



دور الأمن السيبراني في تأمين النشاطات البحرية التجارية The role of cyber security in securing commercial maritime activities

سعيد دالع¹

المركز الجامعي مغنية- الجزائر

s.dalaa@cu-maghnia.dz

مخبر القانون البحري و النقل

تاريخ القبول للنشر: 2026-05-08

تاريخ الاستلام: 2026-01-25

ملخص:

يعد القطاع البحري التجاري أحد القطاعات الاقتصادية التي تكتسي مكانة هامة في الاقتصاد الدولي والداخلي على حد سواء، وبحكم التحول الرقمي الذي عرفه هذا القطاع أصبح هو الآخر في مرمى التهديدات والمخاطر السيبرانية، من هنا جاءت الحاجة إلى تبني حلول الأمن السيبراني الذي تقوم على إستراتيجيات أمنية شاملة لحماية النشاط البحري بمختلف مكوناته، من أنظمة معلومات وبيانات تخص كل من السفن والموانئ البحرية والعاملين عليها.

الكلمات المفتاحية: السفن، الموانئ، المخاطر السيبرانية، توصيات، الأمن السيبراني.

Abstract:

The commercial maritime sector is one of the economic sectors that plays an important role in both the international and domestic economies. Due to the digital transformation that this sector has undergone, it has also become vulnerable to cyber threats and risks. Hence the need to adopt cybersecurity solutions based on a comprehensive security policy and strategy to protect maritime activity in all its components, from information and data systems relating to ships, ports, and their workers.

Keywords: Ships, ports, cyber risks, recommendations, cybersecurity.

¹ سعيد دالع

مقدمة:

يتسم النشاط البحري التجاري بالتعقيد، نظرا لكثرة المتدخلين فيه وضخامة الاستثمارات التي يستقطبها. ومع ظهور تكنولوجيات الإعلام والاتصال الحديثة اتجهت أنظار المجتمع البحري للاستفادة من هذه التكنولوجيات لإيجاد حلول ذكية لتيسير مختلف العمليات البحرية وزيادة في كفاءتها، وقد تحقق ذلك بالفعل على عدة مستويات فأصبح بالإمكان تتبع البضاعة وتقليص مدة مكوث السفن في الموانئ والتقليل من التكاليف إلى غير ذلك من النتائج.

إلا أن هذا الانتقال التكنولوجي اصطدم بتهديد جديد لا يقل خطورة عن التهديدات التقليدية، فهو يatal البنية التحتية الرقمية للنشاط البحري من سفن وموانئ، ويجعل من امكانية توقعه وتحديد مصدره أمرا صعبا، هذا بالإضافة إلى جسامه الأضرار التي قد يسببها.

أمام هذا الواقع، سارع المجتمع البحري من خلال المنظمة البحرية الدولية ومنظوماته التشريعية الداخلية إلى وضع مجموعة من المبادئ جاءت في شكل توصيات اعتمدت على توظيف الأمن السيبراني في مواجهة المخاطر والتهديدات التي تستهدف البنى التحتية الرقمية.

ليثور التساؤل حول: مضمون المبادئ الدولية التي جاءت للتصدي للتهديدات السيبرانية، وعلى المستوى الداخلي كيف تصدى المشرع الجزائري لهذه التهديدات؟. تحقيقا لمناقشة هذه الإشكالية اعتمدنا المنهج الوصفي و المنهج التحليلي، فالمنهج الوصفي استخدم في جمع المعلومات حول ظاهرة التهديدات السيبرانية والأمن السيبراني، أما المنهج التحليلي فقد تم توظيفه لتحليل النصوص القانونية للوصول إلى فهم أحكامها. وقد قسمت هذا الدراسة إلى ثلاث محاور الأول تم تخصيصه لإعطاء مفهوم للأمن السيبراني (أولا)، لتتطرق بعد ذلك لدراسة المبادئ التي جاءت بها المنظمة البحرية الدولية (ثانيا)، واختتمنا هذه الدراسة بتسليط الضوء على الحلول التي جاء بها المشرع الجزائري للتصدي للتهديدات السيبرانية التي تطل النشاط البحري التجاري (ثالثا).

1- تعريف الأمن السيبراني:

سنخصص هذا المحور لإبراز أهم التعريفات التي وضعت للأمن السيبراني انطلاقاً من التعريف اللغوي والإصطلاحي، وصولاً للتعريف القانوني.

1.1- التعريف اللغوي والإصطلاحي للأمن السيبراني:

1.1.1- التعريف اللغوي للأمن السيبراني:

تنقسم عبارة "الأمن السيبراني" إلى لفظتين، الأولى "الأمن" والثانية "السيبراني".
أ- الأمن: مصدره الفعل أَمِنَ، يَأْمَنُ، ويقصد به: الإطمئنان وذهاب الخوف .
ب- السيبراني: باللغة الفرنسية "Cyber"، يعود أصلها إلى الكلمة اليونانية "kubernan" المذكورة في ملحمة الأوديسا "Odyssee" لكتابها هيروميس، ويقصد بها المتحكم في القيادة، أو موجه السفينة (فارس، 2019، صفحة 1).
يعود الاستخدام الأول للفظ اللاتيني Cyber إلى الرياضي الأمريكي Norbert Wiener (1894-1964) في قوله: "إننا قررنا أن نُطلق على مجال نظرية التحكم والاتصال بأكملها، سواء في الآلة أو في الحيوان، اسم السيبرنوطيقا" (Norbert, 1985, p. 11).

ولقد لاقى هذا المصطلح استعمالاً واسعاً في تلك الفترة، ليهمل بعد وفاة هذا الرياضي، ليعود بعد ذلك للظهور في سنوات التسعينات ويستخدم كمقطع أول في الكثير من المصطلحات، كما هو الحال في كلمة "Cybersecurite" والتي تعني الأمن السيبراني، وكلمة "Cyberwar" التي تعني الحرب السيبرانية، كلمة "Cybercrime" التي تعني الجريمة السيبرانية... إلخ (AVENAS, 2019).

2.1.1- التعريف الإصطلاحي للأمن السيبراني:

لقد وجدت عدة تعريفات للأمن السيبراني، حيث عرفه كل من الكاتب Lehto martti و Neittaanmäki Pekka على أنه: "عبارة عن مجموعة من الإجراءات المتخذة ضد هجمات قراصنة الكمبيوتر وعواقبها، ويشمل ذلك تنفيذ التدابير المضادة المطلوبة." (Lehto & Neittaanmaki, 2015, p. 25)

أما الاتحاد الدولي للاتصالات فعرفه بأنه حزمة من الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية من مستعملين ومؤسسات. (لمحة عامة عن الأمن السيبراني، 2008، صفحة 02).

في حين عرفته وزارة الدفاع الأمريكية على أنه مجموعة من التدابير التنظيمية الكفيلة بحماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم كالتجسس والتخريب والهجمات الإلكترونية. (بركان ورمل، 2024، صفحة 4).

من خلال تحليلنا لهذه التعريفات يتضح لنا جليا أن التعريف الذي جاء به الاتحاد الدولي للاتصالات هو الأشمل، وذلك من خلال استخدامه لمصطلح السياسات الذي يعبر عن خطة شاملة متكاملة محددة الأهداف للوصول إلى تأمين كامل للمعلومات.

2.1- التعريف القانوني للأمن السيبراني:

1.2.1- التعريف التشريعي:

لقد عرف المشرع الجزائري الأمن السيبراني في المادة 10 الفقرة 03 من القانون 04-18 (القانون رقم 04-18، 2018)، على أنه مجموعة من الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة.

وعليه، لأنه بهذا التعريف يكون هذا النص قد تبنى المفهوم الواسع للأمن السيبراني الذي جاء به الاتحاد الدولي للاتصالات في تعريفه السابق.

لم يعرف القانون الفرنسي الأمن السيبراني، وإنما قام بالإشارة إليه في قانون تأمين وتنظيم الفضاء الرقمي من خلال إلزام الشركات والهيئات العمومية بتعزيز أنظمتها الأمنية لحماية البيانات الاستراتيجية والحساسة تحت طائلة التعرض لعقوبات جزائية (Loi n°2024-449، 2024).

في حين عرفه الاتحاد الأوروبي في المادة 2 الفقرة الثانية من اللائحة 881/2019 (Règlement européenne 2019-881)، بأنه تلك الأنشطة اللازمة لحماية الشبكات وأنظمة المعلومات، ومستخدمي هذه الأنظمة، والأشخاص الآخرين المتأثرين بالتهديدات السيبرانية، ويضيف الإتحاد الأوروبي في الفقرة 8 من المادة 2 أن الأمن السيبراني لا يتعلق فقط بالتكنولوجيا وإنما يرتبط كذلك بالسلوك البشري، الذي يعد الموجه والمشجع للمجتمعات والشركات والمنظمات على اعتماد معلومات سليمة من خلال التقيد بالإجراءات للتقليل من مخاطر التهديدات السيبرانية.

2.2.1- التعريف الفقهي للأمن السيبراني:

تعرف الدكتورة منى الأشقر جبور الأمن السيبراني على أنه ذلك المجال الذي يتعلق بإجراءات ومعايير الحماية ومواجهة التهديدات التي قد تطل الشبكات والأنظمة المعلوماتية والبيانات والأجهزة المتصلة بالإنترنت (منى الأشقر، دون سنة نشر، صفحة 25).

وفي تعريف آخر عرفت الدكتورة أميرة عبدالعظيم محمد الجواد الأمن السيبراني على أنه حزمة من التدابير التي يتم اتخاذها للحد أو الدفاع ضد هجمات الكمبيوتر أو البرمجيات، وذلك من خلال الوسائل والأدوات المستخدمة في مواجهة تلك المخاطر (عبدالعظيم محمد عبدالجواد، 2020، صفحة 388).

2- الإطار التشريعي الدولي لاستغلال الأمن السيبراني في تأمين النشاطات البحرية:

يعود أول اهتمام تشريعي دولي لمواجهة التهديدات المتعلقة بأمن البيانات في المجال البحري إلى المدونة الدولية لأمن السفن والمرافق المينائية (ISPS) (المرسوم 83-510، 1983)، حيث أكدت هذه المدونة في العديد من المواضع على ضرورة البحث على نقاط الضعف في الأنظمة والشبكة المعلوماتية على متن السفن والموانئ، وبذل الجهد في سد هذه الثغرات الأمنية التي يمكن استغلالها من طرف

قراصنة المعلومات للإضرار بالنشاط البحري. غير أن هذه المدونة اتسمت بنصوصها بالعمومية في التأسيس للأمن السيبراني لمواجهة الهجمات السيبرانية.

1.2 - الإرشادات التوجيهية للمنظمة البحرية الدولية لسنة 2017:

لقد كان على المجتمع البحري الانتظار إلى غاية سنة 2017، حيث أصدرت المنظمة البحرية الدولية أول إرشادات توجيهية تضمنت مجموعة من المبادئ في الأمن السيبراني لمواجهة التهديدات التي قد تطال النشاط البحري (Guidelines on maritime cyber risk management, 5 July 2017)، وأكدت على كل الفاعلين في قطاع النقل البحري الأخذ بها بشكل متزامن ومتواصل ودمجها في إدارة المخاطر السيبرانية، وقد اختصرت هذه المبادئ في خمس كلمات وردت في المادة 3 الفقرة 5، وهي: التحديد، الحماية، الكشف، الإستجابة والتعافي.

فمبدأ التحديد يراد به إسناد الأدوار والمسؤوليات على وجه الدقة للعاملين في المجال البحري لإدارة المخاطر السيبرانية، مع ضرورة تحديد الأنظمة والبيانات والأجهزة التي قد يؤدي تعطيلها إلى تهديد نشاط السفن البحرية. أما الحماية فتقوم على أساس اعتماد اجراءات ومعايير لمراقبة الأخطار السيبرانية، وفي نفس الوقت وضع مخططات استعجالية لمواجهة أي تهديد من شأنه المساس باستمرارية العمليات البحرية.

في حين يقوم مبدأ الكشف على إلزام كل الهيئات على تطوير وتنفيذ جميع المهام اللازمة للكشف عن أي حدث سيبراني في الوقت المناسب، حتى يتسنى لها التدخل الناجع للتصدي لكل التهديدات.

أما الاستجابة فتعتمد على تطوير وتنفيذ الخطط اللازمة لتوفير المرونة في استعادة الأنظمة المعلوماتية الخاصة بعمليات الشحن البحري، والخدمات المعطلة بصفة عامة بسبب الهجمات السيبرانية.

ويأتي في الأخير مبدأ التعافي الذي يركز أساسا على تحديد التدابير اللازمة لإنشاء نسخة احتياطية من البيانات والأنظمة لاستعادتها لضمان التعافي الكامل للأنشطة البحرية المتضررة بالأحداث السيبرانية.

2.2 - تعديل الإرشادات التوجيهية للمنظمة البحرية الدولية لسنة 2021:

بعد اجتماع كل من لجنة السلامة البحرية (MSC) ولجنة تيسير الملاحة البحرية (FAL) المنصويتين تحت مظلة المنظمة البحرية الدولية، تقرر مراجعة المبادئ التوجيهية المتعلقة بالأمن السيبراني في المجال البحري لسنة 2017، هذه المراجعة توجت بإصدار نسخة محينة من هذه المبادئ بتاريخ 14 جوان سنة 2021 تضمنت تعديلا واحدا (Guidelines on maritime cyber risk management, 14 June 2021)، تمثل في إضافة البند 2 إلى المادة 4 الفقرة 2 و الذي ينص على الأخذ بالتوصية الموحدة للجمعية الدولية لشركات التصنيف (IACS) المتعلقة بمواجهة السفن للتهديدات السيبرانية (Recommendation on cyber resilience n°166, April 2022).

بالرجوع لتوصيات الجمعية الدولية لشركات التصنيف التي جاءت لتدعم توصيات المنظمة البحرية الدولية نجدها تؤكد بصفة عامة في المادة الأولى الفقرة الأولى البند 2 على ضرورة تجهيز السفن بحيث تكون قادرة على مواجهة التهديدات السيبرانية طيلة مدة خدمتها. مع التركيز على عامل الوقاية من الأخطار السيبرانية أكثر من علاج الأضرار الناتجة عنها لما لهذه الأضرار من تبعات.

كما تهدف هذه التوصية من خلال مجموعة من الإرشادات إلى تبيان كيفية التخفيف من الأضرار التي تخلفها الهجمات السيبرانية على أنظمة السفينة، والذي قد يمتد أثرها ليمس بسلامة الطاقم البشري والبيئة البحرية، بالإضافة إلى حثها على ضمان التشغيل الآمن للأنظمة المعلوماتية من خلال الصيانة وتوفير وسائل الحماية لسد الطريق أمام أي دخول غير مصرح به للمعلومات أو إساءة استخدامها، أو التعديل فيها، أو تدميرها، أو تسريب هاته المعلومات المستخدمة سواء كانت مخزنة في النظام المعلوماتي للسفن، أو المتداولة عبر الشبكات، وهذا وفقا لنص المادة الأولى الفقرة الأولى البند 3 و البند 4.

3.2 - تعديل الإرشادات التوجيهية للمنظمة البحرية الدولية لسنة 2022:

أما التعديل الثاني للمبادئ التوجيهية المتعلقة بالأمن السيبراني في المجال البحري فقد صدر بتاريخ 07 جوان 2022 (Guidelines on maritime cyber risk management, 7 June 2022)، وقد طال التعديل المادة 4 الفقرة 2 فقط، وذلك بإضافة البند 5 إليها والذي يحيل إلى العمل بإرشادات الاتحاد الدولي للموانئ والمرافئ. (IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2 July 2021)

بالرجوع لمضمون هذه الإرشادات، نجدها جاءت لإرساء خطة متكاملة لمواجهة التهديدات السيبرانية عن طريق حزمة من التوصيات، بدءا بإبراز حجم التهديدات السيبرانية والأضرار التي يمكن أن تسببها لقطاع النقل البحري التجاري، مع التأكيد على جميع المتدخلين في النشاطات المينائية بضرورة وضع استراتيجيات لمواجهة الأخطار السيبرانية من خلال التوعية وتخصيص ميزانية لتمويل مشاريع الأمن السيبراني. وصولا إلى التركيز على تطوير استراتيجيات قيادية لتعزيز الأمن من خلال تكوين كفاءات متخصصة في المجال ضمن منظومة الموانئ.

بدورها المبادئ التوجيهية لسنة 2023 التي جاءت لاستحداث الشباك الموحد، أكدت على ضرورة الاستجابة للتوصيات المتعلقة بالأمن السيبراني التي جاءت بها المبادئ التوجيهية السابقة، وذلك في المادة 6 الفقرة 9. (Guidelines for setting up a maritime single window, 31 March 2023)

4.2 - تعديل الإرشادات التوجيهية للمنظمة البحرية الدولية لسنة 2025 :

بتاريخ 04 أبريل 2025، أصدرت المنظمة البحرية الدولية آخر تعديل للمبادئ التوجيهية (Guidelines on maritime cyber risk management, 5 Avril 2025). وقد تميزت هذه النسخة بالتوسع أكثر في المبادئ الخمس التي جاءت بها المبادئ التوجيهية لسنة 2017، وهي: التحديد، الحماية، الكشف، الاستجابة والتعافي، مع إضافة مبدأ جديد على رأس هذه المبادئ وهو مبدأ الإدارة.

فمبدأ الإدارة يقضي بضرورة وضع الإستراتيجيات والخطط اللازمة لإدارة المخاطر السيبرانية المتوقعة، وهذه الخطوة لا تتحقق إلا بتحديد الأدوار والمسؤوليات المنوطة بالموظفين العاملين في هذا المجال على مستوى إدارة المنشآت المينائية والسفن. هؤلاء الموظفين يكون اختيارهم على أساس الكفاءة والخبرة، مع ضرورة تزويدهم بكل الصلاحيات والإمكانات اللازمة لإدارة هذه المخاطر، وهذا طبقا للبند الأول من المادة 3 الفقرة 5.

أما مبدأ التحديد فيقوم على أساس رصد التهديدات السيبرانية التي يمكن أن تتعرض لها المنشآت المينائية والسفن على حد سواء، ويكون ذلك باتباع مجموعة من الخطوات، تبدأ بتحديد وجرّد الأنظمة والبيانات والخدمات والشبكات التي قد تكون عرضة لمخاطر سيبرانية، ويؤدي تعطّلها إلى مخاطر على نشاط السفن وسلامة الإنسان والبيئة، بما في ذلك سلسلة توريد الأجهزة والبرامج، تأتي بعد ذلك مرحلة تقييم هذه المخاطر المحتمل وقوعها وتأثيرها على أنظمة السفينة وخدماتها، بالإضافة إلى الكشف المستمر عن نقاط الضعف في الأنظمة المختلفة للسفينة، وهذا وفقا لما جاء به البند 2 من المادة 3 الفقرة 5.

أما المبدأ الثالث وهو الحماية، فيقوم على اتخاذ كل أنواع التدابير اللازمة لحماية الأنظمة المعلوماتية من الحوادث السيبرانية ضمانا لاستمرارية أعمال الشحن وسلامة الإنسان والسفن والبيئة، وتعتمد هذه التوصية في سبيل تحقيق هذا المبدأ على مجموعة من الأسس تبدأ بالتحكم في حسابات الدخول إلى الأنظمة المعلوماتية عن طريق فصل حسابات المستخدمين العاديين عن الذين لديهم امتيازات، مع إلغاء تنشيط حسابات المستخدمين المنتهية فترة خدمتهم. بالإضافة إلى ذلك تغيير كلمات المرور التلقائية بكلمات مرور قوية، ووضع تدابير أخرى لإدارة التحكم في الوصول لحسابات المستخدمين للحماية من الهجمات السيبرانية التي تستعمل أساليب مختلفة.

فضلا عما سبق، يقوم مبدأ الحماية على التقليل من استخدام شبكة الإنترنت مع التحقق من البرامج وتخزين البيانات على الوسائط الموجودة على السفن بشكل

آمن، والصيانة الدورية لأنظمة المعلومات والشبكات ومعالجة الثغرات الأمنية فيها، دون إهمال للعامل البشري الذي يعد محور أي سياسة أمنية في هذا المجال، حيث تؤكد التوصية في هذا المبدأ على إخضاع المستخدمين لتكوين سنوي في مجال الأمن السيبراني وتدريب خاص بتكنولوجيا أنظمة التشغيل، بالإضافة للاحتفاظ بنسخ احتياطية للبيانات والأنظمة للاستجابة للحوادث وصيانتها، وهذا ما نص عليه البند 3 من المادة 3 الفقرة 5.

إضافة لما جاء في مبادئ سنة 2017، فإن مبدأ الكشف طبقا لتعديل سنة 2025 يركز كذلك على الاحتفاظ بسجلات الهجمات السيبرانية ذات الصلة بالنشاط البحري، وكذا طرق تدخل الجهات الفاعلة في معالجة هذا النوع من التهديدات، مع التأكيد على إخضاع المستخدمين لدورات تكوينية تتضمن أساليب الكشف عن التهديدات السيبرانية، وهذا طبقا للبند 4 من المادة 3 الفقرة 5.

أما فيما يخص مبدأ الاستجابة، فقد أضافت توصيات 2025 عنصريين أساسيين، الأول يكمن في ضرورة التبليغ عن المخاطر السيبرانية في الآجال الزمنية المحددة للإدارة المسؤولة عن معالجة المخاطر. أما الثاني فيقضي بوضع سجلات خاصة بالحوادث السيبرانية قصد تحليلها، والعودة لها عند اللزوم، هذا بالإضافة إلى تكوين المستخدمين دوريا في مجال الاستجابة للحوادث السيبرانية، وهذا وفقا للبند 5 من المادة 3 الفقرة 5.

يأتي في الأخير مبدأ التعافي، الذي يهدف إلى استعادة الأنظمة المعلوماتية على متن السفينة وكل النشاطات المرتبطة بها المتأثرة بحادث إلكتروني. ولا يتأتى ذلك إلا عن طريق تطوير استراتيجيات لاستعادة تشغيل الأنظمة الأساسية، إلى جانب ذلك وجب إجراء تحليل دقيق للوصول للسبب الحقيقي وراء الحوادث السيبرانية والعمل على سد الثغرات لمنع تكرار مثل تلك الحوادث، دون إهمال لعامل التكوين لإكساب المستخدمين في المجال مهارات إعادة العافية للأنظمة المعلوماتية للسفن، وهذا ما جاء به البند 6 من المادة 3 الفقرة 5.



تجدر الإشارة في نهاية هذا المحور، أن المنظمة البحرية الدولية في كل مبادئها التوجيهية المتعلقة بالأمن السيبراني أكدت في المادة 4 على الدول الأعضاء ضرورة إطلاع جهاتها المعنية بمضمون هذه المبادئ.

3- الإطار التشريعي الجزائري لاستغلال الأمن السيبراني في تأمين النشاطات البحرية:

لم يختص المشرع الجزائري الأمن السيبراني في تأمين النشاطات البحرية التجارية بنص تشريعي خاص، فيما عدا بعض النصوص المتفرقة التي تطرقت لمسألة تأمين البيانات بمناسبة تنظيمها للتحويل الرقمي بصفة عامة والتحول الرقمي في قطاع الموانئ بصفة خاصة.

1.3 - القانون رقم 04-09:

لقد أسند هذا النص التشريعي (القانون رقم 04-09 ، 2009) مهمة الوقاية من الجرائم المعلوماتية هي مسؤولية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك عن طريق التنسيق مع السلطات القضائية والشرطة القضائية، كما وسع من اختصاص هذه الهيئة لتمتد مهامها خارج الوطن لتبادل المعلومات مع الجهات المختصة في الخارج للتعرف على مرتكبي الجرائم المقيمين في هذه الدول، سواء تعلق الأمر بالجرائم الماسة بالإفراد أو المؤسسات الوطنية بمختلف فروعها بما فيها الاقتصادية، وهذا طبقا لنص المادة 14 و 15.

2.3 - القانون رقم 04-18:

لقد نصت المادة 4 الفقرة 2 من القانون 04-18 (القانون رقم 04-18، 2018)، على أن أمن وسلامة شبكات الاتصالات مسؤولية الدولة، وفي مقابل ذلك شدد هذا القانون في المادة 13 الفقرة 15 على متعاملي البريد والاتصالات الإلكترونية احترام الأحكام القانونية التنظيمية المتعلقة أساسا بالأمن السيبراني، لضمان خصوصية البيانات والمعلومات التي يتم تبادلها عن طريق شبكات الاتصالات، مع

حماية الحياة الخاصة للمشاركين والبيانات ذات الطابع الشخصي، طبقا لنص المادة 97 الفقرة 2 و 3.

3.3 - المرسوم التنفيذي رقم 147-21 :

لقد جاء هذا المرسوم (المرسوم التنفيذي رقم 147-21، 2021) لوضع نظام المجتمع المينائي في الجزائر (APCS) وطريقة سيره، هذا النظام يعد امتدادا لأنظمة مجتمع الموانئ في العالم. ويعرف على أنه منصة إلكترونية محايدة ومفتوحة تضمن التبادل الآلي والأمن للمعلومات بين مختلف المتدخلين في النشاط البحري التجاري سواء كانوا من القطاع أو الخاص، وذلك من أجل الرفع من الكفاءة والوضع التنافسي لمجتمع الموانئ البحرية (أبركان و حوباد، 2024، صفحة 138).

ويعد هذا النظام أحد ثمار التحول الرقمي في الجزائر، والذي استهدفت من ورائه الاندماج في المجتمع المينائي الدولي عن طريق ربط قواعد بياناتها وأنظمة معلوماتها بباقي الموانئ لتسهيل الإجراءات الإدارية وتبسيط العمليات اللوجستية ومراقبة وتتبع البضائع من خلال التدفق الدائم للمعلومات المتعلقة بها، كل ذلك تحقيقا للشفافية والتكامل والسلاسة في النشاطات التجارية البحرية.

من منطلق كون هذا النظام هو نظام رقمي بحت، كان لابد على المشرع الجزائري في هذا المرسوم النص صراحة على إخضاع هذا النظام لقواعد الأمن السيبراني، حيث نصت المادة 6 من المرسوم على ضمان المنصة سرية و أمن المعلومات والبيانات المجمعة والمتبادلة، أما المادة 7 فقد أسندت هذه المهمة للسلطة المينائية باعتبارها المتحكم الوحيد في هذه المنصة الالكترونية.

بالإضافة لما سبق، فإن المادة 20 من المرسوم 147-21 أحالت تدابير حماية البيانات ذات الطابع الشخصي التي يتم جمعها وتبادلها عن طريق نظام المجتمع المينائي الجزائري إلى القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي (القانون رقم 07-18، 2018).

من خلال استقراءنا لهذا النص نجد أنه في الكثير من المواضع يشدد على حماية البيانات ذات الطابع الشخصي، فعلى سبيل المثال لا الحصر تفرض المادة 38 على



المسؤول عن معالجة هذه البيانات وضع التدابير التقنية والتنظيمية لضمان سلامتها من المخاطر التي ترتبط بالمعالجة، وكذا المادة 32. الخاتمة :

في نهاية هذه القراءة لمختلف المبادئ التي جاءت بها المنظمة البحرية الدولية، يتضح لنا جليا الاستشعار المبكر للمجتمع البحري بخطورة التهديدات السيبرانية على كل مكونات النشاط البحري التجاري من سفن ومنشآت مينائية وإنسان وبيئة، وقد ترجم هذا الاستشعار إلى حزمة من الحلول القانونية والتقنية المتكاملة، والتي أحالت بدورها لتوصيات أخرى تتعلق بتصنيف السفن من خلال تأهيلها لجعلها قادرة على مواجهة المخاطر السيبرانية، نفس القول ينطبق على الإتحاد الدولي للموانئ والمرافئ التي خصص توصية كاملة لمواجهة التهديدات الإلكترونية التي قد تطال المنشآت المينائية.

أما في الجزائر، فرغم توجه قطاع النقل البحري التجاري بقوة نحو التحول الرقمي على غرار باقي الدول ، فإننا لا نجد نصوصا تشريعية خاصة تؤسس للأمن السيبراني لحماية هذا القطاع الاقتصادي الحيوي من التهديدات. من هذا المنطلق وجب على المشرع الجزائري تدارك هذا القصور من خلال سن نصوص تشريعية هدفها تأمين النشاطات البحرية التجارية من المخاطر السيبرانية، سواء كانت هذه النصوص متصلة بتلك المنظمة للنقل البحري التجاري على غرار القانون البحري، أو منفصلة عنه. مع ضرورة إشراك كل الفاعلين في مجال النقل البحري وخبراء الأمن سيبراني أثناء التحضير لهذه النصوص القانونية، ضمانا لنجاحها في مواجهة هذه المخاطر.

قائمة المصادر والمراجع :

أولاً- المراجع باللغة العربية:

1. النصوص القانونية:

أ- القانون رقم 04-09 . (المؤرخ في 5 أوت 2009). المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها، الجريدة الرسمية العدد47، المؤرخة في 16 أوت 2009.

ب- القانون رقم 04-18 . (مؤرخ في 10 ماي 2018). المتضمن القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، الجريدة الرسمية العدد 27 المؤرخة في 13 ماي 2018.

ت- القانون رقم 07-18 . (المؤرخ 10 جوان 2018). المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر العدد 34، المؤرخة في 10 جوان 2018.

ث- المرسوم 510-83 . (المؤرخ في 27 أوت 1983). المتضمن المصادقة على الاتفاقية الدولية لسلامة الأرواح في البحر (SOLAS)، الجريدة الرسمية العدد 36، المؤرخة في 30 أوت 1983.

ج- المرسوم التنفيذي رقم 21-147 . (المؤرخ في 14 أفريل 2021). المتضمن وضع منصة المجتمع المينائي لتبادل البيانات الرقمية، الجريدة الرسمية العدد 31، المؤرخة في 27 أفريل 2021.

2. المؤلفات:

أ- جبور منى الأشقر. (دون سنة نشر). السيرانية هاجس العصر. المركز العربي للبحوث القانونية.

3. المقالات العلمية:

أ-عبدالعظيم محمد عبدالجواد، أميرة . (2020). المخاطر السيرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون، المجلد 3، العدد5.

ب- أبركان، عبدالمالك و حوباد، حياة . (2024). دور نظام المجتمع المينائي الجزائري في تطوير قطاع النقل البحري للبضائع. مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 2.

ت- لمحة عامة عن الأمن السيراني. (أفريل، 2008). التوصية 1205، الاتحاد الدولي للاتصالات.

4. ملتقيات علمية:

أ- إكرام، بركان و فهميم، رملي. (14-13 فيفري، 2024). واقع وإشكالات الأمن السيراني في الجزائر. ورقة بحثية مقدمة للمؤتمر العلمي تحقيق أهداف الأمن الشامل والتنمية المستدامة. جامعة صالح بونيدر-قسنطينة3.



5. مواقع إلكترونية:

أ- قره فارس. (28, 08, 2019). الأمن السيبراني. تاريخ الاسترداد 19 سبتمبر, 2025, من الموسوعة السياسية:

<https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A>

ثانيا- المراجع باللغة الأجنبية:

1. Lehto, m., & Neittaanmaki, P. (2015). cyber security: Analytics, Technology and Automation. Switzerland: Spring international publishing.
2. Norbert, W. (1985). CYBERNETIC: or control and communication in the animal and machine. United State of America.
3. AVENAS, P. (2019, decembre). Robotique et intelligence artificielle. Consulté le septembre 19, 2025, sur Magazine jaune rouge: <https://www.lajauneetlarouge.com/robotique/>
4. Guidelines on maritime cyber risk management, 5 July 2017. (n.d.). from: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf>
5. Guidelines on maritime cyber risk management, 14 june 2021. (n.d.). Retrieved septembre 20, 2025, from: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf>
6. IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2 july 2021. (n.d.). Retrieved from: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/IAPH%20Cybersecurity%20Guidelines%20for%20Ports%20and%20Port%20Facilities%20v1.pdf>
7. Guidelines on maritime cyber risk management, 7 June 2022. (n.d.). Retrieved from: [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\)%20\(1\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf)
8. Guidelines for setting up a maritime single window, 31 march 2023. (n.d.).
9. Guidelines on maritime cyber risk management, 5 Avril 2025. (n.d.). Retrieved from: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf>
10. Règlement européenne 2019-881 17). Avril, 2019.
11. Recommendation on cyber resilience n°166, April 2022. (n.d.).
12. Loi n°2024-449 .(2024, mai 24). visant à sécuriser et à réguler l'espace numérique, JORF n°117 du 22 mai 2024.