smart-port standards.

Figure 2: Indicator score profile heatmap (2023)

Figure 2 shows profiles across the seven LPI indicators. Singapore's high, balanced scores show an advanced logistics system. India's lower scores in infrastructure, customs, and competence point to limits for smart ports without basic reforms.

parameters	**India**		**Singapore**		**China**		**Japan**		**Gap (India - Singapore)**
	Mean (2023)	**Rank (among 4)**	**Mean (2023)**	**Rank (among 4)**	**Mean (2023)**	**Rank (among 4)**	**Mean (2023)**	**Rank (among 4)**	**Value**
LPI Overall Score	3.4	4	4.3	1	3.7	3	3.9	2	-0.9
Infrastructure Score	3.2	4	4.6	1	4	3	4.2	2	-1.4
Tracking & Tracing Score	3.4	4	4.4	1	3.8	3	4	2	-1
Logistics Competence Score	3.5	4	4.4	1	3.8	3	4.1	2	-0.9

Timeliness Score	3.6	4	4.3	1	3.7	3	4	2	-0.7
International Shipments Score	3.5	3	4	1	3.6	2	3.3	4	-0.5
Customs Score	3	4	4.2	1	3.3	3	3.9	2	-1.2

Table 2: Comparative LPI 2023 Indicator Scores, Rankings, and India–Singapore Gaps for Selected Economies

Singapore ranks first in all LPI indicators among these four countries. India ranks last except in International Shipments, where it is third and Japan fourth. The largest gaps with Singapore are in Infrastructure and Customs, followed by Tracking & Tracing.

4.1.2 Visualization

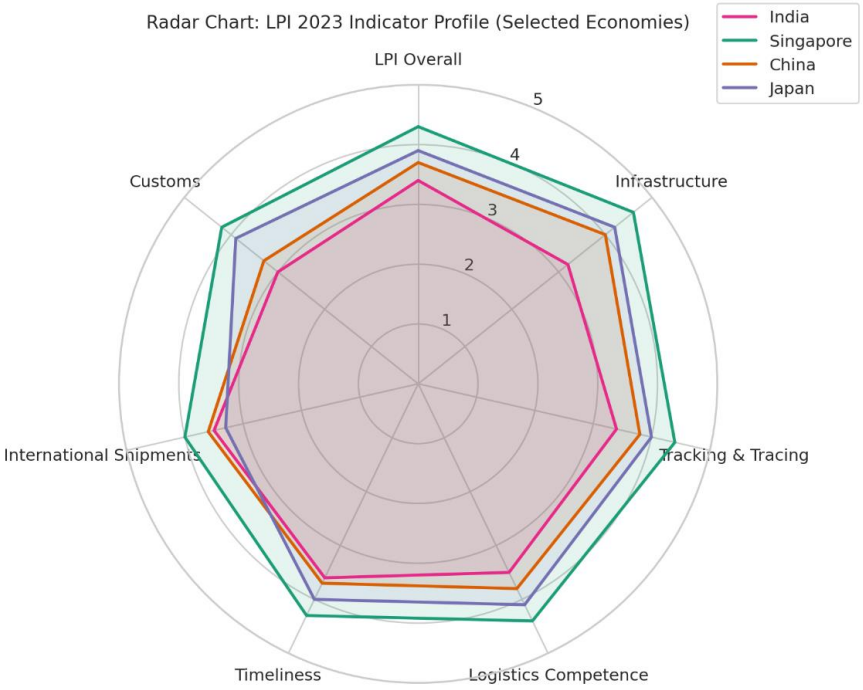

Figure 3: Radar chart comparing India, Singapore, China, and Japan across seven LPI indicators (2023)

Figure 3 shows LPI 2023 radar charts for the four countries. Singapore has the widest, most balanced profile, indicating strong logistics performance. Japan performs well overall but is weaker in international shipments. China shows moderate-to-high scores but trails Singapore

and Japan. India's smaller profile reveals major gaps in infrastructure and customs, limiting smart-port readiness.

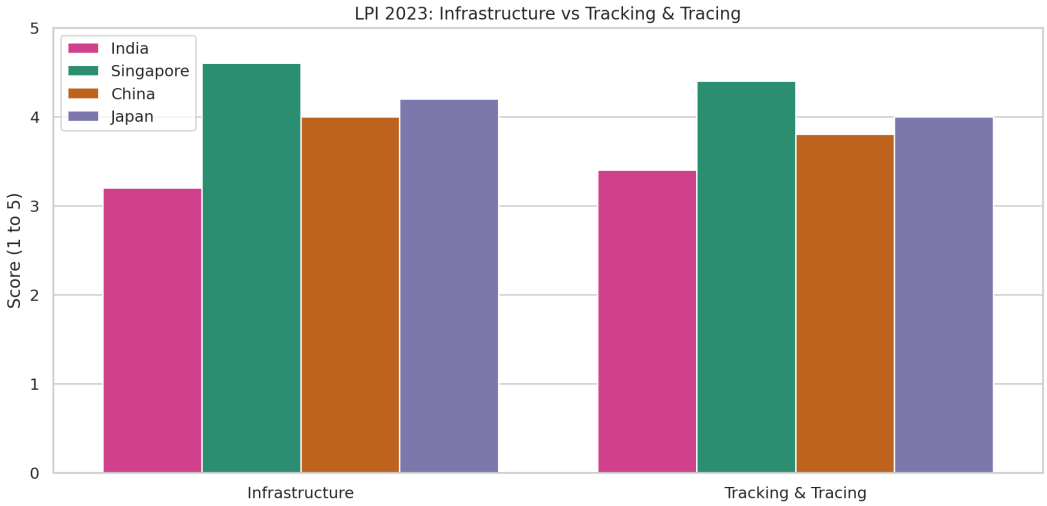

Figure 4: Infrastructure vs Tracking & Tracing (India, Singapore, China, Japan)

Figure 4 compares Infrastructure and Tracking & Tracing scores from LPI 2023 for India, Singapore, China, and Japan. Singapore leads both, with strong physical and digital logistics. Japan is balanced and strong. China has better infrastructure than tracking. India trails in both, showing gaps in capacity and tracking that hinder smart ports.

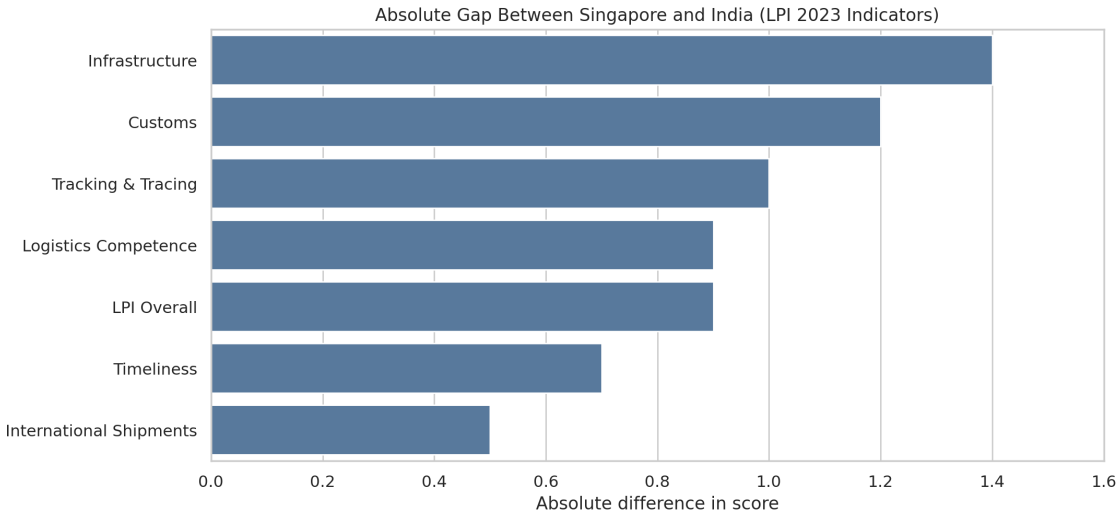

Figure 5: Absolute difference between India and Singapore (7 indicators)

Figure 5 shows absolute score differences between India and Singapore across the seven LPI 2023 indicators. The largest gaps are in Infrastructure and Customs, followed by Tracking & Tracing and Logistics Competence—highlighting India's shortfalls in physical capacity and

process efficiency. Smaller gaps in International Shipments and Timeliness indicate closer performance on outcomes than foundational areas.

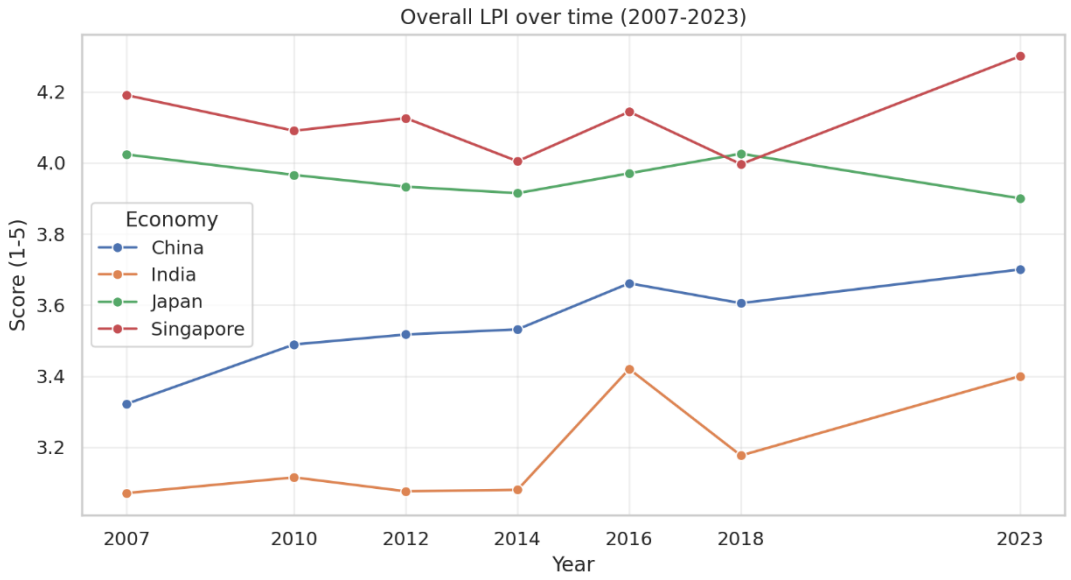

Figure 6: Overall LPI Scores for Selected Economies from 2007 to 2023

Figure 6 shows LPI trends from 2007 to 2023 for the four economies. Singapore leads consistently, with a sharp rise in 2023. Japan stays high and stable. China improves gradually. India trails overall but shows modest recent gains.

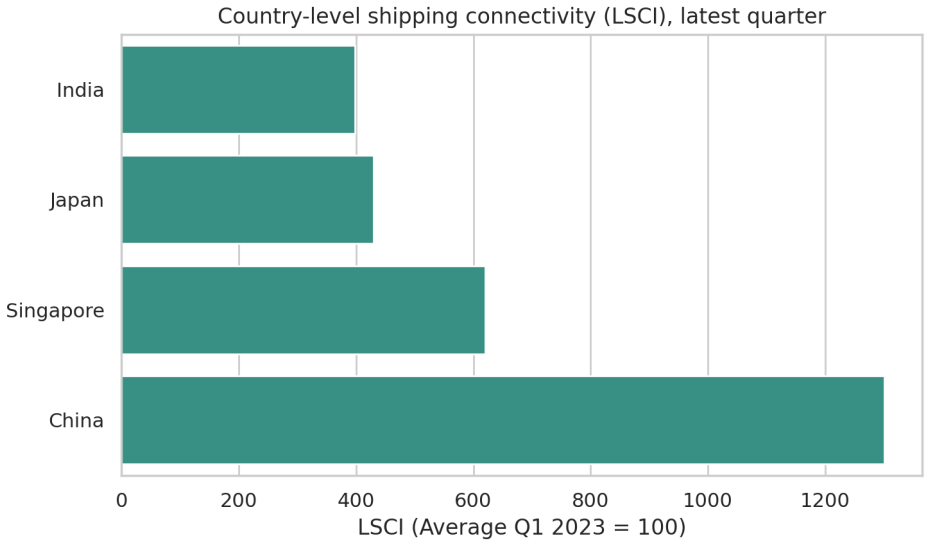

Figure 7: Country-level shipping connectivity (LSCI)

Figure 7 shows country-level liner shipping connectivity in the latest quarter for India, Singapore, China, and Japan. China leads with much higher connectivity, showing strong

global integration. India's lower score than Japan and Singapore suggest weaker networks, limiting smart-port and autonomous shipping compared to top hubs.

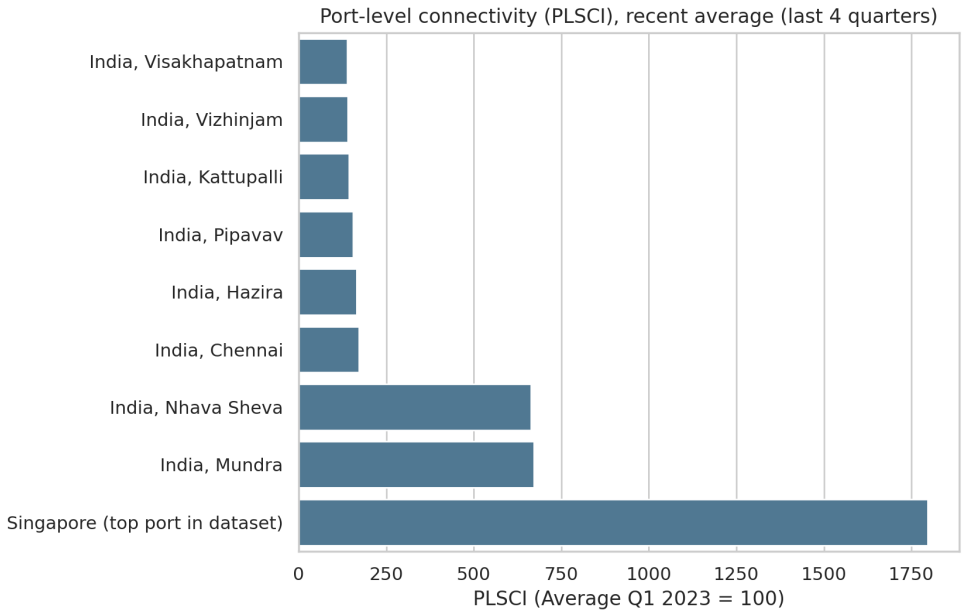

Figure 8: Port-level connectivity (PLSCI)

Figure 8 compares recent average port-level liner shipping connectivity for selected Indian ports and Singapore. Singapore's connectivity is much higher than all Indian ports, even top ones like Mundra and Nhava Sheva. This gap shows India lags global leaders and stresses the need for regulatory, digital, and data reforms to enable smart ports and autonomous shipping, which depend on strong networks.

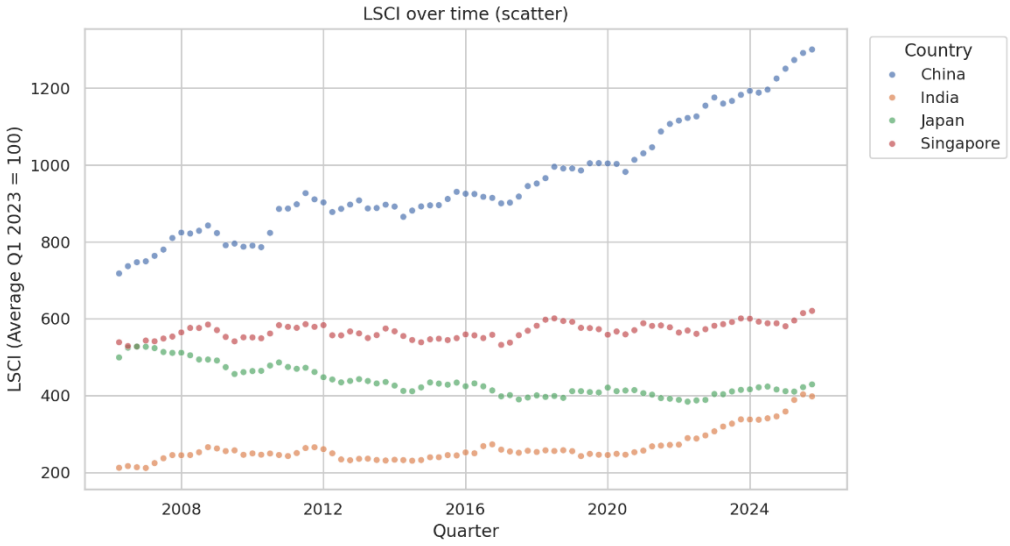

Figure 9: Quarterly Liner Shipping Connectivity Index (LSCI) Trends for Selected Economies (2007–2025)

Figure 9 shows quarterly Liner Shipping Connectivity Index trends for India, Singapore, China, and Japan. China's line rises steadily, showing growing global links. Singapore stays high. Japan dips then level off. India stays low overall, with small recent gains, showing a lasting gap vs. top hubs.

4.2 Analysis and Discussion

India's shift to autonomous shipping and smart ports faces legal hurdles from international conventions, national laws, and global norms. Programs like Sagarmala and Maritime India Vision 2030 drive digitization (Mohanty, 2024), but laws assume manned ships and manual ports (Alamoush & Ölçer, 2025). This analysis covers four areas: maritime laws for MASS, liability, smart-port rules, and international fitness.

First, India's Merchant Shipping Act assumes human masters, crew, and operations, with no provisions for remote or autonomous vessels. The Inland Vessels Act is similar. Like SOLAS and COLREGs, which reference human roles (Llave et al., 2025), Indian laws have gaps. Draft rules for inland autonomous vessels are limited and do not cover oceans, creating a major regulatory void needing updates or a new MASS framework.

Second, liability for autonomous vessels is unclear. Traditional law's base fault on human negligence, but MASS rely on AI, sensors, and remotes. Accidents could spark disputes over responsibility (e.g., owner, developer, operator). Global studies suggest strict or hybrid liability (Ahmed et al., 2024). Cyberattacks and insurance gaps add risks without MASS-specific rules.

Third, smart-port regulations lag. Ports use Port Community Systems and automation (Mohanty, 2024) but lack cybersecurity standards unlike EU's NIS2. The IT Act is general, not maritime-focused (Earthy, 2023; Mohanty, 2024). Weak data governance hinders interoperability and raises cyber risks (Andrei & Scarlat, 2024).

Finally, India trails leaders like EU, Norway, Singapore, and Japan, who have MASS trials, cybersecurity, and data rules. India's policies like Sagarmala lack legal backing (Mohanty, 2024). Reforms needed: define MASS/remote operators, update Merchant Shipping Act, add port cybersecurity/data standards, and set AI liability. Without these, tech advances will lack legal support.

5. Policy Recommendations

India's transition to autonomous shipping and smart ports requires strong regulations to fix gaps in current maritime laws, which focus on manned ships and traditional ports. Key recommendations, based on the best global practices, include updating laws, improving liability rules, boosting cybersecurity, setting data standards, and building skills.

5.1 Rules for Maritime Autonomous Surface Ships

Update the Merchant Shipping Act with clear definitions for "autonomous vessel," "remote operator," and related terms. Follow IMO guidelines for safety, operator training, system backups, and emergency plans. Extend inland waterway rules to coastal and offshore areas for uniform national standards.

5.2 Liability for Autonomous Shipping

Replace old fault-based rules with a mix of strict liability for operators and fault liability for makers and providers. Define when remote operators are responsible (e.g., negligence). Update marine insurance to cover cyber risks, AI failures, and software issues, matching global trends.

5.3 Cybersecurity for Smart Ports

Set mandatory standards like EU NIS2 or U.S. guidelines, including risk checks, incident reports, supply-chain reviews, and audits for cranes, IoT, and digital systems. Create a maritime cyber unit under the Directorate General of Shipping and train port staff.

5.4 Data Governance for Smart Ports

Develop rules for data ownership, access, sharing, and platform use to avoid conflicts and monopolies. Draw from EU Data Act and Singapore's model for fair access and interoperability. This will drive innovation, protect privacy, and prevent anti-competitive practices.

5.5 Institutional and Capacity Building

Set up a national center for MASS research and testing at Indian Maritime University. Create training for shore control operators. Use public-private partnerships for pilots, digital twins, and AI tests. Join IMO groups and partner with leaders like Singapore and Norway.

In summary, these reforms—law updates, liability fixes, cyber and data protections, and skill-building—will make India safe, efficient, and competitive in autonomous shipping and smart ports.

6. Conclusion

India stands at a pivotal moment in maritime development, as autonomous ships and smart ports transform global shipping. This study assessed India's legal and regulatory readiness, focusing on laws, liability for autonomous operations, smart-port infrastructure, and alignment with global standards. Despite initiatives like Sagarmala and Maritime India Vision 2030, India's laws remain outdated and human-focused, unfit for digital and autonomous tech.

Key findings: Laws such as the Merchant Shipping Act and Inland Vessels Act fail to address autonomous navigation, certification, seaworthiness, and duties. Fault-based liability does not handle AI errors, system failures, or cyberattacks—requiring strict liability, manufacturer accountability, and cyber safeguards. Indian smart ports lack mandatory cybersecurity, data-sharing standards, and digital protections.

Compared to leaders like Europe, Singapore, Norway, and Japan, India lags in regulations, cybersecurity, and data governance, risking slower tech adoption. Yet, India can adapt global best practices to foster innovation, safety, and competitiveness.

Recommendations include legislative updates, cybersecurity protocols, data governance, training programs, and industry partnerships. India's framework must evolve to be flexible, collaborative, and globally aligned. Future research should add empirical data on port efficiency, cyber risks, and pilots. These reforms will position India as a leader in autonomous and digital maritime technologies.

References

Ahmed, Y. A., Θεοτοκάτος, Γ., Maslov, I., Wennersberg, L. A. L., & Nesheim, D. A. (2024). Regulatory and legal frameworks recommendations for short sea shipping maritime autonomous surface ships. *Marine Policy*, *166*, 106226. https://doi.org/10.1016/j.marpol.2024.106226

Alahmadi, D., Baothman, F., Alrajhi, M. M., Alshahrani, F., & Albalawi, H. (2021). Comparative analysis of blockchain technology to support digital transformation in ports and shipping. *Journal of Intelligent Systems*, *31*(1), 55. https://doi.org/10.1515/jisys-2021-0131

Alamoush, A. S., & Ölçer, A. I. (2025). Automated and remote engineering, maintenance, and repair in Maritime Autonomous Surface Ships (MASS). *Journal of Shipping and Trade*, *10*(1). https://doi.org/10.1186/s41072-025-00210-6

Andrei, N., & Scarlat, C. (2024). Marine applications: The Future of Autonomous Maritime Transportation and Logistics. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.1004275

Corsi, P., Jakovlev, S., Figari, M., & Djačkov, V. (2025). Analysis and Definition of Certification Requirements for Maritime Autonomous Surface Ship Operation. *Journal of Marine Science and Engineering*, *13*(4), 751. https://doi.org/10.3390/jmse13040751

Domenighini, C. (2024). Autonomous inland navigation: a literature review and extracontractual liability issues [Review of *Autonomous inland navigation: a literature review and extracontractual liability issues*]. *Journal of Shipping and Trade*, *9*(1). Springer Nature. https://doi.org/10.1186/s41072-024-00171-2

Durmaz, F. (2024). Cyber Risks on Autonomous Ships and Challenges in the International Law of the Sea. *European Journal of Commercial Contract Law*, *16*(1), 2. https://doi.org/10.7590/187714624x17132716463937

Earthy, J. (2023). Industrial and regulatory progress. In *CRC Press eBooks* (p. 95). Informa. https://doi.org/10.1201/9781003430957-8

Heikkilä, M., Saarni, J., & Saurama, A. (2022). Innovation in Smart Ports: Future Directions of Digitalization in Container Ports. *Journal of Marine Science and Engineering*, *10*(12), 1925. https://doi.org/10.3390/jmse10121925

Kim, T.-E., Perera, L. P., Sollid, M.-P., Batalden, B.-M., & Sydnes, A. K. (2022). Safety challenges related to autonomous ships in mixed navigational environments. *WMU Journal of Maritime Affairs*, *21*(2), 141. https://doi.org/10.1007/s13437-022-00277-z

Lee, Y.-G., Lee, C., Jeon, Y.-H., & Bae, J.-H. (2024). Transformative Impact of the EU AI Act on Maritime Autonomous Surface Ships. *Laws*, *13*(5), 61. https://doi.org/10.3390/laws13050061

Li, M., Zhou, J., Chattopadhyay, S., & Goh, M. (2024). Maritime Cybersecurity: A Comprehensive Review [Review of *Maritime Cybersecurity: A Comprehensive*

Review]. *arXiv (Cornell University)*. Cornell University. https://doi.org/10.48550/arxiv.2409.11417

Llave, R. G., Andrade, F., & Coronil-Huertas, D. J. (2025). Autonomous ships and flag state: challenges and opportunities in international maritime law. *Journal of Transportation Security*, *18*(1). https://doi.org/10.1007/s12198-025-00304-z

Luchenko, D., Georgiievskyi, I., & Bielikova, M. (2023). Challenges and Developments in the Public Administration of Autonomous Shipping. *Lex Portus*, *9*(1). https://doi.org/10.26886/2524-101x.9.1.2023.2

Mohanty, S. K. (2024). Prospects of the Blue Economy in India: Emerging Policy Challenges and the Way Forward. *Current Science*, *126*(2), 161. https://doi.org/10.18520/cs/v126/i2/161-168

Ringbom, H., Røsæg, E., & Solvang, T. (2020). *Autonomous Ships and the Law*. https://doi.org/10.4324/9781003056560

Sani, R. M., & Suhrab, M. I. R. (2025). Operating autonomous tanker vessels in Malaysian territorial waters: Focus on security and emergency response preparedness. *Maritime Technology and Research*, *8*(1), 277455. https://doi.org/10.33175/mtr.2026.277455

Transport 2040: Automation, Technology, Employment - The Future of Work. (2019). https://doi.org/10.21677/itf.20190104

Turner, A., McCombie, S., & Uhlmann, A. J. (2024). Editorial: The impacts of cyber threat in the maritime ecosystem. *Frontiers in Computer Science*, *6*. https://doi.org/10.3389/fcomp.2024.1378160

Watson, R. T., Lind, M., & Haraldson, S. (2017, January 1). Physical and Digital Innovation in Shipping: Seeding, Standardizing, and Sequencing. *Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2017.579