Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
5 (3) 2025, Page: 33659-33668

Revolusi Digital Maritim: Analisis Yuridis Keamanan Siber di Pelabuhan dan Kekuatan Pembuktian Electronic Bill of Lading

Alfian[1], Mariani Loise[2], Andi Suryani[3]
Politeknik Maritim AMI Makassar
Corresponding Author: Alfian, e-mail: Alfianumar54@gmail.com

Published: December, 2025

ABSTRACT

This study analyzes the juridical implications of the maritime digital revolution in Indonesia, focusing on two critical pillars: port cybersecurity and the evidentiary strength of the Electronic Bill of Lading (E-B/L). The purpose is to identify the legal gaps created by the rapid adoption of digital technology, which has outpaced the existing legal framework, resulting in a significant 'regulatory lag' and 'digital trust deficit.' This research applies a normative juridical approach, supported by a statute approach to analyze regulatory conflicts and a comparative approach to benchmark against international instruments like the UNCITRAL Model Law on Electronic Transferable Records (MLETR) and IMO guidelines. Primary legal materials, including the Indonesian Commercial Code (KUHD) and the Law on Electronic Information and Transactions (ITE Law), are analyzed alongside secondary materials from academic journals and policy papers. The findings reveal two major gaps: (1) cybersecurity regulations for ports as Vital Information Infrastructure (IIV) are largely voluntary, lacking a mandatory, enforceable liability framework; and (2) the E-B/L faces significant legal uncertainty, as its function as a 'document of title' conflicts with the paper-based assumptions of the KUHD, despite de jure recognition from the ITE Law. The study concludes that Indonesia requires urgent legal harmonization. Strengthening the digital maritime ecosystem necessitates establishing a mandatory cybersecurity framework for ports and ratifying international instruments to provide full legal certainty for the E-B/L, thereby bridging the gap between technological advancement and legal preparedness.

Keywords: Cyber Security, Electronic Bill of Lading (E-B/L), Maritime Law, Regulatory Lag

© The Author(s). 2025 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Sektor maritim, yang secara historis identik dengan aset fisik seperti baja, kargo, dan dokumen kertas, kini berada di episentrum revolusi digital. Transformasi ini menjanjikan optimalisasi masif dengan smart ports yang terotomatisasi, pelacakan kargo real-time berbasis Internet of Things (IoT), dan efisiensi birokrasi melalui perdagangan paperless (Hawari et al., 2024; Slamet et al., 2024). Namun, efisiensi ini datang dengan paradoks yang fundamental. Semakin terintegrasi dan terkoneksi sebuah sistem logistik secara digital, semakin besar pula kerentanan (vulnerability) yang dihadapinya. Paradoks antara efisiensi dan kerentanan inilah yang menjadi titik sentral permasalahan hukum maritim kontemporer, yang menuntut penyesuaian regulasi secara cepat dan presisi (Baig et al., 2025).

Kerentanan ini bukan lagi ancaman teoretis. Insiden serangan siber NotPetya pada tahun 2017, yang melumpuhkan operasional raksasa pelayaran Maersk di seluruh dunia dan menyebabkan kerugian ditaksir ratusan juta dolar, menjadi bukti nyata (Atmoko et al., 2025). Serangan tersebut mengekspos fakta bahwa pelabuhan modern bukan lagi sekadar infrastruktur fisik, melainkan infrastruktur informasi vital (IIV) yang sangat kompleks. Kelumpuhan operasional akibat serangan

siber di pelabuhan, baik melalui ransomware, malware, atau spionase data manifes kargo, tidak hanya merugikan korporasi, tetapi juga mengancam kedaulatan dan keamanan ekonomi negara ((Ammar & Khan, 2024).

Ancaman siber di pelabuhan menjadi unik dan sangat berbahaya karena adanya konvergensi antara Information Technology (IT) dan Operational Technology (OT) (Progoulakis et al., 2023). Sistem IT mengelola data administrasi (pemesanan, manifes, penagihan), sementara sistem OT mengendalikan operasi fisik (misalnya Automated Guided Vehicles (AGV) dan container cranes). Serangan yang berhasil menembus sistem IT kini berpotensi untuk mengambil alih sistem OT. Ini memperluas spektrum ancaman dari sekadar pencurian data atau kelumpuhan administratif, menjadi sabotase fisik yang dikendalikan dari jarak jauh, yang membahayakan keselamatan jiwa dan aset pelabuhan (Parvez et al., 2023).

Di sisi lain dari revolusi digital, dorongan untuk efisiensi juga berupaya menggantikan dokumen paling fundamental dalam perdagangan maritim: Bill of Lading (B/L) atau Konosemen. Selama ratusan tahun, B/L fisik berfungsi sebagai tiga hal: tanda terima barang, kontrak pengangkutan, dan yang paling krusial, sebagai document of title (dokumen kepemilikan) yang dapat dinegosiasikan (Luling et al., 2022). Transisi ke Electronic Bill of Lading (E-B/L) menawarkan penghematan waktu dan biaya yang luar biasa, memangkas proses administrasi dari hitungan minggu menjadi jam. Namun, ia juga melahirkan ketidakpastian hukum (legal uncertainty) yang mendalam (Galib et al., 2023).

Problematika yuridis E-B/L berpusat pada fungsi B/L sebagai document of title. Hukum dagang konvensional mensyaratkan adanya penguasaan (possession) atas dokumen fisik asli untuk dapat mengklaim barang di pelabuhan tujuan (Kasi, 2021). Pertanyaan hukum fundamentalnya adalah: Bagaimana konsep penguasaan dan keunikan (singularity) sebuah dokumen fisik dapat direplikasi secara digital? Bagaimana sistem hukum memastikan bahwa E-B/L tidak dapat digandakan, dan bagaimana proses pengalihannya (transfer) diakui sah secara hukum, setara dengan penyerahan B/L fisik dari tangan ke tangan?

Untuk mengatasi kebuntuan dalam transisi menuju dokumen elektronik, berbagai upaya telah dilakukan oleh komunitas internasional dan pelaku sektor swasta. Dari sisi regulasi, instrumen hukum seperti Rotterdam Rules dan UNCITRAL Model Law on Electronic Transferable Records (MLETR) dirancang untuk memberikan kepastian hukum terhadap penggunaan dokumen digital dalam perdagangan internasional (Digital Container Shipping Association (DCSA), 2022). Sementara itu, dari sisi teknologi, inovasi seperti Distributed Ledger Technology (Blockchain) serta pengembangan platform digital seperti Bolero, essDOCS, dan TradeLens menawarkan solusi teknis yang mampu menjamin keunikan dan ketertelusuran dokumen elektronik seperti Electronic Bill of Lading (E-B/L). Meski demikian, adopsi global terhadap solusi hukum dan teknologi ini masih berlangsung secara bertahap dan belum seragam di berbagai yurisdiksi.

Indonesia, sebagai negara maritim dengan ambisi menjadi poros maritim dunia, berada tepat di persimpangan dua tantangan digital ini. Di satu sisi, pemerintah gencar mendorong digitalisasi pelabuhan melalui program National Logistics Ecosystem (NLE) untuk menekan biaya logistik. Di sisi lain, kerangka hukum nasional masih berjuang mengejar kecepatan adopsi teknologi. Terjadi regulatory lag (keterlambatan regulasi) yang signifikan. Secara akademis, celah penelitian (research gap) yang ada adalah kecenderungan untuk meneliti kedua isu ini secara terpisah. Padahal, keduanya adalah dua sisi mata uang yang sama: Kepercayaan Digital (Digital Trust). Pelaku usaha membutuhkan kepercayaan bahwa (1) infrastruktur pelabuhan aman dari sabotase siber, dan (2) dokumen digital mereka memiliki kekuatan hukum yang sama dengan kertas.

Oleh karena itu, tulisan ini mendesak untuk melakukan analisis yuridis terhadap dua pilar revolusi digital maritim tersebut secara holistik. Menganalisis kesiapan hukum keamanan siber dan kepastian hukum E-B/L secara bersamaan adalah krusial untuk memetakan kesiapan Indonesia secara utuh. Penelitian ini akan menganalisis kesiapan dan efektivitas kerangka hukum Indonesia dalam mitigasi risiko keamanan siber di pelabuhan, sekaligus menguji kekuatan pembuktian Electronic Bill of Lading (E-B/L) dalam lanskap hukum dagang nasional yang masih bersifat transisional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif (normative juridical), yang berfokus pada analisis norma, prinsip, dan doktrin hukum yang mengatur revolusi digital di sektor maritim (Tamanaha, 1997). Pendekatan ini digunakan untuk mengkaji kesiapan kerangka hukum Indonesia dalam menghadapi dua isu krusial: keamanan siber (cyber security) di pelabuhan dan kekuatan pembuktian Electronic Bill of Lading (E-B/L).

Penelitian ini menggunakan beberapa pendekatan turunan. Pertama, pendekatan perundang-undangan (statute approach), yang digunakan untuk menelaah dan menganalisis secara sistematis berbagai regulasi. Bahan hukum yang dianalisis mencakup, namun tidak terbatas pada, Kitab Undang-Undang Hukum Dagang (KUHD) terkait konosemen, Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Undang-Undang No. 17 Tahun 2008 tentang Pelayaran, serta berbagai Peraturan Presiden dan Peraturan Kepala Badan Siber dan Sandi Negara (BSSN) terkait keamanan siber dan perlindungan infrastruktur informasi vital.

Kedua, pendekatan konseptual (conceptual approach), digunakan untuk memahami dan menafsirkan makna dari konsep-konsep kunci seperti infrastruktur kritis, keamanan siber maritim, dan document of title (dokumen kepemilikan) dalam konteks dokumen elektronik. Pendekatan ini penting untuk menjembatani terminologi teknis digital dengan doktrin hukum maritim yang bersifat tradisional. Ketiga, pendekatan komparatif (comparative approach), digunakan untuk membandingkan kerangka hukum nasional dengan instrumen hukum internasional dan best practices global, seperti UNCITRAL Model Law on Electronic Transferable Records (MLETR), Rotterdam Rules, dan pedoman keamanan siber dari International Maritime Organization (IMO).

Data yang digunakan dalam penelitian ini adalah data sekunder, yang diperoleh seluruhnya melalui studi kepustakaan (library research). Sumber bahan hukum dikategorikan menjadi tiga: (1) Bahan hukum primer, yang terdiri dari seluruh peraturan perundang undangan nasional dan konvensi internasional yang disebutkan di atas; (2) Bahan hukum sekunder , meliputi literatur ilmiah, artikel jurnal hukum dan teknologi, buku teks, laporan penelitian, dan rilis kebijakan dari lembaga terkait (misal: BSSN, Kemenhub, IMO); dan (3) Bahan hukum tersier, seperti kamus hukum, ensiklopedia, dan glosarium teknis untuk memperkuat pemahaman terminologi.

Analisis data dilakukan secara kualitatif-deskriptif. Seluruh data yang terkumpul dianalisis melalui proses interpretasi hukum, utamanya interpretasi sistematis (melihat keterkaitan antar-pasal dan antar-undang-undang) dan interpretasi teleologis (mencari tujuan/maksud pembuat undang-undang). Secara khusus, penelitian ini akan melakukan analisis sinkronisasi vertikal dan horizontal. Sinkronisasi vertikal dilakukan untuk menilai keselarasan antara hukum nasional (misal: KUHD) dengan instrumen internasional (misal: Rotterdam Rules). Sinkronisasi horizontal dilakukan untuk mengidentifikasi potensi konflik norma antar-regulasi nasional yang setara, khususnya antara KUHD yang konvensional dan UU ITE yang modern. Hasil analisis ini akan digunakan untuk merumuskan implikasi hukum dari regulatory lag yang ada dan memberikan rekomendasi kebijakan yang aplikatif.

HASIL DAN PEMBAHASAN

1. Urgensi Keamanan Siber Maritim: Status Pelabuhan sebagai Infrastruktur Informasi Vital (IIV)

Transformasi digital telah secara fundamental mengubah hakikat operasional pelabuhan. Secara tradisional, pelabuhan dipandang sebagai aset fisik kumpulan dermaga, derek (crane), dan gudang. Namun, dalam ekosistem logistik modern, fungsi utamanya kini dijalankan oleh sistem digital yang saling terhubung. Pelabuhan modern beroperasi di atas jaringan kompleks yang mengintegrasikan Terminal Operating Systems (TOS), Port Community Systems (PCS), dan sistem bea cukai, yang semuanya bergantung pada aliran data (Pallis et al., 2024). Ketergantungan inilah yang menggeser status yuridis pelabuhan dari sekadar objek vital menjadi Infrastruktur Informasi Vital (IIV), yakni sistem informasi yang memiliki dampak kritikal terhadap keamanan nasional, ekonomi, dan layanan publik jika mengalami gangguan.

Urgensi perlindungan hukum terhadap pelabuhan sebagai IIV tidak lagi bersifat teoretis, melainkan telah terbukti secara empiris. Serangan ransomware NotPetya pada tahun 2017 terhadap Maersk, salah satu perusahaan pelayaran terbesar di dunia, adalah studi kasus definitif. Serangan siber ini tidak hanya mengenkripsi data IT perusahaan, tetapi juga melumpuhkan operasional terminal pelabuhan mereka di berbagai negara, termasuk APM Terminals di Rotterdam, sebagaimana dijelaskan oleh Greenberg dalam investigasinya terhadap serangan NotPetya (Greenberg, 2019). Insiden ini mengungkap kerentanan masif dalam rantai pasok global dan membuktikan bahwa satu serangan siber mampu menghentikan perdagangan fisik, menyebabkan kerugian ekonomi miliaran dolar dan mengganggu stabilitas logistik global (IMO, 2021).

Ancaman di pelabuhan modern diperparah oleh fenomena konvergensi antara Information Technology (IT) dan Operational Technology (OT). Sistem IT merupakan domain yang mengelola data administratif seperti pemesanan, manifes kargo, dan dokumentasi, sedangkan sistem OT mengendalikan perangkat fisik seperti Automated Guided Vehicles (AGV), derek kontainer, dan sistem navigasi pelabuhan. Keduanya memiliki arsitektur dan risiko keamanan yang berbeda, namun semakin terintegrasi dalam ekosistem pelabuhan digital (*Reference Architecture for Integrating OT and Modern IT*, 2023). Di masa lalu, sistem IT dan OT beroperasi secara terpisah (air-gapped), namun demi efisiensi operasional, keduanya kini terintegrasi. Integrasi ini menciptakan vektor serangan baru yang sangat berbahaya: peretas yang berhasil menembus sistem IT—misalnya melalui teknik phishing—berpotensi mengakses dan menyabotase sistem OT, sehingga ancaman bergeser dari pencurian data menjadi gangguan fisik yang dapat membahayakan keselamatan jiwa dan aset (Dimakopoulou et al., 2024).

Dari perspektif hukum di Indonesia, pengakuan pelabuhan sebagai IIV menempatkannya di bawah yurisdiksi keamanan siber nasional. Regulasi seperti Peraturan Presiden (Perpres) No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Tata Kelola Keamanan Siber menuntut adanya perlindungan terhadap infrastruktur kritis. Namun, tantangan utamanya adalah menerjemahkan mandat perlindungan umum ini ke dalam kerangka hukum yang spesifik, teknis, dan mengikat secara hukum (legally binding) bagi operator pelabuhan di sektor maritim.

2. Analisis Kesiapan Regulasi Keamanan Siber Pelabuhan di Indonesia

Menghadapi ancaman siber yang telah terbukti, kesiapan kerangka hukum Indonesia menjadi pertaruhan utama. Secara de jure, Indonesia telah memiliki beberapa instrumen hukum yang menjadi fondasi keamanan siber, seperti Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang No. 27

Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU ITE, khususnya, memberikan landasan bagi penyelenggara sistem elektronik (PSE) untuk menjamin operasional sistem yang aman. Sementara UU PDP memberikan mandat perlindungan data, yang dalam konteks pelabuhan, mencakup data manifes kargo, data kru, dan data pelanggan (*Https://Peraturan.Bpk.Go.Id/*, 2022).

Lembaga utama yang bertugas mengoordinasikan keamanan siber adalah Badan Siber dan Sandi Negara (BSSN), yang dibentuk untuk melindungi infrastruktur informasi vital (IIV). BSSN telah mengeluarkan berbagai pedoman dan standar, seperti Peraturan BSSN No. 8 Tahun 2020 tentang Sistem Manajemen Pengamanan Informasi Nasional. Masalah yuridis utamanya, bagaimanapun, terletak pada implementasi dan kekuatan mengikat dari regulasi ini di sektor maritim yang sangat spesifik. Hingga saat ini, banyak standar keamanan siber di sektor pelabuhan masih bersifat sukarela atau berupa pedoman umum, bukan standar teknis minimum yang bersifat wajib dan dapat ditegakkan dengan sanksi hukum. Hal ini menciptakan kesenjangan antara kebutuhan operasional dan perlindungan sistem kritis, sebagaimana diakui oleh International Maritime Organization dan belum sepenuhnya diadopsi dalam regulasi nasional (IMO, 2021).

Kesenjangan regulasi dalam sektor maritim digital telah menciptakan ketidakpastian hukum yang signifikan, khususnya terkait alokasi tanggung jawab apabila terjadi insiden siber. Hingga kini, belum terdapat kejelasan normatif mengenai siapa yang harus menanggung kerugian apabila serangan ransomware melumpuhkan terminal peti kemas dan menyebabkan kerugian finansial besar bagi pemilik barang. Pertanyaan hukum yang muncul adalah apakah operator pelabuhan dapat berlindung di balik klausul force majeure, atau justru dapat digugat atas dasar kelalaian karena tidak menerapkan standar keamanan yang memadai. UU ITE belum secara eksplisit mengatur skenario pertanggungjawaban hukum atas kegagalan sistem akibat serangan siber terhadap Infrastruktur Informasi Vital (IIV), sehingga menimbulkan ruang interpretasi yang luas dalam praktik hukum maritim digital (Herera & Sebyar, 2023).

Kedua, masih terjadi regulatory lag (keterlambatan regulatif), di mana regulasi sektoral dalam hal ini Kementerian Perhubungan sebagai otoritas pelabuhan—belum sepenuhnya mengadopsi atau mewajibkan standar teknis keamanan siber yang telah dirumuskan oleh Badan Siber dan Sandi Negara (BSSN). Fokus kebijakan Kementerian Perhubungan masih didominasi oleh aspek keamanan fisik (physical security) dan keselamatan pelayaran (safety), sementara dimensi keamanan siber (cybersecurity) belum terintegrasi secara sistematis sebagai komponen wajib dalam proses perizinan maupun audit operasional pelabuhan. Akibatnya, banyak operator pelabuhan hanya berupaya memenuhi standar minimum untuk kepatuhan administratif, tanpa insentif regulatif yang kuat untuk berinvestasi dalam sistem pertahanan siber yang tangguh dan berkelanjutan (advokatbatam.com, 2025).

3. Problematika Yuridis Electronic Bill of Lading (E-B/L) sebagai Document of Title

Sejalan dengan digitalisasi infrastruktur pelabuhan, revolusi digital juga menuntut de-materialisasi dokumen pengangkutan. Dokumen sentral dalam perdagangan maritim adalah Bill of Lading (B/L) atau Konosemen. Selama ratusan tahun, B/L fisik (kertas) telah menjadi fondasi hukum perdagangan internasional, menjalankan tiga fungsi vital secara simultan: (1) sebagai tanda terima barang oleh pengangkut (receipt of goods); (2) sebagai bukti adanya kontrak pengangkutan laut (contract of carriage); dan (3) sebagai document of title (dokumen kepemilikan) atas barang (Bokareva, 2019). Transisi ke Electronic Bill of Lading (E-B/L) dapat dengan mudah mereplikasi dua fungsi pertama. Namun, fungsi ketigalah yang menciptakan problematika yuridis yang fundamental.

Fungsi B/L sebagai document of title berarti siapa pun yang memegang (possess) dokumen B/L asli yang sah, ia berhak untuk menuntut penyerahan barang di pelabuhan tujuan. Dokumen ini

bersifat negotiable (dapat dipindahtangankan), yang berarti kepemilikan atas barang dapat dialihkan dari satu pihak ke pihak lain misalnya dari eksportir ke bank, lalu ke importir hanya dengan menyerahkan dokumen fisik tersebut (Ayu et al., 2020). Seluruh kerangka hukum ini bertumpu pada prinsip keunikan (singularity) dan penguasaan fisik (physical possession) atas dokumen asli. Hukum mengasumsikan bahwa hanya ada satu dokumen asli yang sah, dan kepemilikan atas barang dibuktikan melalui penguasaan fisik atas dokumen tersebut (Alarie, 2016).

Tantangan utama dalam penerapan Electronic Bill of Lading (E-B/L) adalah mereplikasi prinsip penguasaan fisik dalam lingkungan digital. Berbeda dengan dokumen fisik, file elektronik dapat disalin tanpa batas, tanpa biaya, dan tanpa perbedaan antara salinan dan dokumen asli (Brin et al., 1995). Kondisi ini menimbulkan persoalan hukum yang mendasar mengenai pengakuan E-B/L sebagai document of title yang bersifat unik. Sistem hukum perlu menetapkan bagaimana konsep penguasaan (control atau possession) atas data elektronik dapat disamakan secara fungsional dan legal dengan penguasaan fisik atas dokumen kertas. Selain itu, mekanisme pengalihan (transfer of title) atas E-B/L harus dirancang agar menjamin keamanan, keabsahan hukum, dan kesetaraan dengan proses endosemen pada B/L fisik.

Kerangka hukum dagang Indonesia, yakni Kitab Undang Undang Hukum Dagang (KUHD), yang merupakan warisan kolonial Belanda (Wetboek van Koophandel), secara eksplisit dirancang pada era pra-digital. Ketentuan-ketentuan dalam KUHD yang mengatur konosemen secara implisit mengasumsikan keberadaan dokumen fisik yang diterbitkan dan diserahkan secara manual kepada pihak terkait. Ketiadaan pengakuan eksplisit terhadap dokumen pengangkutan elektronik dalam KUHD menjadi sumber utama ketidakpastian hukum (legal uncertainty) bagi pelaku usaha—seperti bank, perusahaan pelayaran, dan asuransi yang ingin beralih ke sistem tanpa kertas (paperless trade) (Ali Riza, 2016).

4. Konflik Norma Kekuatan Pembuktian E-B/L: Antara KUHD dan UU ITE

Ketidakpastian hukum mengenai E-B/L di Indonesia berpangkal pada konflik norma antara dua rezim hukum yang berbeda. Kitab Undang-Undang Hukum Dagang (KUHD) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). KUHD, sebagai lex generalis (hukum umum) perdagangan yang telah berusia lebih dari satu abad, secara implisit menghendaki adanya dokumen fisik untuk B/L, terutama terkait fungsinya sebagai surat berharga yang dapat dialihkan (negotiable instrument) (Suwadi et al., 2023). KUHD tidak pernah mengantisipasi adanya dokumen elektronik yang memiliki fungsi setara.

Di sisi lain, Indonesia telah memberlakukan UU ITE sebagai respons terhadap era digital. UU ITE secara fundamental mengakui eksistensi dan kekuatan hukum dokumen elektronik. Pasal 5 ayat (1) UU ITE menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Pasal ini secara de jure memberikan pengakuan penuh terhadap dokumen elektronik, termasuk E-B/L, sebagai alat bukti yang setara dengan dokumen fisik di pengadilan. Prinsip ini dikenal sebagai non-diskriminasi terhadap media, di mana hukum tidak boleh mendiskriminasi sebuah dokumen hanya karena bentuknya elektronik (Sugiarto, 2016).

Konflik timbul ketika UU ITE yang bersifat umum (lex generalis untuk transaksi elektronik) berhadapan dengan KUHD yang bersifat spesifik (lex specialis untuk hukum dagang/maritim) (Marpaung & Sazali, 2025). Para pelaku usaha, terutama perbankan (yang memegang B/L sebagai jaminan Letter of Credit) dan asuransi, membutuhkan kepastian mutlak. Mereka menghadapi pertanyaan: Apakah pengadilan akan memenangkan prinsip modern dalam UU ITE, atau akan berpegang teguh pada interpretasi historis KUHD mengenai document of title?. Tanpa adanya

yurisprudensi yang kokoh atau revisi undang-undang yang eksplisit, E-B/L berada dalam wilayah abu-abu secara hukum.

Meskipun platform teknologi seperti Blockchain atau sistem registri terpusat (misal: Bolero) telah menyediakan solusi teknis untuk menjamin keunikan dan penguasaan (control) E-B/L, solusi teknis ini tidak secara otomatis menyelesaikan masalah yuridis (Zachariadis et al., 2019). Hukum harus secara eksplisit mengakui bahwa penguasaan digital (misalnya, memegang private key dalam sistem Blockchain) adalah setara secara hukum dengan penguasaan fisik B/L. Tanpa pengakuan ini, adopsi E-B/L di Indonesia akan terus terhambat, mengurangi daya saing logistik nasional dan menafikan efisiensi yang ditawarkan oleh revolusi digital.

5. Implikasi dan Rekomendasi Harmonisasi Hukum di Era Revolusi Digital Maritim

Temuan dari kedua analisis di atas kesenjangan regulasi keamanan siber pelabuhan dan konflik norma E-B/L menunjukkan satu implikasi utama: Indonesia mengalami kelambanan harmonisasi hukum (legal harmonization lag) dalam merespons revolusi digital maritim. Regulatory lag ini menciptakan defisit kepercayaan digital (digital trust deficit) yang signifikan di kalangan pelaku usaha. Di satu sisi, operator pelabuhan tidak memiliki standar keamanan wajib yang jelas. Di sisi lain, pelaku dagang (bank, asuransi, dan pemilik barang) enggan beralih ke E-B/L karena ketidakpastian hukum (legal uncertainty). Kondisi ini secara langsung menghambat efisiensi logistik nasional dan mendelegitimasi program strategis seperti National Logistics Ecosystem (NLE) yang sangat bergantung pada adopsi teknologi (advokatbatam.com, 2025).

Untuk mengatasi kesenjangan ini, diperlukan dua langkah harmonisasi hukum yang fundamental. Pertama, terkait keamanan siber pelabuhan, pemerintah, melalui koordinasi antara BSSN dan Kementerian Perhubungan, didesak untuk beralih dari pendekatan sukarela (*voluntary*) ke pendekatan wajib (mandatory). Diperlukan pembentukan Kerangka Kerja Keamanan Siber Maritim Nasional yang spesifik, auditabel, dan mengikat secara hukum bagi seluruh operator infrastruktur informasi vital (IIV) di sektor pelabuhan. Regulasi ini harus secara eksplisit mengatur standar teknis minimum serta alokasi pertanggungjawaban hukum (liability framework) jika terjadi insiden akibat kelalaian standar keamanan (*Strategi Keamanan Siber Nasional - Www.Bssn.Go.Id*, 2025).

Kedua, terkait E-B/L, ketidakpastian hukum akibat konflik KUHD dan UU ITE harus segera diakhiri. Solusi jangka pendek dapat berupa penerbitan Peraturan Pemerintah (PP) atau Peraturan Mahkamah Agung (PERMA) yang secara spesifik menegaskan bahwa UU ITE berlaku sebagai lex specialis untuk transaksi elektronik, termasuk E-B/L, sehingga mengesampingkan ketentuan fisik dalam KUHD. Namun, untuk solusi jangka panjang dan fundamental, Indonesia harus segera melakukan ratifikasi instrumen hukum internasional seperti *UNCITRAL* Model Law on Electronic Transferable Records (MLETR) atau Rotterdam Rules. Ratifikasi ini akan memberikan landasan hukum yang kuat dan diakui secara internasional, yang kemudian harus diikuti dengan revisi komprehensif terhadap KUHD agar selaras dengan praktik perdagangan digital abad ke-21 (*Strategi Keamanan Siber Nasional - Www.Bssn.Go.Id*, 2025).

Harmonisasi kedua pilar hukum ini bukanlah sekadar penyesuaian teknis, melainkan sebuah kebutuhan strategis. Tanpa adanya payung hukum yang kokoh untuk keamanan infrastruktur (siber) dan keamanan dokumen (E-B/L), revolusi digital maritim di Indonesia hanya akan berjalan parsial, tidak aman, dan tidak pasti secara hukum.

KESIMPULAN

Konsep Blue Economy merupakan paradigma baru dalam pengelolaan sumber daya laut yang menekankan keseimbangan antara pemanfaatan ekonomi dan pelestarian lingkungan. Dalam konteks

hukum Indonesia, penerapan konsep ini memperkuat amanat konstitusi sebagaimana tertuang dalam Pasal 33 UUD 1945 yang menegaskan bahwa kekayaan alam harus dikelola untuk kemakmuran rakyat secara berkelanjutan. Prinsip ekonomi biru memberikan arah bagi pembentukan sistem hukum kelautan yang adaptif terhadap dinamika global dan berorientasi pada keberlanjutan sumber daya laut nasional.

Dari aspek yuridis, implementasi ekonomi biru menuntut harmonisasi regulasi antara pusat dan daerah, serta keselarasan dengan ketentuan hukum internasional seperti United Nations Convention on the Law of the Sea (UNCLOS) 1982. Ketidaksinkronan regulasi dan lemahnya penegakan hukum di wilayah laut masih menjadi hambatan utama dalam realisasi prinsip ekonomi biru di Zona Ekonomi Eksklusif (ZEE) Indonesia. Oleh sebab itu, penyusunan kerangka hukum yang terpadu dan komprehensif menjadi kebutuhan mendesak untuk menjamin efektivitas kebijakan tersebut.

Selain itu, aspek kelembagaan juga perlu diperkuat melalui pembentukan badan koordinatif yang berperan sebagai pengendali dan pengawas implementasi kebijakan ekonomi biru lintas sektor. Upaya pengawasan dan penegakan hukum perlu ditingkatkan agar prinsip good governance dan marine sustainability dapat terwujud secara nyata. Penegasan peran negara dalam mengontrol aktivitas eksploitasi laut juga harus diimbangi dengan partisipasi masyarakat pesisir sebagai bagian integral dari sistem hukum ekonomi biru.

Secara keseluruhan, penguatan hukum terhadap implementasi Blue Economy di Indonesia harus diarahkan pada integrasi prinsip ekonomi, ekologi, dan sosial dalam satu kesatuan kebijakan nasional. Pemerintah perlu memastikan bahwa setiap regulasi dan kebijakan kelautan mengandung mekanisme perlindungan terhadap lingkungan laut, sekaligus memberikan ruang bagi peningkatan kesejahteraan masyarakat pesisir. Dengan demikian, keseimbangan antara konservasi dan eksploitasi sumber daya laut di ZEE Indonesia dapat tercapai secara berkelanjutan dan berkeadilan.

REFERENSI

advokatbatam.com. (2025, October 29). Serangan Siber pada Sistem Pelabuhan: Perlindungan Hukum Infrastruktur Kemaritiman Indonesia. *Kantor Advokat Di Kota Batam*. https://advokatbatam.com/serangan-siber-sistem-pelabuhan-perlindungan-hukum/

Alarie, B. (2016). The path of the law: Towards legal singularity. *University of Toronto Law Journal*, *66*(4), 443–455. https://doi.org/10.3138/UTLJ.4008

Ali Riza, 13912091. (2016). *PERLINDUNGAN HUKUM BAGI EKSPORTIR DALAM PEMBAYARAN TRANSAKSI PERDAGANGAN INTERNASIONAL MELALUI TELEGRAPHIC TRANSFER* [Thesis, UNIVERSITAS ISLAM INDONESIA]. https://dspace.uii.ac.id/handle/123456789/8558

Ammar, M., & Khan, I. A. (2024). *Cyber Attacks on Maritime Assets and their Impacts on Health and Safety Aboard: A Holistic View* (No. arXiv:2407.08406). arXiv. https://doi.org/10.48550/arXiv.2407.08406

Atmoko, R. A., Arfianto, A. Z., Hasin, M. K., Rahmat, M. B., & Kurniawan, L. A. (2025). Cybersecurity in Digital Maritime Infrastructure. In M. Elsisi, N. Rinanto, & C.-L. Su (Eds.), *Maritime Infrastructure for Energy Management and Emission Reduction Using Digital Transformation* (pp. 127–183). Springer Nature. https://doi.org/10.1007/978-981-96-4438-4_6

Ayu, F. D., Widiati, I. A. P., & Arthanaya, I. W. (2020). Prosedur Penerapan Dokumen Bill Of Lading Dalam Aktivitas Ekspor-Impor. *Jurnal Analogi Hukum*, *2*(1), 22–26. https://doi.org/10.22225/ah.2.1.2020.22-26

Baig, M. Z., Lagdami, K., & Mejia Jr, M. Q. (2025). Safeguarding maritime transport: Disclosing the paradox of safety in domestic ferry operations. *Australian Journal of Maritime & Ocean Affairs*, *17*(3), 496–525. https://doi.org/10.1080/18366503.2024.2354558

Bokareva, O. (2019). *Uniformity of Transport Law through International Regimes*. Edward Elgar Publishing.

Digital Container Shipping Association (DCSA). (2022). *Electronic Bill of Lading standard | DCSA*. DCSA - Digital Container Shipping Association. https://dcsa.org/standards/bill-of-lading

Dimakopoulou, A., Rantos, K., Dimakopoulou, A., & Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6). https://doi.org/10.3390/jmse12060919

Galib, M., Haerani, S., Maming, J., & Munir, A. (2023). *The Effect of Using Social Media Marketing and Market Orientation on the Performance of Culinary MSMEs in Makassar*.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Knopf Doubleday Publishing Group.

Hawari, S. M., Semin, & Adiyono, S. (2024). *Transformasi Digital pada Manajemen Pelabuhan*. Penerbit NEM.

Herera, D. A., & Sebyar, M. H. (2023). *PERLINDUNGAN HUKUM TERHADAP SERANGAN SIBER: TINJAUAN ATAS KEBIJAKAN DAN REGULASI TERBARU*. *1*(5).

Https://peraturan.bpk.go.id/. (2022). Database Peraturan | JDIH BPK. http://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

IMO. (2021). *Maritime cyber risk*. https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx

Kasi, A. (2021). Shipping Documents. In A. Kasi (Ed.), *The Law of Carriage of Goods by Sea* (pp. 21–78). Springer. https://doi.org/10.1007/978-981-33-6793-7_2

Luling, Z., Zhengxiong, J., Lvzhen, R., & Chaoyang, Y. (2022). Reconsideration of the Bill of Lading as a Document of Title. *International Journal of Law and Society*, *5*(1), 66–72. https://doi.org/10.11648/j.ijls.20220501.18

Marpaung, H. W., & Sazali, H. (2025). Multitafsir UU ITE Sebagai Koridor Hukum: Studi Pada Intensitas User Conflicts di Media Sosial. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *6*(2), 1439–1450. https://doi.org/10.63447/jimik.v6i2.1438

Pallis, A. A., Kladaki, P., & Notteboom, T. (2024). Port economics, management and policy studies (2009–2020): A bibliometric analysis. *WMU Journal of Maritime Affairs*, *23*(2), 217–255. https://doi.org/10.1007/s13437-023-00325-2

Parvez, N., Merson, J., & Picu, R. C. (2023). Stiffening mechanisms in stochastic athermal fiber networks. *Physical Review E*, *108*(4), 044502. https://doi.org/10.1103/PhysRevE.108.044502

Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure. In T. M. Johansson, D. Dalaklis, J. E. Fernández, A. Pastra, & M. Lennan (Eds.), *Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance* (pp. 227–248). Springer International Publishing. https://doi.org/10.1007/978-3-031-25296-9_12

Reference Architecture for Integrating OT and Modern IT. (2023). Gartner. https://www.gartner.com/en/documents/4586599

Strategi Keamanan Siber Nasional—Www.bssn.go.id. (2025, June 25). https://www.bssn.go.id/strategi-keamanan-siber-nasional/

Sugiarto, E. (2016). Implikasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Terhadap Informasi Elektronik Dan/Atau Dokumen Elektronik Dan/Atau Hasil Cetaknya Sebagai Alat Bukti Dalam Perkara Perdata. *Rechtidee*, *11*(2), 182–199. https://doi.org/10.21107/ri.v11i2.2171

Slamet, S., & Citta, A. B. (2024). Artificial Intelligence and Global Economic Inequality: Causes, Solutions, and Impacts. In IECON: International Economics and Business Conference (Vol. 2, No. 2, pp. 970-979).

Suwadi, P., Manthovani, R., & Assyifa, A. (2023). Legal Comparison of Electronic Contract in Electronic Commerce Between Indonesia and the United States Based on the United Nations Commission on International Trade Law. *Journal of Law and Sustainable Development*, *11*, e714. https://doi.org/10.55908/sdgs.v11i3.714

Tamanaha, B. Z. (1997). *Realistic Socio-legal Theory: Pragmatism and a Social Theory of Law*. Clarendon Press.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105–117. https://doi.org/10.1016/j.infoandorg.2019.03.001