الذكاء الاصطناعي والفضاء السيبراني
(رؤية قانونية للتحديات والمسؤولية الدولية)

ريم صالح عبيد الزبن

DOI:10.15849/ZJJLS.250330.05

قانون دولي عام . **تاريخ استلام البحث:11/05/2025**
تاريخ قبول البحث: 11/05/2025

* للمراسلة:reemalzaben51@yahoo.com

الملخص

يتناول البحث التحديات القانونية التي يفرضها الاستخدام المتزايد للذكاء الاصطناعي في الفضاء السيبراني، خصوصاً فيما يتعلق بالمسؤولية الدولية عن الجرائم السيبرانية، ودراسة الإطار القانوني لهذه الظاهرة، والإشكاليات المرتبطة بتحديد المسؤولية، والقصور في النصوص القانونية القائمة، كما استعرضت الجهود الدولية والمبادرات الوطنية لمواجهة هذه التحديات مع إيلاء اهتمام خاص بالتجربة الأردنية، وقد اعتمد البحث على المنهج التحليلي والوصفي في دراسة النصوص القانونية ذات الصلة، إلى جانب المنهج المقارن لعرض أوجه التشابه والاختلاف في التشريعات الدولية والوطنية، وقد خلص البحث إلى وجود فراغ قانوني دولي واضح فيما يتعلق بتنظيم الفضاء السيبراني، ما أدى إلى تعدد التوجهات واختلاف التشريعات الوطنية، ما يقضي التوصية بإنشاء هيئة دولية متخصصة تعنى بمتابعة الجرائم السيبرانية وتنظيم استخدام الذكاء الاصطناعي، بما يحقق التوازن بين حماية الأمن القومي وضمان احترام حقوق الإنسان، وتطوير قواعد القانون الدولي لمواكبة التطورات التكنولوجية وضبط استخدام الذكاء الاصطناعي في الفضاء السيبراني، بما يضمن توفير حماية فعالة ويحد من الانتهاكات السيبرانية.

الكلمات الدالة: الذكاء الاصطناعي، الفضاء السيبراني، المسؤولية الدولية، الجرائم السيبرانية، القانون الدولي حماية البيانات، الأمن السيبراني، التشريعات الوطنية والدولية، التنظيم القانوني للتكنولوجيا، حقوق الإنسان الرقمية.

Artificial Intelligence and Cyberspace
(A Legal Vision for Challenges and International Responsibility)

Reem Saleh Obaid Al-Zaben

Public International Law , Jordan.

Recived:05/112025

Accepted:05/11/2025

*** Crossponding author:** reemalzaben51@yahoo.com

Abstract

This study addresses the legal challenges posed by the increasing use of artificial intelligence in cyberspace, particularly regarding international responsibility for cybercrimes. It examines the legal framework governing this phenomenon and explores the complexities related to the attribution of responsibility and the shortcomings of existing legal provisions. The research also reviews international efforts and national initiatives to confront these challenges, with special emphasis on the Jordanian experience. The study adopts both analytical and descriptive methodologies to examine relevant legal texts, in addition to a comparative approach to highlight similarities and differences in international and national legislation. The findings reveal a clear international legal vacuum concerning the regulation of cyberspace, resulting in divergent approaches and inconsistent national legislations. Accordingly, the study recommends the establishment of a specialized international body to oversee cybercrime and regulate the use of artificial intelligence, aiming to strike a balance between national security protection and the safeguarding of human rights. Furthermore, it calls for the development of international legal norms to keep pace with technological advancements and to ensure the responsible use of artificial intelligence in cyberspace, thereby providing effective protection and limiting cyber violations.

Keywords: Artificial Intelligence, Cyberspace, International Responsibility, Cybercrimes, International Law, Data Protection, Cybersecurity, National and International Legislation, Legal Regulation of Technology, Digital Human Rights.

المقدمة:

شهد العالم في العقود الأخيرة تطوراً تكنولوجياً هائلاً، أدى إلى تحولات جذرية في مختلف المجالات الاقتصادية والاجتماعية والسياسية، وقد برز الذكاء الاصطناعي كأحد أهم هذه الابتكارات التكنولوجية، حيث أصبح يشكل عنصـــراً رئيســـياً في تطوير الأنظمة الحديثة، لما يمتلكه من قدرات تحليلية فائقة وإمكانيات هائلة في معالجة البيانات واتخاذ القرارات بشـــكل ســـريع ودقيق، ولعل من أبرز المجالات التي اســـتفادت من تقنيات الذكاء الاصطناعي، مجال الأمن السيبراني الذي يعد ركيزة أساسية لحماية الفضاء الرقمي وضمان سلامة المعلومات وحماية الخصوصية.

و مع تزايد الاعتماد على البنية الرقمية وتوسع استخدام الإنترنت والخدمات الإلكترونية، ازدادت التهديدات والهجمات السيبرانية بشكل غير مسبوق، مما جعل من الضروري تطوير حلول مبتكرة وفعالة للتصدي لها، وفي هذا الســياق ظهر الذكاء الاصــطناعي كأداة واعدة تســاعد في الكشــف المبكر عن التهديدات وتحليل ســلوك المستخدمين والتنبؤ بالهجمات المحتملة، مما يعزز قدرات الدفاع الرقمي ويقلل من زمن الاستجابة لها.

إلا أن توظيف الذكاء الاصـــطناعي في الأمن الســـيبراني يثير في المقابل العديد من التحديات القانونية والأخلاقية والتقنية، إذ تظهر تساؤلات معقدة حول حدود المسؤولية القانونية عند وقوع الهجمات أو فشل الأنظمة الذكية في منعها، فضــلاً عن المخاوف المتعلقة بالخصــوصــية وحماية البيانات، واحتمال إســاءة اســتخدام هذه التقنيات من قبل جهات معادية لتحقيق أهداف إجرامية أو تخريبية.

ويضـاف إلى ذلك التحديات المرتبطة بسـرعة تطور تقنيات الذكاء الاصـطناعي، مما يفرض على التشـريعات المحلية والدولية ضـرورة التكيف المسـتمر ومراجعة القوانين والسـياسـات لضـمان مواكبة هذه المسـتجدات وحماية الأفراد والمؤسسات من المخاطر المحتملة.

من هنا، تبرز أهمية هذا البحث الذي يسـعى إلى دراسـة العلاقة بين الذكاء الاصـطناعي والأمن السـيبراني، وتحليل الأدوار التي يمكن أن يؤديها الذكاء الاصـــطناعي في دعم اســـتراتيجيات الحماية الرقمية، إضـــافة إلى اسـتعراض التحديات التي تواجه تطبيقه، واسـتكشـاف الفرص التي يوفرها لتعزيز الأمن السـيبراني على المسـتويين الوطني والدولي.

كما يهدف البحث إلى تقديم توصيات عملية وقانونية تساعد في وضع إطار متكامل ينظم استخدام تقنيات الذكاء الاصطناعي بشكل يضمن تحقيق أقصى درجات الأمان الرقمي، مع احترام الحقوق والحريات الأساسية للأفراد.

مشكلة الدراسة:

تتمثل مشكلة هذه الدراسة في التساؤل حول مدى إمكانية إسناد المسؤولية القانونية عن الأفعال السيبرانية التي تنفذها أو تشارك في تنفيذها أنظمة الذكاء الاصطناعي، وذلك في ضوء الإطار التشريعي الأردني الحالي وأحكام القانون الدولي.

وتنبع هذه الإشكالية من ضرورة تحديد الجهة أو الأطراف التي يمكن تحميلها هذه المسؤولية، سواء كانت الشركات المطورة، أو المستخدمين، أو مزودي الخدمات، بما يضمن تحقيق العدالة القانونية ويواكب التطورات التكنولوجية الحديثة.

وتزداد أهمية هذه الإشكالية في ظل الاستخدام المتنامي لتقنيات الذكاء الاصطناعي في المجالات السيبرانية، بما يترتب عليه من مخاطر وتهديدات قانونية وأمنية عابرة للحدود، ومن هنا تبرز الحاجة الماسة إلى تطوير إطار قانوني دقيق وشامل يحدد المسؤولية ويوضح المعايير التي يمكن الاستناد إليها في مساءلة الأطراف المختلفة، كما تهدف الدراسة إلى الإسهام في سد الفجوة التشريعية القائمة، وتقديم توصيات عملية تسهم في تعزيز الحماية القانونية ومواكبة التطورات التقنية على المستويين الوطني والدولي.

أهمية الدراسة:

تبرز أهمية هذه الدراسة في التعامل مع فجوة واضحة في النصوص التشريعية الدولية والوطنية بشأن استخدام الذكاء الاصطناعي في الفضاء السيبراني، إذ لم تتناول معظم القوانين الحديثة مسؤولية الجهات الفاعلة عن الأفعال التي تنفذها أنظمة ذكية، مما يوجب الإضاءة على هذه الإشكالية من زاوية قانونية مقارنة.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

1-تحليل الإطار القانوني الدولي والوطني المرتبط بالذكاء الاصطناعي في الفضاء السيبراني.

2-تحديد أوجه القصور في تشريعات الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

3-دراسة تجارب دولية مختارة والاستفادة منها في تطوير الإطار التشريعي الأردني.

4-اقتراح آليات تشريعية لضمان مساءلة فعالة وحماية قانونية متكاملة.

الكلمات الافتتاحية:

-الذكاء الاصـطناعي: يقصـد به الأنظمة أو البرامج الحاسـوبية القادرة على محاكاة السـلوك البشـري، والتعلم، واتخاذ القرارات بشكل مستقل، بما يسهم في تنفيذ مهام معقدة دون تدخل بشري مباشر.

-الأمن السـيبراني: هو مجموعة الإجراءات والتدابير التقنية والتنظيمية والقانونية الهادفة إلى حماية الأنظمة الإلكترونية، والشبكات والبيانات من الهجمات أو التهديدات أو الاستخدامات غير المشروعة.

-الفضـاء السـيبراني: هو بيئة افتراضـية تنشـأ من تفاعل مسـتخدمي الإنترنت مع الشـبكات وأنظمة المعلومات، وتعتبر ساحة رئيسية للنشاطات الرقمية سواء المشروعة أو الإجرامية.

-الهجمات السـيبرانية: هي أفعال عدوانية تنفذ باسـتخدام تقنيات إلكترونية تسـتهدف إحداث ضـرر أو اختراق أو تدمير في الأنظمة والشبكات المعلوماتية.

أسئلة الدراسة:

1-ما أبرز التحديات القانونية التي تعيق مساءلة مستخدمي أو مطوري الذكاء الاصطناعي في المجال السيبراني؟

2-ما هي أوجه استخدام الذكاء الاصطناعي في الهجمات والدفاعات السيبرانية؟

3-كيف تعاملت التشريعات المقارنة مع قضايا المساءلة القانونية في هذا السياق؟

4-ما مدى كفاية القوانين الأردنية الحالية في التعامل مع الأفعال التي تصـــدر عن أنظمة الذكاء الاصطناعي؟

منهج الدراسة:

-المنهج التحليلي والوصـفي: تعتمد الدراسـة على هذا المنهج في تحليل واسـتعراض المفاهيم القانونية المرتبطة بالذكاء الاصطناعي والأمن السيبراني.

-المنهج المقارن: تعتمد الدراسة على هذا المنهج بدراسة نماذج من التشريعات الأجنبية المتقدمة ومقارنتها بالواقع التشريعي الأردني، بهدف تحديد نقاط القوة والقصور واقتراح تعديلات أو إضافات تشريعية مناسبة.

خطة الدراسة:

تقسيم هذه الدراسة ضمن مقدمة وثلاثة مباحث، وهما:

المبحث الأول: الإطار النظري والتقني للذكاء الاصطناعي والأمن السيبراني.

-المطلب الأول: تطور الذكاء الاصطناعي وتطبيقاته السيبرانية.

-المطلب الثاني: الأمن السيبراني في ظل الذكاء الاصطناعي(التحديات والفرص).

المبحث الثاني: التحديات القانونية في مواجهة الجرائم السيبرانية.

المطلب الأول: حدود المسؤولية الدولية في الجرائم السيبرانية.

المطلب الثاني: القصور التشريعي في مواجهة الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

المبحث الثالث: الجهود الدولية والوطنية في تقنين الفضاء السيبراني.

المطلب الأول: المبادرات الدولية لتنظيم الأمن السيبراني.

المطلب الثاني: الجهود التشريعية الأردنية في مواجهة التحديات السيبرانية.

الخاتمة: النتائج والتوصيات.

المبحث الأول

الإطار النظري والتقني للذكاء الاصطناعي والأمن السيبراني

مع التطور المتسارع في التقنيات الرقمية، بات من الضروري فهم الركائز النظرية التي يقوم عليها كل من الذكاء الاصـطناعي والأمن السـيبراني، باعتبارهما من أبرز مجالات التقاطع في العصـر الرقمي، إذ يمثل الذكاء الاصـطناعي أداة فعالة لتحسـين أداء الأنظمة، في حين يشـكل الأمن السـيبراني الدرع الواقي لتلك الأنظمة من التهديدات الرقمية، ويأتي هذا المبحث لتوضـيح المفاهيم الأسـاسـية لكلا المصـطلحين، وتحليل العلاقة المتبادلة بينهما في ضوء الاستخدامات الحديثة[1]

إن العلاقة المتبادلة بين الذكاء الاصـــطناعي والأمن الســـيبراني تمثل تحدياً مركزياً في الفكر القانوني المعاصر، إذ لم يعد العالم الرقمي مجرد مساحة للابتكار والتطوير، بل أصبح مساحة معقدة للصراع التكنولوجي والاقتصادي والسياسي.

ويكتسـب هذا الموضـوع حسـاسـية متزايدة نظراً لتأثيره المباشـر على السـيادة الوطنية، والقانون الدولي وحقوق الإنســـان، ولذلك تبرز الحاجة إلى تحليل الإطار النظري لهذين المفهومين، من حيث النشـــأة والتطور والتهديدات التي قد تنشـــأ عند تقاطعهما، تمهيداً لدراســـة الأبعاد القانونية والتنظيمية التي ســـيعالجها البحث في المباحث القادمة.[2]

ستقوم الباحثة بتقسيم هذا المبحث إلى مطلبين كالتالي:

-المطلب الأول: تطور الذكاء الاصطناعي وتطبيقاته السيبرانية.

-المطلب الثاني: الأمن السيبراني في ظل الذكاء الاصطناعي(التحديات والفرص)

[1] أبو العز، خالد(2021)، الأمن السيبراني في ظل الذكاء الاصطناعي، مجلة الدراسة الأمنية والقانونية، المجلد 6،العدد1، عمان- الأردن، ص 90 . 93.

[2] المرجع السابق، ص 94.

المطلب الأول

تطور الذكاء الاصطناعي وتطبيقاته السيبرانية

يعرف الذكاء الاصـــطناعي بأنه قدرة الآلات والبرامج على تنفيذ مهام تتطلب عادةً تدخلاً بشـــرياً، مثل التفكير والفهم واتخاذ القرار، وقد تطور هذا المفهوم منذ منتصـــف القرن العشـــرين، ومر بمراحل متعددة شـــملت الأنظمة الخبيرة وتعلم الآلة، والتعلم العميق، وصـــولاً إلى الأنظمة التنبؤية القادرة على التكيف مع المتغيرات دون تدخل بشري مباشر.[1]

أصـبح الذكاء الاصـطناعي اليوم جزءاً أسـاسـياً في العديد من التطبيقات مثل الأمن والصـناعة والتعليم والطب والخدمات الحكومية، هذا التوســـع في الاســـتخدام عزز الحاجة لفهم الأطر القانونية والتنظيمية التي تضبطه، خصوصاً في سياقات تمس الحقوق والحريات.[2]

يعد الذكاء الاصـــطناعي من أبرز مخرجات الثورة الرقمية، وقد تجاوز في قدراته المفهوم التقليدي للبرمجيات الحاسـوبية، فهو لا يعتمد فقط على التعليمات المسـبقة، بل على تحليل البيانات والتعلم المسـتمر ما يتيح له التكيف مع المواقف المستجدة واتخاذ قرارات مستقلة، ويعتمد الذكاء الاصطناعي على خوارزميات متقدمة أهمها خوارزميات التعلم العميق، التي تحاكي عمل الدماغ البشري في معالجة المعلومات.[3]

ومن أبرز تطبيقات الذكاء الاصطناعي في السياق السيبراني ما يلي:

1-التنبؤ بالتهديدات الأمنية: من خلال تحليل البيانات السابقة وتحديد أنماط الهجمات.

2-أنظمة الدفاع الذكية: مثل أنظمة تحليل سلوك المستخدم للكشف عن الدخول غير المشروع.

3-أتمتة إدارة الأزمات السيبرانية: باتخاذ قرارات استجابة سريعة دون تدخل بشري مباشر.

---

[1] محمد، فايز(2020) الذكاء الاصطناعي ومستقبل الإنسان، ط1 دار الفكر العربي، مصر ص 41-44.

[2] العتيبي، عبد العزيز(2022) " تطبيقات الذكاء الاصطناعي وتحدياتها في العالم العربي"، مجلة جامعة نايف للعلوم الأمنية، المجلد 41، العدد2، ص 130-132. Russell,s,Norvig,P.(2020)Artifial lntelligence:A Modern Approach. 4 th ed. Pearson,pp.15-20.

[3] محمد، فايز(2020) الذكاء الاصطناعي ومستقبل الإنسان، مرجع سابق، ص 45.

ومع ذلك فإن نفس هذه القدرات يمكن اســتغلالها في تطوير هجمات ســيبرانية ذكية، عبر توليد برمجيات خبيثة قادرة على التكيف، أو تجاوز جدران الحماية من خلال" الهندســة الاجتماعية الذكية"، مما يزيد من خطورة هذا المجال ويخلق ثغرات قانونية وأخلاقية حادة.[1]

ترى الباحثة أنه وحتى هذه اللحظة لا يوجد إطار قانوني دولي موحد ينظم اســتخدام الذكاء الاصــطناعي في المجال الأمني أو العسكري، وهو ما يشكل فراغاً تشريعياً كبيراً قد يؤدي إلى فوضى قانونية على الصعيد الدولي.

المطلب الثاني

الأمن السيبراني في ظل الذكاء الاصطناعي(التحديات والفرص)

إن الأمن الســيبراني هو مجموعة من العمليات والســياســات والأدوات التقنية المصــممة لحماية الأنظمة الرقمية، والمعلومات والشبكات من الوصول غير المصرح به، أو التلاعب أو التدمير أو السرقة، ويعد اليوم أحد أبرز القضايا التي تواجه الدول والمنظمات، نظراً لتزايد الاعتماد على التكنولوجيا في مختلف القطاعات.

أصبحت تقنيات الذكاء الاصطناعي شريكاً أساسياً في مجال الأمن السيبراني، من خلال تطوير أنظمة قادرة على كشــف التهديدات وتحليل ســلوك المســتخدمين واســتباق الهجمات، وهو ما يوفر وقتاً وجهداً كبيراً في عملية الحماية، وفي المقابل فإن استخدام الذكاء الاصطناعي من قبل الجهات المهاجمة شكل تحدياً جديداً يتمثل في الهجمات الذكية التي يصعب التنبؤ بها أو التصدي لها بالوسائل التقليدية.[2]

تزايد الاعتماد على البنية التحتية الرقمية في المؤســســات الحســاســة، مثل القطاعات المالية والصــحية والدفاعية، دفع إلى تصاعد أهمية الأمن السيبراني، ليصبح مكوناً استراتيجياً في الأمن القومي للدول، ومع إدخال الذكاء الاصطناعي في هذا المجال نشأت فرص عظيمة، كما ظهرت تحديات قانونية وتنظيمية غير مسبوقة.[3]

أولاً– التحديات:

---

[1] فتحي، ياسر،(2023)، الذكاء الاصطناعي والحوكمة العالمية، ط 1، مكتبة لبنان القانونية، بيروت، ص 88–95.
Bostrom,N.(2014).superintelligence:paths,Dangers,Strategies.Oxford University Press,UK,PP,127-139.

[2] الشمري، ناصر(2022)، مخاطر الفضاء السيبراني وسبل مواجهتها، ط1 الرياض، مركز الدراسات المستقبلية، ص 57–60.

[3] غانم، خالد.(2021)، السياسات الدفاعية في الفضاء السيبراني، ط1، دار الفكر القانوني، القاهرة، ص 117–123.

رغم التقدم الكبير في تقنيات الذكاء الاصـــطناعي وإمكانياته الواعدة في مجال الأمن الســـيبراني، إلا أن هذا التقدم لا يخلو من التحديات التي تهدد فعاليته وســـلامة تطبيقه، فقد أفرز الاعتماد المتزايد على الذكاء الاصطناعي مجموعة من الإشكاليات القانونية والتقنية، أبرزها ما يلي:-

1- المسـؤولية القانونية: يصـعب تحديد المسـؤولية القانونية في حال وقوع أخطاء أو أضـرار ناتجة عن قرارات اتخذتها أنظمة الذكاء الاصـــطناعي، نظراً لاســـتقلالية هذه الأنظمة في التحليل واتخاذ الإجراءات، وهذا يثير تساؤلات حول من يتحمل المسؤولية، هل هو المطور، أم المبرمج، أم المستخدم النهائي؟

2-قابلية التفسير والشفافية: تعتمد خوارزميات الذكاء الاصطناعي على نماذج معقدة قد تكون غير مفهومة بشكل كامل حتى لمطوريها، مما يؤدي إلى صعوبة الجهات القضائية أو الرقابية.

3-الخصـوصـية وحماية البيانات: يتطلب تشـغيل تقنيات الذكاء الاصـطناعي في الأمن السـيبراني جمع ومعالجة كميات ضخمة من البيانات، مما قد يعرض خصوصية الأفراد والمؤسسات للخطر إذا لم يتم وضع ضوابط قانونية صارمة تكفل حماية هذه البيانات.

4-الأمن والثغرات التقنية: قد يستغل المهاجمون الثغرات الموجودة في خوارزميات الذكاء الاصطناعي، مما يجعل النظام ذاته هدفاً للهجمات الإلكترونية، ويؤدي إلى مضاعفة المخاطر بدلاً من تقليلها.([1])

ثانياً- الفرص:

في مقابل التحديات التي يفرضها الذكاء الاصطناعي في ميدان الأمن السيبراني، تبرز فرص واعدة يمكن أن تحدث تحولاً جذرياً في طرق الحماية والدفاع الرقمي، وأهم هذه الفرص:

1-الكشـــف المبكر عن التهديدات: يمكن للذكاء الاصـــطناعي تحليل كميات هائلة من البيانات بشـــكل ســـريع واكتشاف الأنماط المشبوهة، مما يساعد في رصد التهديدات والهجمات قبل وقوعها، وتعزيز الوقاية الاستباقية.

2-الاســـتجابة التلقائية للحوادث: يتيح الذكاء الاصـــطناعي إمكانية بناء أنظمة قادرة على اتخاذ قرارات ســـريعة وفعالة للتصدي للهجمات الإلكترونية، وتقليل الأضرار الناتجة عنها بشكل كبير.

3- التكيف والتعلم المستمر: تتميز تقنيات الذكاء الاصطناعي بقدرتها على التعلم المستمر من الهجمات الجديدة، وتطوير استراتيجيات دفاعية متقدمة، مما يمنح الأنظمة مرونة أكبر في مواجهة المخاطر المستحدثة.

---

[1] الكويتي، محمد، .(2023)، الأمن السيبراني في عصر الذكاء الاصطناعي، مركز تريندز للبحوث والاستشارات، أبو ظبي، ط1، ص34-38.

4-تحسين كفاءة الموارد البشرية: يساعد الذكاء الاصطناعي في تخفيف العبء عن الفرق الأمنية، من خلال أتمتة المهام الروتينية المعقدة، وتمكين الخبراء من التركيز على القضايا الاستراتيجية والتخطيطية ذات الأولوية.[1]

ما زال القانون الدولي العام يواجه صعوبات في مواكبة التطورات التكنولوجية، إذ لا توجد معايير دولية ملزمة لتنظيم استخدام الذكاء الاصطناعي في الدفاع السيبراني(مثل اتفاقية بودابست) لا تتناول الذكاء الاصطناعي بشكل مباشر ما يتطلب مراجعة وتحديث الإطار القانوني.[2]

ترى الباحثة، أن التطور المتسارع في تقنيات الذكاء الاصطناعي وما يرافقه من توسع في الفضاء السيبراني يشكل في الوقت نفسه تحدياً وفرصة للمجتمع القانوني، فمن جهة تبرز تحديات قانونية كبيرة تتعلق بغياب إطار تشريعي واضح وشامل يحدد المسؤولية القانونية بدقة، خاصة في ظل الطبيعة غير المادية والمعقدة للأفعال السيبرانية، وتداخل المسؤوليات بين المطورين والمستخدمين والدول.

ومن جهة أخرى، أعتقد أن هذه التحديات تمثل فرصة ثمينة لدفع عجلة تطوير التشريعات الوطنية والدولية، وفتح آفاق جديدة أمام الفقه القانوني لتبني رؤى مبتكرة تتناسب مع واقع الذكاء الاصطناعي، إن صياغة إطار قانوني عادل وفعال سيعزز الثقة في هذه التقنيات، ويدعم استخدامها في تحقيق التنمية، مع ضمان احترام مبادىء العدالة وحماية الحقوق والحريات الأساسية.

لذلك، أرى أن من واجب الباحثين والمشرعين التعاون لإيجاد حلول قانونية عملية توازن بين تشجيع الابتكار وحماية المجتمع من المخاطر المحتملة.

---

(1) United Nations.(2021),Report of the Group of Governmental Experts on Advancing Responsile State Behavior in Cyberspace. New. York:UN Publications.

(2) Taddeo,M,&Floridi,L.(2018), "Regulate artificial intelligence to avert cyber arms.race". Nature, 556, 296-298

المبحث الثاني

التحديات القانونية في مواجهة الجرائم السيبرانية

شـهد العالم خلال العقدين الأخيرين تصـاعداً كبيراً في التهديدات المرتبطة بالفضـاء السـيبراني، الذي بات ساحة جديدة للصراعات العابرة للحدود بما في ذلك الهجمات الإلكترونية، والاختراقات التي تستهدف البنية التحتية الحيوية للدول، وبالرغم من أهمية هذه القضايا إلا أن القانون الدولي لم يواكب بشكل كاف حجم التحولات التقنية، ما أفرز حالة من الغموض القانوني فيما يتعلق بكيفية التعامل مع هذه الأفعال من منظور المسـؤولية القانونية الدولية.[1]

إن من أبرز الإشكاليات التي تثيرها الجرائم السيبرانية، عدم وضوح الأساس القانوني الذي يمكن الاستناد إليه لتحديد المسـؤولية الدولية للدول أو الجهات الفاعلة غير الحكومية، مثل الجماعات الإجرامية أو حتى الأفراد، ويضاف إلى ذلك صعوبة إثبات مصدر الهجمات ما يجعل مسألة النسب أو الإسناد القانوني للهجوم أمراً معقداً، ومن هنا يظهر تسـاؤل رئيسـي حول مدى قدرة القانون الدولي التقليدي وبخاصـة قواعد المسـؤولية الدولية، على الاستجابة للتطورات المرتبطة بالعالم الرقمي.[2]

وانطلاقاً من هذه التحديات، ستتناول الباحثة هذا المبحث ضمن مطلبين وهما:

المطلب الأول: حدود المسؤولية الدولية في الجرائم السيبرانية.

المطلب الثاني: القصور التشريعي في مواجهة الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

المطلب الأول

حدود المسؤولية الدولية في الجرائم السيبرانية

تشـــكل الجرائم الســـيبرانية تحدياً معقداً للنظام القانوني الدولي، حيث إنها غالباً ما تنفذ عبر الحدود وتستهدف البنية التحتية الحيوية للدول، مما يجعل مسألة تحديد المسؤولية الدولية أمراً في غاية الصعوبة، فغياب إطار قانوني دولي موحد يعالج هذه المسائل يضعف من قدرة الدول على ملاحقة الجناة أو مساءلتهم أمام المحاكم الوطنية أو الدولية.

---

[1] يوسف، خليل.(2019)، المسؤولية الدولية في ظل الجرائم الإلكترونية، دار الثقافة للنشر والتوزيع، الأردن، ط1، ص67-70.

[2] عطية، رامي.(2020)، القانون الدولي والفضاء السيبراني: دراسة تحليلية. دار الصفاء للنشر والتوزيع، الأردن، ط1، ص41-43.

وفي هذا السياق، تظهر الحاجة الماسة لتطوير القواعد القانونية الدولية التي تنظم العلاقة بين الدول في حالة حدوث هجمات سيبرانية، خاصة إذا كانت تلك الهجمات تدار أو تمول من كيانات تابعة لدول معينة، وتعد اتفاقية بودابســـت بشـــأن الجريمة الإلكترونية (2001) إحدى المحاولات الدولية المهمة إلا أنها لم تحظ بقبول عالمي، ولم تتناول بشكل كاف موضوع المسؤولية الدولية للدول عن الأفعال السيبرانية.[1]

من ناحية أخرى، فإن مبدأ " عدم التدخل في الشؤون الداخلية للدول" الذي يعد من المبادىء الراسخة في القانون الدولي، يثير تساؤلات حول ما إذا كانت الهجمات السيبرانية تعد خرقاً لهذا المبدأ، وخاصة إذا كانت تؤدي إلى شلل في أنظمة الاتصالات أو المرافق العامة في الدولة المستهدفة.[2]

ومع ذلك، تبقى مســـألة الإثبات والتتبع التقني لأصـــل الهجمات من أكبر المعوقات أمام تفعيل مبدأ المسؤولية الدولية، حيث تعتمد هذه الهجمات على تقنيات عالية في التمويه وتغيير الهويات الرقمية.[3]

المطلب الثاني

القصور التشريعي في مواجهة الجرائم السيبرانية المدعومة بالذكاء الاصطناعي

يعد الذكاء الاصطناعي (AI) من أبرز التحديات القانونية الحديثة في ميدان مكافحة الجرائم السيبرانية، إذ يضـفي بعداً تقنياً أكثر تعقيداً على هذه الجرائم، ويزيد من فجوة التكييف القانوني للوقائع الناشـئة عنها فمع تطور أدوات الذكاء الاصـطناعي أصـبحت الهجمات السـيبرانية أكثر تطوراً وأشـد فتكاً، مثل الهجمات التي تعتمد على خوارزميات تعلم الآلة للتعرف على الثغرات واستغلالها دون تدخل بشري مباشر.[4]

ورغم إدراك المشرعين في بعض الدول لخطورة هذه الجرائم، إلا أن معظم التشريعات العربية لا تزال تفتقر إلى نصـوص قانونية واضـحة تنظم هذا النوع من الأفعال، مما يخلق فراغاً تشـريعياً يمنع تحقيق العدالة، كما أن القوانين السارية لا تواكب طبيعة هذه الجرائم من حيث التعقيد والسرعة والإخفاء.[5]

---

[1] عبد العزيز،علي،(2020)، الجرائم الإلكترونية والمسؤولية الجنائية الدولية،ط1، دار الفكر الجامعي، القاهرة، ص 131.

[2] الغرايبة،خالد،(2022)، القانون الدولي العام وتحديات الفضاء السيبراني، ط1، دار الثقافة، عمان، ص 98.

[3] ياسين، محمد،(2021)، القانون الدولي وتكنولوجيا المعلومات، ط1، منشورات الحلبي الحقوقية، بيروت، ص 77.

[4] الزعبي، حسام،(2023)، الذكاء الاصطناعي والقانون الجنائي، ط1، دار وائل، عمان،ص 142.

[5] مراد، فاطمة،(2022)، الجرائم الإلكترونية في ضوء التشريع العربي المقارن، رسالة ماجستير، جامعة بيروت العربية، ص65.

كما أن الجدل لا يزال قائماً حول المسؤولية الجنائية للأشخاص الاعتباريين عند استخدامهم أنظمة الذكاء الاصطناعي لارتكاب الجرائم السيبرانية، حيث لم تحسم بعد مسألة ما إذا كانت هذه الأنظمة تعد أدوات أم شركاء في الجريمة، خصوصاً إذا تصرفت بطريقة غير متوقعة أو خارجة عن سيطرة مطورها.[1]

ترى الباحثة أن التحديات القانونية التي تواجه المجتمع الدولي في التصدي للجرائم السيبرانية ما تزال تتسم بالتعقيد والغموض، إذ إن غياب إطار قانوني موحد وشامل على المستوى الدولي إلى جانب التفاوت الكبير في القدرات التقنية والتشريعية بين الدول يؤدي إلى تفاقم تلك التحديات، كما أن تطور تقنيات الذكاء الاصطناعي يزيد من صعوبة تحديد المسؤولية الجنائية ويضع التشريعات التقليدية أمام اختبارات غير مسبوقة.

المبحث الثالث

الجهود الدولية والوطنية في تقنين الفضاء السيبراني

في ظل التطور المتسارع لتقنية الذكاء الاصطناعي وتزايد التهديدات السيبرانية، أصبحت الحاجة ملحة لإيجاد إطار قانوني شامل ومنظم للفضاء السيبراني يوازن بين حرية الاستخدام والمسؤولية القانونية، وقد ظهرت على الساحة جهود متعددة من جانب المنظمات الدولية والدول منفردة، لمحاولة ضبط هذا الفضاء ووضع قواعد تضمن أمنه وعدالته خصوصاً في ظل التهديدات المتزايدة من الهجمات السيبرانية، وتضارب المفاهيم حول السيادة الرقمية وحرية التعبير وحقوق المستخدمين، حيث ستتناول الباحثة في هذا المبحث الجهود الدولية المبذولة لتنظيم هذا الفضاء وكذلك تجربة الأردن في تقنينه كنموذج عربي يستحق الدراسة.[2]

وعليه سيتم تقسيم هذا المبحث إلى مطلبين كالتالي:

المطلب الأول: المبادرات الدولية لتنظيم الأمن السيبراني.

المطلب الثاني: الجهود التشريعية الأردنية في مواجهة التحديات السيبرانية.

---

[1] الكيلاني، ناديا،(2021)، الذكاء الاصطناعي والمسؤولية الجنائية،ط1،مكتبة الفلاح القانونية،الكويت، ص 93.

[2] –عبد العاطي، سامح،(2020)،القانون الدولي وأمن الفضاء السيبراني، دار الفكر الجامعي، الإسكندرية، ص33.

المطلب الأول

المبادرات الدولية لتنظيم الأمن السيبراني

تسـعى المنظمات الدولية والإقليمية إلى بلورة قواعد قانونية تتعامل مع خصـوصـية الفضـاء السـيبراني، وتضع معايير موحدة للتعامل مع الجرائم السيبرانية والهجمات الرقمية. تتمثل بالآتي:-

أولاً-جهود الأمم المتحدة: تعد الأمم المتحدة أحد أبرز الفاعلين في مجال تطوير المبادىء القانونية للفضـــاء الســـيبراني، وقد أنشـــأت ما يعرف ب(فريق الخبراء الحكوميين) الذي قدم عدة تقارير منذ عام 2010، تسـعى لتحديد قواعد السـلوك المسـؤولة للدول في الفضـاء السـيبراني، إلى جانب تأكيد احترام القانون الدولي الإنساني وميثاق الأمم المتحدة.

لكن هذه التقارير لم تتحول بعد إلى معاهدة دولية ملزمة، نتيجة غياب الإجماع بين القوى الكبرى، خصـوصـاً بسـبب الخلافات بين المعسـكر الغربي من جهة وروسـيا والصـين من جهة أخرى، حول مسـألة حرية الإنترنت ومراقبة المحتوى مما يعيق التوصل إلى اتفاق ملزم.[1]

ثانياً-اتفاقية بودابست للجرائم الإلكترونية: رغم أنها اتفاقية أوروبية إلا أنها أصبحت مرجعاً دولياً في مجال مكافحة الجرائم الإلكترونية، حيث تنص على تجريم الأفعال الســـيبرانية كالقرصـــنة، وتخريب البيانات والتحايل باستخدام الحاسوب، كما تقدم آليات للتعاون القضائي وتبادل المعلومات.

ومع ذلك، فإن غياب بعض الدول الكبرى عنها مثل روســيا والصــين حد من فاعليتها، كما واجهت انتقادات تتعلق بعدم مراعاتها خصوصية بعض الأنظمة القانونية في الدول النامية.[2]

ثالثاً- مبادرات الاتحاد الأوروبي: قام الاتحاد الأوروبي بإطلاق" اســـتراتيجية الأمن الســـيبراني" في عام 2013، وجرى تحديثها لاحقاً وتضـمنت خططاً لتعزيز البنية التحتية الرقمية، وزيادة التعاون بين الدول الأعضـاء

(1) - United Nations."Report Of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc A\75\816,2021,p.8.

(2) Council Of Europe."Convention on Cybercrime," Budapest, 2001,Articles 2-13.

وتأسيس وكالة ENISA للأمن السيبراني، كما أقر " قانون الأمن السيبراني الأوروبي" الذي دخل حيز التنفيذ عام 2019، ويدعو إلى تقييم مخاطر الأمن الرقمي بشكل دوري.[1]

رابعاً– تحديات التقنين الدولي: رغم الجهود والمبادرات الدولية المستمرة لتنظيم الأمن السيبراني، لا تزال عملية وضع إطار قانوني دولي شامل وفعال تواجه عدة تحديات معقدة، من أبرزها:

1–غياب اتفاق دولي موحد ينظم الأمن السيبراني بشكل شامل.

2–الطبيعة العابرة للحدود للهجمات السيبرانية، مما يعقد تحديد الاختصاص والمسؤولية.

3–صعوبة تحديد الفاعل المسؤول عن الهجمات، خصوصاً مع استخدام تقنيات الذكاء الاصطناعي.

4–تضارب المصالح بين الدول، حيث تستغل الفضاءات السيبرانية لتحقيق أهداف سياسية واستراتيجية.

5–سرعة التطور التكنولوجي، بما يخلق فجوة تشريعية مستمرة.[2]

ويتضح للباحثة من خلال هذا المطلب أن الجهود الدولية لا تزال في طور التطوير والتحديث لمواكبة التحديات المتسارعة في الفضاء السيبراني، ورغم التقدم الملحوظ في بعض المبادرات، إلا أن الحاجة تبقى ملحة لتعزيز التعاون الدولي، وسن تشريعات أكثر شمولية ومرونة تضمن حماية فعالة وتتصدى بجدية لمخاطر الذكاء الاصطناعي في المجال السيبراني.

المطلب الثاني

الجهود التشريعية الأردنية في مواجهة التحديات السيبرانية

في العالم العربي يعتبر الأردن من الدول السباقة في التصدي للجرائم الإلكترونية وتطوير تشريعات تواكب البيئة الرقمية، ذلك في إطار السعي لحماية الأمن الوطني السيبراني، حيث أدرك الأردن مبكرا خطورة التهديدات السيبرانية، وسعى إلى تطوير بنية تشريعية ومؤسسية قادرة على مواكبة هذا النوع الجديد من التحديات، بدءاً من إصدار قانون الجرائم الإلكترونية، وحتى تأسيس مركز وطني مختص بالأمن السيبراني.[3]

---

(1)– ENISA. "Cybersecurity Act", Regulation (EU) 2019\881,p.4.

(2) Kesan ,Jay P. et al. Cybersecurity and the Law: The Legal and Technical Landscape, Carolina Academic Press, USA,2019,P.115.

(3) بني سلامة، بسمة،(2021)، تحليل واقع الأمن السيبراني في الأردن، ط1، دار الحامد، عمان، ص 20.

1-قانون الجرائم الإلكترونية الأردني: صـــدر أول قانون للجرائم الإلكترونية في الأردن عام 2010، وتم تعديلة عام 2015، ثم أقر قانون جديد رقم 17 لسنة 2023، الذي يعتبر الأكثر شمولاً حتى الآن.[1]

يتضــمن القانون نصــوصــاً واضــحة تجرم :الاختراق غير المشــروع، ونشــر معلومات كاذبة والابتزاز الإلكتروني وخطاب الكراهية والتحريض.

وترى الباحثة أن هذا القانون يعد من أبرز أدوات الدولة في مكافحة الجريمة السـيبرانية، لكنه واجه أيضـاً انتقادات من قبل منظمات حقوق الإنسان بسبب ما اعتبر تقييداً لحرية التعبير، ويمنح سلطات موسعة للنيابة في الرقابة على المحتوى.

2- قانون الأمن السـيبراني الأردني رقم 16 لسـنة 2019: في سـياق التشـريعات الوطنية، صـدر هذا القانون بهدف حماية الفضـاء السيبراني الوطني، وتنظيم الإجراءات والسياسـات اللازمة لتعزيز الأمن السيبراني، وضمان استمرارية عمل الأنظمة والبنى التحتية الحيوية، والحد من المخاطر الناجمة عن الهجمات السيبرانية.

وقد نصت المادة(2) من القانون على مجموعة من التعريفات الرئيسية، من أبرزها:

-الأمن السـيبراني: هو الإجراءات المتخذة لحماية الأنظمة والشـبكات الإلكترونية ومكوناتها وبياناتها من أي اختراق أو هجوم أو تعطيل أو تعديل أو إتلاف أو دخول غير مشروع.

-الفضـاء السـيبراني: هو البيئة الافتراضـية الناتجة عن التفاعل بين مكونات الحوسـبة والاتصـالات والبرمجيات والإنترنت.

-الحادث السيبراني: هو أي حدث يؤدي أو قد يؤدي إلى الإضرار بالأمن السيبراني أو يؤثر في توافر أو موثوقية أو سرية البيانات أو الخدمات الإلكترونية.

إن هذا القانون لا يتضــمن نصــوصــاً مباشــرة لعقوبات جزائية بالتفصــيل مثل قانون الجرائم الإلكترونية، وإنما يركز على تنظيم البنية المؤسسية، وإنشاء المركز الوطني للأمن السيبراني ووضع السياسات العامة.

لكن وفقاً للقانون، للجهات المختصة صلاحيات فرض التدابير الإدارية مثل:

-وقف أي نشاط إلكتروني يشكل تهديداً للأمن السيبراني.

[1] الجريدة الرسمية الأردنية، قانون الجرائم الإلكترونية رقم 17 لسنة 2023، عمان- الأردن،ص4.

-اتخاذ الإجراءات اللازمة لمنع أو معالجة أي حادث سيبراني.

-إحالة المخالفات إلى الجهات القضائية المختصة في حال تبين وجود أفعال مجرمة بموجب قوانين أخرى، كقانون العقوبات أو قانون الجرائم الإلكترونية.[1]

ترى الباحثة أن هذا القانون محطة تشريعية هامة في مسار بناء منظومة الحماية السيبرانية الوطنية، إذ أسس لإطار مؤسسي منظم من خلال إنشاء المركز الوطني للأمن السيبراني وتحديد الأمن القومي الرقمي.

إلا أن تركيز القانون على الجوانب الإدارية والتنظيمية دون تضمين نصوص جزائية محددة يثير تساؤلات جوهرية حول مدى قدرته على تحقيق الردع الخاص والعام، خصوصاً في ظل تنامي الجرائم السيبرانية وتطور أدواتها، الأمر الذي يحد من فعاليته في الردع.

2-المركز الوطني للأمن السيبراني: أنشىء المركز الوطني للأمن السيبراني في الأردن عام 2020 ليكون الجهة الرسمية المسؤولة عن حماية البنية التحتية الرقمية، والتنسيق بين المؤسسات الأمنية والمدنية في حالة الهجمات السيبرانية.[2]

يعمل المركز على:-

-إعداد الاستراتيجية الوطنية للأمن السيبراني.

-بناء قدرات بشرية متخصصة.

-إصدار تحذيرات ومتابعة الحوادث الرقمية.

يسهم المركز في إعداد السياسات والاستراتيجيات الوطنية للأمن السيبراني، إلى جانب تدريب الكوادر المختصة والتعاون مع شركاء دوليين، وبناء شراكات مع القطاع الخاص والمؤسسات الدولية، مما يعكس توجه الأردن إلى الانخراط في المنظومة العالمية.[3]

3-التحديات التي تواجه الأردن: رغم هذه الجهود، لا تزال هناك تحديات كبيرة تقف في وجه الأردن أبرزها:

- نقص الكفاءات المتخصصة.

---

[1] راجع قانون الأمن السيبراني الأردني رقم 16 لسنة 2019.

[2] الموقع الرسمي للمركز الوطني للأمن السيبراني الأردني، تقرير الأداء السنوي 2022،ص6.

[3] وزارة الاقتصاد الرقمي والريادة، الاستراتيجية الوطنية للأمن السيبراني 2022-2025، عمان، ص9.

-محدودية التمويل المخصص لتقنيات الحماية.

-عدم تحديث مستمر للقوانين بما يواكب تطور التهديدات.[1]

وفي سياق متصل لجهود المملكة في مواجهة التهديدات السيبرانية، أعلنت دائرة المخابرات العامة بتاريخ 15 أبريل 2025، عن إحباط مخطط إرهابي كان يستهدف أمن المملكة الداخلي عبر استخدام وسائل تكنولوجية متطورة، شملت تصنيع صواريخ محلية الصنع وتطوير طائرات مسيرة(درونز) باستخدام مكونات إلكترونية معقدة، وقد عثر على مواد شديدة الانفجار مثل(C4 وTNT)، وتمت مداهمة مواقع تخزينها في عمان والزرقاء، وكشفت التحقيقات أن عناصر الخلية تلقوا تدريبات خارجية ولديهم خبرات تقنية على مستوى عالٍ، ما يعكس تنامي استخدام التكنولوجيا الحديثة في التخطيط لعمليات تهدد الأمن الوطني.[2]

تبرز هذه الحادثة أهمية تعزيز التنسيق بين الجهات الأمنية والمؤسسات السيبرانية، من أجل رصد أي نشاط إلكتروني مشبوه قبل تحوله إلى تهديد فعلي، كما تؤكد على ضرورة تطوير أدوات المراقبة والتحليل السيبراني، وبناء قدرات بشرية قادرة على مواجهة هذا النوع من التحديات، لا سيما مع تنامي الروابط بين الإرهاب التقليدي والتقنيات الرقمية.

ولم تقتصر جهود الأردن على الجانب الأمني فقط، بل سعت الدولة إلى تعزيز الوعي المجتمعي بأهمية الأمن السيبراني من خلال حملات وطنية وتعاون مع القطاعين العام والخاص، كما تم إصدار تعليمات جديدة في أبريل 2025، تحدد ضوابط المخالفات السيبرانية مما يعكس تطوراً مستمراً في البنية التنظيمية والتشريعية للفضاء الرقمي في المملكة.[3]

ترى الباحثة أن التجربة الأردنية في مجال الأمن السيبراني تعد نموذجاً يحتذى به على مستوى المنطقة العربية، حيث أظهرت قدرة ملحوظة على الجمع بين الإرادة السياسية والتشريعات المتقدمة والجاهزية التقنية، ويبرز ذلك بوضوح من خلال الجهود المستمرة في تطوير البنية التحتية الرقمية، ورفع الوعي المجتمعي وتحديث السياسات السيبرانية، كما أن إحباط العملية الإرهابية الأخيرة التي كانت تعتمد على وسائل تكنولوجية متطورة،

---

[1] أبو العز،خالد،(2022)، القانون والفضاء الرقمي -دراسة تحليلية، الأردن، دار الثقافة للنشر، ط1، ص55.

[2] دائرة المخابرات العامة الأردنية،2025.

[3] المركز الوطني للأمن السيبراني، الأردن.

يؤكد أن التهديدات الأمنية في العصـــر الرقمي لم تعد تقليدية بل باتت تعتمد بشـــكل كبير على أدوات الفضـــاء السيبراني.

وانطلاقاً من ذلك، تؤكد الباحثة أن حماية الفضـــاء الســـيبراني لا تقتصـــر على الجانب التقني فقط، بل تتطلب منظومة متكاملة من التشـريعات والتنسـيق المؤسـسـي والتدريب، إلى جانب اليقظة المسـتمرة لرصـد أي تهديدات ناشـئة، ومن هذا المنظور فإن تعزيز قدرات الدولة في هذا المجال يشـكل ركيزة أسـاسـية للحفاظ على السيادة الوطنية والأمن العام.

الخاتمة:

مع التطور الهائل الذي يشـهده العالم في ميدان التكنولوجيا والاتصـالات، بات من الضـروري أن يتواكب الإطار القانوني مع هذا التحول الرقمي السـريع، لا سـيما في ظل تصـاعد التهديدات السـيبرانية التي باتت تمس الأمن القومي والسـيادة الرقمية للدول، وتنال من حقوق الأفراد والمؤسـسـات على حد سـواء، وقد تناول هذا البحث التحديات القانونية التي يفرضـها الفضـاء السـيبراني، خاصـة فيما يتعلق بالمسـؤولية الدولية والتحديات المرتبطة بالذكاء الاصطناعي.

كما اســتعرضــت الباحثة الجهود الدولية والمحلية الرامية إلى تقنين هذا الفضــاء، ومن أبرزها المبادرات الأممية واتفاقية بودابست، إضـافة إلى التجربة الأردنية الرائدة في هذا المجال من خلال إصـدار تشـريعات متقدمة وتأسيس مؤسسات متخصصة، إلا أن الفجوة التشريعية ما زالت قائمة والحاجة ملحة إلى وضع أطر قانونية دولية موحدة تضمن التوازن بين حماية الأمن السيبراني وضمان الحقوق والحريات الرقمية.

إن تقنين الفضـاء السـيبراني لا يتطلب فقط إرادة سـياسـية وتشـريعية، بل يسـتدعي أيضـاً تعاونا دولياً عابراً للحدود، ورؤية شـاملة تراعي الخصـوصـيات السـيادية للدول، دون المسـاس بالقيم العالمية لحقوق الإنسـان وحكم القانون.

وخلصت الدراسة إلى العديد من النتائج والتوصيات نذكرها على النحو التالي:

أولاً– النتائج:

1. يلاحظ وجود فراغ قانوني دولي واضح فيما يتعلق بتنظيم الفضاء السيبراني، ما أدى إلى تعدد التوجهات واختلاف التشريعات الوطنية، وبالتالي ضعف الجهود الدولية في مواجهة التهديدات السيبرانية.

2. أظهر البحث أن هناك حاجة ملحة لتجريم الأفعال السيبرانية الخطيرة، مثل الهجمات على البنية التحتية الحيوية وسرقة البيانات، بنصوص قانونية واضحة وصريحة في القوانين الوطنية والدولية.
3. على الرغم من الجهود الوطنية المبذولة، بما في ذلك التجربة الأردنية، فإن الاعتماد على التشـــريع الوطني وحده يظل قاصراً عن مواجهة التهديدات السيبرانية ذات الطابع العابر للحدود، ما يستدعي دمج هذه الجهود في إطار قانوني دولي موحد وملزم، يضــمن تنســيق التعاون وتوحيد المعايير القانونية بين الدول.
4. إن التطور المســتمر في تقنيات الذكاء الاصــطناعي يمثل تحدياً قانونياً جديداً، خصــوصــاً فيما يتعلق بحماية البيانات والخصوصية وضمان عدم استخدامها بشكل مسيء أو غير مشروع.
5. بين البحث أهمية إنشــاء جهة دولية متخصــصــة تكون مرجعاً قانونياً وفنياً في متابعة الجرائم السـيبرانية والذكاء الاصطناعي، وتسهم في تحقيق الأمن الرقمي العالمي.

ثانياً –التوصيات:

1- ضرورة إصدار قانون خاص ينظم استخدام تقنيات الذكاء الاصطناعي، وتحديد الإطار القانوني والأخلاقي لهذا الاســتخدام، بما يضــمن حماية الحقوق والحريات العامة، ويحافظ على خصــوصــية الأفراد، ويمنع إســاءة استعمال هذه التقنيات.

2- الدعوة إلى تبني مبادرة دولية لصـياغة اتفاقية دولية شـاملة تنظم الفضـاء السـيبراني، وتضـع قواعد قانونية موحدة تلتزم بها الدول, بما يعزز التعاون الدولي ويحد من التباين في التشريعات الوطنية.

3- تعزيز التعاون الدولي في مجال الأمن الســـيبراني والتشـــريع الرقمي، وتبادل الخبرات والمعلومات الفنية والتشريعية، ودعم بناء قدرات الهيئات الوطنية في مجال الأمن السيبراني.

4- العمل على تعديل التشريعات الوطنية، وتضمينها نصوص تفصيلية تجرم الهجمات السيبرانية بكافة أشكالها، وتحدد العقوبات الرادعة لحماية البنية التحتية الرقمية والأمن الوطني.

5- الإسراع في وضـع إطار تشريعي شـامل ينظم جميع جوانب الذكاء الاصـطناعي، ويراعي المخاطر الأمنية، ويحقق التوازن بين الابتكار وحماية الحقوق والحريات الأساسية.

هذه جملة من التوصيات والاقتراحات التي نرجو الله أن تكون بين أيدي أصحاب القرار، بهدف العمل معاً من أجل التصدي للتهديدات السيبرانية التي باتت تمس الأمن القومي والسيادة الرقمية للدول.

والله ولي التوفيق

المراجع والمصادر:

1- الكتب القانونية :

- أبو العز،خالد، القانون والفضاء الرقمي –دراسة تحليلية، ط1، دار الثقافة للنشر، عمان، 2022.
- بني سلامة، بسمة، تحليل واقع الأمن السيبراني في الأردن، ط1، دار الحامد، عمان، 2021.
- الزعبي، حسام، الذكاء الاصطناعي والقانون الجنائي، ط1، دار وائل، عمان،2023.
- الشمري، ناصر،مخاطر الفضاء السيبراني وسبل مواجهتها، ط1، مركز الدراسات المستقبلية،الرياض، 2022.
- عبد العاطي، سامح، القانون الدولي وأمن الفضاء السيبراني، دار الفكر الجامعي،الإسكندرية، 2020.
- عبد العزيز،علي، الجرائم الإلكترونية والمسؤولية الجنائية الدولية، ط1، دار الفكر الجامعي، القاهرة، 2020.
- عطية، رامي، القانون الدولي والفضاء السيبراني: دراسة تحليلية، ط1، دار الصفاء للنشر والتوزيع، الأردن،2020.
- غانم، خالد. السياسات الدفاعية في الفضاء السيبراني، ط1، دار الفكر القانوني، القاهرة،2021.
- الغرايبة،خالد، القانون الدولي العام وتحديات الفضاء السيبراني، ط1، دار الثقافة، عمان، 2022.
- فتحي، ياسر، الذكاء الاصطناعي والحوكمة العالمية، ط 1، مكتبة لبنان القانونية، بيروت، 2023.
- الكيلاني، ناديا، الذكاء الاصطناعي والمسؤولية الجنائية، ط1،مكتبة الفلاح القانونية،الكويت، 2021.
- الكويتي، محمد، الأمن السيبراني في عصر الذكاء الاصطناعي،ط1،مركز تريندز للبحوث والاستشارات،أبو ظبي، 2023.
- محمد، فايز،الذكاء الاصطناعي ومستقبل الإنسان، ط1، دار الفكر العربي، مصر،2020.
- ياسين، محمد، القانون الدولي وتكنولوجيا المعلومات، ط1، منشورات الحلبي الحقوقية، بيروت، 2021.
- يوسف، خليل، المسؤولية الدولية في ظل الجرائم الإلكترونية،ط1، دار الثقافة للنشر والتوزيع، الأردن، 2019.

2- الرسائل العلمية والبحوث:

- أبو العز، خالد، الأمن السيبراني في ظل الذكاء الاصطناعي، مجلة الدراسة الأمنية والقانونية، المجلد 6،العدد1، عمان- الأردن،(2021)
- العتيبي، عبد العزيز، " تطبيقات الذكاء الاصطناعي وتحدياتها في العالم العربي"، مجلة جامعة نايف للعلوم الأمنية، المجلد 41، العدد2، 2022.
- مراد، فاطمة، الجرائم الإلكترونية في ضوء التشريع العربي المقارن، رسالة ماجستير، جامعة بيروت العربية، 2022.

3- المواثيق والاتفاقيات:

- الجريدة الرسمية الأردنية، قانون الجرائم الإلكترونية رقم 17 لسنة 2023، عمان- الأردن.

- دائرة المخابرات العامة الأردنية، تقرير سنوي، عمان،2025.
- قانون الأمن السيبراني الأردني رقم 16 لسنة 2019.
- المركز الوطني للأمن السيبراني الأردني، تقرير الأداء السنوي 2022،عمان، من الموقع الرسمي.
- المركز الوطني للأمن السيبراني، بيانات رسمية وتقارير تقنية، عمان- الأردن.
- وزارة الاقتصاد الرقمي والريادة، الاستراتيجية الوطنية للأمن السيبراني، عمان، 2022-2025.

4- المراجع الأجنبية:

1. United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/75/816, 2021.
2. Council of Europe. Convention on Cybercrime. Budapest, 2001, Articles 2–13.
3. ENISA. Cybersecurity Act: Regulation (EU) 2019/881. European Union, 2019.
4. Kesan, Jay P., et al. Cybersecurity and the Law: The Legal and Technical Landscape. Carolina Academic Press, USA, 2019.
5. United Nations. Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace. New York: UN Publications, 2021.
6. Taddeo, M., & Floridi, L. "Regulate artificial intelligence to avert cyber arms race". Nature, Vol. 556, 2018, pp. 296–298.
7. Bostrom, Nick. Superintelligence: Paths, Dangers, Strategies. Oxford University Press, UK, 2014.
8. Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach. 4th ed., Pearson, 2020.