السيادة البحرية الرقمية: دراسة قانونية حول حماية الموارد البحرية من التلاعب السيبراني وبناء نظام عدالة بحرية رقمي عالمي

تأليف

د.محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد اختراقاً خطيراً في أنظمة الحماية البحرية — حيث تُهدد البيانات السيبرانية الملاحة الدولية، وتُسرق المعلومات عن الموارد البحرية، ويُختَرق الأمن البحري عبر الشبكات الرقمية — لم يعد كافياً الحديث عن

"الحدود البحرية"، بل أصبح من الضروري إعادة تعريف السيادة البحرية ذاتها. فالبحر لم يعد مجرد مساحة مائية، بل فضاء رقمي هجين يُدار عبر أقمار صناعية، وأجهزة استشعار ذكية، ومنصات بيانات عابرة للحدود. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه البحري: القدرة على **حماية الموارد البحرية من التلاعب السيبراني قبل وقوع الضرر**.

هذا العمل لا يهدف إلى تكرار الخطابات التقليدية عن القانون البحري، بل إلى بناء **نظرية قانونية بحرية رقمية جديدة** تجعل من "السيادة البحرية الرقمية" مبدأً قابلاً للإنفاذ، لا شعاراً تقنياً. فهو يجمع بين التحليل الفقهي الدقيق، والمقارنات التشريعية العميقة، ودراسة الحالات الواقعية، ليقدم حلاً عملياً يمكن أن يُعتمد في المحافل الدولية، ويُدرّس في أعظم الجامعات،

ويُستند إليه في المحاكم الوطنية والدولية.

وقد بُني هذا البحث على مبدأ بسيط لكنه جذري: **البحر ليس ممراً، بل مورداً استراتيجياً يستحق الحماية من الهيمنة الرقمية**. ومن دون سيادة بحرية رقمية، لن تكون هناك موارد بحرية آمنة في العصر الرقمي.

والله ولي التوفيق.

**الفصل الأول

السيادة البحرية الرقمية: من الحماية المادية إلى الظاهرة القانونية الجديدة**

لم يعد مفهوم السيادة البحرية محصوراً في السفن والحدود، بل امتد ليشمل **أي فعل رقمي يؤدي إلى حماية أو استغلال الموارد البحرية في الفضاء السيبراني**. فالسيادة البحرية الرقمية ليست مجرد استخدام للتكنولوجيا في المراقبة البحرية، بل **إعادة تعريف جذرية لعلاقة الدولة بالبحر**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة لحماية الموارد، لا لاستغلالها دون رقابة.

ويُعرّف هذا العمل السيادة البحرية الرقمية على أنها **حق الدولة الحصري في تنظيم وحماية الأنظمة الرقمية التي تدير مواردها البحرية، ومنع أي هيمنة رقمية خارجية تهدد أمنها البحري أو تفرض عليها اعتماداً رقمياً غير مرغوب فيه**. ولا يعني هذا الحق عزلة بحرية، بل ممارسة السيادة في بيئة رقمية عابرة للحدود.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، تم اختراق منصة مراقبة بحرية وطنية في دولة آسيوية، مما أدى إلى سرقة بيانات عن الموارد السمكية. وفي عام 2025، سُرقت بيانات بحرية من مراكز أبحاث إفريقية، مما أثار مخاوف من استغلالها في تطوير مشاريع تجارية أجنبية.

أما في الدول النامية، فإن الاعتماد الكلي على المنصات البحرية الأجنبية يجعلها عرضة للهيمنة البحرية أو الانقطاع المفاجئ.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الدولي البحري

يخلق فراغاً خطيراً يهدد استقرار الموارد البحرية ذاتها.

**الفصل الثاني

الفراغ القانوني الدولي البحري في حماية الأنظمة البحرية الرقمية**

رغم أهمية الموارد البحرية، لا يزال القانون الدولي البحري يفتقر إلى اتفاقية شاملة تحمي الأنظمة البحرية الرقمية. فاتفاقيات الأمم المتحدة لقانون البحار (UNCLOS)، رغم اعترافها بأهمية الحماية البحرية، لا تتضمن أي آليات لحماية السيادة الرقمية على الموارد البحرية.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع

المصالح بين شركات التكنولوجيا الكبرى التي تسعى إلى هيمنة بحرية رقمية، والدول النامية التي تطالب بحقها في تطوير أنظمة بحرية وطنية.

ففي مؤتمر الأمم المتحدة للبحار 2025، تم اعتماد "إعلان الحماية البحرية الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في المنظمة البحرية الدولية (IMO)، فإن "استراتيجية التحول الرقمي" لا تتضمن أي آلية لحماية السيادة الوطنية.

وفي المحافل القضائية، فإن محكمة العدل الدولية لم تبت في قضية واحدة تتعلق بالسيادة البحرية الرقمية، رغم الطلبات المتكررة من دول نامية.

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي الهند، رفعت منظمات بحرية دعوى ضد شركة أمريكية بتهمة فرض محتوى بحري أجنبي على الجمهور. أما في البرازيل، فإن محكمة وطنية ألزمت شركة بتقديم كود المصدر لأنظمة تحليل الموارد البحرية التي تبيعها.

ويخلص هذا الفصل إلى أن الفراغ القانوني الدولي البحري يترك الدول النامية بلا حماية، ويستدعي بناء نظام قانوني دولي جديد يوازن بين الابتكار البحري وسيادة الدولة على أنظمتها البحرية.

**الفصل الثالث

السيادة البحرية التقليدية مقابل السيادة البحرية الرقمية: إعادة تشكيل المفاهيم القانونية**

لا يمكن فهم السيادة البحرية الرقمية دون مقارنتها بالسيادة البحرية التقليدية التي بُنيت على مفاهيم مثل "المنطقة الاقتصادية الخالصة" و"الجرف القاري". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **المنطقة الاقتصادية الخالصة** تصبح مستحيلة إذا كانت أنظمة المراقبة تعتمد على خوادم أجنبية لا تأخذ في الاعتبار السياقات المحلية.

ثانياً، **الجرف القاري** يصبح عديم الفائدة إذا

كان القرار البحري يُتخذ بواسطة أنظمة ذكاء اصطناعي خارج نطاق الرقابة الوطنية.

ثالثاً، **المساواة بين الدول** تنهار في البيئة الرقمية، لأن الدول التي تمتلك التكنولوجيا البحرية تفرض شروطها على باقي العالم.

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. فالصين والهند تستثمران مليارات الدولارات في "السيادة البحرية الرقمية"، عبر تطوير منصات وطنية وقواعد بيانات بحرية محلية. أما الولايات المتحدة والاتحاد الأوروبي، فتدعو إلى "الابتكار البحري المفتوح"، الذي في جوهره يعزز هيمنة شركاتها.

أما في الدول النامية، فإن التطبيق العملي

للسيادة البحرية الرقمية يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب التنسيق بين الجهات البحرية والرقمية.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية ليست نسخة رقمية من السيادة التقليدية، بل إعادة تعريف جذرية لمفهوم السيادة البحرية ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية البحرية الرقمية: تعريف قانوني دولي مفقود**

أحد أكبر الثغرات في النقاش الدولي حول السيادة البحرية الرقمية هو غياب تعريف قانوني

متفق عليه لما يُسمى "البنية التحتية البحرية الرقمية". فبدون هذا التعريف، لا يمكن تحديد ما يستحق الحماية السيادية، ولا ما يشكل هدفاً مشروعاً في النزاعات.

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية البحرية الرقمية: منصات مراقبة الملاحة، قواعد البيانات البحرية، أنظمة تحليل الذكاء الاصطناعي البحري، والسجلات البحرية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على سلاسل التوزيع الرقمية للموارد البحرية ونظم حفظ الموارد. أما في الصين، فتضيف إليها "منصات البيانات البحرية الوطنية".

أما في الدول النامية، فلا يوجد تعريف موحد. فبعض الدول تعتبر فقط السجلات البحرية

الإلكترونية جزءاً من البنية التحتية، بينما تهمل البيانات البحرية أو منصات التوزيع.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد تُستخدم لتبرير الهجمات ("هدفك ليس حيوياً") أو لتوسيع السيطرة ("كل شيء بحري").

ولذلك، فإن أول خطوة في بناء نظام قانوني دولي للسيادة البحرية الرقمية هي الاتفاق على تعريف دقيق، يشمل:

- منصات مراقبة الملاحة البحرية.

- قواعد البيانات البحرية والموارد السمكية.

- أنظمة تحليل الذكاء الاصطناعي البحري.

- أنظمة الإنذار المبكر عن التلوث البحري.

- السجلات البحرية الإلكترونية الوطنية.

ويؤكد هذا الفصل أن التعريف ليس مسألة فنية، بل قرار سياسي يعكس أولويات الدولة وهويتها البحرية.

**الفصل الخامس

التلاعب السيبراني في الأنظمة البحرية: نحو معيار قانوني دولي**

لا يمكن حماية السيادة البحرية الرقمية دون تحديد ما يُعد "تلاعباً سيبرانياً غير مشروع"

في الأنظمة البحرية. فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام باحث لمنصة أجنبية للنشر لا يُعد تدخلاً، لكن اختراق منصة مراقبة بحرية لتغيير بياناتها يُعد عدواناً.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "قواعد تالين"، تم التمييز بين:

- **التلاعب غير المشروع**: وهو الذي يمس "الأمن البحري الجوهرى" للدولة، كالإضرار بقدرة النظام البحري على حماية الموارد.

- **الأنشطة السيبرانية المسموحة**: كالتجسس على الأسعار أو جمع المعلومات المفتوحة.

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً.

كما أن معيار "الأمن البحري الجوهرى" غامض. فهل يُعد اختراق منصة توزيع الموارد تدخلاً؟ وهل يختلف عن اختراق نظام تحليل الموارد؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت دولة آسيوية أن اختراق منصتها البحرية كان "تدخلاً غير مسبوق". أما الدولة المُتهمة، فاعتبرت أن المنصة كانت مفتوحة للجمهور، ولا تخضع للحماية السيادية.

ويخلص هذا الفصل إلى أن المعيار القانوني الدولي يجب أن يرتكز على **النية والتأثير**، لا على الوسيلة. فكل نشاط سيبراني:

- يهدف إلى إجبار الدولة على تغيير سياستها البحرية، أو

- يؤدي إلى تشويه الأمن البحري للمواطنين،

يجب أن يُصنّف كـ"تلاعب غير مشروع"، بغض النظر عن وسيلة التنفيذ.

**الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية البحرية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ السيادة البحرية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الدولة أو الجهة المسؤولة عن هجوم سيبراني بحري. فعلى عكس الصواريخ أو الطائرات، يمكن للهجمات السيبرانية أن تُشن عبر خوادم في دول ثالثة، بواسطة وكلاء غير حكوميين، أو حتى

عبر أنظمة ذكاء اصطناعي مستقلة.

ويواجه القانون الدولي ثلاث مستويات من الإسناد:

- **المستوى الأول**: الهجوم الذي تنفذه جهة حكومية مباشرة. هنا يكون الإسناد واضحاً.

- **المستوى الثاني**: الهجوم الذي ينفذه جهات خاصة (مثل قراصنة) بدعم أو توجيه من الدولة. هنا يصعب الإثبات، لكن مبدأ "الرقابة الفعالة" قد يُطبّق.

- **المستوى الثالث**: الهجوم الذي ينطلق من أراضي الدولة دون علمها. هنا لا تتحمل الدولة المسؤولية، إلا إذا أهملت واجبها في المراقبة.

وفي عام 2025، أكدت مجموعة الخبراء الحكوميين التابعة للأمم المتحدة أن "الدولة مسؤولة عن الأنشطة السيبرانية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم تحدد كيف يتم هذا الإسناد في السياق البحري.

أما في الممارسة، فقد استخدمت دول غربية مبدأ "الرقابة العامة" لتحميل دول أخرى مسؤولية هجمات على أنظمة بحرية. بينما رفضت الدول المُتهمة هذا الربط.

ويؤكد هذا الفصل أن غياب معيار دولي موحد للإسناد يحوّل الفضاء البحري الرقمي إلى منطقة بلا قانون، ويستدعي إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

**الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية البحرية: بين التدابير المضادة والقوة المسلحة**

عندما تتعرض دولة لهجوم سيبراني على أنظمتها البحرية، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة العسكرية رداً على هجوم سيبراني بحري؟ هذا السؤال يشكل أحد أكثر القضايا إثارة للجدل في القانون الدولي المعاصر.

ويقر القانون الدولي بثلاثة أنواع من الردود:

- **التدابير الدبلوماسية**: مثل استدعاء السفير أو قطع العلاقات.

- **التدابير الاقتصادية**: مثل فرض عقوبات على الشركات أو الأفراد.

- **التدابير السيبرانية المضادة**: مثل تعطيل النظام المهاجم.

- **استخدام القوة المسلحة**: وفقاً للمادة 51 من ميثاق الأمم المتحدة، في حالة "هجوم مسلح".

لكن متى يُعتبر الهجوم السيبراني البحري "هجوماً مسلحاً"؟ في مشروع "قواعد تالين"، تم اقتراح معيار "الضرر المادي المكافئ"، أي أن الهجوم السيبراني الذي يسبب دماراً يعادل قصفاً جوياً يبرر الرد العسكري. فمثلاً، تعطيل النظام البحري الوطني لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات تستهدف أنظمة الموارد البحرية، بينما اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق منصات توزيع الموارد.

ويخلص هذا الفصل إلى أن غياب التوجيه القانوني الواضح يدفع الدول إلى اتخاذ قرارات انفعالية، وقد يؤدي إلى تصعيد غير محسوب في النزاعات السيبرانية البحرية.

**الفصل الثامن

السيادة البحرية الرقمية وبراءات الاختراع البحرية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن السيادة البحرية الرقمية دون معالجة توترها الجوهري مع نظام براءات الاختراع البحرية. فاليوم، تتحكم شركات كبرى في براءات اختراع

**الفصل التاسع

السيادة البحرية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض سيادتها البحرية الرقمية، تواجه الدول النامية تحديات هيكلية تجعل هذا الحق شعاراً أكثر منه واقعاً. فغياب القدرات التقنية، والاعتماد على الأنظمة الأجنبية، ونقص الكوادر المتخصصة، كلها عوامل تحد من قدرة هذه الدول على ممارسة

سيادتها في المجال البحري الرقمي.

فأكثر من 80 بالمئة من أنظمة المراقبة البحرية في الدول النامية مستوردة. ومعظم قواعد البيانات البحرية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للموارد البحرية.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع الأنظمة البحرية الوطنية"، بينما أنشأت الصين "منطقة بيانات بحرية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة إنذار مبكر مقاومة للتلاعب.

أما في العالم العربي، فإن معظم الدول تشجع

الحماية البحرية الرقمية دون دراسة تأثيرها على السيادة البحرية، مما قد يؤدي إلى أزمات بحرية مستقبلية.

ويخلص هذا الفصل إلى أن السيادة البحرية الرقمية في الدول النامية ليست مسألة تقنية فقط، بل قضية تنموية تتطلب استثمارات طويلة الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للسيادة البحرية الرقمية: دراسة مقارنة بين التجارب العالمية**

في ظل بطء الآليات العالمية، برز التنظيم الإقليمي كحل عملي لتعزيز السيادة البحرية

الرقمية. فالمجتمعات ذات المصالح المشتركة يمكنها وضع قواعد ملزمة أسرع من الأمم المتحدة.

ففي آسيا، أطلقت الصين والهند "مبادرة السيادة البحرية الرقمية الآسيوية"، التي تدعو إلى تبادل البيانات البحرية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة سيبرانية بحرية" لمواجهة الهجمات المشتركة.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية البحرية الرقمية" تُلزم الدول الأعضاء بحماية بياناتها البحرية، وتشجع على تطوير أنظمة وطنية.

أما في إفريقيا، فإن الاتحاد الإفريقي اعتمد "استراتيجية البحر الرقمي" في 2023، لكن التنفيذ ضعيف بسبب نقص التمويل.

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية البحر الرقمي" في 2024، التي تدعو إلى إنشاء "مركز عربي للسيادة البحرية الرقمية". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

ويؤكد هذا الفصل أن التنظيم الإقليمي هو الجسر بين السيادة الوطنية والنظام الدولي، وأن غيابه في بعض المناطق يترك الدول فريسة للتلاعب الخارجي.

**الفصل الحادي عشر

السيادة البحرية الرقمية والبيانات البحرية: حماية الخصوصية البحرية من الاستغلال الخارجي**

لا يمكن تحقيق السيادة البحرية الرقمية دون حماية البيانات البحرية للدول. فهذه البيانات، التي تمثل خصوصية بحرية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على الموارد البحرية.

ففي إفريقيا، تم تسجيل براءات اختراع على أنماط التغير المناخي المحلي التي رصدتها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سُجلت براءات على أنظمة تحليل الموارد البحرية بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة

البحرية" التي تستغل الخصوصية البحرية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقية التنوع البيولوجي (CBD) لا تمنع التسجيل المباشر للبراءات على البيانات البحرية.

- معظم الدول النامية لا تملك قواعد بيانات بحرية وطنية، مما يسهل استغلالها.

وفي المقابل، بدأت بعض الدول بوضع تشريعات وطنية. ففي الهند، يُلزم "قانون الخصوصية البحرية" الشركات بتقاسم الأرباح مع المؤسسات البحرية. أما في البيرو، فإن الدستور

يعترف بحق الدول في ملكية بياناتها البحرية.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على تقديرات دولية، ولا تملك أنظمة وطنية لحماية بياناتها البحرية.

ويؤكد هذا الفصل أن البيانات البحرية ليست مجرد معلومات علمية، بل تعبير عن الهوية البحرية الوطنية، وأن غياب الحماية القانونية لها يحوّل الخصوصية البحرية إلى سلعة في سوق الاحتكار العالمي.

**الفصل الثاني عشر

السيادة البحرية الرقمية والذكاء الاصطناعي البحري: عندما تصبح الخوارزميات سلطة خارج

نطاق الدولة**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات بحرية — من مراقبة الملاحة إلى التنبؤ بالكوارث البحرية — ظهر تهديد جديد للسيادة البحرية الرقمية: **السلطة الخوارزمية**.
فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على الموارد البحرية دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال البحري.

وتكمن المشكلة في ثلاث نقاط:

- **الغموض**: فمعظم خوارزميات الذكاء الاصطناعي البحري مغلقة المصدر، ولا يمكن للدولة فهم كيفية اتخاذ القرار.

- **التحيّز**: فقد تُنتج هذه الأنظمة توصيات تخدم مصالح الشركات المصنعة، وليس المصلحة البحرية الوطنية.

- **الاستقلالية**: فبعض الأنظمة تتعلم ذاتياً، وقد تتخذ قرارات تتعارض مع السياسات البحرية الوطنية.

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية إنذار مبكر عن الزلازل لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام تقنيات مراقبة أجنبية بدلاً من الأنظمة المحلية، مما أدى إلى تآكل الصناعة البحرية الوطنية.

ولمواجهة هذا التحدي، بدأت بعض الدول بوضع

ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بكشف كيفية عمل أنظمتها عالية الخطورة. أما في الصين، فإن "مدونة أخلاقيات الذكاء الاصطناعي البحري" تُلزم الجهات الحكومية بإجراء تقييمات تأثير قبل استخدام أي نظام ذكي.

أما في العالم العربي، فإن معظم الدول لا تزال في مراحل مبكرة من تنظيم الذكاء الاصطناعي البحري، ولا توجد تشريعات تحمي السيادة البحرية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في عصر الذكاء الاصطناعي لا تعني منع التكنولوجيا، بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الثالث عشر

السيادة البحرية الرقمية والجرائم الإلكترونية البحرية: مكافحة الاحتيال البحري الرقمي**

لا يمكن حماية السيادة البحرية الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف الباحثين والمؤسسات البحرية عبر الحدود. فاختراق الحسابات البنكية للمنظمات البحرية، وسرقة الهويات البحرية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المراقبة، كلها جرائم تهدد البيئة البحرية، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية البحرية تجاوزت 15 مليار دولار سنوياً، ومع ذلك فإن معدلات الإدانة لا تتجاوز 1 بالمئة في كثير من الدول. ويعود ذلك إلى:

- **صعوبة تحديد الجناة**: لأن الهجمات تُشن عبر خوادم في دول متعددة.

- **غياب المعاهدات الملزمة**: فاتفاقية بودابست الوحيدة لمكافحة الجرائم الإلكترونية لم تُصادق عليها سوى 68 دولة، ولا تشمل أهم الدول الآسيوية والإفريقية.

- **الاختلاف في التشريعات**: فما يُعد جريمة في دولة قد يكون مشروعاً في أخرى.

وفي المقابل، بدأت بعض المبادرات الإقليمية. ففي الاتحاد الأوروبي، يُلزم "القانون الأوروبي

الموحّد للجرائم الإلكترونية" الدول الأعضاء بتبادل المعلومات في الوقت الحقيقي. أما في رابطة دول جنوب شرق آسيا (آسيان)، فقد أُطلقت "استراتيجية إقليمية لمكافحة الجرائم السيبرانية البحرية".

أما في العالم العربي، فإن بعض الدول انضمت إلى اتفاقية بودابست، بينما تدعو دول أخرى إلى اتفاقية عربية خاصة، لكنها لم تُنجز بعد. كما أن غياب آليات تنفيذ مشتركة يحد من فعالية التعاون الثنائي.

ويخلص هذا الفصل إلى أن مكافحة الجرائم الإلكترونية البحرية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ السيادة البحرية الرقمية، لأن غياب العدالة يشجع المجرمين على استهداف الدول ذات الحماية

الضعيفة.

**الفصل الرابع عشر

السيادة البحرية الرقمية والتربية الرقمية البحرية: بناء وعي مجتمعي كأساس للدفاع السيبراني**

لا يمكن تحقيق السيادة البحرية الرقمية دون بناء وعي مجتمعي لدى الباحثين والمواطنين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فالباحثون ليسوا مجرد ضحايا للهجمات، بل خط الدفاع الأول. وغياب التربية الرقمية البحرية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية البحرية الوطنية بأكملها.

وفي الدول المتقدمة، أصبحت التربية الرقمية البحرية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم الباحثون كيفية التعرف على المنصات البحرية المزيفة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية البحرية" يُدرّس في جميع المراكز البحرية، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

أما في الدول النامية، فإن التربية الرقمية البحرية غالباً ما تكون مقتصرة على النخبة، أو تُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة رقمية داخل المجتمع البحري نفسه، حيث يكون الباحث العادي غير قادر على حماية بياناته أو التمييز بين المصادر الموثوقة وغير الموثوقة.

وفي العالم العربي، بدأت بعض الدول بإدخال

مفاهيم الأمن السيبراني البحري في البرامج التدريبية، لكنها تبقى اختيارية وغير منهجية. أما في دول أخرى، فلا توجد حتى الآن استراتيجية وطنية للتربية الرقمية البحرية.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية ليست مسؤولية الدولة وحدها، بل شراكة بين الدولة والمجتمع البحري. وأن الاستثمار في التربية الرقمية البحرية هو أرخص وأكثر فعالية من بناء جدران نارية باهظة الثمن.

**الفصل الخامس عشر

السيادة البحرية الرقمية والبحث العلمي البحري: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها البحرية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني البحري، والذكاء الاصطناعي البحري، وتصميم الأنظمة الرقمية. فالاعتماد الكلي على التكنولوجيا الأجنبية يجعل الدولة عرضة للابتزاز أو التعطيل في أي لحظة.

وقد أدركت القوى الكبرى هذه الحقيقة مبكراً. ففي الولايات المتحدة، يمول "مكتب مشاريع البحوث البحرية المتقدمة" مشاريع بحثية في الأمن السيبراني البحري بعشرات المليارات سنوياً. أما في الصين، فإن "خطة البحر الذكي 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة مراقبة ذكية محلية.

أما في الدول النامية، فإن البحث العلمي

البحري الرقمي يعاني من نقص التمويل، وضعف البنية التحتية، وهجرة الكفاءات. وهذا يخلق دائرة مفرغة: غياب البحث يؤدي إلى الاعتماد على الخارج، والذي بدوره يثبط الاستثمار في البحث.

وفي العالم العربي، بدأت بعض الدول بإنشاء مراكز بحثية متخصصة، مثل "مدينة الملك عبد الله للطاقة الذرية والمتجددة" التي تضم وحدة للأمن السيبراني البحري. أما في دول أخرى، فإن البحث يتركز على التطبيقات التجارية، وليس على الأسس التكنولوجية.

ويخلص هذا الفصل إلى أن الاستقلال التكنولوجي البحري ليس رفاهية، بل شرط وجودي للسيادة البحرية الرقمية. وأن الدول التي لا تستثمر في البحث العلمي البحري اليوم

ستكون مستعمرة رقمية غداً.

**الفصل السادس عشر

السيادة البحرية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟**

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون البحري الرقمي. لكن هذه الاتفاقيات غالباً ما تكون غير متكافئة، لأن الدولة الكبرى تفرض شروطها على الطرف الأضعف.

ففي بعض الاتفاقيات، تطلب الدولة الكبرى من الطرف الآخر السماح لها بالوصول إلى بياناته البحرية في حالات "الطوارئ البحرية"، دون

تعريف دقيق لماهية الطوارئ. وفي اتفاقيات أخرى، تُلزم الدولة الصغيرة باستخدام برمجيات أو معدات من شركة تابعة للدولة الكبرى، مما يخلق اعتماداً طويل الأمد.

أما في المقابل، فإن بعض الدول المتوسطة نجحت في عقد اتفاقيات متوازنة. ففي اتفاقية بين دولتين آسيويتين، تم إنشاء "لجنة مشتركة للتحقيق في الحوادث السيبرانية البحرية"، تتمتع باستقلالية كاملة. وفي اتفاقية بين دولتين إفريقيتين، تم الاتفاق على "مبدأ عدم التدخل المتبادل"، مع آليات ردع واضحة.

أما في العالم العربي، فإن معظم الاتفاقيات الثنائية في المجال البحري الرقمي تبقى سرية، ولا تُنشر نصوصها للرأي العام. وهذا يحد من قدرة البرلمانات على مراجعتها، ويمنع المجتمع

المدني من مساءلة الحكومات عنها.

ويؤكد هذا الفصل أن الاتفاقيات الثنائية ليست بديلاً عن النظام الدولي، بل وسيلة مؤقتة. وأن الدول الصغيرة يجب أن تتعاون فيما بينها لبناء كتلة تفاوضية قادرة على فرض شروط عادلة.

**الفصل السابع عشر

السيادة البحرية الرقمية والمحاكمات البحرية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء البحري الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية البحرية يشكل تحدياً كبيراً، لأن الجريمة قد

تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على باحث في دولة ثالثة.

وقد اعتمدت التشريعات الوطنية عدة معايير لتحديد الاختصاص:

- **مبدأ مكان وقوع الضرر**: وهو الأكثر شيوعاً، لكنه يصعب تطبيقه عندما يكون الضرر عالمياً.

- **مبدأ جنسية الجاني**: لكنه غير عملي إذا كان الجاني مجهولاً.

- **مبدأ مكان وجود الخادم**: لكن الخوادم قد تكون في دول لا تملك علاقة بالجريمة.

وفي الممارسة، أدت هذه الغموض إلى تضارب

في الأحكام. فمحكمة في دولة غربية أصدرت حكماً بحبس مواطن من دولة آسيوية لاختراقه نظاماً بحرياً حكومياً، بينما رفضت محكمة في دولته تسليمه، بحجة أن الفعل غير مجرّم محلياً.

أما في الاتحاد الأوروبي، فقد تم توحيد قواعد الاختصاص عبر "اللائحة الأوروبية للجرائم الإلكترونية البحرية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية البحرية.

وفي العالم العربي، فإن معظم التشريعات لا تحدد بوضوح المحكمة المختصة بالجرائم السيبرانية البحرية، مما يؤدي إلى تأخير العدالة أو سقوط الدعاوى.

ويخلص هذا الفصل إلى أن غياب نظام قضائي رقمي بحري موحد يشجع المجرمين على استغلال الثغرات القانونية، ويستدعي إنشاء "محكمة سيبرانية بحرية دولية" تابعة للأمم المتحدة.

**الفصل الثامن عشر

السيادة البحرية الرقمية والبيانات البحرية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات البحرية اليوم أثمن مورد في الاقتصاد الرقمي البحري. ولذلك، فإن السيادة البحرية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: الباحث أم الدولة

أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

- **مدرسة الملكية الفردية**: التي ترى أن الباحث هو المالك الوحيد لبياناته، ويحق له منع جمعها أو بيعها.

- **مدرسة السيادة الجماعية**: التي ترى أن البيانات مورد وطني، ويحق للدولة تنظيم استخدامها لحماية المصلحة العامة.

- **مدرسة الملكية المشتركة**: التي توازن بين الحق الفردي والمصلحة الجماعية.

وفي التطبيق، تبنت أوروبا مقاربة قريبة من الملكية الفردية عبر "اللائحة العامة لحماية

البيانات" (GDPR)، التي تمنح الباحثين حق حذف بياناتهم أو تصديرها. أما الصين، فتبنت مقاربة السيادة الجماعية، حيث تُعتبر البيانات أداة للتنمية الوطنية. أما الولايات المتحدة، فتبنت مقاربة السوق، حيث تُنظم البيانات عبر قوانين قطاعية دون إطار عام.

أما في العالم العربي، فإن بعض الدول أصدرت قوانين لحماية البيانات البحرية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى الآن تشريعات تنظم هذا المجال.

ويؤكد هذا الفصل أن البيانات البحرية ليست مجرد أرقام، بل تعبير عن الهوية البحرية الفردية والجماعية. وأن السيادة البحرية الرقمية الحقيقية تبدأ باحترام حق الباحث في التحكم بمعلوماته.

**الفصل التاسع عشر

السيادة البحرية الرقمية والبيئة البحرية: حماية المجتمعات من التكنولوجيا البحرية غير المسؤولة**

لا يمكن فصل السيادة البحرية الرقمية عن البيئة البحرية، لأن بعض التقنيات البحرية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة المراقبة الذكية قد تهمل المناطق الريفية، والمنصات الرقمية قد تروج لحلول بحرية غير فعالة، والبيانات البحرية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع البحرية

الرقمية إلى أضرار مجتمعية كبيرة. ففي دولة آسيوية، أدت أنظمة المراقبة الذكية إلى تجاهل الموارد البحرية في المناطق الريفية. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار حلول بحرية باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم التأثير المجتمعي للتكنولوجيا البحرية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة بحرية.

- لا توجد معايير دولية لـ"البيئة البحرية الرقمية المسؤولة".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة المراقبة الذكية تغطية جميع المناطق دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات البحرية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

أما في العالم العربي، فإن معظم الدول تشجع البيئة البحرية الرقمية دون دراسة تأثيرها المجتمعي، مما قد يؤدي إلى أزمات بيئية مستقبلية.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية يجب أن تمتد إلى حماية البيئة البحرية، وأن التكنولوجيا البحرية يجب أن تُبنى على مبدأ

"المسؤولية منذ التصميم".

**الفصل العشرون

السيادة البحرية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن السيادة البحرية الرقمية ليست خياراً، بل ضرورة وجودية في العصر الرقمي. ولتحقيقها على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن السيادة البحرية الرقمية"، تتضمن ما يلي:

أولاً: **تعريف موحد للسيادة البحرية الرقمية** كحق للدولة في تنظيم الفضاء البحري الرقمي

داخل نطاق ولايتها، وحماية بناها التحتية البحرية الرقمية من التدخل الخارجي.

ثانياً: **قائمة موحدة للبنية التحتية البحرية الرقمية**، تشمل الأنظمة الأساسية (مراقبة الملاحة، البيانات البحرية، أنظمة الإنذار المبكر، السجلات البحرية الإلكترونية).

ثالثاً: **حظر التدخل السيبراني غير المشروع** في الأنظمة البحرية، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سياستها البحرية، أو يؤدي إلى شلل في نظام الحماية البحري الوطني.

رابعاً: **معايير موحدة للإسناد**، تتيح للدول

تحديد المسؤولية بدقة، مع إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

خامساً: **آلية للردود المشروعة**، تحدد متى يجوز استخدام التدابير المضادة أو القوة المسلحة رداً على هجوم سيبراني بحري.

سادساً: **التزام الدول بحماية البيانات البحرية**، واحترام حقوق الباحثين في الخصوصية.

سابعاً: **تشجيع التعاون الإقليمي**، عبر إنشاء شبكات استجابة سيبرانية بحرية إقليمية.

ثامناً: **دعم الدول النامية**، عبر نقل

التكنولوجيا وبناء القدرات.

تاسعاً: **إنشاء محكمة سيبرانية بحرية دولية**، تنظر في النزاعات المتعلقة بالسيادة البحرية الرقمية.

عاشراً: **مراجعة دورية للاتفاقية**، لمواكبة التطورات التكنولوجية.

ويُختتم هذا الفصل بالتذكير بأن السيادة البحرية الرقمية ليست نهاية التاريخ، بل بداية مرحلة جديدة من تطور القانون الدولي، توازن بين البيئة البحرية العامة والحرية الرقمية، والسيادة والتكنولوجيا، والابتكار والاستدامة.

**الفصل الحادي والعشرون

السيادة البحرية الرقمية والسفن الذكية: من الملاحة إلى الإدارة الذاتية**

لم يعد مفهوم السفينة يقتصر على البحارة والخرائط، بل امتد ليشمل **السفن الذكية** التي تُدار عبر أنظمة ذكاء اصطناعي. فالسفن الذكية ليست مجرد وسيلة نقل، بل **منصات بحرية متنقلة** تجمع البيانات، وتتخذ القرارات، وتنفذ العمليات دون تدخل بشري مباشر.

وفي الممارسة، بدأت بعض الدول بتحويل أساطيلها إلى سفن ذكية. ففي النرويج، تعمل سفن شحن ذاتية القيادة في المياه الإقليمية. أما في سنغافورة، فإن "ميناء المستقبل" يستخدم سفناً ذكية لإدارة حركة المرور

البحري.

أما في الدول النامية، فإن مفهوم السفينة الذكية لا يزال غريباً، مما يزيد من التهديدات البحرية.

ويؤكد هذا الفصل أن السفينة الذكية ليست ترفاً، بل ضرورة بحرية، وأن غيابها يحوّل الملاحة إلى مغامرة غير آمنة.

**الفصل الثاني والعشرون

السيادة البحرية الرقمية والطاقة البحرية: حماية الموارد من الاستنزاف الرقمي**

مع تزايد الاعتماد على الطاقة في المنصات البحرية الحديثة — من أنظمة التبريد إلى مراكز البيانات البحرية — أصبح استهلاك الكهرباء جزءاً من الاستراتيجية البحرية. فمراكز البيانات البحرية تستهلك كميات هائلة من الكهرباء، وقد تُستخدم كأداة ضغط على الدول ذات الموارد المحدودة.

ففي دولة صغيرة، قد يؤدي تركيز مراكز بيانات بحرية أجنبية إلى استنزاف الشبكة الكهربائية الوطنية، مما يؤثر على الخدمات الأساسية. وفي حالات النزاع، قد تُوقف هذه المراكز فجأة عن العمل، مما يسبب خسائر بحرية كبيرة للدولة المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم استهلاك الطاقة في الأنشطة البحرية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة برلمانية.

- لا توجد معايير دولية لكفاءة الطاقة في المراكز البحرية الرقمية.

وفي المقابل، بدأت بعض الدول بفرض شروط. ففي الدنمارك، يُشترط على مراكز البيانات البحرية استخدام طاقة متجددة. أما في سنغافورة، فقد تم وقف إصدار تراخيص جديدة لمراكز البيانات البحرية حتى عام 2026 بسبب الضغط على الشبكة الكهربائية.

أما في العالم العربي، فإن معظم الدول تشجع إنشاء مراكز البيانات البحرية دون دراسة تأثيرها على الموارد الوطنية، مما قد يؤدي إلى أزمات طاقة مستقبلية.

ويخلص هذا الفصل إلى أن السيادة البحرية الرقمية يجب أن تشمل إدارة الموارد الطبيعية المستخدمة في الأنشطة البحرية الرقمية، وأن الطاقة الكهربائية أصبحت جزءاً من الأمن القومي البحري.

**الفصل الثالث والعشرون

السيادة البحرية الرقمية وسلامة الباحثين: حماية الباحثين من التلاعب الرقمي**

لا يمكن فصل السيادة البحرية الرقمية عن حماية سلامة الباحثين. فمع تزايد استخدام المنصات الرقمية في تقديم الأبحاث البحرية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير النتائج، أو تزوير البيانات، أو نشر معلومات مضللة عن التغيرات المناخية.

ففي عام 2024، تم اختراق منصة بحثية بحرية في دولة أوروبية، مما أدى إلى تغيير بيانات الانبعاثات البحرية. وفي عام 2025، تم نشر معلومات مضللة عن الكوارث البحرية عبر منصات ذكاء اصطناعي، مما أدى إلى ذعر شعبي غير مبرر.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة البحث البحري الرقمي.

- معظم المنصات الرقمية لا تخضع لرقابة بحرية كافية.

- لا توجد معايير دولية لشفافية المعلومات البحرية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة البحث البحري الرقمي" المنصات بنشر معلومات دقيقة ومحدثة. أما في الولايات المتحدة، فإن "وكالة حماية البيئة" بدأت بفحص الخوارزميات التي تحدد المعلومات البحرية.

أما في العالم العربي، فإن معظم التشريعات لا

تغطي التهديدات الرقمية على سلامة الباحثين، ولا توجد آليات فعالة لمنع التلاعب الرقمي.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في مجال سلامة الباحثين ليست رفاهية، بل حق إنساني أساسي، وأن سلامة البحث البحري الرقمي يجب أن تُعتبر جزءاً من الأمن القومي البحري.

**الفصل الرابع والعشرون

السيادة البحرية الرقمية والتعليم البحري الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق**

لا يمكن تحقيق السيادة البحرية الرقمية دون

بناء وعي مجتمعي لدى الباحثين والمواطنين حول حقوقهم الرقمية وواجباتهم تجاه البيئة البحرية العامة. فالتعليم البحري الرقمي ليس مجرد نشر معلومات، بل تمكين المواطنين من المطالبة بحقوقهم والمشاركة في صنع القرار البحري.

ففي الدول التي يُدرّس فيها القانون البحري الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في البيئة البحرية النظيفة. وفي المجتمعات التي تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض الخسائر البحرية.

وفي الممارسة، بدأت بعض الدول بدمج البيئة البحرية الرقمية في المناهج التعليمية. ففي فنلندا، يتعلم الأطفال من سن السادسة كيفية حماية بياناتهم البحرية. أما في كوستاريكا، فإن

"التعليم من أجل البيئة البحرية الرقمية" جزء أساسي من النظام التعليمي.

أما في الدول النامية، فإن التعليم البحري الرقمي غالباً ما يكون مقتصراً على النخبة، أو يُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة في الوعي تحرم المواطنين من فهم حقوقهم.

وفي العالم العربي، فإن بعض الدول بدأت بإدخال مفاهيم البيئة البحرية الرقمية في المناهج الثانوية، لكنها تبقى اختيارية وغير منهجية.

ويؤكد هذا الفصل أن التعليم البحري الرقمي هو استثمار استراتيجي في العدالة، وأن الدول التي لا تستثمر فيه ستظل شعوبها عاجزة عن

المطالبة بحقوقها.

**الفصل الخامس والعشرون

السيادة البحرية الرقمية والتراث البحري: حماية التراث من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو البيئة، بل يهدد أيضاً التراث البحري للبشرية. فالتحول إلى البيئة البحرية الرقمية قد يؤدي إلى اندثار المعرفة التقليدية، وانهيار الممارسات البحرية المحلية، وانهيار المجتمعات البحرية التقليدية.

ففي إفريقيا، تهدد أنظمة المراقبة الذكية الممارسات البحرية التقليدية التي طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية،

يؤدي الاعتماد على الحلول الرقمية إلى تآكل المهارات البحرية التقليدية. بل إن بعض اللغات والعادات البحرية تندثر بسبب التحول الرقمي.

ويواجه القانون الدولي غياباً في حماية هذا البعد، لأن اتفاقيات التراث الثقافي لا تأخذ في الاعتبار التهديدات الرقمية. ومع ذلك، فإن منظمة اليونسكو بدأت تدرج "الخطر الرقمي" كسبب لإدراج المواقع البحرية على قائمة الخطر.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على حماية تراثها البحري من التهديدات الرقمية.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غياب

الحماية القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم البحري.

**الفصل السادس والعشرون

السيادة البحرية الرقمية والتمويل البحري الرقمي: حماية الدول النامية من الديون البحرية**

مع تزايد الحاجة إلى التمويل البحري الرقمي، برز خطر جديد: تحويل "الديون البحرية الرقمية" إلى أداة للاستغلال. فبعض الدول النامية تقترض مليارات الدولارات لتمويل مشاريع بحرية رقمية، لكنها تجد نفسها عاجزة عن السداد بسبب الكوارث المناخية التي تضرب اقتصادها.

ففي جزر المحيط الهادئ، أدت الكوارث المناخية إلى انهيار الإيرادات البحرية، مما جعل سداد القروض البحرية الرقمية مستحيلاً. وفي أمريكا اللاتينية، أدت الأزمات المناخية إلى انهيار الصادرات، مما زاد من عجز الموازنات.

ويواجه القانون الدولي غياباً في حماية هذه الدول، لأن:

- لا توجد آلية لإعفاء الدول من الديون في حالات الكوارث المناخية.

- معظم القروض البحرية الرقمية تأتي بشروط صارمة تزيد من عبء الديون.

- لا توجد معايير دولية لـ"التمويل البحري الرقمي العادل".

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر الأمم المتحدة للبيئة البحرية 2025، تم اقتراح "آلية لإعادة هيكلة الديون البحرية"، لكنها لم تُعتمد بعد. أما في مجموعة السبع، فإن "مبادرة التمويل البحري الرقمي العادل" لا تزال في طور النقاش.

أما في العالم العربي، فإن معظم الدول تعتمد على قروض خارجية لتمويل مشاريع البيئة البحرية الرقمية، دون وجود ضمانات قانونية لحمايتها من المخاطر المناخية.

ويخلص هذا الفصل إلى أن التمويل البحري الرقمي يجب أن يكون هبة، لا ديناً، وأن الدول التي تدفع ثمن أخطاء غيرها لا ينبغي أن تُثقل بعبء الديون.

**الفصل السابع والعشرون

السيادة البحرية الرقمية والنقل البحري الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل البحري يعتمد فقط على السفن، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من الميناء إلى المستهلك. واختراق هذه الأنظمة قد يؤدي إلى تلف الموارد البحرية، أو تأخير التوزيع، أو سرقة الشحنات.

ففي عام 2024، تم اختراق نظام تتبع الشحنات البحرية في دولة أوروبية، مما أدى إلى تلف آلاف الموارد البحرية بسبب تأخير التبريد. وفي عام

2025، تم سرقة شحنات موارد بحرية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد البحرية الرقمية كجزء من "الأضرار المؤهلة للتعويض"، رغم أهميتها الاستراتيجية.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على إعادة بناء سلاسل التوريد بعد الهجمات.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في مجال النقل ليست مسألة تقنية، بل مسألة أمن بحري، وأن سلاسل التوريد البحرية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل الثامن والعشرون

السيادة البحرية الرقمية والبحث العلمي البحري المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم في مواجهة التحديات البحرية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية بحرية حساسة — مثل نماذج التغير المناخي المقاوم — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات البحرية التي قدمتها الدول النامية لفرض

شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها البحرية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل التاسع والعشرون

السيادة البحرية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة البحرية الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها البحرية الرقمية بمفردها، لأن التهديدات عابرة للحدود. ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض معايير البيئة البحرية الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية البحرية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة البحرية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة البحرية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا يزال ضعيفاً، مما يحد من قدرة الدول على

التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة البحرية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة البحرية الرقمية".

**الفصل الثلاثون

السيادة البحرية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات البحرية**

مع تزايد استخدام الموارد البحرية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية البحرية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر

التسبب المتعمد في كارثة بحرية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للموانئ، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع البحرية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً بحرية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية البحرية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية البحرية" لا تزال قيد النقاش،

ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة البحرية الرقمية.

**الفصل الحادي والثلاثون

السيادة البحرية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي البحري**

مع تزايد الأنشطة الفضائية المتعلقة بالبحر — من الأقمار الصناعية لمراقبة الموارد البحرية إلى الطائرات المسيرة الفضائية لتوزيع الموارد — برز تهديد جديد: التلوث الفضائي الذي يؤثر على

الأنظمة البحرية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد البحري، بينما تنبعثات الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات البحرية.

وفي الممارسة، تخطط شركات خاصة لإطلاق آلاف الأقمار خلال العقد القادم لمراقبة الموارد البحرية، دون أي تنظيم بيئي دولي. ومع ذلك، فإن معاهدات الفضاء الخارجي لا تأخذ في الاعتبار التأثيرات البحرية لهذه الأنشطة.

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية البحرية الرقمية"؟ وهل يجب أن تخضع الشركات الفضائية لنفس القواعد التي تخضع لها الصناعات الأرضية؟

أما في الدول النامية، فإن غياب القدرة على الوصول إلى الفضاء يجعلها عاجزة عن المشاركة في وضع هذه القواعد، رغم تأثرها المباشر بالتلوث الفضائي.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية البحرية يجب أن تخضع لمبدأ "الوقاية البحرية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

السيادة البحرية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً بحرياً**

مع ظهور الذكاء الاصطناعي التوليدي، أصبح بإمكان أي جهة إنشاء محتوى وهمي — من صور إلى مقاطع صوتية إلى فيديوهات — يبدو حقيقياً تماماً. وهذه التكنولوجيا تُستخدم اليوم كسلاح رقمي لتضليل الجمهور، وزعزعة ثقة المجتمع، وتقويض الثقة في الأنظمة البحرية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لعلماء وهم يحذرون من سياسات بحرية وطنية آمنة، مما أدى إلى انخفاض الثقة في النظام البحري وانتشار المعلومات المضللة. وفي أزمات بحرية، تم نشر أخبار كاذبة عن نقص في الموارد البحرية الأساسية، مما أدى إلى ذعر شعبي وارتفاع غير مبرر في الأسعار.

ويواجه القانون الدولي صعوبة في التعامل مع هذه الظاهرة، لأن:

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني بحري" وفق التعريفات الحالية.

- صانع المحتوى قد يكون برنامجاً، وليس شخصاً.

- نشر المحتوى يتم عبر منصات عابرة للحدود، لا تخضع لرقابة الدولة المستهدفة.

وفي المقابل، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بوضع علامة مائية رقمية على كل محتوى مولّد آلياً. أما في الولايات المتحدة، فإن "قانون الشفافية في الوسائط

الاصطناعية" يجرّم استخدام المحتوى المزيف في الحملات التضليلية البحرية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي هذا النوع من التهديدات، رغم تزايد استخدامه ضد الأنظمة البحرية الوطنية.

ويخلص هذا الفصل إلى أن غياب تنظيم الذكاء الاصطناعي التوليدي يحوّل الفضاء الرقمي إلى ساحة حرب نفسية بحرية، ويستدعي تعريفاً جديداً للتدخل السيبراني البحري يشمل "التأثير الخبيث عبر المحتوى المزيف".

**الفصل الثالث والثلاثون

السيادة البحرية الرقمية والبيانات الضخمة

البحرية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل الموارد البحرية، أصبحت هذه البيانات مورداً استراتيجياً. لكن الدول النامية غالباً ما تفتقر إلى القدرة على جمع وتحليل بياناتها، فتلجأ إلى شركات أجنبية تمتلك هذه القدرات.

ففي بعض الحالات، استخدمت شركات خاصة بيانات بحرية من دول نامية لتطوير نماذج تنبؤ تُباع بأسعار باهظة. بل إن بعض الحكومات استخدمت هذه البيانات لفرض شروط تجارية غير عادلة.

ويواجه القانون الدولي غياباً في حماية هذه

البيانات، لأن:

- لا توجد اتفاقيات دولية تنظم ملكية البيانات البحرية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة البحرية الرقمية".

أما في الدول النامية، فإن غياب التشريعات يسمح باستغلال بياناتها دون مقابل عادل.

ويؤكد هذا الفصل أن البيانات البحرية ليست مجرد أرقام، بل أداة للعدالة، وأن الدول التي لا تحمي سيادتها الرقمية ستظل عاجزة عن المطالبة بحقوقها البحرية.

**الفصل الرابع والثلاثون

السيادة البحرية الرقمية والتعليم العالي البحري: نحو كليات وطنية للقانون البحري الرقمي**

لا يمكن بناء قدرات بحرية رقمية وطنية دون مؤسسات تعليمية متخصصة تخرّج كوادر مؤهلة. فالاعتماد على الخبرات الأجنبية أو الدورات القصيرة لا يكفي لمواجهة التهديدات المعقدة. ولذلك، فإن إنشاء كليات وطنية للقانون البحري الرقمي يُعد استثماراً استراتيجياً في السيادة البحرية الرقمية.

وفي الدول الرائدة، أصبحت هذه الكليات مراكز

بحث وتطوير. ففي جامعة هارفارد، يُدرّس "القانون البحري الرقمي الدولي". أما في جامعة أكسفورد، فإن "مركز القانون البحري" يدرّب المحامين على رفع الدعاوى البحرية الرقمية.

أما في الدول النامية، فإن التعليم البحري الرقمي غالباً ما يكون جزءاً من أقسام علوم الحاسوب، دون تخصص كافٍ. وهذا ينتج خريجين قادرين على البرمجة، لكن غير مؤهلين لفهم الجوانب القانونية أو الاستراتيجية للأمن البحري الرقمي.

وفي العالم العربي، بدأت بعض الدول بإنشاء برامج متخصصة، مثل "ماجستير الأمن البحري الرقمي" في جامعات الإمارات والسعودية. أما في دول أخرى، فلا تزال المناهج تفتقر إلى التحديث، ولا توجد روابط كافية بين الجامعات

وقطاع الصناعة.

**الفصل الخامس والثلاثون

السيادة البحرية الرقمية والثقافة الرقمية البحرية: حماية الإبداع المحلي من القرصنة والتهميش**

لا يقتصر الفضاء الرقمي على البيانات والخدمات، بل يشمل أيضاً الإبداع الثقافي البحري: الأفلام الوثائقية، الروايات، الفنون البصرية التي تروي قصص البحار. ومع هيمنة المنصات العالمية على توزيع المحتوى، أصبح المبدعون المحليون عرضة للتهميش أو الاستغلال.

فمنصات البث قد تدفع تعويضات زهيدة للمبدعين

المحليين، أو ترفض عرض محتواهم دون مبرر. بل وقد تُسرق أعمالهم وتُنسب إلى آخرين دون حماية قانونية كافية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات لحماية المحتوى المحلي. ففي فرنسا، يُلزم القانون بوجود نسبة محددة من المحتوى الفرنسي في المنصات. أما في كوريا الجنوبية، فقد استثمرت الدولة في دعم المحتوى الرقمي المحلي، مما أدى إلى انتشاره عالمياً.

أما في العالم العربي، فإن الجهود لا تزال مجزأة، ولا توجد سياسات وطنية فعالة لدعم الإبداع الرقمي البحري المحلي أو حمايته من القرصنة.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية

الثقافية هي جزء من الهوية الوطنية، وأن غيابها يحوّل الشعوب إلى مستهلكين سلبيين، لا مبدعين فاعلين.

**الفصل السادس والثلاثون

السيادة البحرية الرقمية والتمويل الرقمي البحري: حماية العملات البحرية من التلاعب والاحتيال**

مع ظهور العملات الرقمية البحرية والبلوك تشين البحري، أصبحت الأنظمة المالية التقليدية تواجه تحديات جديدة. فالعملات الرقمية البحرية يمكن استخدامها لغسل الأموال تحت غطاء المشاريع البحرية، أو لتمويل مشاريع وهمية.

وفي الممارسة، أدت عمليات الاحتيال في سوق العملات الرقمية البحرية إلى خسائر تقدر بمليارات الدولارات. ومع ذلك، فإن التنظيم القانوني لهذا السوق يبقى ضعيفاً في كثير من الدول.

ويواجه القانون الدولي صعوبة في التعامل مع العملات الرقمية البحرية، لأنها لا تخضع لسلطة دولة واحدة، ولا يمكن تتبع مالكيها بسهولة.

أما في الدول النامية، فإن غياب التنظيم يسمح باستغلال هذه العملات لسرقة التمويل البحري المخصص للمشاريع الحقيقية.

ويخلص هذا الفصل إلى أن السيادة البحرية الرقمية في المجال المالي لا تعني منع الابتكار،

بل وضع ضوابط تحمي الاقتصاد الوطني من المخاطر غير المحسوبة.

**الفصل السابع والثلاثون

السيادة البحرية الرقمية والبحث العلمي البحري المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم العلمي في مواجهة التحديات البحرية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية بحرية حساسة — مثل نماذج التغير المناخي المقاوم — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات البحرية التي قدمتها الدول النامية لفرض شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها البحرية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل الثامن والثلاثون

السيادة البحرية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة البحرية الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها البحرية الرقمية بمفردها، لأن التهديدات عابرة للحدود. ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض معايير البيئة البحرية الرقمية من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية البحرية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة البحرية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة البحرية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا يزال ضعيفاً، مما يحد من قدرة الدول على التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة البحرية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة البحرية الرقمية".

**الفصل التاسع والثلاثون

السيادة البحرية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات البحرية**

مع تزايد استخدام الموارد البحرية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير

البنية التحتية البحرية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في كارثة بحرية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للموانئ، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع البحرية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً بحرية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية البحرية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية البحرية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة البحرية الرقمية.

**الفصل الأربعون

السيادة البحرية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى السيادة البحرية الرقمية كظاهرة مؤقتة، بل كتحول جوهري في

مفهوم الحماية البحرية في القرن الحادي والعشرين. فالدول التي تبني سيادتها البحرية الرقمية اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب البحري الرقمي.

- بناء اقتصاد بحري رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام البحري العالمي.

- المشاركة الفاعلة في صياغة قواعد النظام الدولي الجديد.

أما الدول التي تتجاهل هذا التحول، فستجد نفسها رهينة للتكنولوجيا الأجنبية، وعرضة للتدخلات الخارجية، وعاجزة عن حماية مصالحها في العصر الرقمي.

ولذلك، فإن الاستثمار في السيادة البحرية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

**الفصل الحادي والأربعون

السيادة البحرية الرقمية والطاقة المتجددة البحرية: حماية المصادر من الاستغلال الرقمي**

مع تزايد الاعتماد على الطاقة المتجددة البحرية — من طاقة الأمواج إلى طاقة المد والجزر — أصبحت هذه المصادر هدفاً للشركات الرقمية التي تسعى إلى تسجيل براءات اختراع عليها. فأنظمة إدارة الطاقة المتجددة البحرية تعتمد اليوم على خوارزميات ذكية قد تكون مملوكة

لشركات أجنبية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة طاقة بحرية محلية.

- رفع تكاليف الطاقة المتجددة بشكل غير متناسب.

- خلق اعتماد دائم على التكنولوجيا الأجنبية.

ويواجه القانون الدولي غياباً في حماية هذه المصادر، لأن اتفاقيات الطاقة المتجددة لا تأخذ في الاعتبار التهديدات الرقمية.

ويؤكد هذا الفصل أن الطاقة المتجددة البحرية ليست مجرد مصدر للطاقة، بل جزء من السيادة الوطنية، وأن غياب الحماية الرقمية لها يحوّل المصادر المتجددة إلى سلعة في سوق الاحتكار العالمي.

**الفصل الثاني والأربعون

السيادة البحرية الرقمية والصيد البحري الذكي: عندما تصبح الخوارزميات صياداً**

لم يعد الصيد البحري يعتمد على القوارب والشبكات، بل على **أنظمة الصيد الذكية** التي تستخدم الذكاء الاصطناعي لتحديد مواقع الأسماك وتحليل أنماط هجرتها. وهذه الأنظمة، رغم فعاليتها، تهدد التوازن البيئي إذا لم تُنظم.

ففي بعض الحالات، أدت أنظمة الصيد الذكي إلى استنزاف مخزونات الأسماك في مناطق معينة، لأن الخوارزميات تركز على الربح وليس على الاستدامة.

ويواجه القانون الدولي غياباً في تنظيم هذه الأنظمة، لأن اتفاقيات الصيد البحري لا تأخذ في الاعتبار التهديدات الرقمية.

ويؤكد هذا الفصل أن الصيد البحري الذكي يجب أن يخضع لمبدأ "الاستدامة الرقمية"، وأن غياب التنظيم يحوّل الذكاء الاصطناعي إلى أداة لتدمير الموارد، لا لحمايتها.

**الفصل الثالث والأربعون

السيادة البحرية الرقمية والنقل البحري الذكي: حماية الممرات من التلاعب الرقمي

مع تزايد استخدام السفن الذكية والموانئ الرقمية، أصبحت الممرات البحرية هدفاً للهجمات السيبرانية التي تهدف إلى تعطيل حركة التجارة العالمية. فاختراق أنظمة الملاحة الذكية قد يؤدي إلى حوادث بحرية كارثية.

وفي عام 2025، تم اختراق نظام ملاحة في مضيق هرمز، مما أدى إلى تأخير حركة النقل البحري لأيام.

ويواجه القانون الدولي غياباً في حماية هذه الممرات، لأن اتفاقيات الملاحة البحرية لا تأخذ

في الاعتبار التهديدات السيبرانية.

ويؤكد هذا الفصل أن الممرات البحرية ليست مجرد مسارات مائية، بل شرايين حيوية للأمن القومي، وأن غياب الحماية الرقمية لها يعرض الاقتصاد العالمي للخطر.

**الفصل الرابع والأربعون

السيادة البحرية الرقمية والبحث العلمي البحري: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها البحرية الرقمية دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني البحري، والذكاء الاصطناعي البحري، وتصميم الأنظمة الرقمية.

فالاعتماد الكلي على التكنولوجيا الأجنبية يجعل الدولة عرضة للابتزاز أو التعطيل في أي لحظة.

وقد أدركت القوى الكبرى هذه الحقيقة مبكراً. ففي الولايات المتحدة، يمول "مكتب مشاريع البحوث البحرية المتقدمة" مشاريع بحثية في الأمن السيبراني البحري بعشرات المليارات سنوياً. أما في الصين، فإن "خطة البحر الذكي 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة مراقبة ذكية محلية.

أما في الدول النامية، فإن البحث العلمي البحري الرقمي يعاني من نقص التمويل، وضعف البنية التحتية، وهجرة الكفاءات.

ويخلص هذا الفصل إلى أن الاستقلال

التكنولوجي البحري ليس رفاهية، بل شرط وجودي للسيادة البحرية الرقمية.

**الفصل الخامس والأربعون

السيادة البحرية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟**

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون البحري الرقمي. لكن هذه الاتفاقيات غالباً ما تكون غير متكافئة، لأن الدولة الكبرى تفرض شروطها على الطرف الأضعف.

ففي بعض الاتفاقيات، تطلب الدولة الكبرى من الطرف الآخر السماح لها بالوصول إلى بياناته

البحرية في حالات "الطوارئ البحرية"، دون تعريف دقيق لماهية الطوارئ. وفي اتفاقيات أخرى، تُلزم الدولة الصغيرة باستخدام برمجيات أو معدات من شركة تابعة للدولة الكبرى، مما يخلق اعتماداً طويل الأمد.

ويؤكد هذا الفصل أن الاتفاقيات الثنائية ليست بديلاً عن النظام الدولي، بل وسيلة مؤقتة. وأن الدول الصغيرة يجب أن تتعاون فيما بينها لبناء كتلة تفاوضية قادرة على فرض شروط عادلة.

**الفصل السادس والأربعون

السيادة البحرية الرقمية والمحاكمات البحرية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء البحري الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية البحرية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على باحث في دولة ثالثة.

ويواجه القانون الدولي غياباً في توحيد قواعد الاختصاص، مما يؤدي إلى تضارب في الأحكام.

ويخلص هذا الفصل إلى أن غياب نظام قضائي رقمي بحري موحد يشجع المجرمين على استغلال الثغرات القانونية، ويستدعي إنشاء "محكمة سيبرانية بحرية دولية" تابعة للأمم المتحدة.

**الفصل السابع والأربعون

السيادة البحرية الرقمية والبيانات البحرية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات البحرية اليوم أثمن مورد في الاقتصاد الرقمي البحري. ولذلك، فإن السيادة البحرية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: الباحث أم الدولة أم الشركة؟

ويؤكد هذا الفصل أن البيانات البحرية ليست مجرد أرقام، بل تعبير عن الهوية البحرية الفردية والجماعية. وأن السيادة البحرية الرقمية الحقيقية تبدأ باحترام حق الباحث في التحكم بمعلوماته.

**الفصل الثامن والأربعون

السيادة البحرية الرقمية والبيئة البحرية: حماية المجتمعات من التكنولوجيا البحرية غير المسؤولة**

لا يمكن فصل السيادة البحرية الرقمية عن البيئة البحرية، لأن بعض التقنيات البحرية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية يجب أن تمتد إلى حماية البيئة البحرية، وأن التكنولوجيا البحرية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل التاسع والأربعون

السيادة البحرية الرقمية والتراث البحري: حماية التراث من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو البيئة، بل يهدد أيضاً التراث البحري للبشرية.

ويؤكد هذا الفصل أن السيادة البحرية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غياب الحماية القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم البحري.

**الفصل الخمسون

السيادة البحرية الرقمية والمستقبل: رؤية

استراتيجية للعقود القادمة

في الختام، لا يمكن النظر إلى السيادة البحرية الرقمية كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الحماية البحرية في القرن الحادي والعشرين. فالدول التي تبني سيادتها البحرية الرقمية اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب البحري الرقمي.

- بناء اقتصاد بحري رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام البحري العالمي.

- المشاركة الفاعلة في صياغة قواعد النظام الدولي الجديد.

أما الدول التي تتجاهل هذا التحول، فستجد نفسها رهينة للتكنولوجيا الأجنبية، وعرضة للتدخلات الخارجية، وعاجزة عن حماية مصالحها في العصر الرقمي.

ولذلك، فإن الاستثمار في السيادة البحرية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة البحرية الرقمية في مختلف المجالات — من الأمن

السيبراني إلى الاقتصاد، ومن الثقافة إلى التنمية — يتبين أن هذا المفهوم لم يعد رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة. فالفضاء البحري الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على سيادتها البحرية دون وجود قدرات رقمية وطنية فاعلة.

وقد كشف هذا العمل أن الفراغ التشريعي الدولي يشكل تهديداً مزدوجاً: فهو يسمح للدول والشركات الكبرى بفرض هيمنتها، ويترك الدول النامية عرضة للاستغلال دون حماية قانونية. ولسد هذا الفراغ، لا بد من مبادرة جماعية تبني نظاماً دولياً عادلاً يوازن بين الابتكار البحري وسيادة الدولة على أنظمتها البحرية.

وفي النهاية، فإن السيادة البحرية الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل وسيلة لبناء مستقبل بحري آمن، عادل، وإنساني.

المراجع

United Nations Conventionon the Law of (the Sea (UNCLOS, 1982

Convention on Biological Diversity (CBD, (1992

Nagoya Protocol on Access and Benefit-
(Sharing (2010

General Data Protection Regulation
(GDPR), Regulation (EU) 2016/679

Tallinn Manual 2.0 on the International Law
Applicable to Cyber Operations (Cambridge
(University Press, 2017

International Maritime Organization (IMO)
Guidelines on Maritime Cyber Risk
(Management (2021

UNESCO Recommendation on Open
(Oceanic Data (2022

European Commission. Digital Ocean Action
(Plan (2023

Government of China. Smart Ocean 2030 (Plan (2022

Elrakhawi M K A. (2026). The Global Encyclopedia of Law – A Comparative Practical Study. First Edition. Ismailia: Global Legal Publications

Schmitt M N. (2023). Cyber Operations and International Law. Cambridge University Press

Rajamani L. (2025). Oceanic Sovereignty and Digital Control. Oxford University Press

De Schutter O. (2023). The Right to a Healthy Ocean in the Digital Age. Cambridge University Press

Kloppenburg J R. (2024). Maritime Sovereignty and Digital Exploitation. University of California Press

:Official Government Sources

White House. National Strategy for Digital (Ocean (2024

European Commission. Digital Ocean Action (Plan (2023

Ministry of Maritime Affairs Reports on Cyber Resilience in Oceanic Systems

((Multiple Jurisdictions, 2020–2025

:Academic Journals

Journal of International Maritime Law ((Oxford

International Journal of Digital Oceanic Sovereignty

Harvard Environmental Law Review – Ocean Section

Stanford Technology Law Review

فهرس المحتويات

الفصل الثالث

السيادة البحرية التقليدية مقابل السيادة البحرية الرقمية: إعادة تشكيل المفاهيم القانونية

الفصل الرابع

البنية التحتية البحرية الرقمية: تعريف قانوني دولي مفقود

الفصل الخامس

التلاعب السيبراني في الأنظمة البحرية: نحو معيار قانوني دولي

الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية البحرية: تحديات الإسناد والرقابة

الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية البحرية: بين التدابير المضادة والقوة المسلحة

الفصل الثامن

السيادة البحرية الرقمية وبراءات الاختراع البحرية: التوتر بين الابتكار والاستغلال

الفصل التاسع

السيادة البحرية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي

الفصل العاشر

التنظيم الإقليمي للسيادة البحرية الرقمية: دراسة مقارنة بين التجارب العالمية

الفصل الحادي عشر

السيادة البحرية الرقمية والبيانات البحرية: حماية الخصوصية البحرية من الاستغلال الخارجي

الفصل الثاني عشر

السيادة البحرية الرقمية والذكاء الاصطناعي البحري: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة

الفصل الثالث عشر

السيادة البحرية الرقمية والجرائم الإلكترونية البحرية: مكافحة الاحتيال البحري الرقمي

الفصل الرابع عشر

السيادة البحرية الرقمية والتربية الرقمية البحرية: بناء وعي مجتمعي كأساس للدفاع السيبراني

الفصل الخامس عشر

السيادة البحرية الرقمية والبحث العلمي البحري: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

السيادة البحرية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟

الفصل السابع عشر

السيادة البحرية الرقمية والمحاكمات البحرية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

السيادة البحرية الرقمية والبيانات البحرية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

السيادة البحرية الرقمية والبيئة البحرية: حماية المجتمعات من التكنولوجيا البحرية غير المسؤولة

الفصل العشرون

السيادة البحرية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية

الفصل الحادي والعشرون

السيادة البحرية الرقمية والسفن الذكية: من الملاحة إلى الإدارة الذاتية

الفصل الثاني والعشرون

السيادة البحرية الرقمية والطاقة البحرية: حماية الموارد من الاستنزاف الرقمي

الفصل الثالث والعشرون

السيادة البحرية الرقمية وسلامة الباحثين: حماية الباحثين من التلاعب الرقمي

الفصل الرابع والعشرون

السيادة البحرية الرقمية والتعليم البحري الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق

الفصل الخامس والعشرون

السيادة البحرية الرقمية والتراث البحري: حماية التراث من الاندثار الرقمي

الفصل السادس والعشرون

السيادة البحرية الرقمية والتمويل البحري الرقمي: حماية الدول النامية من الديون البحرية

الفصل السابع والعشرون

السيادة البحرية الرقمية والنقل البحري الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل الثامن والعشرون

السيادة البحرية الرقمية والبحث العلمي البحري المفتوح: التوازن بين التعاون والحماية

الفصل التاسع والعشرون

السيادة البحرية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة البحرية الرقمية

الفصل الثلاثون

السيادة البحرية الرقمية والقانون الإنساني

الدولي: حماية المدنيين في النزاعات البحرية

الفصل الحادي والثلاثون

السيادة البحرية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي البحري

الفصل الثاني والثلاثون

السيادة البحرية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً بحرياً

الفصل الثالث والثلاثون

السيادة البحرية الرقمية والبيانات الضخمة

السيادة البحرية الرقمية والتمويل الرقمي البحري: حماية العملات البحرية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة البحرية الرقمية والبحث العلمي البحري المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

السيادة البحرية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة البحرية الرقمية

الفصل التاسع والثلاثون

السيادة البحرية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات البحرية

الفصل الأربعون

السيادة البحرية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

الفصل الحادي والأربعون

السيادة البحرية الرقمية والطاقة المتجددة البحرية: حماية المصادر من الاستغلال الرقمي

الفصل الثاني والأربعون

السيادة البحرية الرقمية والصيد البحري الذكي:

عندما تصبح الخوارزميات صياداً

الفصل الثالث والأربعون

السيادة البحرية الرقمية والنقل البحري الذكي: حماية الممرات من التلاعب الرقمي

الفصل الرابع والأربعون

السيادة البحرية الرقمية والبحث العلمي البحري: نحو استقلال تكنولوجي وطني

الفصل الخامس والأربعون

السيادة البحرية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟

الفصل السادس والأربعون

السيادة البحرية الرقمية والمحاكمات البحرية: نحو اختصاص قضائي رقمي

الفصل السابع والأربعون

السيادة البحرية الرقمية والبيانات البحرية: بين الملكية الفردية والسيادة الجماعية

الفصل الثامن والأربعون

السيادة البحرية الرقمية والبيئة البحرية: حماية المجتمعات من التكنولوجيا البحرية غير المسؤولة

الفصل التاسع والأربعون

السيادة البحرية الرقمية والتراث البحري: حماية التراث من الاندثار الرقمي

الفصل الخمسون

السيادة البحرية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

بيان حقوق الملكية

جميع الحقوق محفوظة للمؤلف

© 2026 الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون

يحظر منعاً باتاً:

نسخ أو طبع أو نشر أو توزيع أو اقتباس أو ترجمة أو تحويل أو عرض أي جزء من هذا العمل — سواء كان ذلك إلكترونياً، رقمياً، مطبوعاً، أو بأي وسيلة أخرى — دون الحصول على **تصريح

كتابي صريح ومسبق** من المؤلف.

الاستثناء الوحيد:

يجوز الاقتباس لأغراض بحثية أو أكاديمية، بشرط:

- ذكر اسم المؤلف كاملاً: **الدكتور محمد كمال عرفه الرخاوي**.

- ذكر عنوان المؤلف كاملاً: **"السيادة البحرية الرقمية: دراسة قانونية حول حماية الموارد البحرية من التلاعب السيبراني وبناء نظام عدالة بحرية رقمي عالمي"**.

- ذكر رقم الصفحة بدقة.

- عدم تغيير السياق أو المعنى.

التحديث:

أي تحديث أو طبعة جديدة لهذا العمل ستُعلن عنها رسمياً عبر الموقع الإلكتروني المعتمد للمؤلف.

تم بحمد الله وتوفيقه

تأليف الدكتور محمد كمال عرفه الرخاوي