# إطار المسؤولية المدنية والجنائية عن الحوادث السيبرانية في النقل البحري الدولي

عبد الرحمن الشامي

د.مرهف محمد كله

نجاح محمد ماهر الدقاق

## الملخص

أدى التحول الرقمي في قطاع النقل البحري إلى بروز الحوادث السيبرانية بوصفها مصدرًا حديثًا للمخاطر، يتميز بلا مادية وسيلته ومادية آثاره التشغيلية، وما ينجم عنها من نتائج قد تمسّ سلامة الملاحة، وحماية البيئة البحرية، واستمرارية تنفيذ عقود النقل. وقد أعاد هذا التطور تشكيل الإطار القانوني للمسؤولية، بحيث لم تعد المساءلة تنحصر في الخطأ الملاحي أو العيب الفني، بل امتدت إلى تقييم الحوكمة المؤسسية وإدارة المخاطر الرقمية.

وتبرز في هذا السياق أهمية معيار العناية الواجبة السيبرانية باعتباره التزام عناية يُقاس بمدى معقولية التدابير الوقائية والتنظيمية المتخذة، في ضوء المعايير الدولية والإرشادات القطاعية، دون اشتراط تحقق نتيجة محددة. كما تتسم هذه الحوادث بخصوصية في الإسناد والسببية نظرًا لتداخل العوامل التقنية والبشرية والتنظيمية، وتعدد الفاعلين في سلسلة التشغيل والتوريد والطابع العابر للحدود وصعوبة الإثبات الرقمي.

ومن ثمّ يفرض الحادث السيبراني البحري إعادة تأطير أدوات التحليل التقليدية في المسؤولية المدنية والجنائية، بما يستوعب خصائصه التقنية والتنظيمية ويضبط توزيع المخاطر في بيئة النقل البحري الدولي.

**الكلمات المفتاحية:**

الحوادث السيبرانية البحرية، المسؤولية المدنية، المسؤولية الجنائية، العناية الواجبة السيبرانية، النقل البحري الدولي.

## The Civil and Criminal Liability Framework for Cyber Incidents in International Maritime Transport


### Abstract

The digital transformation of the maritime transport sector has led to the emergence of cyber incidents as a contemporary source of risk, characterized by the immaterial nature of their means and the material impact of their operational consequences. Such incidents may affect navigational safety, marine environmental protection, and the continuity of contractual performance in carriage of goods by sea. This development has reshaped the traditional framework of liability, extending legal scrutiny beyond navigational fault or technical defect to encompass corporate governance structures and cyber risk management practices.

Within this context, the concept of cyber due diligence assumes central importance as an obligation of conduct rather than result, assessed in light of the reasonableness and proportionality of preventive and organizational measures adopted in accordance with international standards and sectoral guidance. Maritime cyber incidents further present distinctive challenges in terms of causation and attribution, given the interplay of technical, human, and organizational factors, the multiplicity of actors within the operational and supply chain structure, their cross-border character, and the evidentiary complexities associated with digital proof.

Accordingly, maritime cyber incidents necessitate a recalibration of conventional approaches to civil and criminal liability in order to accommodate their technical particularities and regulatory implications within the framework of international maritime transport law.

**Keywords**: Maritime Cyber Incidents, Civil Liability, Criminal Liability, Cyber Due Diligence, International Maritime Transport.

**المقدمة:**

يشـــهد النقل البحري في العقود الأخيرة تحولًا عميقًا بفعل التوســـع في اســـتخدام الأنظمة الرقمية وتقنيات الاتصال والتحكم عن بُعد، بما أعاد تشكيل البيئة التشغيلية للسفن والموانئ وسلاسل الإمداد. وقد أفرز هذا التحول نمطًا مستجدًا من المخاطر يتمثل في الحوادث السيبرانية، التي تتسم بكونها أفعالًا غير مادية في وسيلتها، لكنها قادرة على إنتاج آثار مادية جسيمة تمسّ سلامة الملاحة، وحماية البيئة البحرية، وانتظام تنفيذ عقود النقل.

ويثير هذا الواقع إشكالات قانونية مركبة تتصل بتحديد معيار العناية الواجبة في إدارة المخاطر الرقمية، وضبط رابطة السببية في سياق تتداخل فيه العوامل التقنية والبشرية والتنظيمية، فضلًا عن تعقيدات الإسناد وتنازع الاختصاص في الوقائع ذات الطابع العابر للحدود. كما يفرض الطابع التقني للدليل السيبراني تحديات خاصة في مجال الإثبات وحفظ الأدلة وتقييم المسؤولية، سواء في نطاقها المدني المتصل بالتعويض وتوزيع المخاطر، أم في نطاقها الجنائي المرتبط بالتجريم وبحث الخطأ غير العمدي.

وعليه فإن الحادث السيبراني في النقل البحري لم يعد يُنظر إليه باعتباره واقعة تقنية معزولة، بل بوصفه خطرًا تشغيليًا ذا أبعاد قانونية مباشرة، يستدعي إعادة تأطير أدوات التحليل التقليدية في المسؤولية، بما ينسجم مع التحول الرقمي الذي يشهده القطاع البحري على المستوى الدولي.

**إشكالية البحث :**

أفرز التحول الرقمي في قطاع النقل البحري نمطاً مســـتجدًا من المخاطر يتمثل في الحوادث السيبرانية التي تتسم بخصوصية تقنية وتنظيمية تُعيد تشكيل الإطار التقليدي للمسؤولية القانونية. فالفعل الرقمي رغم طبيعته غير المادية، قد يُفضـي إلى آثار مادية جسيمة تمسّ سلامة الملاحة والبيئة البحرية وتنفيذ الالتزامات التعاقدية. ويثير ذلك تساؤلات حول مدى كفاية القواعد التقليدية للمسؤولية القائمة على الخطأ الملاحي أو العيب الفني لاســـتيعاب هذا النمط من المخاطر وحول كيفية ضـــبط معيار العناية، ورابطة السببية وتوزيع الإسناد في بيئة تشغيلية رقمية متداخلة وعابرة للحدود.

وانطلاقًا من ذلك، تتمثل الإشكالية الرئيسة في التساؤل الآتي:

إلى أي مدى يوفر الإطار القانوني للمسؤولية المدنية والجنائية في النقل البحري معالجة كافية لخصوصية الحوادث السيبرانية، من حيث معيار العناية الواجبة وضبط السببية وتحديد الإسناد والاختصاص

**ويتفرع عن هذا التساؤل الأسئلة الآتية:**

- ما المقصود بالحادث السيبراني في النقل البحري، وما خصائصه القانونية المميزة عن الحوادث التقليدية؟
- ما طبيعة الالتزام الملقى على عاتق أطراف النقل البحري في إدارة المخاطر السيبرانية،هل هو التزام عناية أم التزام نتيجة؟
- كيف يمكن معالجة إشكالية السببية المركبة وتوزيع المسؤولية بين الفاعلين المتعددين في سلسلة التشغيل والتوريد؟
- ما دور الامتثال التنظيمي في تقويم الخطأ المدني والإهمال غير العمدي؟
- كيف تؤثر الطبيعة العابرة للحدود للحادث السيبراني في قواعد الاختصاص وبناء الدليل الرقمي.

**أهمية البحث:**

1. بيان الأثر التحولي لإدماج التقنيات الرقمية في البيئة البحرية على بنية المخاطر القانونية، وما يستتبعه ذلك من إعادة تقويم لقواعد المسؤولية في النقل البحري الدولي.
2. تأصيل مفهوم الحادث السيبراني البحري وضبط حدوده المفاهيمية تمييزًا له عن العطل الفني والخطأ الملاحي، بما يعزز الانضباط الاصطلاحي في المعالجة القانونية.
3. معالجة إشكالية السببية المركبة وتحديد ضوابط الإسناد القانوني في سياق تعدد الفاعلين داخل سلسلة التشغيل والتوريد البحري.
4. إيضاح الدور القانوني للامتثال التنظيمي في تقدير الخطأ المدني والإهمال غير العمدي، مع التمييز بين قرينة العناية ومفهوم الحصانة

**أهداف البحث:**

1. تحديد الإطار المفاهيمي للحادث السيبراني في النقل البحري وضبط عناصره القانونية وخصائصه المميزة.
2. بيان الأساس القانوني للمسؤولية المدنية والجنائية الناشئة عن الحوادث السيبرانية في ضوء القواعد البحرية الدولية والتشريعات ذات الصلة.
3. استخلاص معيار العناية الواجبة السيبرانية وتحديد مضمونه في سياق التزامات السلامة وإدارة المخاطر.
4. تحليل إشكالية السببية المركبة وتحديد ضوابط الإسناد بين الفاعلين المتعددين في سلسلة التشغيل والتوريد البحري.
5. تقويم أثر الامتثال التنظيمي في تقدير الخطأ والإهمال، مدنيًا وجنائيًا.

**منهج البحث:**

اعتمد الباحث على المنهج التحليلي التأصيلي في تفسير القواعد القانونية المنظمة للمسؤولية في النقل البحري، مع توظيف المقارنة عند الاقتضاء، والاستعانة بالمعايير التنظيمية والفنية لتحديد مضمون العناية الواجبة وضبط الإسناد في الحوادث السيبرانية البحرية.

**الدراسات السابقة:**

**1ـــ الدراسة الأولى: الرخاوي، محمد كمال عرفة. السيادة البحرية الرقمية: دراسة قانونية حول حماية الموارد البحرية من التلاعب السيبراني وبناء نظام عدالة بحرية رقمي عالمي(2026)**

انطلق الباحث من إشكالية أن سلاسل التوريد البحرية باتت تُدار بأنظمة رقمية معقدة، وأن اختراقها يُحدث آثارًا تشغيلية/مادية مباشرة (تلف/تأخير/سرقة شحنات) مع غموض في توصيف الضرر وتنظيم الحماية القانونية. واتّبع منهجًا تحليليًا–تقويميًا يركّز على إبراز الفجوات المعيارية في حماية "سلاسل التوريد البحرية الرقمية". وخلص إلى أن اختراق أنظمة التتبع/الموانئ الرقمية قد يحوّل أثرًا رقميًا إلى خسائر مادية وتجارية مباشرة، وأن هناك ضعفًا في تصنيف سلاسل التوريد البحرية الرقمية ضمن المصالح المحمية والتعويضات بوضوح. وأوصى باعتبارها جزءًا من "البنية التحتية الحيوية"، ورفع مستوى الحوكمة والتعاون العابر للحدود، ودعم بناء القدرات والتعافي خصوصًا للدول الأقل.

**2ـ الدراسة الثانية: أبو حسين، حنين جميل، الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمّان، 2021، (مايو)**

انطلق الباحث من إشكالية تزايد الاعتماد على خدمات الأمن السيبراني مقابل تشتّت/تفاوت التنظيم القانوني لهذه الخدمات وما يترتب عليه من ضبابية في المسؤولية والالتزامات وحدود الرقابة عند وقوع حوادث سيبرانية مؤثرة على المرافق والقطاعات الحساسة. واتبع منهجًا وصفيًا–مقارنًا يدمج عرض المفاهيم القانونية للأمن السيبراني وخدماته، مع تحليل نماذج تنظيمية وتشريعية ذات صلة. وخلص إلى نتيجتين أساسيتين: (1) أن الطبيعة المتغيرة للتهديدات تجعل الاكتفاء بأحكام عامة غير كافٍ لضبط واجبات مقدمي الخدمة ومعيار العناية المهنية الواجبة، (2) وأن غياب إطار مؤسسي/تنظيمي واضح يضعف فعالية الحوكمة والإشراف والتنسيق عند الاستجابة للحوادث. وأوصى بـ(2–3) توصيات محورية: تبنّي إطار تشريعي أكثر تحديدًا لخدمات الأمن السيبراني يوضح الالتزامات والمعايير والمسؤوليات، وتعزيز البنية المؤسسية المختصة بالتنسيق والإنفاذ، وإدماج متطلبات واضحة في العقود (الإخطار، إدارة الحوادث، حفظ السجلات) بما يرفع قابلية المساءلة والإثبات .

**3. الدراسة الثالثة:**

**Jin, Yongming, et al. "Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations." Frontiers in Marine Science, 29 Aug 2025.**

انطلق الباحث من إشكالية قصور الإطار القانوني الدولي القائم عن استيعاب العمليات السيبرانية البحرية من حيث الاختصاص والإسناد وحدود الرد المشروع وآليات الإنفاذ في بيئة بحرية عابرة للحدود. واتبع منهجًا تحليليًا مع مقاربة حوكمة متعددة المستويات لبحث الفجوات المعيارية على مستوى القانون الدولي والحوكمة القطاعية. وخلص إلى نتيجتين أساسيتين: (1) استمرار الغموض المرتبط بتوزّع الاختصاص داخل المناطق البحرية المختلفة بما يحد من فعالية الإنفاذ، (2) صعوبة حسم توصيف بعض الأفعال السيبرانية البحرية ضمن أطر "استخدام القوة أو العدوان" وما يستتبعه ذلك من تردد في الاستجابات القانونية. وأوصى بتعزيز الحوكمة عبر تطوير أدوات معيارية أوتنظيمية أو تحديثات قانونية تُعالج خصوصية المجال البحري مع رفع التنسيق الدولي والقطاعي لتقليل فجوة الامتثال والإنفاذ .

**4. الدراسة الرابعة:**

**Petta, Michael. "Malware, a Device Under the 1988 SUA Convention." International Law Studies, Vol. 100(1) (2023)**

انطلق الباحث من إشـــكالية مدى قابلية توظيف اتفاقية SUA 1988 كأداة جنائية لملاحقة الهجمات الســيبرانية التي تســتهدف الســفن، عبر اختبار ما إذا كانت البرمجيات الخبيثة يمكن اعتبارها "جهازًا/وسيلة" بالمعنى المقصود في نصوص الاتفاقية. واتبع منهجًا قانونيًا تحليليًا للنصوص التجريمية في الاتفاقية وتفسيرها في ضوء غاية حماية سلامة الملاحة. وخلص إلى نتيجتين أساسيتين: (1) أن اتفاقية SUA يمكن أن تُســتخدم لمعالجة صــور حديثة من الاعتداءات على الملاحة، (2) وأن "malware"يمكن أن يُكيف بوصـــفه "device" بما يفتح باب الملاحقة في حالات معينة تتوافر فيها شروط النص. وأوصى بـ(2–3) توصيات محورية: إدراج مسار ملاحقات SUA ضمن خطط الاستجابة الوطنية للهجمات الســيبرانية البحرية، ومواءمة التشــريعات الوطنية المنفِّذة للاتفاقية بما يســمح بالتطبيق العملي على الوقائع الســيبرانية، وتحســين التنســيق الإجرائي (التحقيق/الإســناد/التعاون) لرفع فعالية الرد الجنائي.

**المطلب الأول: الإطار المفاهيمي للحوادث السيبرانية في النقل البحري:**

أصبح النقل البحري مع تزايد رقمنته مجالًا تُفضي فيه المخاطر السيبرانية إلى آثار مادية مباشرة تمس السلامة والبيئة والالتزامات التعاقدية، مما يحوّل الخطر السيبراني من مسألة تقنية إلى واقعة قانونية تثير إشكالات المسؤولية ومعيار الخطأ والسببية والاختصاص.

وقد كرست المنظمة البحرية الدولية (International Maritime Organization – IMO) هذا التحول بإدماج إدارة المخاطر السيبرانية ضمن نظام إدارة السلامة وفق مدونة الإدارة الآمنة الدولية (International Safety Management Code – ISM Code) مع إلزام الشركات بمعالجتها داخل نظام إدارة السلامة في موعد أقصاه أول تحقق سنوي لوثيقة الامتثال بعد 2021/1/1[1].

[1] IMO, Resolution MSC.428(98) (2017) – Cyber risk management in SMS no later than first annual verification of DOC after 1 January 2021, P. 1. International Safety Management (ISM) Code – objectives and framework of the SMS, P.5.

كما أرست الإرشادات المحدثة لإدارة المخاطر السيبرانية البحرية (MSC-FAL.1/Circ.3/ Rev.3 (2025 – إطارًا وظيفيًا (التعرّف، الحماية، الكشف، الاستجابة، التعافي) يشكّل معيارًا مرجعيًا لتقدير العناية الواجبة[1].

وعززت الإرشادات الصناعية لعام 2024، إلى جانب المتطلبات الموحدة للرابطة الدولية لهيئات التصنيف (International Association of Classification Societies – IACS) ضمن UR E26 و UR E27، هذا الاتجاه عبر ترسيخ مفهوم "المرونة السيبرانية" وتوسيع نطاق الالتزامات ليشمل التصميم والتجهيز والتشغيل، بما يوسّع دائرة الفاعلين المحتملين قانونًا[2].

UR (Unified Requirements) 15^ هي متطلبات فنية موحّدة تصدر عن الرابطة الدولية لهيئات التصنيف (IACS) بهدف توحيد الحد الأدنى من معايير السلامة والتصميم بين هيئات التصنيف الأعضاء. ويتعلق UR E26 بمتطلبات المرونة السيبرانية الخاصة بأنظمة ومعدات السفينة من حيث التصميم والحماية، بينما ينظم UR E27 تكامل الأنظمة الشبكية على متن السفينة واختبار مقاومتها للمخاطر السيبرانية[3].

**الفرع الأول: ماهية الحوادث السيبرانية في النقل البحري وخصائصها القانونية:**

يقصد بالحادث السيبراني في النقل البحري،كل واقعة تنجم عن تدخل رقمي غير مشروع أو عن قصور جسيم في منظومة الحماية والإدارة (اختراق، تعطيل، تلاعب بالبيانات أو الوظائف) يصيب أنظمة السفينة أو ترابطها مع الأنظمة الشاطئية، ويترتب عليه أثر جوهري على التشغيل أو السلامة أو حماية البيئة البحرية أو استمرارية خدمات النقل[4].

ويتميّز هذا الحادث عن العطل التقني المحض الناشئ عن خلل مادي أو قصور في الصيانة دون عنصر رقمي مؤثر، كما يختلف عن الخطأ الملاحي البشري الذي قد يتداخل معه في النتائج، دون أن يكون منشؤه تدخلاً رقمياً. وتبرز قيمة هذا التمييز قانونيًا في تحديد "محل الإسناد"، هل المطلوب

[1] IMO, MSC-FAL.1/Circ.3/Rev.3, Guidelines on maritime cyber risk management (4 April 2025), P. 6+8.

[2] Industry Guidelines, Guidelines on Cyber Security Onboard Ships, Version 5 (14 Nov 2024), P.88. OCIMF, "The Guidelines on Cyber security onboard Ships" (Version 5 notice/page, (14 Nov 2024), P.9. IACS, "UR E26 and E27 Press Release" (application to new ships incl. July 1, 2024 per IACS update), P.12. ClassNK summary page on IACS UR E26/E27 (cyber resilience requirements, scope/purpose), P.11.

[3] IMO, MSC-FAL.1.

[4] Industry Guidelines, Guidelines on Cyber Security, P. 82.

إثباته هو إهمال سيبراني في الحوكمة والحماية، أم خطأ ملاحي تقليدي، أم تداخل سببي مركب يجمع الاثنين[1].

**أولاً: الصور الأكثر اتصالاً بقيام المسؤولية:**

من ناحية المسؤولية تتكرر أربع صور رئيسية تتسم بقدرة عالية على إحداث ضررٍ موجب للتعويض أو المساءلة:

(1) العبث ببيانات أو أنظمة الملاحة بما يفضي إلى جنوح أو اصطدام.

(2) تعطيل أنظمة التحكم والتشغيل (الطاقة، المحركات، إدارة الحمولة) بما يُفضي إلى توقفٍ أو فقدان قدرة مناورة[2].

(3) هجمات الفدية وتعطيل استمرارية الأعمال وما ينجم عنها من تأخير أو إخلال بالالتزامات التعاقدية[3].

(4) امتداد الواقعة إلى منظومات الميناء واللوجستيات الشاطئية بما يضاعف أطراف العلاقة القانونية ويُصعب توزيع المسؤولية[4].

**ثانياً: الخصائص قانونية للحوادث السيبرانية:**

تتسم الحوادث السيبرانية البحرية بخصائص تجعلها أكثر تعقيداً من الحوادث التقليدية في نطاق الإسناد والإثبات:

1. **لا مادية الوسيلة ومادية الأثر:** إذ قد يبقى الفعل الرقمي غير مرئي بينما تُقاس نتيجته بأضرار بحرية مادية وهو ما يدفع عملياً إلى ترجيح قرائن الامتثال والعناية الواجبة بدل الاقتصار على إثبات فعل الاختراق ذاته[5].

---

[1] IMO, MSC-FAL, P. 12.

[2] Industry Guidelines, Guidelines on Cyber Security, P.21.

[3] op. cit, P.18. IMO, MSC-FAL, P.14-15.

هجمات الفدية (Ransomware) هي شكل من البرمجيات الخبيثة يهدف إلى تشفير الملفات أو تعطيل الأنظمة بما يجعل البيانات/الأنظمة غير قابلة للاستخدام، ثم ابتزاز الضحية بطلب فدية مقابل استعادة الوصول أو فكّ التشفير.

Cybersecurity and Infrastructure Security Agency (CISA)، Ransomware 101 مبادرة ضمن #StopRansomware.

[4] Industry Guidelines V5 (acknowledging NIST CSF 2.0 in 2024 update) – as referenced within V5 document, p.18.

[5] IMO, MSC-FAL, p. 22.

2. **الطابع الدولي للواقعة القانونية:** تتسم الحوادث السيبرانية البحرية بتوزع عناصرها بين أكثر من ولاية قانونية، إذ قد يقع الفعل الرقمي في إقليم دولة، بينما تتحقق آثاره في نطاق دولة أخرى أو على متن سفينة ترفع علم دولة مختلفة، الأمر الذي يُفضي إلى تعدد نقاط الإسناد القانوني وتنازع الاختصاص القضائي ويُصعب تحديد القانون الواجب التطبيق وجمع الأدلة في إطار ما تقرره قواعد اختصاص الدول في قانون البحار[1].
3. **تعدد الفاعلين داخل سلسلة التشغيل والتوريد:** إن انتقال متطلبات المرونة السيبرانية إلى مرحلتي التصميم والتجهيز ولاسيما بموجب المتطلبات الموحدة UR E26 وUR E27، يفضي إلى اتساع دائرة الأشخاص ذوي الصلة القانونية، بحيث لا تنحصر المسؤولية في المالك أو المشغل، بل قد تمتد إلى المديرين والموردين بحسب مدى سيطرتهم الفعلية على عناصر الحماية والتحديث والامتثال التقني[2].
4. **صعوبة الإسناد والإثبات الرقمي:** حيث إن تركيز الإرشادات المحدثة لإدارة المخاطر السيبرانية (Rev.3) على الكشف والاستجابة والتعافي يترجم قانونيًا إلى التزامات تنظيمية وإجرائية تحفظ الأدلة وتحد من إمكان إنكار السببية أو طمسها[3].

**خلاصة القول** إن الحادث السيبراني البحري حادث تشغيلي ذو آثار قانونية مباشرة وتقييمه لا يتوقف على ثبوت واقعة الاختراق فحسب، بل يمتد إلى مدى توافر إدارة خطر معقولة قابلة للتحقق يُساءل عنها القائمون على تشغيل السفينة والشركة[4].

**الفرع الثاني: معيار العناية الواجبة السيبرانية وأثر الامتثال التنظيمي:**

يفرض الطابع غير المرئي للحوادث السيبرانية وصعوبة إسنادها تقنيًا انتقال مركز الثقل القانوني من إثبات "واقعة الاختراق" إلى تقويم "سلوك الإدارة والتشغيل" ومدى التزامه بمتطلبات الوقاية والكشف

[1] United Nations Convention on the Law of the Sea (UNCLOS) – general framework relevant to jurisdictional questions, p.33.
[2] IACS, "UR E26 and E27 Press Release", p.33. ClassNK summary page on IACS UR E26/E27, p.34.
[3] IMO, MSC-FAL, p.6+8.
[4] op, cit, p. 5. Industry Guidelines, Guidelines on Cyber Security, p.82.

والاستجابة. ومن ثم يغدو معيار العناية الواجبة السيبرانية أداة حاكمة لضبط المسؤولية، سواء في نطاق المسؤولية المدنية أو عند بحث الخطأ غير العمدي في المجال الجنائي[1].

**أولًا: استخلاص معيار "العناية الواجبة السيبرانية" بوصفه التزام عناية لا التزام نتيجة:**

تُقاس المسؤولية في الحوادث السيبرانية البحرية مدنيًا وجنائياً بمدى احترام القائمين على تشغيل السفينة وإدارتها لواجب العناية الواجبة في إدارة المخاطر (وقايةً وكشفًا واستجابةً وتعافيًا)، ذلك أن الخطر السيبراني لا يمكن ضمان عدم تحققه بصورة مطلقة وإنما يمكن خفض احتمالاته والحدّ من آثاره عبر تدابير معقولة ومتناسبة مع طبيعة التشغيل. ويستند هذا التصور إلى إدماج إدارة المخاطر السيبرانية ضمن نظام إدارة السلامة بموجب مدونة الإدارة الدولية للسلامة (International Safety Management Code – ISM Code)، تنفيذًا لتوجهات المنظمة البحرية الدولية (International Maritime Organization – IMO) التي أوجبت معالجة هذا الخطر ضمن نظام إدارة السلامة في موعد أقصاه أول تحقق سنوي لوثيقة امتثال الشركة بعد 2021/1/1.[2]

وقد بلورت المنظمة البحرية الدولية في الإرشادات المحدثة لإدارة المخاطر السيبرانية البحرية (April 2025) MSC–FAL.1/Circ.3/Rev.3 تصورًا وظيفيًا لمكونات إدارة الخطر (التعرّف، الحماية، الكشف، الاستجابة، التعافي)، بما يحوّل العناية الواجبة من مفهومٍ إنشائي إلى معيار قابل للاختبار القانوني عند تقدير الخطأ أو الإهمال، عبر قياس ما إذا كانت الشركة أو السفينة قد اتخذت ما يُنتظر منها تنظيمًا وتشغيلًا في ضوء مستوى المخاطر[3].

ولغرض إدماج معيار العناية الواجبة السيبرانية في إطار المسؤولية القانونية، يُستخلص مضمونه من منظومة معيارية متدرجة عبر ثلاثة مستويات: المستوى الدولي البحري المتمثل في إدماج إدارة المخاطر السيبرانية ضمن نظام إدارة السلامة والإرشادات الوظيفية الصادرة عن المنظمة البحرية الدولية[4]

---

[1] IMO، القرار MSC.428(98) (2017) ، بشأن إدارة الخطر السيبراني ضمن نظم إدارة السلامة MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 أبريل 2025), p.5+9. IMO, p.1.

[2] Industry, The Guidelines on Cyber Security Onboard Ships – (14 نوفمبر 2024) ، الإصدار الخامس نص الدليل, p.3-4.

[3] IMO، MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 أبريل 2025), p.34.

[4] IMO، MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 أبريل 2025). IMO، القرار MSC.428(98) (2017) بشأن إدارة الخطر السيبراني ضمن نظم إدارة السلامة .

(IMO)؛ والمستوى الصناعي التشغيلي المتمثل في إرشادات الأمن السيبراني على متن السفن (Guidelines on Cyber Security Onboard Ships – Fifth Edition 2024)بوصفها مرجعًا لتحديد السلوك المهني المتوقع[1]، والمستوى البنيوي التصميمي المتمثل في المتطلبات الموحّدة الصادرة عن الاتحاد الدولي لجمعيات التصنيف (International Association of Classification Societies – IACS) ضمن UR E26 و UR E27، التي تمد معيار العناية إلى مرحلتي التصميم والتجهيز وتوسّع نطاق الإسناد وفق حدود السيطرة الفعلية على عناصر الحماية والتحديث[2].

ويُستأنس، عند تقويم معقولية التنظيم الداخلي وإدارة المخاطر بأطر معيارية عامة بوصفها معايير فنية إرشادية وفي مقدمتها NIST Cybersecurity Framework 2.0 (2024) ومعيار ISO/IEC 27001:2022، بما يساعد في تحديد مضمون العناية الواجبة دون أن يرتقي في ذاته إلى مرتبة الإلزام التعاهدي[3].

**وعليه،** لا يُختزل معيار العناية الواجبة السيبرانية في مجرد وجود سياسات مكتوبة أو تدابير شكلية وإنما يقوم على تبني منهج منظم لإدارة الخطر الرقمي يتضمن تحديد الأصول المعلوماتية الحرجة ونقاط الاتصال الحساسة وإجراء تقييم مخاطر مستمر واعتماد ضوابط حماية متناسبة مع طبيعة النشاط البحري وإنشاء قدرات فعالة للكشف والاستجابة والتعافي، مع إدماج هذه العناصر في نظام إدارة السلامة وتوثيقها وتدريب العاملين عليها ومراجعتها دوريًا[4].

ويرى الباحث أن معيار التقييم لا ينصرف إلى قياس النتيجة ذاتها، أي عدم وقوع الحادث، بل إلى فحص معقولية البنية التنظيمية والضبط الإداري المعتمدين قبل وقوعه باعتبار أن الالتزام هنا هو التزام عناية متطور تتحدد ملامحه في ضوء المعايير المهنية السائدة ومتطلبات الامتثال التنظيمي.

**ثانيًا: أثر الامتثال التنظيمي في قيام المسؤولية المدنية والجنائية**

---

[1] Industry, The Guidelines on Cyber Security Onboard Ships،

[2] IACS، بيان صحفي: UR E26 & UR E27 (تطبيق على السفن الجديدة؛ تحديثات المتطلبات).

ClassNK، بيان/ملخص: تطبيق UR E26/E27 على السفن المتعاقد على بنائها ابتداءً من 1 يوليو 2024.

[3] NIST ،The NIST Cybersecurity Framework (CSF) 2.0 (26 فبراير 2024) – CSWP 29, p.4+15. ClassNK summary page on IACS UR E26/E27, p.32.

[4] IMO ،MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (4 أبريل 2025), p.52. Industry, The Guidelines on Cyber Security Onboard Ships, p.77. NIST ،The NIST Cybersecurity Framework (CSF) 2.0 (26 فبراير 2024) – CSWP 29, p.8.

يضـــطلع الامتثال التنظيمي بوظيفة مزدوجة في منازعات الحوادث الســـيبرانية، إذ يُعد من جهة قرينـة على بـذل العنـايـة الواجبـة ومن جهـة أخرى معيـارًا مرجعيًـا يُقـاس عليـه مـدى الانحراف الموجـب للمسؤولية.

مـدنيًـا، يُعتـد بـالامتثـال ولاســـيمـا متى جرى توثيقـه ضـــمن نظـام إدارة الســـلامـة (Safety Management System – SMS) وفق مدونة الإدارة الدولية للســلامة (International Safety Management Code – ISM Code) المعتمدة في إطار المنظمة البحرية الدولية (International Maritime Organization – IMO) بوصـفه مؤشـرًا على اتخاذ تدابير معقولة ومتناسـبة مع طبيعة المخاطر. غير أن هذا الامتثال لا يرتب حصانة تلقائية، إذ تبقى العبرة بمدى ملاءمة التدابير لخصوصية السـفينة ونشـاطها ومسـتوى تعرضـها للخطر. ويُعد عدم الامتثال أو الامتثال الشـكلي غير الفعّال، قرينةً على الإهمال، لاسـيما في ما يتعلق بضـوابط التحكم في الوصـول وإدارة التحديثات وسـياسـات النسـخ الاحتياطي، وخطط الاســـتجابة للحوادث. ويتكرس هذا البعد تعاقديًا من خلال شـــرط الأمن الســـيبراني الصادر عن المجلس البحري الدولي والبلطيقي (Baltic and International Maritime Council – BIMCO Cyber Security Clause 2019) الذي ينظم التزامات الإخطار والتعاون وتوزيع آثار الحادث عند تأثيره في تنفيذ العقد[1].

جنائيًا، تتجلى أهمية الامتثال عند بحث مدى توافر الإهمال الجســـيم أو الإخلال بواجبات الســـلامة، كما يُســـتدل به في تقييم مســـؤولية الشـــخص الاعتباري عبر فحص أنظمة الحوكمة والرقابة الداخلية والتدريب والاستجابة المؤسسية. ويعزز هذا الاتجاه التوسع في الالتزامات القانونية بموجب توجيه الاتحاد الأوروبي(Directive (EU) 2022/2555) NIS2 ، فضـلًا عن تقارير الوكالة الأوروبية للأمن الســـيبراني (European Union Agency for Cybersecurity – ENISA) التي تُبرز تصـــاعد استهداف قطاع النقل، بما يرفع سقف التوقع المعقول ومعيار العناية الواجبة عند تقدير المسؤولية[2].

---

[1] IMO، MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management (أبريل 4 2025). Industry, The Guidelines on Cyber Security Onboard Ships (14 نوفمبر 2024) – نص الدليل، الإصـــدار الخامس. BIMCO، Cyber Security Clause 2019 (تنظيم التزامات الأطراف عند حادث سيبراني مؤثر على الأداء التعاقدي).

[2] NIST، The NIST Cybersecurity Framework (CSF) 2.0 (26 فبراير 2024) – CSWP 29. ISO، ISO/IEC 27001:2022 – متطلبات نظام إدارة أمن المعلومات (ISMS).

يُقصد بـ MSC–FAL.1/Circ.3/Rev.3 التعميم المشترك الصادر عن لجنة السلامة البحرية (MSC)ولجنة التسهيلات (FAL) في المنظمة البحرية الدولية، المتضمن الإرشادات المحدثة لإدارة المخاطر السيبرانية البحرية (أبريل 2025)[1]؛ وبـ UR E26 و UR E27 المتطلبات الموحّدة الصادرة عن الرابطة الدولية لهيئات التصنيف (IACS) بشأن المرونة السيبرانية للسفن الجديدة[2]؛ وبـ NIST CSF 2.0 (2024)إطار إدارة المخاطر السيبرانية الصادر عن المعهد الوطني الأمريكي للمعايير والتقنية[3]؛ وبـ ISO/IEC 27001:2022 المعيار الدولي لنظام إدارة أمن المعلومات.

**المطلب الثاني: المسؤولية المدنية والجنائية عن الحوادث السيبرانية:**

يُفضي إدماج التقنيات الرقمية في تشغيل السفن وإدارة الموانئ إلى تحوّل بنيوي في طبيعة المخاطر البحرية، إذ أصبحت الحوادث السيبرانية قادرة على إحداث نتائج مادية تقليدية كالجنوح أو التصادم أو التعطّل أو التلوث مع ما يصاحبها من تعقيدات إضافية في مجالات الإسناد والسببية والإثبات وتحديد الاختصاص القضائي. وفي هذا السياق لم تعد مساءلة أطراف النقل البحري مقصورة على صور الخطأ الملاحي أو العيب الفني، بل اتسع نطاقها ليشمل التزامات الحوكمة والرقابة الداخلية وإدارة المخاطر الرقمية باعتبارها امتدادًا لواجب السلامة وحسن التنظيم.

ومن ثم ينصرف هذا المطلب إلى تأصيل أطر المسؤولية الناشئة عن الحوادث السيبرانية في النقل البحري الدولي مدنيًا من زاوية التعويض وتوزيع المخاطر، وجنائيًا من حيث نطاق التجريم وقواعد الاختصاص ومتطلبات بناء الدليل.

**الفرع الأول: المسؤولية المدنية عن الحوادث السيبرانية في النقل البحري الدولي**

تتأطر المسؤولية المدنية الناشئة عن الحوادث السيبرانية في النقل البحري ضمن مستويين متكاملين: أولهما إطار عقدي يستند إلى عقد النقل البحري وما يرتبه من التزامات على عاتق الناقل تجاه الشاحن أو المرسل إليه، وثانيهما إطار تقصيري يُفعَّل في مواجهة الغير أو عند تعذر تأسيس الدعوى

---

الاتحاد الأوروبي، – (NIS2) Directive (EU) 2022/2555الإطار التشريعي لإدارة مخاطر الأمن السيبراني والإبلاغ. ENISA صفحة قطاع النقل: مؤشرات/مخرجات تهديدات النقل واتجاهات الاستهداف (تحديثات 2023–2024 ضمن مواد القطاع).

[1] IMO ،MSC-FAL.1/Circ.3/Rev.3.

[2] IACS، بيان صحفي: UR E26 & UR E27 (تطبيق على السفن الجديدة؛ تحديثات المتطلبات). ClassNK ، بيان/ملخص: تطبيق UR E26/E27 2024 يوليو 1 اعتباراً من على السفن المتعاقد على بنائها ابتداءً من 1 يوليو 2024.

[3] NIST ،The NIST Cybersecurity Framework (CSF) 2.0 (فبراير 2024) – CSWP 29.

على رابطة عقدية قائمة. غير أن خصوصية الحادث السيبراني—بما ينطوي عليه من أبعاد تقنية وتنظيمية متشابكة—تقتضي إعادة تأطير أدوات التحليل المدني عبر ثلاث ركائز أساسية: (1) تحديد نطاق ومضمون العناية الواجبة السيبرانية بوصفها **امتدادًا** لالتزام السلامة وحسن إدارة المخاطر، (2) تحليل رابطة السببية المركبة حيث تتداخل العوامل الرقمية والبشرية والفنية، (3) تنظيم توزيع الإسناد والمسؤولية بين الفاعلين المتعددين في سلسلة التشغيل والتوريد بحسب درجة السيطرة والإسهام السببي لكل منهم.

**أولًا: أساس المسؤولية ومعيار الخطأ:**

لا تزال قواعد لاهاي/لاهاي–فيسبي تمثل الإطار التقليدي الحاكم لمسؤولية الناقل في نقل البضائع بحرًا، من خلال تقرير واجب العناية الواجبة في الصلاحية الملاحية مع ما يقابله من دفوع وإعفاءات محددة. وعلى هذا الأساس تُفهم الصلاحية الملاحية—في منطق القواعد—على أنها مجال التزام إيجابي سابق (due diligence) يترتب عليه أثر مباشر في قيام مسؤولية الناقل أو دفعها[1].

إلا أن اتساع الاعتماد على أنظمة الملاحة والاتصال والتحكم يحول دون قصر مفهوم الصلاحية على العناصر المادية وحدها، لأن هذه الأنظمة أضحت جزءًا من البنية التشغيلية للسفينة. ومن ثم يُطرح مفهوم الصلاحية الملاحية السيبرانية باعتباره امتدادًا وظيفيًا للصلاحية التقليدية؛ بحيث تتسع دائرة العناية الواجبة لتشمل وفق طبيعة المخاطر حوكمة الوصول للأنظمة، وإدارة التحديثات (patching)، وتقسيم الشبكات، وخطط النسخ الاحتياطي، وآليات الاستجابة والتعافي، وتدريب الطاقم على إجراءات التشغيل عند العطب الرقمي.

ويتأكد اتجاه تكيف التزامات الناقل مع التحولات التقنية ضمن قواعد روتردام التي تُقرر التزامًا صريحًا على الناقل بممارسة العناية الواجبة قبل وأثناء الرحلة البحرية لضمان صلاحية السفينة (بمفهومها الوظيفي)، بما يدعم إدراج المخاطر الرقمية ضمن معيار العناية الواجبة عند تقدير الخطأ المدني وتحديد رابطة السببية وتوزيع المخاطر بين أطراف العملية النقلية[2].

[1] International Convention for the Unification of Certain Rules of Law relating to Bills of Lading, 1924 (Hague Rules) as amended by the Brussels Protocol 1968 (Hague–Visby Rules)، (Lex Mercatoria/eurorijn), P.6.

[2] UNCITRAL, United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules), 2008, P. 23.

ومن الزاوية التنظيمية الدولية، جرى إدماج إدارة المخاطر السيبرانية ضمن منظومة السلامة عبر قرار لجنة السلامة البحرية في المنظمة البحرية الدولية MSC.428(98)، الذي أكد أن نظام إدارة السلامة المعتمد ينبغي أن يأخذ في الاعتبار إدارة المخاطر السيبرانية وفق أهداف ومتطلبات مدونة ISM[1]. كما طورت المنظمة البحرية الدولية—في النسخة المُحدثة من الإرشادات المشتركة—وظائف تشغيلية قابلة للتحقق والمراجعة، تُختصر في منطق "الدورة الوظيفية" لإدارة الخطر: التعرّف/التحديد، الحماية، الكشف، الاستجابة، التعافي[2].

وعلى مستوى الإرشاد القطاعي الفني، تُفصل "إرشادات الأمن السيبراني على متن السفن (الإصدار 5)" فكرة مواءمة إدارة الخطر السيبراني مع إجراءات الشركة ونظام إدارة السلامة وتعرض بصورة عملية عناصر التقييم والوقاية والاستجابة والتعافي[3]. كما يعضد هذا المنحى اتساقه مع أطر معيارية عامة لإدارة مخاطر الأمن السيبراني— مثل إطار NIST CSF 2.0 الذي يبرز وظائف الحوكمة/التحديد/ الحماية/الكشف/الاستجابة /التعافي بوصفها مخرجات عليا لإدارة المخاطر[4]. ويتكامل ذلك مع معيار ISO/IEC 27001:2022 الذي يضع متطلبات إنشاء وتشغيل وتحسين نظام إدارة أمن المعلومات وإدارة مخاطر المعلومات[5].

وفيما يتعلق بمعيار الخطأ المدني، فإن مستوى العناية يرتفع طردًا مع قابلية توقع الخطر. وقد غدت المخاطر السيبرانية محل تقارير دولية وقطاعية تدرج "تصاعد مخاطر الهجمات السيبرانية" ضمن أبرز مصادر الهشاشة التشغيلية المعاصرة لقطاع النقل البحري واللوجستيات، مع تأكيد الحاجة إلى استراتيجيات أمن سيبراني وأطر تنظيمية مناسبة[6]. كما تؤكد التحليلات القطاعية القانونية/التأمينية الحديثة أن المخاطر السيبرانية أصبحت من أبرز مخاطر الصناعة البحرية وتتطلب مراجعة مستمرة لضوابط الحماية[7]. وتلفت تقارير متخصصة إلى أن أنماطًا مثل برمجيات الفدية والاختراقات قد تستغل

[1] IMO, Resolution MSC, P.1.
[2] IMO, MSC-FAL P.5.
[3] The Guidelines on Cyber Security Onboard Ships, P.31.
[4] NIST, The NIST Cyber security Framework (CSF) 2.0, 26 February 2024 (NIST.CSWP.29), P.8-9.
[5] ISO/IEC, ISO/IEC 27001:2022 "Information Security Management Systems—Requirements"، 2022, P.5.
[6] UNCTAD, Review of Maritime Transport 2025 – Overview, P.8+27.
[7] Hill Dickinson, "Global maritime industry continues to address cyber risk"، 22 September 2025, P.56.

نقاط الضعف التشغيلية وتؤدي إلى اضطراب واسع، مع إبراز إشكالية توزيع الأدوار والمسؤوليات عبر دورة حياة السفينة[1]. وعلى الصعيد العملي، تُظهر وثائق الوقاية من الخسائر أن برمجيات الفدية قد تعطل الوصول إلى الأنظمة/البيانات وتؤدي إلى توقف تشغيلي وأعباء تشغيلية إضافية وقد تمتد آثارها إلى السلامة إذا طالت أنظمة حرجة للملاحة[2].

وبناءً عليه يثبت الخطأ المدني متى ثبت أن الشركة أو السفينة لم تعتمد تدابير معقولة ومتوقعة قطاعيًا لإدارة المخاطر الرقمية، أو اكتفت بإجراءات شكلية لا تتحقق بها فعليًا وظائف الوقاية أو الكشف أو الاستجابة، بحيث يُعزى الحادث أو تفاقم نتائجه إلى قصور تنظيمي أو تشغيلي ذي صلة سببية مباشرة بالضرر.

**ثانيًا: السببية المركبة، وتعدد المسؤولين، وحدود التعويض:**

تتسم الحوادث السيبرانية في المجال البحري بطابع سببي مركّب؛ إذ قد ينهض العامل الرقمي بوظيفة السبب المباشر للضرر، أو سببًا ممكنًا لوقوع خطأ ملاحي، أو سببًا مُفاقِمًا لعطل تقني قائم، أو العامل الذي يحوِّل واقعة محدودة الأثر إلى ضرر جسيم واسع النطاق نتيجة الإخلال بواجبات الاستجابة وإجراءات التعافي. وفي هذا السياق تكتسب وثائق الامتثال التنظيمي وخطط إدارة الحوادث والسجلات والبيانات الرقمية قيمة قرائنية معتبرة في الإثبات.

كما يتسم هذا النوع من الحوادث بتوزع السيطرة الفعلية والقانونية على عناصر الخطر بين عدد من الفاعلين (مالك السفينة، المشغل/الناقل، الربان، مورّدو الأنظمة والبرمجيات، مزودو الاتصالات...)، وقد يمتد نطاق الإسناد إلى مرحلة التصميم والبناء والتجهيز، لاسيما في ضوء متطلبات الاتحاد الدولي لجمعيات التصنيف المتعلقة بمرونة السفن سيبرانيًا (Cyber Resilience)؛ إذ تُقرر متطلبات موحّدة للسفن تشمل—ضمن نطاقها—حماية الشبكات والضوابط الأساسية مثل مكافحة البرمجيات الخبيثة، وضوابط الوصول، والنسخ الاحتياطي والاستعادة والتعافي[3]. كما تُبرز متطلبات الأنظمة والمعدات على متن السفينة ضرورة إدراج خصائص الأمان السيبراني في مرحلة التصميم والتصنيع مع وضع حد أدنى مشترك لمتطلبات المرونة[4].

---

[1] Thetius; CyberOwl; HFW, The Lifecycle Dilemma، 11 March 2025, P.6.
[2] UK P&I Club, Risk Focus: Cyber (Loss Prevention Guidance)، 25 April 2025, P.5.
[3] IACS, Unified Requirement UR E26 "Cyber Resilience of Ships"، April 2022, P.22.
[4] IACS, Unified Requirement UR E27 (Rev.1 Sep 2023) "Cyber resilience of on-board systems and equipment", P.1.

ومتى ثبتت المسؤولية، فإن نطاق التعويض يظل خاضعًا لقيود عملية وقانونية، في مقدمتها حدود تحديد المسؤولية المنصوص عليها في اتفاقية تحديد مسؤولية المطالبات البحرية لعام 1976 (LLMC)، فضلاً عن حدود التغطية التأمينية وشروطها واستثناءاتها في مخاطر الأمن السيبراني[1]. ويُستأنس كذلك بالمواد/الملخصات الرسمية التعريفية الصادرة على صفحات اتفاقيات المنظمة البحرية الدولية بشأن LLMC من حيث وظيفة نظام الحدّ من المسؤولية وبنيته العامة[2].

أما من زاوية التأمين والشروط التعاقدية، فتؤدي صيغ الشروط/الاستثناءات دورًا محوريًا في تنظيم آثار الحادث، ومنها التحديثات الحديثة لبنود سوق لويدز (LMA) ذات الصلة ببنود الأمن السيبراني في التأمين البحري[3]. كما تسهم الدراسات المتخصصة في بيان طبيعة إدراج مخاطر "السيبر" ضمن بنود الاستثناءات/الملحقات (ومنها LMA5402/LMA5403) وتحليل آثارها القانونية في التأمين البحري[4]. ويظهر عمليًا في نشرات أندية الحماية والتعويض تناولٌ مباشر لحدود إعادة التأمين وتغطيات "السايبر الخبيث" وحدودها التجميعية، بما ينعكس على نطاق التعويض أو القدرة على تنفيذه[5]. وإلى جانب ذلك، تلعب الشروط التعاقدية القطاعية دورًا في ضبط التزامات الإخطار والتعاون وإدارة الحادث، وعلى رأسها شرط الأمن السيبراني الصادر عن BIMCO لعام 2019 الذي يهدف إلى توزيع التزامات الأطراف عند وقوع حادث سيبراني يؤثر في تنفيذ العقد[6].

ويُستخلص مما سبق أن بحث المسؤولية المدنية في الحوادث السيبرانية البحرية لا يقف عند حد إثبات "واقعة الاختراق" بذاتها، بل ينصرف إلى معيار قانوني أدق قوامه التحقق من مدى التزام الأطراف بمعيار العناية الواجبة السيبرانية بالمستوى المعقول والمواكب للتطور، وإمكان إقامة رابطة السببية ضمن تسلسل سببي مركّب، مع ضبط نطاق الإسناد وتوزيعه بين أطراف سلسلة التشغيل والتوريد بحسب درجة

[1] United Nations Treaty Series, Convention on Limitation of Liability for Maritime Claims (LLMC), 1976 (UNTS PDF), P.43.

[2] IMO, Convention on Limitation of Liability for Maritime Claims (LLMC) – صفحة الاتفاقية التعريفية, P.99.

[3] Lloyd's Market Association (LMA), "Cyber Clauses update – 9 December 2024" (يتضمن LMA5402/LMA5403), P.4.

[4] National University of Singapore, Faculty of Law – Centre for Maritime Law (CML), Working Paper CML-WPS-2407 (Dec 2024), P.43.

[5] Gard, Member Circular 13/2024: Reinsurance Arrangements for the 2025 Policy Year (Dec 2024), P.2.

[6] BIMCO, Cyber Security Clause 2019.

السيطرة والإسهام. ومع ذلك، يبقى نطاق التعويض قابلاً للتقييد بحدود تحديد المسؤولية وبحدود التغطية التأمينية واستثناءاتها، فضلاً عن الالتزامات الإجرائية التعاقدية وما يرتبط بها من شروط إخطار وتعاون وآثار الإخلال.

**الفرع الثاني: المسؤولية الجنائية عن الحوادث السيبرانية في النقل البحري الدولي:**

تقوم المسؤولية الجنائية في سياق الحوادث السيبرانية البحرية متى ارتقت الواقعة من مجرد إخلال مدني بالتزامات الحيطة إلى مستوى يُشكل تعريضاً فعلياً ومباشراً لسلامة الملاحة أو إحداث ضرر جسيم بالأشخاص أو البيئة البحرية أو الممتلكات، أو إذا اقترنت بسلوك عمدي ذي طابع إجرامي كأفعال التخريب أو الابتزاز أو الولوج غير المشروع إلى الأنظمة المعلوماتية، أو تأسست على صورة من صور الإهمال الجسيم في إدارة المخاطر السيبرانية على مستوى السفينة أو الشركة المشغِّلة. ويغدو التكييف الجنائي أشد وضوحاً عندما يتحول الفعل السيبراني إلى اعتداء على "سلامة الملاحة" باعتبارها محل حماية مستقل، وهو ما ينسجم مع منطق التجريم في اتفاقية قمع الأفعال غير المشروعة الموجهة ضد سلامة الملاحة البحرية (SUA 1988) [1].

وتتسم هذه المسؤولية بخصوصية إجرائية وموضوعية ناجمة عن تعدد جهات الاختصاص المحتملة، بين دولة العلم ودولة الميناء أو الدولة الساحلية ومكان تحقق النتيجة الإجرامية وربما دولة جنسية الفاعل أو موقع البنية التحتية الرقمية المستخدمة، بما يثير إشكاليات تنازع الاختصاص وتحديد الولاية القضائية. ويُسترشد في ضبط هذا التداخل بالقواعد العامة في قانون البحار وبالأسس التي يعرضها الفقه البحري بشأن ولاية دولة العلم وتداخل ولايات الدولة الساحلية/الموانئية بحسب رابطة الاتصال الإقليمية أو رابطة النتيجة[2]. وفي الجرائم التي تمس سلامة الملاحة، تُقر اتفاقية SUA نظام اختصاص موسعًا وتُفعّل عمليًا مبدأ "التسليم أو المحاكمة" بما يدعم منع الإفلات من العقاب[3].

---

[1] الأمم المتحدة، Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), 1988 (PDF). ص 224–225.

[2] الأمم المتحدة، United Nations Convention on the Law of the Sea (UNCLOS), 1982 (PDF/UNTS). ص 434–435. عادل علي المقدادي، القانون البحري، دار الثقافة للنشر والتوزيع، 2011، ص.

[3] الأمم المتحدة، Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), ص226–227.

ويُضاف إلى ذلك الطابع الفني الحساس للدليل الإلكتروني وقابليته السريعة للمحو أو التلاشي، ما يقتضي آليات تحفظ عاجل وحفظًا لسلسلة الحيازة وفق الأصول الإجرائية. وقد تناولت الأدبيات العربية في إثبات جرائم الإنترنت شروط حجية الدليل الرقمي وضرورة التوثيق الفني والإجرائي لسلامة نسبته، وهو ما ينسجم مع مقتضيات التحقيق في البيئة البحرية حيث يتشتت الدليل بين حائزين متعددين[1].

**1. التكييف الجرمي: بين جرائم تقنية وجرائم تمس سلامة الملاحة:**

يخضع السلوك السيبراني، من حيث الأصل، لنطاق التجريم المقرر في التشريعات الوطنية الخاصة بجرائم تقنية المعلومات ولاسيما ما يتصل بصور الولوج غير المشروع، والتدخل غير المأذون في البيانات أو الأنظمة، وإساءة استخدام أدوات الاختراق، والابتزاز الرقمي وسائر الأفعال الماسة بسرية وسلامة وتوافر النظم المعلوماتية. ويمكن الاستئناس في ضبط صور التجريم وأركانها وشروطها بما تضمنته الشروح العربية المقارنة لقانون جرائم تقنية المعلومات[2].

كما يمكن الاستئناس بالإطار الأممي المستحدث لمكافحة الجريمة السيبرانية لعام 2024 باعتباره مرجعية معيارية لتقريب أنماط التجريم وتعزيز آليات التعاون الدولي في هذا المجال[3].

غير أن الطابع البحري للواقعة قد يفضي إلى تكييف جنائي أشد متى بلغ السلوك حد تعريض السفينة أو سلامة الملاحة البحرية لخطر جسيم، كحالات التلاعب بأنظمة الملاحة أو التحكم بما يؤدي إلى الجنوح أو التصادم أو التعطّل الخطير. وعندئذٍ تبرز قابلية إعمال اتفاقية SUA 1988 وبروتوكولاتها بوصفها سندًا تعاهديًا جنائيًا لحماية سلامة الملاحة، من حيث تحديد الأفعال المُجرّمة وقواعد الاختصاص والتعاون القضائي[4].

**2. الاختصاص الجنائي والتعاون عبر الحدود:**

تتوزع عناصر الواقعة السيبرانية البحرية عبر أقاليم قانونية متعددة، وهو ما يثير إشكاليات تنازع الاختصاص وتحديد القانون الواجب التطبيق. ويُسترشد في ضبط هذا التداخل بقواعد الاختصاص في

---

[1] سمير عوض محمود، إثبات جرائم الإنترنت: دراسة مقارنة، دار النهضة العربية، 2020، ص.

[2] محمد علي سويلم، شرح قانون جرائم تقنية المعلومات (القانون رقم 175 لسنة 2018): دراسة مقارنة، دار المطبوعات الجامعية، 2019، ص102.

[3] الأمم المتحدة، United Nations Convention/Framework against Cybercrime (2024)، ص111.

[4] الأمم المتحدة، Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA)، ص224-225.

قانون البحار، ولاسيما ما يتصل بولاية دولة العلم وبحدود تدخل الدولة الساحلية ودولة الميناء بحسب رابطة الاتصال[1]. كما تكتسب الجرائم الماسة بسلامة الملاحة البحرية خصوصية إضافية في ضوء قواعد الاختصاص الموسعة التي تقررها SUA 1988 ومبدأ "التسليم أو المحاكمة" [2].

وعلى الصعيد الإجرائي، تتوقف فعالية الملاحقة الجنائية إلى حدّ كبير على مدى فعالية أدوات التعاون الدولي في مجال جمع الأدلة الإلكترونية وحفظها ونقلها، ولاسيما في ضوء اتفاقية بودابست 2001 التي تقر صور التجريم الأساسية وتضع إطارًا للتعاون الدولي[3]. كما تُقرر الاتفاقية تدبير "الحفظ العاجل للبيانات" كاستجابة لاحتمال زوال الدليل بسرعة[4].

ويأتي البروتوكول الإضافي الثاني لعام 2022 لتعزيز التعاون المباشر وتسريع الحصول على أنواع من البيانات لدى مزودي الخدمات ضمن ضوابط محددة، وهو ما يخدم التحقيقات العابرة للحدود[5]. ويُشكل الإطار الأممي لعام 2024 دعامة معيارية إضافية لتعزيز التنسيق العالمي[6].

**3. الإسناد الجنائي في الحوادث السيبرانية البحرية:**

في الجرائم غير العمدية المتصلة بسلامة التشغيل البحري، لا ينصرف معيار الإسناد الجنائي إلى مجرد إثبات واقعة الاختراق التقني، وإنما يمتد إلى فحص مدى توافر منظومة متكاملة ومعقولة لإدارة المخاطر السيبرانية (وقاية–كشف–استجابة–تعافٍ) قبل الحادث وأثناءه وبعده، لأن "الإهمال الجسيم" غالبًا ما يتأسس على قصور مؤسسي في الحوكمة والرقابة والتدريب وإدارة التحديثات وخطط الاستجابة والتوثيق[7].

---

[1] الأمم المتحدة، United Nations Convention on the Law of the Sea (UNCLOS), 1982 (PDF/UNTS). ص434–435. عادل علي المقدادي، القانون البحري، ص56.

[2] الأمم المتحدة، Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), ص226-227.

[3] مجلس أوروبا، Convention on Cybercrime (Budapest Convention), 2001 (PDF)، ص2–4، +11-12.

[4] المرجع السابق، ص7-8.

[5] مجلس أوروبا، Second Additional Protocol to the Budapest Convention… (2022) (PDF). ص 6–10.

[6] الأمم المتحدة، United Nations Convention/Framework against Cybercrime (2024)، ص76.

[7] المنظمة البحرية الدولية، Resolution MSC.428(98) (2017) (PDF). ص1. المنظمة البحرية الدولية، MSC-FAL.1/Circ.3/Rev.3 (2025) (PDF). ص5–7.

ويظل الربان، في إطار القانون البحري التقليدي ووفق ما يعرضه الفقه البحري، موضع مساءلة جزائية متى أخل بواجبات السلامة والانضباط البحري أو تقاعس عن اتخاذ التدابير اللازمة لمنع الخطر أو الحد من آثاره، مع مراعاة حدود السيطرة الفعلية وإمكان التدخل وقت الواقعة[1].

غير أن خصوصية الحوادث السيبرانية تكشف، في غير قليل من الحالات، عن قصور تنظيمي داخل الشركة المشغِّلة؛ وعندئذٍ يثور مجال مساءلة الشخص الاعتباري متى ثبت إخلال مؤسسي جسيم تتوافر له صلة سببية بوقوع الخطر أو بتفاقم نتائجه. ويُستأنس في بناء شروط الإسناد وأوجهه وحدوده بالأدبيات المتخصصة في المسؤولية الجنائية للشخص المعنوي في الفقه المقارن[2].

كما يعزز التوجيه الأوروبي NIS2 رفع معيار "التوقع المعقول" وواجبات الإدارة العليا في اعتماد تدابير إدارة مخاطر الأمن السيبراني والإشراف عليها، بما يفيد في التحليل المقارن عند تقدير الإهمال المؤسسي[3].

**4- الإثبات الجنائي الرقمي في البيئة البحرية:**

تتسم الأدلة في الحوادث السيبرانية البحرية بطابع تقني سريع الزوال، فضلًا عن تشتتها بين حائزين متعددين، من قبيل السفينة والشركة المشغلة ومزود الاتصالات ومزود الأنظمة وسلطات الميناء. ويترتب على ذلك أن فعالية التحقيق تقتضي اتخاذ تدابير فورية لحفظ السجلات الرقمية وضمان سلامة سلسلة الحيازة بما يكفل حجيتها وسلامة نسبتها؛ وهو ما تؤكد عليه أدبيات إثبات جرائم الإنترنت من جهة، وما تقتضيه أدوات الحفظ العاجل والتعاون الدولي من جهة أخرى[4].

كما يستلزم الأمر تأمين الأدلة الموجودة لدى أطراف ثالثة عبر آليات التعاون القضائي الدولي ولاسيما في الحالات العابرة للحدود، بما يضمن عدم ضياع البيانات أو العبث بها. وتتأكد هذه الضرورة

[1] علاء الدين زكي، المسؤولية الجنائية لربان السفينة في القانون البحري، دار الفكر الجامعي، 2015، ص117–118. عادل علي المقدادي، القانون البحري، ص55.

[2] أحمد محمد قائد مقبل، المسؤولية الجنائية للشخص المعنوي، ص32. عمر سالم، المسؤولية الجنائية للأشخاص المعنوية وفقًا لقانون العقوبات الفرنسي الجديد، دار النهضة العربية، ص63.

[3] الاتحاد الأوروبي، Directive (EU) 2022/2555 (NIS2 Directive) (PDF)، ص46–47.

[4] سمير عوض محمود، إثبات جرائم الإنترنت: دراسة مقارنة، ص79. مجلس أوروبا، Convention on Cybercrime، ص7-8.

في ضوء التعاون الواسع الذي تقرره اتفاقية بودابست في جمع الأدلة الإلكترونية وتبادلها[1]. ويتعزز عمليًا عبر آليات البروتوكول الإضافي الثاني 2022[2].

ويرى الباحث أن خصوصية الحوادث السيبرانية البحرية تفرض إعادة صياغة المنهج التقليدي في التعامل مع الدليل الجنائي، بحيث لا يُنظر إلى الأدلة الرقمية بوصفها مجرد وسائل إثبات تقنية، بل باعتبارها عنصرًا بنيويًا في تحديد المسؤولية وتقدير درجة الامتثال الواجب. فسرعة زوال البيانات وتعدد حائزيها يفرضان معيارًا أعلى من العناية الإجرائية، سواء في الحفظ الفوري أو في توثيق سلسلة الحيازة أو في تفعيل التعاون الدولي. كما يذهب الباحث إلى أن الامتثال المسبق والموثق لأنظمة إدارة المخاطر السيبرانية ينبغي أن يُعامل كقرينة ذات وزن معتبر في نفي الإهمال أو تخفيفه، دون أن يشكل بذاته سببًا للإعفاء، إذ تبقى العبرة بمدى كفاية المنظومة الوقائية وفعاليتها العملية في منع الخطر أو الحد من آثاره.

**نتائج البحث:**

1. تُمثل الحوادث السيبرانية في النقل البحري نمطًا مستحدثاً من المخاطر التشغيلية، يتميز بلا مادية وسيلته ومادية آثاره بما يفرض إعادة ضبط أدوات الإسناد والسببية في إطار المسؤولية القانونية.
2. لا ينحصر تقويم المسؤولية في إثبات واقعة الاختراق، بل يمتد إلى فحص معقولية منظومة إدارة المخاطر السيبرانية ومدى التزامها بمعيار العناية الواجبة.
3. .3يُعد معيار العناية الواجبة السيبرانية التزام عناية لا التزام نتيجة ويُقاس بمدى ملاءمة التدابير التنظيمية والتشغيلية لطبيعة النشاط ومستوى المخاطر المتوقعة.
4. تتسم الحوادث السيبرانية بسببية مركبة تستدعي تحليل تعدد الأسباب وتوزيع الإسناد بين أطراف سلسلة التشغيل والتوريد وفق حدود السيطرة الفعلية والإسهام السببي.
5. يؤدي الامتثال التنظيمي دورًا قرائنيًا في تقدير الخطأ المدني والإهمال غير العمدي، دون أن يرتب حصانة مطلقة من المسؤولية.
6. يثير الطابع العابر للحدود للحادث السيبراني إشكالات تتعلق بتنازع الاختصاص وتحديد القانون الواجب التطبيق، فضلًا عن تعقيدات الإثبات الرقمي.

[1] مجلس أوروبا، Convention on Cybercrime، ص11-12.

[2] مجلس أوروبا، Second Additional Protocol to the Budapest Convention، ص6-10.

7. تقتضـــي مواجهة هذه الحوادث مقاربة قانونية متكاملة تُنسّـــق بين القواعد البحرية التقليدية والمتطلبات التنظيمية المستحدثة في مجال الأمن السيبراني.

**التوصيات:**

1. إدماج إدارة المخاطر السيبرانية إدماجًا فعليًا ضمن نظم إدارة السلامة البحرية، مع اعتماد آلية مراجعة وتحديث دوري في ضوء تطور التهديدات الرقمية.
2. تطوير أطر حوكمة سيبرانية مؤسسية واضحة تحدد المسؤوليات والصلاحيات، وتعزز نظم الرقابة الداخلية والتوثيق.
3. تعزيز برامج التدريب والتأهيل المتخصص للعاملين في الشركات البحرية وعلى متن السفن في مجال الوعي السيبراني وإدارة الحوادث.
4. اعتماد منهج دوري لتقييم المخاطر يتضـــمن اختبارات الجاهزية، وخطط الاســـتجابة، وآليات التعافي واستمرارية الأعمال.
5. توحيد معايير حفظ الأدلة الرقمية وضـــبط ســـلســـلة الحيازة بما يكفل ســـلامتها وحجيتها في المنازعات المدنية والجنائية.
6. تعزيز آليات التعاون القضـــائي الدولي وتبادل المعلومات في الجرائم الســـيبرانية ذات الطابع البحري العابر للحدود.
7. مواءمة التشـــريعات الوطنية مع التطورات التنظيمية الدولية في مجال الأمن الســـيبراني البحري لضمان الاتساق بين المتطلبات التقنية والقواعد القانونية للمسؤولية.

**References:**

- Ādil ʿAlī al-Maqdādī. Al-Qānūn al-Baḥrī [Maritime Law]. Amman, Jordan: Dār al-Thaqāfah lil-Nashr wa-al-Tawzīʿ, 2011

- Aḥmad Muḥammad Qāʾid Muqbil. Al-Masʾūliyyah al-Jināʾiyyah lil-Shakhṣ al-Maʿnawī: Dirāsah Muqāranah [Corporate Criminal Liability: A Comparative Study]. (PhD dissertation) Cairo University, Faculty of Law, 2005. 468 pp.

- Alāʾ al-Dīn Zaki. Al-Masʾūliyyah al-Jināʾiyyah li-Rubbān al-Safīnah fī al-Qānūn al-Baḥrī [The Criminal Liability of the Ship's Master in Maritime Law]. 1st ed. Alexandria: Dār al-Fikr al-Jāmiʿī, 2015.

- BIMCO ،Cyber Security Clause 2019.

- Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), 1988وبروتوكولاتها.

- Convention on Cybercrime (Budapest Convention), 2001.

- Convention on Limitation of Liability for Maritime Claims (LLMC), 1976

- Council of Europe ،Second Additional Protocol to the Budapest Convention (2022).

- European Union ،Directive (EU) 2022/2555 (NIS2) 2022.

- Gard ،Circular 13/2024: Reinsurance Arrangements for the 2025 Policy Year ، 2024.

- Hague Rules 1924 (as amended) + Visby Protocol 1968 (Hague–Visby Rules).

- Hill Dickinson ،"Global maritime industry continues to address cyber risk" ، 222025 /9/.

- IACS ،Unified Requirements: UR E27 ،Cyber Resilience – On-board Systems / Network Integration.

- IMO) ،MSC-FAL.1/Circ.3/Rev.3 ،Guidelines on Maritime Cyber Risk Management, 4-4-2025.

- International Association of Classification Societies (IACS) ،Unified Requirements: UR E26 ،Cyber Resilience of Ships, 4-2022.

- International Maritime Organization (IMO) ،Resolution MSC.428(98) ،Maritime Cyber Risk Management in Safety Management Systems, 16, 2017.

- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) ،ISO/IEC 27001:2022.

- Jin et al., "Navigating the Digital Seas: Legal Challenges …," Frontiers in Marine Science, 2025.

- Lagouvardou, Maritime Cyber Security: Concepts, Problems and Models, MSc Thesis, 2018.

- Lloyd's Market Association (LMA) ،Cyber Clauses Update (LMA5402/LMA5403) ،9 2024.

- Marchiafava, "Cybercrime and Cybersecurity in Shipping: A Legal …," 2022.

- Mhatre & Mhatre, "Cybersecurity in Maritime Law: Legal Liability for Cyber-Attacks on Ships and Ports," 2025.

- Muḥammad ʿAlī Suwaylim. Sharḥ Qānūn Jarāʾim Taqniyyat al-Maʿlūmāt (al-Qānūn Raqm 175 li-Sanat 2018): Dirāsah Muqāranah [Commentary on the Information Technology Crimes Law (Law No. 175 of 2018): A Comparative Study]. Alexandria, Egypt: Dār al-Maṭbūʿāt al-Jāmiʿiyyah, 2019.

- National Institute of Standards and Technology (NIST) ،Cybersecurity Framework (CSF) 2.0 ،26 2024.

- Park, Cybersecurity Risk Assessment in the Maritime Industry, PhD Thesis, 2024.

- Petta, M., "Malware, a Device Under the 1988 SUA Convention," International Law Studies (U.S. Naval War College), 2023.

- Samīr ʿAwaḍ Maḥmūd. Ithbāt Jarāʾim al-Internet: Dirāsah Muqāranah [Proof of Internet Crimes: A Comparative Study]. Cairo: Dār al-Nahḍah al-ʿArabiyyah lil-Nashr wa-al-Tawzīʿ, 2020.
- Second Additional Protocol to the Budapest Convention, 2022.
- The Guidelines on Cyber Security Onboard Ships ،Version 5 ،14 2024.
- Thetius; CyberOwl; HFW ،The Lifecycle Dilemma ،11/3/ 2025.
- UK P&I Club ،Loss Prevention Guidance / Cyber. 2025
- Umar Sālim. Al-Masʾūliyyah al-Jināʾiyyah lil-Ashkhāṣ al-Maʿnawiyyah Wifqan li-Qānūn al-ʿUqūbāt al-Faransī al-Jadīd [The Criminal Liability of Legal Persons under the New French Penal Code]. 1st ed. Cairo: Dār al-Nahḍah al-ʿArabiyyah, 1995.
- UNCITRAL, (Rotterdam Rules), 2008.
- UNCTAD ،Review of Maritime Transport 2025.
- United Nations Convention against Cybercrime, adopted 24 December 2024 (UN).
- United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules), 2008.
- United Nations Convention on the Law of the Sea (UNCLOS), 1982.