تحليل التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في مجال الأمن السيبراني وفق الأنظمة السعودية المحلية والانظمة الدولية

د. سلوى ادريس
كليات الخليج – السعودية

د. الهندي مختار الشريف
كليات الخليج – السعودية

د. حسام الدين حمد
كليات الخليج – السعودية

مخلص البحث:

تهدف هذه الدراسة إلى تحليل المخاطر القانونية الناشئة عن استخدام تقنيات الذكاء الاصطناعي في حماية الأمن السيبراني، من خلال دراسة مقارنة بين الأنظمة المحلية للمملكة العربية السعودية والأطر الدولية ذات الصلة. تمثل هذه المخاطر تحديًا متناميًا نظرًا لاعتماد الهجمات السيبرانية الحديثة على قدرات الذكاء الاصطناعي في تنفيذ هجمات معقدة وعابرة للحدود.

اعتمدت الدراسة على المنهج الوصفي التحليلي بمراجعة وتحليل الأنظمة المحلية مثل نظام حماية البيانات الشخصية، ونظام مكافحة الجرائم المعلوماتية، والسياسة الوطنية للأمن السيبراني، ومقارنتها مع الأطر الدولية المتمثلة في اللائحة الأوروبية العامة لحماية البيانات (GDPR)، واتفاقية بودابست للجرائم الإلكترونية، والارشادات التوجيهية لوكالة (ENISA)

أظهرت النتائج وجود أوجه تشابه في حماية البيانات وتجريم الهجمات السيبرانية، إلى جانب اختلافات جوهرية في تحديد المسؤولية القانونية وآليات التعاون الدولي. كما رصدت الدراسة مجموعة من الفجوات القانونية أبرزها غياب نصوص واضحة لمسؤولية أنظمة الذكاء الاصطناعي، وضعف المعايير الموحدة للتعامل مع المخاطر العابرة للحدود.

توصي الدراسة بضرورة تطوير الأطر القانونية المحلية والدولية لمواكبة التطور السريع في الذكاء الاصطناعي، وتبني معايير موحدة تعزز الأمن السيبراني وتحمي البيانات من المخاطر المستقبلية.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، المخاطر القانونية، الأنظمة السعودية، الأطر الدولية.

Legal Challenges Resulting from the Use of Artificial Intelligence in the Field of Cybersecurity According to Saudi Domestic Regulations and International Regulations

Salwa Idris Dr. **Alhindi Ahmed Alshreef Mokhtar** **Hosam Aldeen Hamd Dr.**

Abstract

This study examines the legal risks associated with the use of Artificial Intelligence (AI) in cybersecurity through a comparative analysis of the legal framework of the Kingdom of Saudi Arabia and relevant international instruments. As AI technologies increasingly underpin sophisticated cross-border cyberattacks, understanding their legal implications has become both urgent and essential.

Employing a descriptive-analytical methodology, the research reviews and analyses key Saudi legal instruments — including the *Personal Data Protection Law*, the *Anti-Cybercrime Law*, and the *National Cybersecurity Policy* — and compares them with major international frameworks such as the *General Data Protection Regulation (GDPR)*, the *Budapest Convention on Cybercrime*, and the *ENISA Guidelines*.

The findings highlight notable convergence in areas related to data protection and the criminalization of cyberattacks yet, reveal significant divergence regarding the attribution of legal liability and the mechanisms for international cooperation. The study further identifies critical legal gaps, particularly the absence of explicit provisions governing AI system liability and the lack of harmonized standards for managing cross-border cybersecurity risks.

Accordingly, the study recommends the continuous development of both domestic and international legal frameworks to keep pace with AI's rapid evolution, alongside the establishment of unified regulatory standards that strengthen cybersecurity governance and ensure effective data protection against emerging technological threats.

Keywords: Artificial Intelligence, Cybersecurity, Legal Risks, Saudi Legislation, International Frameworks.

المقدمة:

يشهد العالم اليوم تحولًا جذريًا في مجال الأمن السيبراني مع إدماج تقنيات الذكاء الاصطناعي في حماية الأنظمة الرقمية، حيث تُستخدم هذه التقنيات في الكشف المبكر عن التهديدات، وتحليل أنماط الهجمات، والاستجابة الفورية لها. ويعد هذا التطور جزءًا من الجهود العالمية لتعزيز أمن البنية التحتية الرقمية ومواجهة التحديات المتزايدة للجرائم السيبرانية في ظل التحول الرقمي السريع.[11][5]

ورغم الفوائد الكبيرة التي يقدمها الذكاء الاصطناعي في حماية الأمن السيبراني، إلا أن استخدامه يثير العديد من المخاطر القانونية، خاصة في مجالات المسؤولية القانونية عن الأضرار، وحماية البيانات والخصوصية، وصعوبة الإسناد القانوني للهجمات السيبرانية العابرة للحدود. وتزداد هذه المخاطر تعقيدًا مع اختلاف الأطر التشريعية بين الدول، إذ قد تكون الهجمات دولية الطابع بينما تخضع المؤسسات لقيود محلية صارمة.

تركز هذه الورقة على تحليل المخاطر القانونية المرتبطة باستخدام الذكاء الاصطناعي في الأمن السيبراني وفق الأنظمة المحلية للمملكة العربية السعودية، بما في ذلك نظام مكافحة الجرائم المعلوماتية ونظام حماية البيانات الشخصية والسياسة الوطنية للأمن السيبراني، مع ربط هذه التشريعات بالأطر الدولية مثل اللائحة الأوروبية العامة لحماية البيانات (GDPR)واتفاقية بودابست للجرائم الإلكترونية وإرشادات .ENISA وتهدف الدراسة إلى تحديد الفجوات القانونية واقتراح توصيات لتعزيز المواءمة بين التشريعات المحلية والدولية بما يضمن أمنًا سيبرانيًا مستدامًا ومتوافقًا مع التطورات التقنية.[11][6]

خطة الدراسة

تنقسم الورقة إلى ستة محاور رئيسية على النحو التالي:

1. **المستخلص**
   - ملخص يوضح مشكلة الدراسة، منهجيتها، أبرز النتائج، والتوصيات.
2. **المقدمة وأهمية الدراسة**
   - توضيح خلفية الموضوع وأهميته في ظل التحول الرقمي ورؤية المملكة 2030.

- عرض مشكلة الدراسة وأهدافها وأهميتها.

3. **الإطار النظري والدراسات السابقة**

- التعريف بالذكاء الاصطناعي ودوره في الأمن السيبراني.
- مراجعة الدراسات والأدبيات السابقة التي تناولت المخاطر القانونية والتشريعات ذات الصلة.

4. **الإطار القانوني المحلي والدولي**

- **الإطار المحلي** :تحليل الأنظمة واللوائح السعودية (نظام مكافحة الجرائم المعلوماتية، نظام حماية البيانات الشخصية، السياسة الوطنية للأمن السيبراني).
- **الإطار الدولي** :استعراض التشريعات والمعايير الدولية مثلGDPR ، اتفاقية بودابست، وإرشادات.ENISA

5. **تحليل المخاطر القانونية والفجوات**

- المسؤولية القانونية.
- حماية البيانات والخصوصية.
- الإسناد وصعوبة تحديد الفاعل.
- الأمن القومي والسيادة الرقمية.
- مقارنة الأطر المحلية والدولية وتحديد الفجوات القانونية.

6. **التوصيات والخاتمة**

- اقتراح حلول عملية لتعزيز التشريعات المحلية بما يتوافق مع الأطر الدولية.
- التأكيد على أهمية المواءمة القانونية لمواجهة التحديات المستقبلية للأمن السيبراني.

أهمية الدراسة

تنبع أهمية هذه الدراسة من الدور المتزايد الذي يلعبه الذكاء الاصطناعي في مجال الأمن السيبراني، وما يرافقه من تحديات قانونية قد تؤثر على فعالية حماية البنية التحتية الرقمية وسلامة البيانات الحساسة. ومع توجه المملكة العربية السعودية نحو التحول الرقمي الشامل في إطار رؤية 2030، أصبح من الضروري دراسة المخاطر القانونية المرتبطة بتبني

هذه التقنيات الحديثة لضمان التوافق مع الأنظمة المحلية وحماية المؤسسات والأفراد من التبعات القانونية المحتملة.

كما تبرز أهمية هذه الدراسة في توضيح أوجه القصورو فجوات الانظمة المحلية في ضوء الممارسات والمعايير الدولية، بما يساهم في:

- دعم واضعي السياسات وصناع القرار في تطوير أنظمة مرنة تواكب تطور الذكاء الاصطناعي.
- تعزيز حماية البيانات والخصوصية بما يتوافق مع نظام حماية البيانات الشخصية المحلي والتشريعات الدولية مثل.GDPR
- الحد من المخاطر القانونية الناشئة عن الهجمات السيبرانية العابرة للحدود عبر تعزيز المواءمة مع الأطر الدولية.

وبالتالي، فإن هذه الدراسة تشكل إضافة علمية وعملية لدعم الأمن السيبراني من خلال منظور قانوني متكامل يجمع بين البعد المحلي والدولي.

أسئلة الدراسة

تهدف هذه الدراسة إلى الإجابة عن مجموعة من الأسئلة البحثية الرئيسية التي توجّه تحليل المخاطر القانونية، وهي:

- ما أبرز المخاطر القانونية المرتبطة باستخدام الذكاء الاصطناعي في مجال الأمن السيبراني؟
- كيف تتعامل الأنظمة المحلية في المملكة العربية السعودية مع هذه المخاطر القانونية؟
- ما مدى توافق الأنظمة المحلية مع الأطر والأنظمة الدولية مثل GDPRواتفاقية بودابست للجرائم الإلكترونية؟
- ما هي الفجوات القانونية التي تظهر عند مقارنة الأطر المحلية والدولية؟
- ما التوصيات اللازمة لتعزيز المواءمة القانونية وضمان أمن سيبراني مستدام في ظل تطور تقنيات الذكاء الاصطناعي؟

منهج الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، الذي يقوم على جمع المعلومات من المصادر القانونية والأكاديمية وتحليلها لفهم طبيعة المخاطر القانونية المرتبطة باستخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني. وتركزت المنهجية على المحاور التالية:

- تحليل الأطر القانونية المحلية:

دراسة الأنظمة واللوائح المعمول بها في المملكة العربية السعودية، مثل:

- نظام مكافحة الجرائم المعلوماتية (1428هـ)
- نظام حماية البيانات الشخصية (2021م)
- السياسة الوطنية للأمن السيبراني
- الاستراتيجية الوطنية للذكاء الاصطناعي

- مراجعة الأطر الدولية:

تحليل التشريعات والمعايير الدولية ذات الصلة، مثل:

- اللائحة الأوروبية العامة لحماية البيانات(GDPR)
- اتفاقية بودابست للجرائم الإلكترونية
- إرشادات وكالة الأمن السيبراني الأوروبية(ENISA)

- المقارنة بين الأطر المحلية والدولية:

- تحديد أوجه التشابه والاختلاف بين الأنظمة السعودية والمعايير الدولية.
- رصد الفجوات القانونية التي قد تعيق التعامل مع المخاطر الناشئة عن الذكاء الاصطناعي في الأمن السيبراني.

- صياغة التوصيات:

- تقديم مقترحات لتطوير الأنظمة المحلية بما يواكب الممارسات الدولية ويعزز حماية الأمن السيبراني.

1. الإطار النظري والدراسات السابقة

1.1. مفهوم الأمن السيبراني

الأمن السيبراني هو مجموعة من الإجراءات والتقنيات والسياسات المصممة لحماية الأنظمة الرقمية والشبكات والبيانات من التهديدات والهجمات الإلكترونية.
يشمل ذلك حماية البنية التحتية الحيوية، البيانات الحساسة، وأنظمة المعلومات من الاختراق أو التخريب أو سوء الاستخدام.[11]

2.1. دور الذكاء الاصطناعي في الأمن السيبراني

أدى تطور الذكاء الاصطناعي إلى إحداث تحول جذري في آليات حماية الأمن السيبراني، حيث أصبحت الأنظمة الذكية قادرة على:

- اكتشاف التهديدات والتعرف على أنماط الهجمات بسرعة عالية.
- التنبؤ بالهجمات السيبرانية قبل وقوعها من خلال تحليل البيانات الضخمة.
- الاستجابة التلقائية للهجمات وتقليل التدخل البشري.

ورغم هذه المزايا، إلا أن الاعتماد المتزايد على الذكاء الاصطناعي يخلق تحديات قانونية معقدة مرتبطة بالمسؤولية، وحماية البيانات، والجرائم السيبرانية العابرة للحدود.
الأطر القانونية للأمن السيبراني والذكاء الاصطناعي

- الإطار المحلي السعودي :يشمل نظام مكافحة الجرائم المعلوماتية، نظام حماية البيانات الشخصية، والسياسة الوطنية للأمن السيبراني.[5]
- **3.1. الدراسات السابقة**

تناولت العديد من الدراسات الأكاديمية العلاقة بين الذكاء الاصطناعي والمخاطر القانونية في الأمن السيبراني، ومن أبرزها:

- **دراسات حول الذكاء الاصطناعي والأمن السيبراني**
  - دراسة *(Al-Janabi, 2022)* التي ركزت على تأثير الذكاء الاصطناعي في تحسين قدرات اكتشاف التهديدات السيبرانية.[5]

- دراسة *(Zhang et al.، 2021)* التي حللت تحديات تبني الذكاء الاصطناعي في حماية الشبكات السحابية.[12]

- **دراسات حول المخاطر القانونية وحماية البيانات**

- دراسة *(Alotaibi، 2023)* التي تناولت التحديات القانونية لحماية البيانات الشخصية في السعودية في ظل التحول الرقمي.[6]
- دراسة *(Smith & Lee، 2020)* التي قارنت بين التشريعات المحلية والدولية في مواجهة الجرائم السيبرانية.

- **دراسات مقارنة بين الأطر المحلية والدولية**

- دراسة *(Kshetri، 2021)* التي أشارت إلى أن معظم التشريعات المحلية في الدول النامية تحتاج إلى تحديثات لتتوافق مع المعايير الدولية مثل[9].GDPR

استخلاص من الدراسات السابقة:

تشير أغلب الدراسات إلى أن الاعتماد على الذكاء الاصطناعي في الأمن السيبراني يعزز الحماية التقنية لكنه يفتح الباب أمام مخاطر قانونية معقدة، تتطلب مواءمة التشريعات المحلية مع الأطر الدولية وتوضيح المسؤوليات القانونية بشكل أكثر تحديدًا.

2. الإطار القانوني المحلي والدولي

1.2. الإطار القانوني المحلي السعودي للأمن السيبراني والذكاء الاصطناعي

شهدت المملكة العربية السعودية خلال السنوات الأخيرة تطورًا ملحوظًا في منظومتها التشريعية والتنظيمية لحماية الفضاء السيبراني ومواكبة التحول الرقمي في إطار رؤية المملكة 2030 .ويشمل الإطار القانوني المحلي للأمن السيبراني والذكاء الاصطناعي مجموعة من الأنظمة واللوائح والسياسات التي تهدف إلى تحقيق التوازن بين الاستفادة من التقنيات الحديثة وتقليل المخاطر القانونية المرتبطة بها.

- نظام مكافحة الجرائم المعلوماتية (1428هـ)
- يمثل الأساس القانوني لمواجهة الجرائم السيبرانية في المملكة.

- يحدد العقوبات على الأفعال التي تشمل اختراق الشبكات، الوصول غير المصرح به، وسرقة البيانات.

يشكل هذا النظام مظلة قانونية للتعامل مع الأضرار الناتجة عن استخدام أنظمة الذكاء الاصطناعي في الهجمات الإلكترونية، لكنه لا يحدد مسؤوليات واضحة على مطوري أو مشغلي هذه الأنظمة.[2]

- نظام حماية البيانات الشخصية (2021م)
- يهدف إلى حماية خصوصية الأفراد والتحكم في جمع ومعالجة البيانات الشخصية.
- يلزم الجهات الحكومية والخاصة بوضع ضوابط لتخزين البيانات ومعالجتها بشكل آمن.
- يعد هذا النظام أساسيًا في إطار استخدام الذكاء الاصطناعي الذي يعتمد على تحليل البيانات الضخمة، حيث يفرض مسؤوليات قانونية عند حدوث أي اختراق أو تسريب للبيانات.[1]
- السياسة الوطنية للأمن السيبراني
- أصدرتها الهيئة الوطنية للأمن السيبراني لتكون مرجعًا استراتيجيًا للجهات الحكومية والخاصة.
- تحدد الأدوار والمسؤوليات المؤسسية وتضع معايير لحماية البنية التحتية الحساسة.
- تدعم إدماج تقنيات الذكاء الاصطناعي ضمن استراتيجيات الأمن السيبراني مع التأكيد على التوافق مع المتطلبات القانونية.[3]
- الاستراتيجية الوطنية للذكاء الاصطناعي
- أطلقتها المملكة ضمن إطار رؤية 2030 لتعزيز مكانتها كقوة إقليمية رائدة في الذكاء الاصطناعي.
- تشمل محاور خاصة باستخدامات الذكاء الاصطناعي في القطاعات الحيوية، مع التركيز على الأطر الأخلاقية والتنظيمية.

تمثل هذه الاستراتيجية خطوة نحو وضع معايير قانونية لضمان استخدام آمن وفعّال للذكاء الاصطناعي في الأمن السيبراني.[4]

على الرغم من تطور الإطار القانوني المحلي، إلا أن هناك فجوات تحتاج إلى معالجة، أبرزها:

- غياب نصوص قانونية محددة توضح المسؤولية القانونية عن أخطاء أو تقصير أنظمة الذكاء الاصطناعي.
- الحاجة إلى لوائح تنفيذية متخصصة تواكب سرعة التطور التقني في الأمن السيبراني المدعوم بالذكاء الاصطناعي.
- ضرورة مواءمة هذه الأنظمة مع الأطر الدولية لتسهيل التعامل مع الجرائم السيبرانية العابرة للحدود.

2.2. الإطار القانوني الدولي للأمن السيبراني والذكاء الاصطناعي

مع الطبيعة العابرة للحدود للهجمات السيبرانية والتطور السريع لتقنيات الذكاء الاصطناعي، ظهرت الحاجة إلى أطر قانونية دولية لضمان حماية البيانات والأمن السيبراني على مستوى عالمي. تهدف هذه الأطر إلى توحيد القواعد القانونية بين الدول، وتعزيز التعاون الدولي في مواجهة الجرائم الإلكترونية والمخاطر القانونية الناشئة عن استخدام الذكاء الاصطناعي. ومن أبرز هذه الأطر:

اللائحة الأوروبية العامة لحماية البيانات(GDPR)

- اعتمدها الاتحاد الأوروبي عام 2018 لتنظيم جمع ومعالجة البيانات الشخصية داخل دول الاتحاد وخارجها عند التعامل مع بيانات مواطنيه.
- تتسم بأنها أكثر التشريعات صرامة عالميًا فيما يتعلق بالخصوصية وحماية البيانات.
- تفرض على المؤسسات:
  - الحصول على موافقة صريحة قبل جمع البيانات.
  - ضمان حماية البيانات أثناء التخزين والمعالجة والنقل.
  - الإبلاغ الفوري عن أي اختراق أو تسريب للبيانات.

- بالنسبة للأمن السيبراني المدعوم بالذكاء الاصطناعي، فإن GDPR يُعد مرجعًا دوليًا يحدد مسؤولية الجهات التي تستخدم تقنيات تحليل البيانات الذكية في حال انتهاك الخصوصية أو تسريب البيانات.[5]

اتفاقية بودابست للجرائم الإلكترونية

- تُعرف رسميًا باسم اتفاقية مجلس أوروبا للجرائم السيبرانية(2001) ، وهي أول اتفاقية دولية ملزمة قانونيًا لمكافحة الجرائم الإلكترونية.[9]
- أهدافها الرئيسية:
  - توحيد تعريفات الجرائم السيبرانية بين الدول.
  - تسهيل التعاون الدولي في التحقيقات والملاحقات القضائية.
  - تمكين تبادل الأدلة الرقمية بسرعة بين الدول الأطراف.
- بالنسبة لاستخدام الذكاء الاصطناعي في الهجمات أو الدفاع السيبراني، توفّر الاتفاقية إطارًا للتعاون الدولي في التحقيق مع الفاعلين عبر الحدود، وهو عنصر أساسي لمعالجة التحديات القانونية الناتجة عن الطبيعة العالمية للهجمات المدعومة بالذكاء الاصطناعي.[6]

إرشادات وكالة الأمن السيبراني الأوروبية(ENISA)

- تصدر الوكالة الأوروبية للأمن السيبراني ENISA تقارير وإرشادات فنية وقانونية لتعزيز حماية البنية التحتية الرقمية في الاتحاد الأوروبي.
- تركّز هذه الإرشادات على:
  - إدارة المخاطر السيبرانية للأنظمة المعتمدة على الذكاء الاصطناعي.
  - وضع معايير أمنية وأخلاقية لتطوير ونشر تقنيات الذكاء الاصطناعي.
  - تشجيع تبني سياسات توحّد الأطر القانونية بين الدول الأوروبية لتسهيل الاستجابة للهجمات السيبرانية.
- تمثل إرشادات ENISA مرجعًا **استشاريًا** يكمّل التشريعات الملزمة مثل GDPR ويوجّه الدول والمؤسسات لاعتماد أفضل الممارسات.[7]

3. تحليل المخاطر القانونية والفجوات

على الرغم من التطورات التشريعية في المملكة العربية السعودية وفي الأطر الدولية المتعلقة بالأمن السيبراني والذكاء الاصطناعي، لا تزال هناك مجموعة من الفجوات القانونية التي قد تحد من القدرة على التعامل مع المخاطر الناشئة عن استخدام الذكاء الاصطناعي في هذا المجال، من أبرزها:

- **غياب نصوص محددة للمسؤولية القانونية عن أخطاء أنظمة الذكاء الاصطناعي**
- لا توجد في الأنظمة المحلية نصوص تفصيلية تحدد من يتحمل المسؤولية في حال وقوع أضرار ناجمة عن أخطاء أو قرارات خاطئة لأنظمة الذكاء الاصطناعي المستخدمة في الأمن السيبراني.
- علي الصعيد الدولي و رغم صرامة GDPR ، إلا أنه لا يوجد إطار موحد يحدد المسؤولية عن الأضرار الناتجة عن أنظمة الذكاء الاصطناعي بشكل شامل.
- **ضعف آليات التعاون الدولي في التحقيقات السيبرانية**
- الأنظمة المحاية في المملكة العربية السعودية تركز علي حماية البيئة الوطنية، مع محدودية التعاون الدولي الا في نطاق الاتفاقيات الثنائية.
- الهجمات المدعومة بالذكاء الاصطناعي غالبًا ما تكون عابرة للحدود وتتطلب تنسيقًا سريعًا لتبادل الأدلة الرقمية، وهو ما توفره جزئيًا اتفاقية بودابست.
- **قصور اللوائح التنفيذية والتشريعات المتخصصة**
- بعض التشريعات السعودية، مثل نظام حماية البيانات الشخصية ونظام مكافحة الجرائم المعلوماتية، تحتاج إلى لوائح تنفيذية واضحة توضح كيفية تطبيقها على استخدامات الذكاء الاصطناعي في الأمن السيبراني.
- كما أن معظم المعايير الدولية مثل ENISA تقدم إرشادات فنية، لكنها تفتقر إلى القوة القانونية الملزمة عالميًا.
- **تأخر تحديث التشريعات لمواكبة التطور التقني السريع**

- التطور السريع في قدرات الذكاء الاصطناعي يتطلب تحديثات دورية في الأنظمة والقوانين، وهو ما يعد تحديًا محليًا ودوليًا على حد سواء.
- الأنظمة الحالية تركز على الهجمات التقليدية أكثر من الهجمات الذكية القائمة على التعلم الآلي والتشغيل الذاتي.
- **غياب معايير موحدة للأمن السيبراني المدعوم بالذكاء الاصطناعي**
- تفتقر البيئة القانونية العالمية إلى معايير موحدة تحدد كيفية تطوير واستخدام أنظمة الذكاء الاصطناعي بطريقة آمنة وقابلة للمساءلة قانونيًا.
- يؤدي ذلك إلى صعوبة مواءمة الممارسات بين الدول وزيادة المخاطر القانونية عند التعامل مع الجرائم السيبرانية المعقدة.

جدول يوضح الفجوات القانونية التي تعيق التعامل مع المخاطر الناشئة عن الذكاء الاصطناعي في الأمن السيبراني:

المحور	الأنظمة السعودية	الأطر الدولية	أوجه التشابه والاختلاف	الفجوات القانونية الرئيسية
حماية البيانات	نظام حماية البيانات الشخصية(2021)	GDPR (2018)	تشابه في حماية البيانات وحقوق الأفراد	الحاجة لتعزيز آليات نقل البيانات العابرة للحدود
مكافحة الجرائم السيبرانية	نظام مكافحة الجرائم المعلوماتية)2007(	اتفاقية بودابست (2001)	تشابه في تجريم الهجمات السيبرانية	غياب آليات فعّالة للتعاون الدولي وإنفاذ القانون
الأمن السيبراني العام	السياسة الوطنية للأمن السيبراني)2019(	ENISA إرشادات	تقارب في أهداف الحماية والوقاية	عدم وجود معايير موحدة للتعامل مع الهجمات الذكية
مسؤولية أنظمة الذكاء الاصطناعي	غير محددة بوضوح	غير موحدة عالميًا	كلاهما يعاني من نقص في تحديد المسؤوليات	الحاجة إلى إطار واضح لمسؤولية الأنظمة الذكية
تحديث التشريعات	محدود ويعتمد على اللوائح التنفيذية	مستمر ومرتبط بالمعايير الأوروبية	تفوق الأطر الدولية في التحديث الدوري	بطء التحديث المحلي مقارنة بالتطور التقني السريع

جدول(1):يوضح الفجوات القانونية التي تعيق التعامل مع المخاطر الناشئة عن الذكاء الاصطناعي في الأمن السيبراني

النتائج:

تطور الأطر القانونية المحلية

تشهد المملكة العربية السعودية تطورًا ملحوظًا في تشريعات الأمن السيبراني وحماية البيانات، مثل نظام حماية البيانات الشخصية والسياسة الوطنية للأمن السيبراني، إلا أن هذه الأطر لا تزال تفتقر إلى نصوص واضحة لمعالجة مسؤولية أنظمة الذكاء الاصطناعي بشكل مباشر.

تشابه جزئي مع الأطر الدولية

هناك أوجه تشابه مع الأنظمة الدولية مثل GDPRواتفاقية بودابست في ما يتعلق بحماية البيانات وتجريم الجرائم السيبرانية، لكن يظل الاختلاف في تحديد المسؤولية القانونية وآليات التعاون الدولي العابر للحدود.

رصد فجوات قانونية واضحة

أبرز الفجوات تتمثل في:

غياب معايير موحدة لمسؤولية أنظمة الذكاء الاصطناعي عن الأضرار.

ضعف آليات التعاون الدولي في الجرائم السيبرانية المدعومة بالذكاء الاصطناعي.

بطء تحديث التشريعات المحلية مقارنة بسرعة تطور التقنيات الذكية.

قصور في اللوائح التنفيذية

بعض التشريعات السعودية كـ نظام مكافحة الجرائم المعلوماتية ونظام حماية البيانات الشخصية تحتاج إلى لوائح تنفيذية أكثر وضوحًا لتغطية استخدامات الذكاء الاصطناعي في الأمن السيبراني.

الحاجة إلى معايير موحدة

غياب معايير دولية موحدة للأمن السيبراني المدعوم بالذكاء الاصطناعي يزيد من المخاطر القانونية ويعيق التنسيق بين الدول في مواجهة الهجمات الذكية.

التوصيات:

تطوير الأطر القانونية المحلية

ضرورة تعديل وتحديث نظام حماية البيانات الشخصية ونظام مكافحة الجرائم المعلوماتية لإضافة نصوص صريحة تُنظّم استخدام أنظمة الذكاء الاصطناعي في الأمن السيبراني، مع تحديد المسؤولية القانونية عن الأخطاء والأضرار الناتجة عنها.

إصدار لوائح تنفيذية متخصصة

الحاجة إلى إصدار لوائح تنفيذية مفصلة تُغطي جميع سيناريوهات استخدام الذكاء الاصطناعي في حماية الشبكات والأنظمة المعلوماتية، بما في ذلك إدارة المخاطر والاستجابة للهجمات السيبرانية الذكية.

تعزيز التعاون الدولي

العمل على توسيع الاتفاقيات الدولية مع الدول والمنظمات المعنية، والانضمام إلى مبادرات عالمية مثل اتفاقية بودابست لتقوية آليات تبادل الأدلة الرقمية ومواجهة الجرائم العابرة للحدود.

إنشاء معايير وطنية متوافقة مع المعايير الدولية

تبني معايير وطنية للأمن السيبراني المدعوم بالذكاء الاصطناعي تتماشى مع **إرشادات** ENISAوالمعايير الأوروبية، لتسهيل التوافق مع القوانين الدولية وتقليل المخاطر القانونية.

التحديث الدوري للتشريعات

ضرورة وضع خطة استراتيجية لتحديث الأنظمة واللوائح القانونية بشكل دوري لمواكبة التطور السريع في تقنيات الذكاء الاصطناعي وأساليب الهجمات السيبرانية الحديثة.

تعزيز الوعي القانوني والتدريب المتخصص

توفير برامج تدريبية للمختصين القانونيين ومسؤولي الأمن السيبراني حول الجوانب القانونية لاستخدام الذكاء الاصطناعي، بما يضمن قدرة المؤسسات على الالتزام بالمعايير المحلية والدولية.

الخاتمة

أظهرت هذه الدراسة أن استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني يمثل ثورة تقنية ذات إمكانات كبيرة في حماية الأنظمة الرقمية وكشف التهديدات المعقدة. ومع ذلك، فإن هذه الثورة التقنية تطرح تحديات قانونية عميقة تتعلق بالمسؤولية، وحماية البيانات، والتعاون الدولي. من خلال المقارنة بين الأطر القانونية المحلية في المملكة العربية السعودية والأطر الدولية، تبين أن هناك تشابهًا في حماية البيانات وتجريم الجرائم السيبرانية، بينما توجد اختلافات واضحة في معالجة المسؤولية القانونية والمعايير الموحدة للتعامل مع المخاطر العابرة للحدود.

كما كشفت الدراسة عن فجوات قانونية مهمة أبرزها غياب نصوص واضحة لمسؤولية أنظمة الذكاء الاصطناعي، وضعف آليات التعاون الدولي في الجرائم السيبرانية المدعومة بالذكاء الاصطناعي، إلى جانب الحاجة الماسة لتحديث التشريعات المحلية بشكل دوري لمواكبة التطور التقني السريع.

وتؤكد هذه النتائج على ضرورة تبني استراتيجية شاملة تجمع بين تطوير التشريعات المحلية ومواءمتها مع المعايير الدولية، مع تعزيز التعاون الدولي والوعي القانوني لضمان توظيف آمن وفعال لتقنيات الذكاء الاصطناعي في حماية الأمن السيبراني.

المصادر والمراجع

1. الهيئة الوطنية للأمن السيبراني .(2019) .*السياسة الوطنية للأمن السيبراني* . الرياض، المملكة العربية السعودية.
2. الهيئة السعودية للبيانات والذكاء الاصطناعي .(2020) .(SDAIA) *الاستراتيجية الوطنية للذكاء الاصطناعي* .الرياض.
3. هيئة الاتصالات والفضاء والتقنية .(2021) .*نظام حماية البيانات الشخصية* . المملكة العربية السعودية.
4. هيئة الاتصالات وتقنية المعلومات. (1428هـ) .*نظام مكافحة الجرائم المعلوماتية* .المملكة العربية السعودية.
5. *Al-Janabi, S. (2022). Artificial intelligence in cybersecurity: Enhancing threat detection and response.*
6. *Alotaibi, M. (2023). Legal challenges of data protection in the Saudi digital transformation era. Arab Journal of Law and Technology.*
7. *Council of Europe. (2001). Budapest Convention on Cybercrime.*
8. *European Union. (2018). General Data Protection Regulation (GDPR).*
9. *European Union Agency for Cybersecurity (ENISA). (2023). AI cybersecurity guidelines and best practices.*
10. *OECD. (2021). Artificial intelligence principles.*
11. *Smith, J., & Lee, K. (2020). Comparative study of cybersecurity legal frameworks: Local vs. international standards.*
12. *Zhang, Y., Li, W., & Chen, H. (2021). AI-driven cybersecurity in cloud environments. Journal of Information Security, 14(3), 102–115.*