

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

الفصل التمهيدي

المقدمة:

لقد أصبحت جرائم الأمن السيبراني واحدة من أخطر التحديات التي تواجه الدول الحديثة مع استمرار الثورة الرقمية في تغيير جميع جوانب الحياة. حيث بات الاعتماد على التكنولوجيا الرقمية والبنية التحتية الإلكترونية ضرورة لا غنى عنها في إدارة مختلف القطاعات الحكومية والخاصة، إلا أن هذا التحول الرقمي صاحبه ظهور تهديدات سيبرانية متطورة تهدد الأمن الوطني وسلامة الأفراد والمؤسسات. تشمل هذه التهديدات الاختراقات السيبرانية، وسرقة البيانات، والهجمات الإلكترونية الموجهة ضد البنى التحتية الحيوية¹.

وفي مواجهة هذه التحديات، ظهرت الحاجة الماسة لوضع أطر قانونية وتشريعات فعّالة قادرة على مكافحة هذه الجرائم وتعزيز الحماية القانونية للبيانات والمعلومات. يمثل هذا النهج خطوة جوهرية نحو حماية الأمن الداخلي للدول واستقرارها الاقتصادي، فضلاً عن حماية خصوصية الأفراد في الفضاء الرقمي. في هذا السياق، تعكس التشريعات في كل من الأردن والسعودية اهتماماً ملحوظاً بوضع قوانين متخصصة لمكافحة الجرائم السيبرانية، بما يدل على إدراك واضح لأهمية تعزيز الأمن السيبراني على المستوى الوطني².

ومع التطورات التقنية السريعة التي يشهدها العالم، بات من الضروري دراسة ومقارنة هذه التشريعات لفهم مدى فعاليتها في مواجهة التحديات السيبرانية المتزايدة. من هنا، تأتي أهمية هذه الدراسة التي تهدف إلى مقارنة الأطر القانونية الأردنية والسعودية في مكافحة جرائم الأمن السيبراني. تسلط الدراسة الضوء

¹ برادة، عبد الرازق. (2024). الأمن السيبراني ودوره في الحد من الهجمات الإلكترونية. في الجريمة

الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، المركز المغاري-شرق أدنى للدراسات الإستراتيجية.

² مسلم، نيراس، (2021). الجرائم السيبرانية وأثرها على الأمن السيبراني، كلية القانون، جامعة بغداد.

على نقاط القوة والتحديات في كل نظام قانوني، وتحلل مدى تكامل هذه التشريعات مع التطورات التكنولوجية الحديثة. كما تقدم الدراسة اقتراحات لتحسين الأطر القانونية وتعزيز التعاون بين البلدين في هذا المجال الحيوي، من أجل مواجهة التهديدات السيبرانية بشكل أكثر شمولية وكفاءة³.

مشكلة الدراسة

مع التطور التكنولوجي السريع، أصبحت جرائم الأمن السيبراني تمثل تهديدًا خطيرًا على دول العالم، بما في ذلك الأردن والمملكة العربية السعودية. ورغم وجود تشريعات قانونية متقدمة في كلا البلدين، إلا أن هناك فجوات تشريعية تعيق التصدي لبعض الجرائم السيبرانية المستحدثة، مما يثير الحاجة إلى تحسين الإطار القانوني لمواكبة هذه التحديات. لذا، تتمثل مشكلة الدراسة في:

. كيف يمكن تطوير وتحسين الإطار التشريعي لكل من الأردن والمملكة العربية السعودية لمكافحة

جرائم الأمن السيبراني بشكل أكثر فعالية وشمولية؟

. ما هي أوجه التشابه والاختلاف بين التشريعات الأردنية والسعودية في كيفية التصدي للجرائم

السيبرانية وحماية الأمن الرقمي؟

تعالج الدراسة هذه الأسئلة من خلال تحليل مقارن بين التشريعات في البلدين، مع التركيز على دور هذه القوانين في حماية دوائر الدولة من التهديدات السيبرانية.

أسئلة الدراسة

1. ما هي الإطار القانوني لجرائم الأمن السيبراني في الأردن والسعودية؟

2. ما هي أبرز الجرائم السيبرانية التي تواجه دوائر الدولة؟

³ محيدين، علي، وحامي، عادل. (2022). الآليات القانونية لحماية الأمن السيبراني. في مؤتمر الآليات القانونية لحماية الأمن السيبراني. جامعة غرداية، الجزائر.

3. كيف تختلف العقوبات والإجراءات الوقائية بين القانون الأردني والقانون السعودي؟

أهداف الدراسة

1. تحليل الإطار القانوني لمكافحة جرائم الأمن السيبراني في التشريعات الأردنية والسعودية:

يتناول هذا التحليل الأنظمة القانونية المعتمدة في كل من الأردن والسعودية لمكافحة الجرائم السيبرانية مثل نظام مكافحة جرائم المعلوماتية في السعودية وقانون الجرائم الإلكترونية في الأردن. يركز التحليل على كيفية تحديد هذه التشريعات للجرائم السيبرانية وتحديد العقوبات المترتبة عليها.

2. تحديد أوجه التشابه والاختلاف بين القانونين في مواجهة الجرائم السيبرانية:

تتشترك التشريعات الأردنية والسعودية في الكثير من الأهداف والمبادئ لمكافحة الجرائم الإلكترونية، ولكن تختلف في تفاصيل التطبيق والعقوبات. يتمثل الاختلاف في مرونة التشريعات الأردنية التي تجدد بشكل مستمر لمواكبة التهديدات الجديدة، بينما تفتقر التشريعات السعودية إلى التحديث المستمر في هذا المجال.

3. تقديم توصيات لتحسين التشريعات القانونية في الأردن والسعودية وتعزيز التعاون المشترك:

يوصى بتطوير التشريعات في كلا البلدين لمواكبة التطورات السريعة في تكنولوجيا المعلومات وأمنها السيبراني. بالإضافة إلى ذلك، يجب تعزيز التعاون بين الدولتين لتبادل المعلومات والأبحاث المتعلقة بالأمن السيبراني وتحقيق التنسيق المشترك لمكافحة الجرائم السيبرانية العابرة للحدود.

أهمية الدراسة

تتبع أهمية هذه الدراسة من تسليطها الضوء على القضايا الأمنية والقانونية الحساسة المرتبطة بحماية المعلومات الحكومية ومكافحة الجرائم السيبرانية، حيث تعكس التحديات المتزايدة التي تواجه الأنظمة الرقمية في العصر الحديث. كما تكتسب الدراسة أهمية إضافية من خلال تحليلها المقارن بين التشريعات الأردنية والسعودية، وهو تحليل نادر يسهم في تحسين الإطار القانوني في البلدين وتعزيز قدرتهما على مواجهة التهديدات السيبرانية بفعالية. بالإضافة إلى ذلك، تقدم الدراسة توصيات عملية للمشرعين وجهات إنفاذ القانون، بهدف سد الثغرات القانونية، وتعزيز الاستراتيجيات الوقائية، وتوفير إطار قانوني قوي ومرن قادر على التصدي للتحديات السيبرانية المستجدة.

منهجية الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التحليلي لفهم القوانين المتعلقة بجرائم الأمن السيبراني وتحليلها، حيث يتم استعراض التشريعات الحالية وتقييم مدى فعاليتها في مواجهة التحديات السيبرانية. كما تستعين الدراسة بالمنهج المقارن للكشف عن أوجه التشابه والاختلاف بين التشريعات الأردنية والسعودية، مما يساعد في تقديم توصيات بناءة تساهم في تحسين هذه التشريعات وتعزيز الإطار القانوني لمكافحة الجرائم السيبرانية بشكل أكثر كفاءة وفعالية.

مصطلحات الدراسة

1. **التحديات القانونية (Legal Challenges) :** يشير المصطلح إلى العقبات التي تواجه

المشرعين والقضاة والمحامين في صياغة وتطبيق القوانين التي تنظم مجال معين، مثل قوانين

مكافحة الجرائم السيبرانية، والتي قد تشمل تعقيدات تقنية، عدم وضوح النصوص القانونية، أو تضارب القوانين بين الدول المختلفة⁴.

2. مكافحة الجرائم (Crime Prevention) : مجموعة الإجراءات والسياسات التي تتخذها الدولة

أو المؤسسات القانونية بهدف الحد من وقوع الجرائم، سواءً من خلال تشديد العقوبات، أو تحسين نظم الرقابة الإلكترونية، أو تعزيز الوعي القانوني والتقني لدى المؤسسات الحكومية والمجتمع⁵.

3. جرائم الأمن السيبراني (Cybersecurity Crimes) : الجرائم التي تستهدف أو تُرتكب

باستخدام التقنيات الحديثة والشبكات الإلكترونية، وتشمل جرائم مثل الاختراق (Hacking) ،

التجسس الإلكتروني (Cyber Espionage) ، سرقة البيانات (Data Breach) ، والهجمات

الإلكترونية (Cyber Attacks) مثل هجمات الحرمان من الخدمة (DDoS)⁶.

4. دوائر الدولة (Government Sectors) : تشمل المؤسسات والإدارات الحكومية التي تعمل

على تقديم الخدمات العامة وتنفيذ القوانين. في سياق الأمن السيبراني، تشمل دوائر الدولة

⁴ رفاعي، محمد، (2023). التحديات القانونية والإدارية لخصخصة المرافق العامة: دراسة مقارنة. مجلة البحوث القانونية والاقتصادية (المنصورة)، المجلد 13(84).

⁵ الصبحي، شهد، والربابغ، ريم، (2022). مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة 2030: دراسة مسحية لدى طلبة كلية الآداب والعلوم الإنسانية بجامعة الملك عبد العزيز بجدة، العدد (40).

⁶ مصطفى، إسلام، (2022). جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري. المجلة القانونية، المجلد 12(3).

الجهات المسؤولة عن حماية البنية التحتية الرقمية، مثل الوزارات والهيئات الحكومية ومراكز البيانات الوطنية⁷.

5. القانون الأردني (Jordanian Law) : الإطار القانوني الذي يحكم المملكة الأردنية الهاشمية، والذي يستمد أصوله من الشريعة الإسلامية والقانون المدني الفرنسي. يتضمن القانون الأردني مجموعة من التشريعات التي تنظم الجرائم السيبرانية، مثل قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015⁸.

6. القانون السعودي (Saudi Law) : الإطار القانوني الذي يحكم المملكة العربية السعودية، ويستمد أصوله من الشريعة الإسلامية. يحتوي القانون السعودي على أنظمة تنظم الأمن السيبراني ومكافحة الجرائم السيبرانية، مثل نظام مكافحة الجرائم المعلوماتية الصادر عام 2007، والذي يهدف إلى حماية البيانات الرقمية والبنية التحتية الإلكترونية⁹.

⁷ الحصري، طارق، (2019). الجهاز الإداري للدولة في مصر: المفهوم، التحديات، ورؤية التطوير، الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري.

⁸ الوصيف، آية، (2018). نص قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. تشريعات أردنية - قانون الجرائم الإلكترونية.

⁹ المركز الوطني للتنافسية. (2024). الاستراتيجية الوطنية للأمن السيبراني.

الدراسات السابقة:

أولاً: الدراسات العربية:

1-دراسة نصار (2024) بعنوان: واقع الحماية الجزائية للأمن السيبراني دراسة مقارنة: الأردن-

قطر

تهدف هذه الدراسة المقارنة بين الأردن وقطر إلى تقييم واقع الحماية الجزائية للأمن السيبراني في كلا البلدين وتحليل استراتيجياتهما في مواجهة التهديدات السيبرانية. تعتمد الدراسة على تحليل القوانين والتشريعات، بالإضافة إلى مراجعة السياسات الأمنية وأدوار المؤسسات المعنية. توصلت النتائج إلى أن الأردن قد اتخذ خطوات مهمة في تعزيز الحماية الجزائية من خلال إقرار قوانين جديدة وتطوير قدرات الأجهزة الأمنية والقضائية، بينما برزت قطر كرائدة إقليمية بتنفيذ استراتيجية وطنية متكاملة، وتعزيز التعاون بين القطاعين العام والخاص. توصي الدراسة بضرورة تحديث التشريعات في كلا البلدين لمواكبة تطور الجرائم السيبرانية، وتكثيف التدريب للكوادر المتخصصة، وتعزيز التعاون المشترك وتبادل الخبرات في مجال الأمن السيبراني.¹⁰

التعقيب: تسلط هذه الدراسة الضوء على الجهود المبذولة في الأردن وقطر لتعزيز الحماية القانونية للأمن السيبراني، مع التركيز على التشريعات الحديثة التي تم إدخالها في كلا البلدين. بينما قدمت قطر نموذجاً رائداً في التعاون بين القطاعين العام والخاص لتعزيز الأمن السيبراني، تبرز الحاجة إلى تحديث القوانين والتشريعات بشكل مستمر لضمان فعالية الاستجابة للتحديات السيبرانية المتجددة، وهو ما يعد محوراً أساسياً في توصيات الدراسة.

¹⁰ الوصيف، آية، (2018). نص قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. تشريعات أردنية – قانون الجرائم الإلكترونية.

2-دراسة الخضيرى (2024) بعنوان: سبل مكافحة الجرائم السيبرانية العابرة للحدود

تناولت هذه الدراسة الجرائم السيبرانية باعتبارها من أخطر التهديدات التي تواجه الأمن القومي للدول، حيث تتميز بقدرتها على تجاوز الحدود الجغرافية والسياسية والثقافية. يزداد خطر هذه الجرائم مع التطور المستمر لتكنولوجيا المعلومات والاتصالات، مما أدى إلى تهديد السيادة الوطنية وأثر سلباً على الاقتصاد والأمن الوطني. وتشمل الجرائم السيبرانية تهديدات متنوعة، أبرزها الإرهاب السيبراني الذي لا يعترف بالحدود، مما يتطلب استجابة دولية ومحلية عاجلة. توصي الدراسة بضرورة تعزيز التدابير الوقائية من خلال تحديث التشريعات، تطوير القدرات التقنية، وزيادة الوعي المجتمعي بخطورة هذه الجرائم، إلى جانب تعزيز التعاون الدولي لمواجهتها والحد من أثارها السلبية.

التعقيب: تؤكد هذه الدراسة على أهمية التعاون الدولي في مكافحة الجرائم السيبرانية العابرة للحدود، حيث تتطلب هذه التهديدات جهوداً منسقة بين الدول لضمان استجابة فعالة. كما تسلط الدراسة الضوء على الحاجة الملحة لتحديث التشريعات باستمرار لمواكبة التطورات السريعة في الفضاء الإلكتروني. بالإضافة إلى ذلك، يظهر بوضوح أهمية تطوير القدرات التقنية وتعزيز البنية التحتية الرقمية، لضمان قدرة الدول على التصدي للهجمات السيبرانية المعقدة، مما يعزز الأمن الرقمي على المستويين الوطني والدولي.¹¹

11 الصبحي، شهد، والرابع، ريم، (2022). مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة 2030: دراسة مسحية لدى طلبة كلية الآداب والعلوم الإنسانية بجامعة الملك عبد العزيز بجدة، العدد (40).

3- دراسة الخالدي وآخرون (2023) بعنوان: دور الأمن العام في مكافحة الجرائم الإلكترونية عبر

شبكات التواصل الاجتماعي: دراسة تحليلية

هدفت الدراسة إلى التعرف على دور الأمن العام في مكافحة الجرائم الإلكترونية عبر شبكات التواصل الاجتماعي، وتحليل أهم الموضوعات التي يتم نشرها وأساليب التوعية التي يعتمد عليها الأمن العام عبر هذه الشبكات. اعتمدت الدراسة على المنهج الوصفي التحليلي، وتوصلت إلى نتيجة مفادها أن الجمهور الأردني يعتمد بشكل مباشر على الحملات التوعوية المتعلقة بالجرائم الإلكترونية التي ينشرها الأمن العام عبر موقعه الرسمي على وسائل التواصل الاجتماعي. كما أشارت الدراسة إلى الدور البارز والفعال لجهاز الأمن العام في مكافحة الجرائم الإلكترونية وتعريف الجمهور بمخاطرها والعقوبات المترتبة عليها. وفي ضوء هذه النتائج، أوصت الدراسة بتكثيف الجهود الأمنية في نشر الحملات التوعوية عبر شبكات التواصل الاجتماعي التي تهدف إلى مكافحة الجرائم الإلكترونية بمختلف أنواعها، بالإضافة إلى تغليظ العقوبات القانونية على مرتكبي هذه الجرائم للحد من انتشارها.

التعليق: تعد الدراسة التي تناولت دور الأمن العام في مكافحة الجرائم الإلكترونية عبر شبكات التواصل الاجتماعي خطوة هامة لفهم كيفية التصدي لهذه الجرائم التي تهدد الأفراد والمجتمع. تظهر الدراسة فعالية الحملات التوعوية التي يبثها الأمن العام عبر الوسائل الاجتماعية في توعية الجمهور الأردني بمخاطر الجرائم الإلكترونية وعواقبها. ومع ذلك، يمكن تعزيز هذه الجهود من خلال تنويع أساليب التوعية لتشمل فئات أوسع من المجتمع، بما في ذلك الذين لا يستخدمون الشبكات الاجتماعية بشكل كبير. كما أن تغليظ العقوبات يمكن أن يكون رادعاً، لكنه يجب أن يكون موازناً مع سياسات وقائية وتعليمية تركز على الحد من الجرائم قبل وقوعها. في النهاية، تعتبر هذه الدراسة أساساً مهماً للتطوير المستقبلي في مجال الأمن السيبراني من خلال التعاون بين القطاعين العام والخاص وتوسيع نطاق التوعية.

4- دراسة حميدة (2021) بعنوان: الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي: نحو تفعيل

دور الأمن السيبراني المعلوماتي

تهدف هذه الدراسة إلى تحذير الجيل الجديد من الجرائم السيبرانية التي تتسم بخطورتها وصعوبة إثباتها، مع التركيز على الجرائم التي تُرتكب عبر مواقع التواصل الاجتماعي وتأثيرها على الأمن القومي للدول. اعتمدت الدراسة على المنهج الوصفي التحليلي لاستعراض وتحليل مظاهر الجرائم الإلكترونية وأساليب الحماية السيبرانية المتاحة لمواجهتها. توصلت الدراسة إلى أن الانتشار العشوائي لمواقع التواصل الاجتماعي وضعف التشريعات القانونية والرقابة يزيد من خطورة هذه الجرائم، مما يهدد البيانات الشخصية وأمن المؤسسات الوطنية. توصي الدراسة بضرورة تطوير تشريعات متخصصة لمكافحة الجرائم السيبرانية، تعزيز وسائل الحماية المعلوماتية، ورفع مستوى الوعي المجتمعي بأهمية الأمن السيبراني.

التعقيب: تسلط هذه الدراسة الضوء على حجم المخاطر المتزايدة التي تشكلها الجرائم الإلكترونية عبر منصات التواصل الاجتماعي، حيث أصبحت هذه المنصات بيئة خصبة للاختراقات، والاحتيال الإلكتروني، وانتهاك الخصوصية. تؤكد الدراسة على أهمية وجود تشريعات متخصصة تنظم الاستخدام الآمن لهذه المنصات، وتحمي المستخدمين من الاستغلال السيبراني. كما تشدد على ضرورة زيادة الوعي المجتمعي حول حماية المعلومات الشخصية، وتعزيز الثقافة الرقمية التي تساعد الأفراد على تجنب الوقوع ضحية لهذه الجرائم، مما يساهم في بناء فضاء إلكتروني أكثر أمانًا وثقة.

5-دراسة مهدي (2021) بعنوان: الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري

تهدف هذه الدراسة إلى تحليل التحولات العميقة التي شهدتها العالم نتيجة للتطور التكنولوجي، مع التركيز على الجرائم السيبرانية باعتبارها أحد التحديات الرئيسية الناتجة عن هذه التحولات. اعتمدت الدراسة على المنهج الوصفي التحليلي لفهم طبيعة هذه الجرائم وتأثيرها على المجتمع الجزائري، في ظل كونها جرائم عابرة للحدود الجغرافيا لا تميز بين المجتمعات. توصلت الدراسة إلى أن الجزائر شهدت في السنوات الأخيرة ارتفاعاً ملحوظاً في مؤشر الجرائم السيبرانية، مما دفع المشرع إلى سن تشريعات تهدف إلى الحد من هذه الظاهرة. توصي الدراسة بضرورة تعزيز الإطار القانوني لمكافحة الجرائم السيبرانية، وتطوير قدرات الجهات الأمنية، مع نشر الوعي المجتمعي حول مخاطر الجرائم السيبرانية وسبل الوقاية منها.

التعليق: تقدم هذه الدراسة تحليلاً هاماً للتهديدات السيبرانية في الجزائر، حيث تسلط الضوء على التحديات القانونية والتقنية التي تفرضها هذه الجرائم على التشريع الجزائري. يبرز في الدراسة الحاجة إلى تعزيز التشريعات الوطنية وتطوير القوانين لتواكب التطورات السريعة في الجريمة السيبرانية، بما يضمن حماية فعالة للبنية التحتية الرقمية والمعلومات الحساسة، ويساهم في تحسين قدرة الدولة على التصدي للهجمات الإلكترونية بفعالية وكفاءة أكبر.

6- دراسة المرداس (2021) بعنوان: الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)

يهدف البحث إلى التعرف على واقع الأمن السيبراني في المملكة العربية السعودية مع التركيز على الوضع الحالي والمستقبلي لهذا المجال المهم، في ظل التحديات الاقتصادية والسياسية. اعتمدت الدراسة على المنهج الوصفي من خلال مراجعة الأدبيات السابقة، حيث تم شرح مفهوم أمن المعلومات

والأمن السيبراني وأهمية هذا المجال في حماية المعلومات. كما تم استعراض جهود المملكة في مكافحة الجرائم السيبرانية، وأشارت النتائج إلى أن مكافحة الجرائم الإلكترونية العابرة للحدود تعد من أكبر التحديات التي تواجه الدول، وتستدعي التعاون الدولي والإقليمي لمواجهتها. أوصى البحث بعدد من التوصيات المهمة، أبرزها نشر ثقافة الأمن السيبراني في المجتمع، توفير البنية التحتية اللازمة، تدريب الكوادر البشرية في هذا المجال، تمكين المرأة في العمل في الأمن السيبراني، بالإضافة إلى حماية الأطفال من الجرائم السيبرانية أثناء استخدام الإنترنت.

التعليق: تعتبر هذه الدراسة خطوة مهمة لفهم التحديات التي تواجه الأمن السيبراني في المملكة العربية السعودية، وخاصة فيما يتعلق بـ الجرائم الإلكترونية العابرة للحدود. التوصيات التي تم طرحها تعتبر أساسية لضمان حماية المعلومات وتعزيز الأمن الرقمي. من المهم أن تتبّع المملكة هذه التوصيات بشكل عاجل، خاصة في مجالات التدريب والتأهيل للكوادر، بالإضافة إلى تمكين المرأة في هذا القطاع لتعزيز التنوع. كما أن حماية الأطفال يجب أن تكون أولوية في مواجهة التهديدات المتزايدة على الإنترنت.

ثانياً: الدراسات الأجنبية

1-دراسة (Yousfi, 2024) بعنوان:

Cybersecurity Challenges and International Cooperation

تهدف هذه الدراسة إلى تعريف الأمن السيبراني وتقنياته، وتحديد مخاطر الجرائم الإلكترونية، مع إبراز الجهود الوطنية والدولية لمكافحة هذه الجرائم وتقييم مدى فعاليتها، مع التركيز على استجابة المشرع الجزائري لهذه المخاطر التي تهدد الأمن والمصالح الفردية. اعتمدت الدراسة على

المنهج الاستنباطي (التحليلي) والمقارن لتوضيح مفهوم الأمن السيبراني وحماية البيانات الشخصية، إضافة إلى تناول الآليات القانونية المتاحة لحمايتها ضد التهديدات الرقمية. توصلت الدراسة إلى أن النصوص التشريعية الجنائية الحالية بحاجة إلى تعزيز لضمان حماية فعالة للأمن السيبراني. توصي الدراسة بتطوير الأطر القانونية الوطنية لتحقيق توازن بين تبادل المعلومات في إطار التعاون الدولي وحماية البيانات الشخصية، مع تعزيز التعاون الدولي لمواجهة الجرائم الرقمية المتزايدة.

التعليق: تسلط هذه الدراسة الضوء على أهمية تعزيز الأطر القانونية في الجزائر لمواجهة الجرائم السيبرانية المتزايدة، حيث تتطلب التطورات الرقمية المتسارعة تحديث التشريعات الوطنية لضمان استجابة فعالة لهذه التهديدات. كما توصي الدراسة بتطوير التعاون الدولي بين الجزائر والدول الأخرى لمكافحة الجرائم الرقمية العابرة للحدود، والتي تشكل خطرًا على الأمن الفردي والمؤسسي، مما يستدعي جهودًا منسقة لتعزيز الأمن السيبراني على المستويين الوطني والدولي.

2-دراسة (Al-Kasassbeh1 at el., 2024) بعنوان:

Digital Human Rights in Jordanian Legislation and International Agreement

تهدف هذه الدراسة إلى تحليل واقع حقوق الإنسان الرقمية في التشريعات الأردنية والاتفاقيات الدولية، حيث تشمل هذه الحقوق الحريات المرتبطة بالتواصل، وتبادل المعرفة، وحرية الرأي، وحماية الخصوصية والبيانات، بالإضافة إلى ضمان الوصول العادل إلى البنية التحتية والخدمات التكنولوجية. استخدمت الدراسة منهجًا قانونيًا نوعيًا يعتمد على تحليل النصوص القانونية والبيانات المتاحة عبر المنصات الإلكترونية. توصلت الدراسة إلى أن الحقوق الرقمية تُعد جزءًا لا يتجزأ من حقوق الإنسان

الأساسية، حيث ظهر مفهوم "الحقوق الرقمية" بالتزامن مع تطور خطاب حقوق الإنسان المعاصر. وقد أكدت المنظمات الدولية على ضرورة الاعتراف بهذه الحقوق وضمان حمايتها. ومع ذلك، تواجه الحقوق الرقمية تحديات معقدة تشمل الجوانب التشريعية، والاستراتيجية، والتقنية، حيث أصبح استغلال البيانات الشخصية من قبل الشركات التكنولوجية الكبرى وتوظيفها لأغراض تجارية أو أمنية مصدر قلق كبير. توصي الدراسة بضرورة تعزيز الآليات التنظيمية لحماية الحقوق الرقمية، مع مراعاة التوازن بين حماية هذه الحقوق واحترام النظام العام والأخلاقيات المجتمعية.

التعقيب: تبرز هذه الدراسة أهمية حقوق الإنسان الرقمية في التشريع الأردني في ظل التحول الرقمي السريع، حيث تسلط الضوء على الحاجة إلى تعزيز آليات حماية هذه الحقوق وضمان توازنها مع النظام العام. كما تؤكد الدراسة على أهمية تطوير القوانين لضمان الخصوصية، حرية التعبير، وحماية البيانات الشخصية، بما يواكب التحديات الرقمية الحديثة ويحفظ حقوق الأفراد في البيئة الرقمية.

3-دراسة (Rawindaran et al., 2023) بعنوان:

Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom

تتناول هذه الدراسة مقاومة الشركات الصغيرة والمتوسطة في السعودية والمملكة المتحدة لتدابير الأمن السيبراني ضمن سياق الصناعة 5.0، مع التركيز على الحوكمة والسياسات المؤثرة. تبحث الدراسة في العوامل الثقافية والاقتصادية التي تسهم في هذه المقاومة، مثل ضعف الوعي بمخاطر الأمن السيبراني، والقيود المالية، والأولويات المتنافسة. اعتمدت الدراسة على منهج الأساليب المختلطة، بما

في ذلك مقابلات مع أصحاب الشركات وخبراء الأمن السيبراني، وكشفت النتائج عن حاجة ملحة لتعزيز الوعي والتدريب حول الأمن السيبراني. أوصت الدراسة بتطوير الأطر التنظيمية وتكثيف الشراكات بين القطاعين العام والخاص، إلى جانب تحسين وثائق التوجيه الرسمية في كلا البلدين لتعزيز الامتثال وزيادة الثقة في ممارسات الأمن السيبراني.

التعليق: تقدم هذه الدراسة فكرة شاملة عن التحديات التي تواجه الشركات الصغيرة والمتوسطة في

مجال الأمن السيبراني في كل من السعودية والمملكة المتحدة، حيث تعاني هذه الشركات من نقص الموارد والخبرات اللازمة لحماية أنظمتها الرقمية. كما تبرز الدراسة أهمية التوعية والتدريب في تحسين فعالية السياسات الأمنية، حيث يعد رفع مستوى الوعي السيبراني بين الموظفين وأصحاب الأعمال عاملاً حاسماً في التصدي للتهديدات الرقمية، وتعزيز قدرة هذه الشركات على حماية بياناتها وأصولها من الهجمات الإلكترونية.

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

الفصل الأول: الإطار المفاهيمي للجرائم السيبرانية والأمن السيبراني

تمهيد:

يتناول الفصل التالي الإطار المفاهيمي للدراسة مشتملاً على التعريف بموضوع الدراسة الذي يركز على تحليل قضايا الأمن السيبراني، أحد المواضيع الأكثر أهمية في عصرنا الحديث. ستنم مناقشة النظريات المختلفة المتعلقة بالأمن السيبراني وتطور تكنولوجياته التي ظهرت مع تقدم الابتكارات الرقمية. كما سيتم تناول التحديات العامة التي تواجه هذا المجال بما في ذلك تطور أساليب الهجمات الرقمية، بالإضافة إلى تسليط الضوء على تعريف الجرائم السيبرانية وأنواعها، والخصائص التي تميز هذه الجرائم عن الجرائم التقليدية. كما سيركز الفصل على التأثيرات العميقة التي تحدثها هذه الجرائم على الأمن الوطني، مما يعكس تأثيرها المباشر على استقرار الدول وسلامتها.

المبحث الأول: الجرائم السيبرانية والأمن السيبراني

المطلب الأول: تعريف جرائم الأمن السيبراني وخصائصه

أولاً: مفهوم جرائم الأمن السيبراني

تُعرَّف الجرائم السيبرانية بأنها "أي نشاط إجرامي يتم باستخدام أجهزة الكمبيوتر أو الشبكات أو يستهدفها، ويشمل ذلك مجموعة واسعة من الأنشطة غير القانونية التي تتم عبر الإنترنت أو باستخدام الأجهزة الإلكترونية". تشمل هذه الجرائم، على سبيل المثال لا الحصر، الاختيال الإلكتروني، سرقة الهوية، توزيع البرمجيات الخبيثة، الهجمات الموزعة لحجب الخدمة (DDOS)، والابتزاز الإلكتروني باستخدام برامج الفدية. تتعدد دوافع ارتكاب هذه الجرائم، فقد تكون مالية، سياسية، أيديولوجية، أو حتى بدافع التحدي والتسلية. تتطلب مكافحة الجرائم السيبرانية اتباع مجموعة من الإجراءات الوقائية والتدابير الأمنية، مثل تحديث الأنظمة والبرامج بانتظام، استخدام برامج مكافحة الفيروسات، وتوعية المستخدمين بممارسات الأمان السيبراني. نظرًا للطبيعة العابرة للحدود لهذه الجرائم، يُعد التعاون الدولي وتبادل المعلومات بين الدول أمرًا حيويًا لتعقب المجرمين وتقديمهم للعدالة.¹²

ثانياً: خصائص الجرائم السيبرانية

¹² العتيبي، زياد. (2021). جرائم السيبرانية المرتكبة عبر الوسائط الرقمية. المجلة الأكاديمية العالمية للدراسات القانونية.

تُعَدُّ الجرائم السيبرانية من الظواهر الإجرامية الحديثة التي نشأت مع تطور التكنولوجيا الرقمية وانتشار الإنترنت، حيث باتت تشكل تهديدًا متزايدًا للأفراد والمؤسسات والدول. وتتميز هذه الجرائم بعدة خصائص تجعلها مختلفة عن الجرائم التقليدية، أبرزها:

1-اللامحدودية الجغرافية: يمكن ارتكاب الجرائم السيبرانية من أي مكان في العالم، مما يجعل تحديد مكان الجريمة صعبًا. يستغل المجرمون الفضاء السيبراني الذي لا حدود له، مما يتيح لهم تنفيذ هجماتهم بسرعة ودون الحاجة للتواجد الفعلي في مكان الجريمة. هذا اللامحدودية تجعل من الصعب تتبع المجرمين وتحديد مواقعهم بدقة.¹³

2-السرعة والخفاء: تُنفَّذ هذه الجرائم بسرعة ودون ترك آثار واضحة، مما يصعب اكتشافها وملاحقة مرتكبيها. يستفيد المجرمون من الطبيعة الرقمية للجرائم، حيث يمكنهم تنفيذ الهجمات بسرعة ودون ترك آثار ملموسة، مما يجعل اكتشاف الجريمة وملاحقة الجناة أمرًا صعبًا.¹⁴

3-التنوع والتطور المستمر: تتعدد أشكال الجرائم السيبرانية وتتنوع، مثل الاحتيال الإلكتروني، والقرصنة، والتصيد الاحتيالي، وتستمر في التطور مع تقدم التكنولوجيا. مع تقدم التكنولوجيا، تظهر أساليب وتقنيات جديدة لارتكاب الجرائم السيبرانية، مما يتطلب تحديثًا مستمرًا في استراتيجيات المكافحة والتشريعات القانونية لمواكبة هذه التطورات.

¹³ نفس المرجع السابق

¹⁴ حلز الله، محمد. (2020). جرائم الأنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية. مجلة المفكر.

4-استهداف الأفراد والمؤسسات: قد تستهدف الجرائم السيبرانية الأفراد للحصول على معلومات

شخصية أو مالية، أو تستهدف المؤسسات بهدف سرقة البيانات أو تعطيل العمليات. يستهدف المجرمون الأفراد للحصول على معلومات حساسة مثل البيانات البنكية أو المعلومات الشخصية، كما قد يستهدفون المؤسسات لسرقة بياناتها أو تعطيل عملياتها، مما يؤدي إلى خسائر مالية كبيرة.¹⁵

5-استخدام تقنيات متقدمة: يعتمد مرتكبو الجرائم السيبرانية على تقنيات متقدمة وأدوات متخصصة

لتنفيذ هجماتهم، مما يتطلب خبرة عالية. يستخدم المجرمون أدوات وتقنيات متطورة لتنفيذ هجماتهم، مثل البرمجيات الخبيثة، والهندسة الاجتماعية، وتقنيات التشفير، مما يتطلب من الجهات المعنية تطوير مهاراتها وقدراتها لمكافحة هذه الجرائم.

6-صعوبة التحقيق والملاحقة القانونية: نظرًا للطبيعة الرقمية للجرائم، قد تكون الأدلة غير ملموسة،

مما يجعل التحقيقات والملاحقات القانونية أكثر تعقيدًا. تنسم الجرائم السيبرانية بصعوبة في جمع الأدلة، حيث تكون الأدلة رقمية وغير ملموسة، مما يتطلب تقنيات متخصصة في التحقيقات الرقمية وملاحقة الجناة عبر الحدود الدولية.¹⁶

ثالثًا: أنواع الجرائم السيبرانية المختلفة

أنواع الجريمة السيبرانية تتنوع وفقًا للوسائل المستخدمة، الهدف من ارتكاب الجريمة، والأساليب التقنية المتبعة. فيما يلي بعض الأنواع التي يتم تصنيفها:

¹⁵الربيعي، نورهان محمد. (2024). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). مجلة الفلاري للعلوم الإنسانية، 3(1)

¹⁶المطيري، سعد. (2023). مفهوم الجرائم الإلكترونية وسماحتها. المجلة القانونية 16(5).

جرائم الاستغلال والتسلل: تشمل محاولات الوصول غير المصرح به إلى الأنظمة المعلوماتية، مثل الاختراقات (Hacking) التي تتم عن طريق استخدام أدوات وتقنيات متطورة. تهدف هذه الجرائم إلى الحصول على بيانات حساسة مثل المعلومات الشخصية أو البيانات المالية أو لتخريب النظام، مما قد يسبب خسائر كبيرة في البيانات ويؤثر على سمعة المؤسسات. قد تكون هذه الهجمات مُنفذة بواسطة أفراد أو مجموعات، مما يزيد من تعقيد التحقيقات في مثل هذه الجرائم.

الاحتيال الإلكتروني: يتعلق بسرقة الأموال من خلال تقنيات الإنترنت مثل الاستيلاء على البيانات المصرفية، واستخدام تقنيات التصيد الاحتيالي (Phishing) لسرقة الهوية أو الأموال من الأفراد. يُعد الاحتيال الإلكتروني من الجرائم التي قد تؤدي إلى تدمير الثقة في الخدمات الإلكترونية، كما تتسبب في خسائر مالية كبيرة للأفراد والشركات. يُظهر تطور تقنيات الاحتيال قدرة المهاجمين على إخفاء هويتهم وابتكار أساليب جديدة للتهديد.

جرائم الفيروسات والبرامج الضارة: تشمل نشر الفيروسات والبرمجيات الضارة (Malware) التي تُلحق الضرر بأنظمة الكمبيوتر أو تشويش البيانات أو سرقتها. تعتمد هذه الجرائم على إصابة الأنظمة ببرمجيات خبيثة تهدف إلى تعطيل العمليات، سرقة البيانات الحساسة، أو تدمير الأنظمة. هذه الجرائم تمثل تهديدًا مستمرًا للمؤسسات الكبرى التي تعتمد بشكل أساسي على الأنظمة الرقمية والبيانات الضخمة¹⁷.

الجرائم المتعلقة بالمحتوى: تتضمن نشر المحتوى الضار مثل المواد الإباحية أو المواد التي تحرض على العنف والكراهية عبر الإنترنت. تشمل هذه الجرائم الانتهاكات المتعلقة بحرية التعبير على

¹⁷ نفس المرجع السابق

الإنترنت واستخدامها لنشر رسائل ضارة قد تضر بالمجتمع. تثير هذه الجرائم قلقًا اجتماعيًا، إذ يمكن أن تؤدي إلى تأثيرات سلبية على الأفراد والجماعات، مثل التأثير على القيم المجتمعية وزيادة مظاهر العنف.

الهجمات الإلكترونية الموجهة: تتضمن الهجمات المنظمة من قبل جهات غير حكومية أو حكومية على أنظمة أو مؤسسات كبيرة بهدف سرقة البيانات أو تدمير البنية التحتية التقنية. هذه الهجمات تُنفذ بشكل متقن وتستهدف عادة القطاعات الحيوية مثل المالية والطاقة والاتصالات. غالبًا ما تتم هذه الهجمات باستخدام تقنيات متقدمة مثل الهجمات الموزعة (DDOS) أو البرامج الضارة الموجهة لتخريب الأنظمة بشكل تدريجي أو تدميرها.

المطلب الثاني: الأمن السيبراني

أولاً: مفهوم الأمن السيبراني

الأمن السيبراني يشير إلى مجموعة من الإجراءات التقنية والتنظيمية التي تهدف إلى حماية الأنظمة، والشبكات، والبرامج، والبيانات من الهجمات الرقمية أو غير المصرح بها. يتعامل الأمن السيبراني مع حماية المعلومات من مجموعة واسعة من التهديدات مثل الفيروسات، والهجمات الإلكترونية، والبرمجيات الخبيثة، والاختراقات التي قد تستهدف سرية البيانات، سلامتها، وتوافرها. يتضمن أيضاً استراتيجيات لتوفير حماية قوية ضد الوصول غير المصرح به للمعلومات المخزنة عبر الإنترنت أو داخل الأنظمة الرقمية، ويشمل تقنيات مثل التشفير، ومراقبة الشبكات، وإدارة الهوية، والتحقق من الهوية عبر الإنترنت، بالإضافة إلى برامج مراقبة واكتشاف التهديدات. الأمن السيبراني يعد

عنصراً أساسياً في حماية الأفراد والشركات من المخاطر المرتبطة بتكنولوجيا المعلومات في العالم الرقمي المتطور بسرعة.¹⁸

ثانياً: تطور التكنولوجيا وتأثيرها على الأمن السيبراني:

شهدت السنوات الأخيرة تقدماً هائلاً في مجالات التكنولوجيا، مما أدى إلى تغييرات جذرية في كيفية تعامل الأفراد والمؤسسات مع المعلومات والبيانات. ومع هذا التطور، برزت تحديات جديدة في الأمن السيبراني، حيث أصبحت التهديدات أكثر تعقيداً وتنظيماً، مما يستدعي تبني استراتيجيات متقدمة لحماية البيانات والأنظمة، ومن أبرز التحديات والاتجاهات في الأمن السيبراني:

1. التحول الرقمي وتوسيع نطاق الحماية:

مع توسع استخدام الحوسبة السحابية وإنترنت الأشياء، لم يعد تأمين المحيط الداخلي للشبكة كافياً، حيث أصبحت البيانات منتشرة عبر مواقع متعددة، مما يتطلب استراتيجيات أمان جديدة لحماية البيانات أثناء انتقالها عبر الشبكات المختلفة وتأمين الأجهزة الطرفية المتصلة بالشبكة.

2. الذكاء الاصطناعي في مواجهة التهديدات السيبرانية:

أصبح الذكاء الاصطناعي أداة قوية وفعالة في التنبؤ بالهجمات الإلكترونية، حيث يُستخدم في تحليل البيانات الضخمة بسرعة وكفاءة، مما يساهم في الكشف المبكر عن الأنماط المشبوهة والتعامل مع

¹⁸ القاضي، مروء، وسلطان، سوزان. (2024). واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة: دراسة حالة. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، 4(2)

التحديات قبل وقوعها. هذه القدرة تعزز من مقدرة المؤسسات على مواجهة المخاطر السيبرانية بشكل فعال، مما يساهم في تقليل الخسائر والأضرار الناجمة عن الهجمات الإلكترونية. كما أن الذكاء الاصطناعي يُمكن أنظمة الأمان السيبراني من التعلم والتكيف مع أساليب الهجمات الجديدة، مما يزيد من قدرتها على التعامل مع التحديات المتطورة بشكل مستمر.

3. التحديات المرتبطة بتقدم الذكاء الاصطناعي:

في الوقت الذي يوفر فيه الذكاء الاصطناعي إمكانيات متقدمة لـ تعزيز الأمن السيبراني، إلا أنه قد يُستغل أيضاً من قبل المهاجمين لتطوير هجمات سيبرانية أكثر تعقيداً. هذا الاستغلال قد يؤدي إلى خلق تهديدات جديدة وصعبة الاكتشاف، مما يزيد من الحاجة إلى تطوير استراتيجيات دفاعية متقدمة. يتطلب هذا الأمر مواكبة التطورات المتسارعة في تقنيات الذكاء الاصطناعي، لضمان قدرة الأنظمة الأمنية على التعامل مع هذه التحديات المتطورة بكفاءة. وبالتالي، يصبح من الضروري تحديث الأدوات الدفاعية والتكامل بين الذكاء الاصطناعي وأدوات الأمن السيبراني لمواكبة هذه التحديات¹⁹.

¹⁹ يونس، ي. ر. (2020). التحديات القانونية للجرائم السيبرانية في القانون الدولي. موسوعة ودق القانونية.

4. دور الذكاء الاصطناعي في تعزيز الأمن السيبراني خلال التحول الرقمي:

مع التوسع السريع في التحول الرقمي، أصبحت المؤسسات تعتمد بشكل متزايد على التكنولوجيا الرقمية في عملياتها اليومية، مما يعرضها بشكل أكبر إلى الهجمات السيبرانية المنظمة. في هذا السياق، يعد الذكاء الاصطناعي عنصرًا حيويًا في تحسين الأمن السيبراني، حيث يساعد في مراقبة التهديدات بشكل مستمر، ويتيح الاستجابة السريعة لهذه التهديدات، مما يساهم في التقليل من نقاط الضعف الأمنية. يساعد الذكاء الاصطناعي في تحليل البيانات بسرعة كبيرة للكشف عن أي أنماط مشبوهة، مما يعزز قدرة المؤسسات على التصدي للهجمات بشكل فعال، ويضمن حماية أكبر للبنية التحتية الرقمية.

مع تزايد تعقيد التهديدات السيبرانية، أصبح من الضروري اعتماد نهج شامل ومبتكر لتعزيز الأمن الرقمي. يتطلب ذلك التعاون بين الحكومات والمؤسسات، وتحديث السياسات الأمنية، وتعزيز استخدام الذكاء الاصطناعي كأداة رئيسية في الدفاع السيبراني، لضمان بيئة رقمية أكثر أمانًا واستقرارًا في المستقبل.²⁰

ثالثًا: دور التكنولوجيا في تعزيز الأمن السيبراني:

التكنولوجيا تلعب دورًا محوريًا في تعزيز الأمن السيبراني من خلال تقديم أدوات وتقنيات متقدمة تهدف إلى الكشف المبكر عن التهديدات، الوقاية منها، والاستجابة الفعالة لها. من بين هذه الأدوات برامج مكافحة الفيروسات، جدران الحماية، أنظمة الكشف عن التسلل، تقنيات التشفير، إضافة إلى الذكاء الاصطناعي والتعلم الآلي. هذه التقنيات تساعد في مراقبة الأنماط غير الطبيعية، التنبؤ

²⁰ طرق، سلة. (2020). كيف يؤثر الذكاء الاصطناعي في الأمن السيبراني؟ مجلة عالم التكنولوجيا، 5(4)

بالتهديدات المستقبلية، وتسريع الاستجابة للهجمات السيبرانية، مما يزيد من قدرة الأنظمة على التأقلم مع الهجمات الجديدة.

بالإضافة إلى ذلك، تساهم بعض التقنيات الحديثة مثل الذكاء الاصطناعي في تعزيز قدرات الدفاعات الإلكترونية. يمكن استخدام الذكاء الاصطناعي لتحليل كميات ضخمة من البيانات واكتشاف الأنماط المشبوهة، مما يساهم في التنبؤ بالتهديدات قبل حدوثها، وبالتالي تحسين فاعلية الإجراءات الأمنية.²¹

من جانب آخر، من المعروف أن تطور تقنيات الخصوصية له دور كبير في حماية البيانات الشخصية، حيث تعمل بعض الأدوات على ضمان امتثال المؤسسات للوائح حماية البيانات. هذه التدابير تساهم في تعزيز ثقة العملاء بالمؤسسات، حيث يشعرون بالأمان في استخدام خدماتها دون القلق بشأن سرية بياناتهم.²²

إجمالاً، فإن التكنولوجيا الحديثة، خاصة الذكاء الاصطناعي، أصبحت من العوامل الرئيسية في تعزيز الأمن السيبراني، وذلك من خلال تحسين القدرة على الكشف المبكر عن التهديدات، التعامل مع التهديدات المستقبلية، وتقديم استجابات سريعة، مما يساعد في حماية المعلومات والأنظمة الرقمية بشكل فعال.

المبحث الثالث: التأثيرات والتحديات في الأمن السيبراني

المطلب الأول: الآثار المترتبة على جرائم الأمن السيبراني:

²¹ دحماني، محمد. (2023). الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني. مجلة الفكر القانوني والسياسي، 7(2)،

²² عبد المجيد، داليا. (2024). خمس توجهات للأمن السيبراني عام 2025: استشراف مستقبل الدفاع الرقمي. كوكب العلم.

https://www.bibalex.org/SCIplanet/ar/Article/Details?id=18061&utm_source=chatgpt.com

أولاً: الآثار القانونية والاقتصادية المترتبة على جرائم الأمن السيبراني:

تعد جرائم الأمن السيبراني من أخطر التهديدات التي تواجه الأفراد، الشركات، والمؤسسات الحكومية، لما تسببه من أضرار قانونية، اقتصادية، واجتماعية قد تمتد آثارها لفترات طويلة. وتتراوح هذه الآثار بين خسائر مالية ضخمة، وانتهاك للخصوصية، وتهديد للأمن الوطني، فضلاً عن التأثير النفسي الذي يترتب على الضحايا. وفيما يلي تفصيل للآثار المترتبة على هذه الجرائم:

1. الآثار القانونية

تؤدي جرائم الأمن السيبراني إلى تداعيات قانونية خطيرة، حيث يجد الأفراد والشركات أنفسهم متورطين في قضايا قانونية قد تمتد لسنوات، سواء كانوا ضحايا لهذه الجرائم أو متهمين بارتكابها. تشمل هذه الآثار:

- **المساءلة القانونية عن انتهاك القوانين السيبرانية:** في حال كان مرتكب الجريمة فرداً أو منظمة، فقد يواجه عقوبات قانونية صارمة مثل السجن، الغرامات المالية الكبيرة، أو حتى الحظر من مزاولة الأنشطة الإلكتروني

- **المسؤولية المدنية والتعويضات:** قد يجبر الأفراد أو الشركات المتضررة على اللجوء إلى القضاء للمطالبة بتعويضات مالية عن الأضرار التي لحقت بهم بسبب جرائم مثل سرقة البيانات أو الهجمات السيبرانية التي تعطل أعمالهم²³.

²³ العمارة، م.، & عبدالرزاق، م. (2024). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. مجلة طبنة للدراسات العلمية الأكاديمية، 7(1)، 1337-1353.

- التحديات القانونية في ملاحقة المجرمين السيبرانيين: نظرا لأن مرتكبي هذه الجرائم غالبًا ما يعملون من دول مختلفة، فإن تعقيدات القوانين الدولية قد تعيق القبض عليهم أو محاكمتهم، مما يجعل من الصعب تحقيق العدالة.

2. الآثار الاقتصادية تشكل جرائم الأمن السيبراني تهديدا مباشرا للاقتصاد العالمي، حيث تؤدي إلى خسائر مالية تقدر بمليارات الدولارات سنويا. ومن أبرز التأثيرات الاقتصادية لهذه الجرائم:

- الخسائر المالية المباشرة: نتيجة لسرقة الأموال من الحسابات المصرفية، أو الاحتيال عبر الإنترنت، أو برامج الفدية التي تطالب الشركات بدفع مبالغ ضخمة لاستعادة بياناتها.

- انهيار الشركات وتراجع ثقة المستثمرين: عندما تتعرض شركة كبرى لهجوم سيبراني يؤدي إلى تسريب بياناتها أو تعطيل أنظمتها، فإن ذلك قد يتسبب في انخفاض قيمة أسهمها، وتراجع ثقة العملاء والمستثمرين، مما قد يدفع بعض الشركات إلى الإفلاس.

- زيادة تكاليف الأمن السيبراني: تضطر الشركات إلى إنفاق مبالغ طائلة على تعزيز أنظمتها الأمنية، وتوظيف خبراء أمن معلومات، وتحديث بنيتها التحتية الرقمية لتجنب الوقوع ضحية لمثل هذه الهجمات.

ثانيا: الآثار الاجتماعية والنفسية المترتبة على جرائم الأمن السيبراني:

3- تؤثر جرائم الأمن السيبراني بشكل مباشر على الأفراد، ليس فقط من الناحية المالية، بل أيضا

من الناحية النفسية والاجتماعية، حيث تؤدي إلى مشكلات عديدة منها²⁴:

- انتهاك الخصوصية وفقدان الثقة في التكنولوجيا: عند اختراق البيانات الشخصية للمستخدمين، مثل الصور، المحادثات الخاصة، أو المعلومات المصرفية، فإن ذلك يسبب لهم صدمة نفسية ويدفعهم إلى فقدان الثقة في استخدام الخدمات الرقمية.

- الابتزاز والتشهير الإلكتروني: قد يقع العديد من الأشخاص ضحايا للابتزاز الإلكتروني، حيث يستخدم المجرمون معلوماتهم الشخصية لتهديدهم، مما يؤدي إلى مشاكل نفسية مثل القلق والاكتئاب، بل وقد يصل الأمر إلى الانتحار في بعض الحالات.

- تفكك العلاقات الأسرية والاجتماعية: في بعض الحالات، يمكن أن تؤدي جرائم مثل الاختراقات الإلكترونية والابتزاز إلى تدمير العلاقات بين الأزواج أو الأصدقاء، بسبب نشر معلومات شخصية أو رسائل خاصة تؤدي إلى فقدان الثقة بين الأطراف المعنية²⁵.

²⁴ اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (2023). الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية. الأمم المتحدة.

²⁵ محمد، م. (2024). القانون الدولي والتحديات المعاصرة: الجريمة السيبرانية نموذجا. مجلة كلية الحقوق للبحوث القانونية والاقتصادية، 1(2)، 850-809.

4. الآثار على الأمن الوطني والاستقرار السياسي لم تعد جرائم الأمن السيبراني تقتصر على الأفراد

والشركات فقط، بل أصبحت تهدد الأمن الوطني للدول، حيث تستخدم بعض الجماعات الإجرامية والإرهابية الفضاء السيبراني لتحقيق أهداف سياسية وعسكرية، ومن أبرز هذه الآثار:

- الهجمات السيبرانية على البنية التحتية: تستهدف بعض الهجمات السيبرانية أنظمة حكومية حساسة، مثل شبكات الكهرباء، المطارات، أو أنظمة الدفاع، مما قد يؤدي إلى شلل كامل في بعض القطاعات الحيوية داخل الدولة.

- نشر المعلومات المضللة والتلاعب بالرأي العام: تلجأ بعض الجهات الإجرامية إلى نشر أخبار كاذبة أو التلاعب بالبيانات على وسائل التواصل الاجتماعي لتوجيه الرأي العام نحو أهداف معينة، وهو ما قد يؤثر على نتائج الانتخابات أو يسبب اضطرابات اجتماعية.

- التجسس الإلكتروني وسرقة المعلومات السرية: تستخدم بعض الدول أو المنظمات الإجرامية تقنيات متطورة لاختراق أنظمة الدول الأخرى، بهدف سرقة بيانات استخباراتية أو عسكرية حساسة، مما يشكل تهديدًا كبيرًا للأمن القومي.

5. تأثير جرائم الأمن السيبراني على التعليم والصحة

حتى القطاعات الحيوية مثل التعليم والصحة لم تسلم من الآثار السلبية لجرائم الأمن السيبراني، حيث أصبحت المؤسسات التعليمية والمستشفيات هدفا رئيسيا للهجمات السيبرانية.

- تعطيل أنظمة المستشفيات وسرقة بيانات المرضى: قد تؤدي الهجمات الإلكترونية إلى تعطيل أنظمة المستشفيات، مما يعرض حياة المرضى للخطر، خاصة في الحالات الحرجة التي تعتمد على الأجهزة الطبية المتصلة بالإنترنت.

- استهداف الجامعات والمؤسسات التعليمية: حيث يتم اختراق أنظمة الجامعات وسرقة بيانات الطلاب والموظفين، أو حتى تدمير المناهج الدراسية والمواد التعليمية المخزنة على الإنترنت، مما يسبب فوضى في العملية التعليمية.

تعد جرائم الأمن السيبراني تهديدًا خطيرًا على جميع المستويات، سواء للأفراد أو المؤسسات أو حتى الحكومات، حيث تؤثر على الاقتصاد، المجتمع، الأمن القومي، والقطاعات الحيوية مثل الصحة والتعليم. لذا، من الضروري تكثيف الجهود لمكافحة هذه الجرائم من خلال تعزيز القوانين السيبرانية، رفع مستوى الوعي الأمني لدى المستخدمين، وتطوير تقنيات متقدمة للحماية من الهجمات السيبرانية المتزايدة.

المطلب الثاني: التحديات الحديثة التي تواجه الأمن السيبراني

أولاً: التحديات المتعلقة بالتكنولوجيا السريعة والاعتماد المتزايد على التقنيات الرقمية

يواجه الأمن السيبراني في العصر الحديث العديد من التحديات المعقدة والمتزايدة، نتيجة للتطور التكنولوجي السريع والاعتماد المتزايد على التقنيات الرقمية. فيما يلي بعض من أبرز هذه التحديات²⁶

1. الهجمات الإلكترونية المتطورة:

²⁶ يونس، ي. ر. (2016). التحديات القانونية للجرائم السيبرانية في القانون الدولي. موسوعة ودق القانونية.

مع تقدم التكنولوجيا، أصبح المهاجمون قادرين على استخدام أدوات وتقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي لشن هجمات معقدة ومتطورة. هذه التقنيات تمكّن المهاجمين من تنفيذ هجمات صعبة الاكتشاف في وقت مبكر، مما يزيد من صعوبة التصدي لها في الوقت المناسب. يمكن أن تستهدف هذه الهجمات المؤسسات والأفراد على حد سواء، مما يعرّض البيانات والمعلومات الحساسة للخطر. وبسبب تطور أساليب الهجوم، أصبح من الضروري تطوير استراتيجيات دفاعية أكثر تطورًا وتقنيات مراقبة للكشف عن هذه الهجمات المتقدمة قبل أن تتمكن من تحقيق أهدافها.

2. نقص الوعي والتدريب:

يُعتبر نقص الوعي والتدريب في مجال الأمن السيبراني من أبرز التحديات التي تواجه الأفراد والمؤسسات. العديد من الأفراد لا يمتلكون المعرفة الكافية حول كيفية حماية بياناتهم وأنظمتهم من التهديدات الإلكترونية، مما يعرضهم للخطر. هذا النقص في الوعي يمكن أن يؤدي إلى ممارسات غير آمنة، مثل استخدام كلمات مرور ضعيفة أو عدم تحديث البرمجيات بانتظام، مما يفتح المجال للمهاجمين لاستغلال الثغرات الأمنية. لذلك، يصبح من الضروري رفع مستوى الوعي بين الأفراد والشركات، وتوفير برامج تدريبية مستمرة لضمان تطبيق أفضل ممارسات الأمان السيبراني وحماية البيانات من التهديدات المتزايدة.²⁷

3. التهديدات الداخلية:

²⁷ البهي، رغبة. (2021). الأمن السيبراني في 2020: بين الفرص والتحديات والحماية. لمركز المصري للفكر والدراسات الاستراتيجية

لا تقتصر التهديدات السيبرانية على المهاجمين الخارجيين فقط، بل تشمل أيضًا التهديدات الداخلية التي قد تأتي من موظفين أو متعاونين لديهم وصول إلى المعلومات الحساسة، وقد يستغلون هذا الوصول لأغراض ضارة. هذه الأنواع من التهديدات قد تكون صعبة الاكتشاف لأن الشخص المسؤول عن الهجوم يكون بالفعل جزءًا من النظام ويمكنه التحرك بحرية دون إثارة الشكوك. لذا، فإن التعامل مع هذه التهديدات يتطلب استراتيجيات خاصة، مثل مراقبة السلوكيات غير المعتادة، وفرض قيود الوصول بناءً على مبدأ الحد الأدنى من الامتيازات، بالإضافة إلى تدريب الموظفين على أهمية حماية البيانات والامتثال لأفضل ممارسات الأمان.

4. نقص التشريعات الموحدة:

تواجه العديد من الدول نقصًا في التشريعات الموحدة التي تنظم وتحدد معايير الأمن السيبراني، مما يخلق تحديات كبيرة في مكافحة الجرائم الإلكترونية. هذا النقص في التشريعات يجعل من الصعب محاكمة المهاجمين الإلكترونيين وتحديد المسؤوليات بوضوح، مما يعوق الجهود المبذولة للتصدي لهذه الجرائم. نتيجة لذلك، يكون من الصعب تنفيذ العقوبات بشكل فعال أو توحيد الأساليب القانونية عبر الحدود، مما يزيد من التحديات القانونية في التحقيق والملاحقة. ومن هنا، تظهر الحاجة الملحة إلى تحديث التشريعات وتوحيدها على المستوى الدولي لضمان تعزيز الأمن السيبراني وحماية البيئة الرقمية من التهديدات المتزايدة²⁸.

5. التحديات التقنية في البنية التحتية:

²⁸ عالم القانون، (2024). الأمن السيبراني: تحديات معاصرة وتشريعات متجددة.

مع تزايد الاعتماد على التقنيات الحديثة مثل الإنترنت للأشياء (IoT) والحوسبة السحابية، تزداد

المخاطر الأمنية المتعلقة بالثغرات في هذه الأنظمة. قد تحتوي بعض الأجهزة المتصلة على ثغرات أمنية غير مكتشفة أو غير مُعالجة، مما يجعلها عرضة للهجمات السيبرانية. قد تستغل الهجمات الإلكترونية هذه الثغرات للوصول إلى البيانات الحساسة أو الأنظمة الحيوية، مما يؤدي إلى تعريض الأفراد والشركات لأضرار جسيمة. لذلك، يصبح من الضروري تطوير استراتيجيات أمنية شاملة وإجراء فحوصات دورية للأنظمة والأجهزة المتصلة لضمان التقليل من الثغرات الأمنية وحماية المعلومات من التهديدات المتزايدة.

6. نقص البيانات في الذكاء الاصطناعي:

تحتاج أنظمة الذكاء الاصطناعي إلى كميات كبيرة من البيانات للتدريب، وهذا قد يكون تحديًا كبيرًا في مجال الأمن السيبراني حيث يصعب الحصول على بيانات دقيقة وكافية. علاوة على ذلك، يمكن أن تعكس أنظمة الذكاء الاصطناعي التحيزات الموجودة في البيانات التي تم تدريبها عليها، مما يؤدي إلى اتخاذ قرارات غير عادلة أو مضللة. على سبيل المثال، قد تؤدي التحيزات في البيانات إلى تمييز ضد فئات معينة أو إهمال تهديدات معينة، مما يؤثر على فعالية النظام في التعرف على التهديدات السيبرانية أو اتخاذ الإجراءات المناسبة. لذلك، من الضروري تحسين جودة البيانات وتطوير خوارزميات أكثر دقة لضمان أن تكون أنظمة الذكاء الاصطناعي في الأمن السيبراني منصفة وفعالة في التعامل مع المخاطر المتزايدة.

7. التهديدات المستمرة والمتجددة:

تتسم التهديدات في مجال الأمن السيبراني بأنها مستمرة ومتجددة، حيث يقوم المهاجمون بتطوير تقنيات وأساليب جديدة باستمرار. هذا يتطلب من المؤسسات والأفراد تحديث استراتيجياتهم الدفاعية بشكل دوري لمواكبة هذه التهديدات.²⁹

لمواجهة هذه التحديات، من الضروري تعزيز الوعي والتدريب في مجال الأمن السيبراني، وتطوير تشريعات موحدة، وتبني تقنيات متقدمة للكشف عن التهديدات والتصدي لها. كما يجب على المؤسسات تبني استراتيجيات شاملة لحماية بياناتها وأنظمتها من المخاطر المتزايدة.

ثانياً: تأثير الجرائم السيبرانية على الأمن الوطني:

تعد الجرائم السيبرانية من التهديدات الحديثة التي تؤثر بشكل كبير على الأمن الوطني للدول. تتعدد تأثيرات هذه الجرائم، حيث تستهدف البنى التحتية الحيوية، وتؤدي إلى تدهور الحالة الأمنية والاقتصادية، وتهدد القيم والأخلاق، وتدمر البنية التحتية. ومن أهم أشكال تأثير الجرائم السيبرانية على الأمن الوطني:

- **استهداف البنى التحتية الحيوية:** تستهدف الجرائم السيبرانية المؤسسات الحكومية والشركات الكبرى، بالإضافة إلى القطاعات الحيوية مثل الطاقة والاتصالات. هذه الهجمات قد تؤدي إلى تعطيل الخدمات الأساسية مثل الطاقة أو الاتصالات، مما يسبب تعطيل الحياة اليومية ويؤثر على

²⁹ Garrison, S. (2020, July 16). Challenges and solutions in cybersecurity. Stellar Cyber.

الاستقرار الاجتماعي والاقتصادي. كما يمكن أن تؤدي هذه الهجمات إلى فقدان السيطرة على أنظمة حيوية قد تضر بالأمن القومي وتعرق تقديم الخدمات المهمة للمواطنين³⁰.

-تدهور الحالة الأمنية والاقتصادية: تسبب الجرائم السيبرانية خسائر مالية ضخمة للشركات والمؤسسات، حيث تؤدي إلى سرقة الأموال أو تعطيل العمليات التجارية، مما يُترجم إلى تدهور الثقة في المؤسسات. كما يؤدي هذا إلى ضعف الاستقرار الاقتصادي والأمني للدولة، حيث تُعطل الهجمات السيبرانية الاقتصاد الرقمي وتؤثر على قدرة الشركات على العمل بكفاءة، مما يُجبر الحكومات على زيادة الإنفاق على إجراءات الأمان وتعويض الخسائر³¹.

-تهديد القيم والأخلاق: تُستخدم الجرائم السيبرانية لنشر المعلومات المضللة أو التلاعب بالرأي العام من خلال وسائل الإعلام الاجتماعية أو الإنترنت. مثل هذه الأنشطة قد تهدد القيم الاجتماعية والأخلاقية، حيث يمكن للمحتوى المضلل أن يثير الاضطرابات الاجتماعية أو يعزز الأيديولوجيات الضارة التي تهدد استقرار المجتمع. كما يمكن أن يضعف ثقة الجمهور في الإعلام والأنظمة الحاكمة.

تدمير البنية التحتية: قد تؤدي الهجمات السيبرانية إلى تدمير أو تعطيل البنية التحتية الرقمية، مثل أنظمة التشغيل المصرفية أو الشبكات الحكومية. هذه الهجمات تؤثر على العمليات اليومية

³⁰ اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (2023). الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية. الأمم المتحدة.

³¹ Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

للمؤسسات والأفراد، مثل توقف الخدمات المصرفية الإلكترونية، مما يؤدي إلى تعطيل حياة الأفراد والشركات، وقد يتسبب في انهيار الاقتصاد الرقمي في بعض الحالات³².

المبحث الثالث: استراتيجيات وتطوير التشريعات لمكافحة الجرائم السيبرانية

المطلب الأول: استراتيجيات مواجهة الجرائم السيبرانية:³³

أولاً: تعزيز الأمن السيبراني والتعاون الدولي

-**تعزيز الأمن السيبراني:** يجب على الدول والمؤسسات تطوير تقنيات وأدوات متقدمة لحماية المعلومات والأنظمة من الهجمات، مثل تحسين البرمجيات المضادة للفيروسات، وأنظمة الكشف عن التسلل، واستخدام تقنيات الذكاء الاصطناعي للتعرف على الهجمات السيبرانية والتعامل معها بسرعة وفعالية. كما أن تطوير أنظمة تشفير قوية وتعزيز البنية التحتية للأمن السيبراني يعدان من الركائز الأساسية لحماية البيانات الحساسة.

-**التعاون الدولي:** يجب تبادل المعلومات والتنسيق بين الدول لمكافحة الجرائم السيبرانية على مستوى عالمي، حيث إن العديد من الجرائم السيبرانية عابرة للحدود وتتطلب جهوداً منسقة من جميع الأطراف. يمكن تحقيق ذلك من خلال إنشاء تحالفات دولية متخصصة في الأمن السيبراني، وتوقيع اتفاقيات تعاون لتبادل المعلومات حول التهديدات الإلكترونية، وتعزيز التعاون بين الأجهزة الأمنية والجهات التنظيمية المختصة.

³² العمارات، فارس. (2023). إشكالية الاستقرار والأمن الوطني في ظل الجريمة السيبرانية. آفاق سياسية، 104،

³³ عبد الجواد، نجوان. (2023). الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية. مجلة كلية الآداب جامعة

الفيوم، 15(1)

ثانياً: التوعية والتدريب في مجال الأمن السيبراني

-التوعية والتدريب : من الضروري رفع الوعي بين الأفراد والمؤسسات حول مخاطر الجرائم السيبرانية، وتدريبهم على كيفية الوقاية منها من خلال تطوير مهارات الأمان السيبراني وتوفير تعليم مستمر في هذا المجال. يمكن تنفيذ حملات توعية دورية، وإدراج برامج الأمن السيبراني ضمن المناهج الدراسية، وإنشاء دورات تدريبية متخصصة للموظفين لتمكينهم من التعامل مع الهجمات السيبرانية المحتملة بكفاءة.

-تطوير التشريعات : يجب على الحكومات سن قوانين وتشريعات تجرم الجرائم السيبرانية وتحدد العقوبات المناسبة، مما يساعد في ردع المهاجمين وحماية الفضاء الرقمي. يشمل ذلك تحديث القوانين بشكل دوري لمواكبة تطور التهديدات الإلكترونية، وتعزيز قدرات الجهات المختصة على تنفيذ القوانين من خلال توفير الموارد التقنية والبشرية اللازمة.

-تعزيز الاستجابة للحوادث السيبرانية : يجب إنشاء فرق استجابة للطوارئ السيبرانية (CERTs) في كل دولة، بحيث تكون مسؤولة عن مراقبة التهديدات، والاستجابة الفورية للهجمات، وتقديم الدعم اللازم للمؤسسات المتضررة. كما يجب تبني استراتيجيات لاختبار واكتشاف الثغرات الأمنية بشكل دوري للحد من المخاطر المستقبلية³⁴.

³⁴ الهيئة الوطنية للأمن السيبراني. (2021). الإطار السعودي للأمن السيبراني. الرياض: الهيئة الوطنية للأمن السيبراني.

-تشجيع الاستثمار في البحث والتطوير: يُعد الاستثمار في البحث والتطوير من العوامل الأساسية لتعزيز الأمن السيبراني، حيث يمكن من خلاله تطوير تقنيات مبتكرة قادرة على التصدي للهجمات السيبرانية المتزايدة. يجب دعم الأبحاث في مجالات التشفير، والذكاء الاصطناعي، وتحليل البيانات لتعزيز القدرة على التنبؤ بالتهديدات قبل وقوعها.

من خلال هذه الاستراتيجيات المتكاملة، يمكن للدول تعزيز قدرتها على مواجهة التهديدات السيبرانية وحماية أمنها الوطني بشكل فعال، مما يساهم في بناء فضاء إلكتروني أكثر أمانًا واستقرارًا.

ثالثًا: العلاقة بين الجرائم السيبرانية وحماية البيانات الشخصية:

تعد الجرائم السيبرانية تهديدًا متزايدًا في العصر الرقمي، حيث تستهدف الأفراد والمؤسسات على حد سواء. تتضمن هذه الجرائم مجموعة متنوعة من الأنشطة غير القانونية التي تتم عبر الإنترنت، مثل سرقة الهوية، والاحتيال المالي، والاختراقات الأمنية.

تعد حماية البيانات الشخصية أمرًا بالغ الأهمية في مواجهة هذه التهديدات. تتضمن حماية البيانات الشخصية مجموعة من التدابير والإجراءات التي تهدف إلى ضمان سرية وسلامة المعلومات الشخصية للأفراد. تشمل هذه التدابير استخدام تقنيات التشفير، وتطبيق سياسات الوصول المحدود، وتوفير التدريب المستمر للمستخدمين حول أفضل ممارسات الأمان السيبراني.

تظهر الدراسات أن الجرائم السيبرانية غالبًا ما تستهدف البيانات الشخصية كجزء من استراتيجياتها. على سبيل المثال، قد يقوم المهاجمون بسرقة المعلومات الشخصية لاستخدامها في أنشطة احتيالية أو لبيعها في الأسواق السوداء. لذلك، يُعتبر تعزيز حماية البيانات الشخصية جزءًا أساسيًا من استراتيجيات مكافحة الجرائم السيبرانية، ومن خلال فهم العلاقة بين الجرائم السيبرانية وحماية البيانات الشخصية، يمكن تطوير استراتيجيات فعالة للتصدي لهذه التهديدات، مما يساهم في تعزيز الأمان السيبراني وحماية الأفراد والمؤسسات من المخاطر المحتملة.³⁵

³⁵ Almanna, A. (2023). Cybercrime. In: Legal Translation between English and Arabic. Palgrave Macmillan, Cham https://doi.org/10.1007/978-3-031-14838-5_11

المطلب الثاني: تطور التشريعات القانونية وتحليل فعاليتها

أولاً: تطور التشريعات القانونية لمكافحة الجرائم السيبرانية

تعد الجرائم السيبرانية من التحديات الكبرى التي تواجه المجتمعات الحديثة، نظراً لتزايد الاعتماد على التكنولوجيا والإنترنت في مختلف جوانب الحياة. لذلك، شهدت التشريعات القانونية تطوراً مستمراً لمكافحة هذه الجرائم، بهدف حماية الأفراد والمؤسسات من المخاطر المرتبطة بالفضاء السيبراني.

1. التشريعات الدولية:

على الصعيد الدولي، تم تبني اتفاقية بودابست بشأن الجرائم السيبرانية عام 2001 من قبل مجلس أوروبا، وهي أول معاهدة دولية تهدف إلى مكافحة الجرائم المرتكبة عبر الإنترنت. تركز الاتفاقية على توفير إطار قانوني متماسك لمكافحة الجرائم السيبرانية على مستوى عالمي، وتُعنى بالجرائم التي تهدد الأمن السيبراني، بما في ذلك التحايل المالي والاحتيال الإلكتروني. كما تتضمن الاتفاقية تدابير قانونية وتقنية لتسهيل التعاون بين الدول في مجال التحقيقات الجنائية عبر الإنترنت، بالإضافة إلى وضع معايير لتبادل المعلومات بين السلطات القضائية لضمان محاكمة المجرمين عبر الحدود.³⁶

³⁶فياله، محمد. (2024). القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجاً. مجلة الحقوق للبحوث القانونية والاقتصادية، 2(1)

2. التشريعات الوطنية:

على المستوى الوطني، قامت العديد من الدول بتطوير تشريعات خاصة لمكافحة الجرائم السيبرانية. على سبيل المثال، في الولايات المتحدة، تم إصدار قانون مكافحة الجرائم السيبرانية عام 1986 تحت اسم "قانون مكافحة الجرائم والاحتيال عبر الكمبيوتر"، والذي تم تعديله لاحقاً ليشمل جرائم جديدة تتعلق بالإنترنت مثل القرصنة، الاحتيال الإلكتروني، والاعتداءات على بيانات المستخدمين. كما أصدرت دول أخرى قوانين مشابهة تتناول الجرائم السيبرانية بشكل محدد، مثل قانون حماية البيانات في الاتحاد الأوروبي وقانون الجرائم الإلكترونية في الهند، حيث تهدف هذه التشريعات إلى توفير إطار قانوني قوي لمكافحة الجرائم الإلكترونية وحماية الأفراد والشركات من تهديدات الفضاء الرقمي.³⁷

3. التحديات والفرص:

رغم التقدم في التشريعات، إلا أن هناك تحديات مستمرة في مواجهة الجرائم السيبرانية، مثل تطور تقنيات الجريمة وتعدد أساليبها. مع تزايد استخدام تقنيات مثل الذكاء الاصطناعي وتحليل البيانات، أصبح المهاجمون قادرين على تنفيذ هجمات أكثر تعقيداً. لذلك، يُنصح بتطوير استراتيجيات شاملة تشمل التعاون الدولي بين الحكومات والهيئات التنظيمية، وتبادل المعلومات بشكل مستمر لمكافحة التهديدات

³⁷ بطيخ، حاتم. (2021). تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات: دراسة تحليلية مقارنة. مجلة

الدراسات القانونية والاقتصادية، 7

السيبرانية العابرة للحدود. بالإضافة إلى ضرورة تدريب الكوادر القانونية والتقنية لتعزيز قدرتهم على مواجهة الأساليب الجديدة والتعامل مع الحالات المعقدة.³⁸

في الختام، يُعتبر تطوير التشريعات القانونية لمكافحة الجرائم السيبرانية عملية مستمرة تتطلب تضام الجهود على المستويين الوطني والدولي. التعاون بين الدول، تبادل المعرفة والخبرات، وتبني التقنيات الحديثة ضروري لضمان بيئة آمنة في الفضاء السيبراني وتقديم الحماية الفعالة للمؤسسات والأفراد من تهديدات الفضاء الرقمي.

ثانياً: تحليل فعالية التشريعات الوطنية في مواجهة الجرائم السيبرانية

تعد الجرائم السيبرانية تحديًا متزايدًا يتطلب تقييمًا دقيقًا لفعالية التشريعات الوطنية في مواجهتها. في دراسة بعنوان "الجرائم الإلكترونية" تم التأكيد على أن الجرائم الإلكترونية تفرض أنماطًا جديدة، مما يستدعي تعديل الأركان المادية للجريمة لتشمل الأعمال التحضيرية، مثل "إعداد الفيروسات على الحاسب تمهيدًا لبثها". يشير هذا إلى ضرورة تحديث التشريعات لتشمل هذه الأفعال التحضيرية كجرائم قائمة بذاتها.³⁹

بالإضافة إلى ذلك، أظهرت مراجعة منهجية بعنوان "الوقاية والسيطرة على الاحتيال المالي: مراجعة استكشافية" أن هناك زيادة في الوعي الدولي بالأضرار الناجمة عن الاحتيال المالي، مما أدى إلى تكثيف

³⁸ عالم القانون. (2024، 19 نوفمبر). تعزيز الأمن السيبراني: تحديات الحاضر وحلول المستقبل. عالم القانون. <https://alamalkanoun.com/featured-cybersecurity-challenges>
³⁹ Almanna, A. (2023). Cybercrime. In *Legal Translation between English and Arabic* (pp. 197–212). Springer Nature.

الجهود لمنع ومكافحته. ومع ذلك، لا تزال الأدبيات المتعلقة بإجراءات مكافحة الاحتيال المالي غير مُراجعة أو مُلخصة بشكل منهجي. تشير هذه الدراسة إلى أن معظم الأبحاث تركز على "المراقبة"، بينما تحظى جوانب "التنفيذ" باهتمام أقل، مما يبرز الحاجة إلى تعزيز التشريعات الوطنية في هذا المجال.⁴⁰

⁴⁰ Gotelaere, S., & Paoli, L. (2022). Prevention and control of financial fraud: A scoping review. *European Journal on Criminal Policy and Research*. Springer Nature.

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

الفصل الثاني: التحديات القانونية في كل من المملكة العربية السعودية والمملكة الأردنية

الهاشمية

تمهيد:

يتناول الفصل التالي التحديات القانونية التي تواجه موضوع الأمن السيبراني في كل من المملكة العربية السعودية والمملكة الأردنية الهاشمية، بما في ذلك التحديات التقنية والتنظيمية التي تبرز نتيجة للتطور السريع في مجال تكنولوجيا المعلومات. سيتم استعراض أهم القوانين التي أصدرتها المملكتان في هذا المجال، مثل نظام مكافحة جرائم المعلوماتية ونظام حماية البيانات الشخصية، وكيف تساهم هذه التشريعات في تعزيز الأمن السيبراني وحماية الأفراد والمؤسسات. كما سيتناول الفصل دور الحكومة في تعزيز الأمن السيبراني من خلال استراتيجيات ومبادرات متعددة تهدف إلى حماية الفضاء السيبراني الوطني، بالإضافة إلى الجهود المبذولة لتطوير البنية التحتية الرقمية وتعزيز الوعي المجتمعي حول أهمية الأمن السيبراني.

المبحث الأول: التحديات القانونية من المملكة العربية السعودية

أولاً: القوانين السعودية لمكافحة الجرائم السيبرانية

تُعَدُّ المملكة العربية السعودية من الدول الرائدة في تبني تشريعات لمكافحة الجرائم السيبرانية، حيث أصدرت عدة قوانين تهدف إلى حماية الفضاء الإلكتروني وتعزيز الأمن السيبراني. تسعى هذه التشريعات إلى تنظيم استخدام التقنية الرقمية، وحماية الأفراد والمؤسسات من التهديدات الإلكترونية، ومعاقبة مرتكبي الجرائم السيبرانية مثل الاختراق، الاحتيال الإلكتروني، وانتهاك الخصوصية. كما تعمل المملكة على تطوير البنية التحتية للأمن السيبراني وتعزيز التعاون مع الجهات الدولية لمواجهة التحديات الرقمية الحديثة، مما يعكس التزامها بحماية فضاءها السيبراني وضمان بيئة إلكترونية آمنة ومستقرة.

أ-نظام مكافحة جرائم المعلوماتية:

صدر بالمرسوم الملكي رقم م/17 بتاريخ 8 ربيع الأول 1428هـ (27 مارس 2007)،

ويهدف إلى الحد من الجرائم المعلوماتية وتعزيز الأمن المعلوماتي، مع تحديد العقوبات على الجرائم مثل الوصول غير المصرح به إلى الأنظمة، الاحتيال الإلكتروني، وانتهاك الخصوصية، لحماية الأفراد والمؤسسات من التهديدات الرقمية وضمان بيئة إلكترونية آمنة.⁴¹

ب-نظام مكافحة غسل الأموال:

صدر نظام مكافحة غسل الأموال وتمويل الإرهاب بالمرسوم الملكي رقم م/39 بتاريخ 21 رجب

1424هـ (الموافق 17 سبتمبر 2003)، ويهدف إلى مكافحة عمليات غسل الأموال والتصدي لتمويل

الأنشطة الإرهابية، بما في ذلك الجرائم السيبرانية. يشمل النظام الجرائم المرتبطة بالأنشطة الإلكترونية غير القانونية، مثل غسل الأموال الناتج عن الاحتيال الإلكتروني، والاختراقات المالية، والأنشطة المشبوهة عبر الفضاء الرقمي، مما يعزز دور المملكة في مكافحة الجريمة المنظمة وضمان نزاهة الأنظمة المالية الرقمية.⁴²

ج-نظام مكافحة الإرهاب وتمويله:

⁴¹ هيئة الخبراء بمجلس الوزراء. (2007). نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم م/17.

⁴² هيئة الخبراء بمجلس الوزراء. (2003). نظام مكافحة غسل الأموال بالمرسوم الملكي رقم م/39.

صدر هذا النظام بالمرسوم الملكي رقم م/21 بتاريخ 24 رجب 1439هـ (10 أبريل 2018)،

ويهدف إلى مكافحة الجرائم المرتبطة بالإرهاب في الفضاء الإلكتروني، مثل التحريض على الإرهاب عبر الإنترنت، ونشر الأفكار المتطرفة، مع تحديد العقوبات المترتبة على هذه الجرائم، لضمان حماية الأمن الوطني والتصدي للتهديدات الرقمية التي تستهدف الاستقرار.⁴³

د-نظام حماية البيانات الشخصية:

صدر هذا النظام بالمرسوم الملكي رقم م/19 بتاريخ 9 رجب 1443هـ (الموافق 10 فبراير

2022). يهدف النظام إلى حماية خصوصية الأفراد في الفضاء الإلكتروني، وتحديد كيفية جمع واستخدام وتخزين البيانات الشخصية، بالإضافة إلى إنشاء هيئة حماية البيانات الشخصية للإشراف على تطبيق أحكام هذا النظام.⁴⁴

ثانياً: القوانين والتشريعات المعمول بها في المملكة العربية السعودية لمكافحة جرائم الأمن السيبراني

تولي المملكة العربية السعودية اهتماماً بالغاً بالأمن السيبراني نظراً للتطور التكنولوجي المتسارع وزيادة التهديدات الرقمية التي تستهدف الأفراد والمؤسسات والبنية التحتية الوطنية. ولذلك، وضعت السعودية إطاراً قانونياً قوياً لمكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني، يتضمن مجموعة من القوانين والأنظمة التي تحدد الجرائم والعقوبات المرتبطة بها، إضافة إلى السياسات التنظيمية التي تعزز حماية البيانات والمعلومات الرقمية.

⁴³ هيئة الخبراء بمجلس الوزراء. (2018). نظام مكافحة الإرهاب وتمويله بالمرسوم الملكي رقم م/21.

⁴⁴ هيئة الخبراء بمجلس الوزراء. (2022). نظام حماية البيانات الشخصية بالمرسوم الملكي رقم م/19.

1. نظام مكافحة الجرائم المعلوماتية (مرسوم ملكي رقم م/17 لعام 1428هـ - 2007م)

يعد هذا النظام من أهم القوانين التي تنظم مكافحة الجرائم السيبرانية في السعودية، حيث يهدف إلى الحد من الجرائم التي تُرتكب عبر الإنترنت وحماية المصلحة العامة والمجتمع من التهديدات الرقمية. يحدد النظام الأفعال التي تعتبر جرائم معلوماتية، مثل:

الوصول غير المشروع إلى الأنظمة الإلكترونية: حيث يعاقب كل من يخترق نظامًا معلوماتيًا دون تصريح، بغرامات مالية وعقوبات بالسجن.

التجسس الإلكتروني: أي التنصت أو اعتراض البيانات أو الاتصالات الإلكترونية دون إذن قانوني.

الاحتيال المالي عبر الإنترنت: ويشمل سرقة المعلومات المصرفية أو تنفيذ عمليات مالية غير قانونية عبر الوسائل الرقمية.

انتهاك الخصوصية: مثل تصوير الأشخاص أو تسجيل محادثاتهم دون إذن، أو نشر بياناتهم الشخصية دون موافقتهم.

إثارة الفتنة والإضرار بالنظام العام عبر الإنترنت: مثل نشر أخبار كاذبة أو محتوى تحريضي يهدف إلى زعزعة الاستقرار.

ويفرض النظام عقوبات مشددة تصل إلى السجن لمدة عشر سنوات، وغرامات مالية تصل إلى خمسة ملايين ريال سعودي، وذلك بحسب نوع الجريمة ومدى خطورتها⁴⁵.

2. نظام الجرائم الإلكترونية الجديد (التعديلات المقترحة 2023)

بسبب تطور الجرائم السيبرانية، تعمل السعودية على تحديث نظام مكافحة الجرائم المعلوماتية من خلال تعديلات جديدة تشمل:

تعزيز العقوبات على جرائم الاحتيال المالي الإلكتروني. وتشديد العقوبات على الجرائم المتعلقة بانتهاك الخصوصية، خاصة في ظل انتشار وسائل التواصل الاجتماعي. أيضا تنظيم المحتوى الرقمي وتوسيع نطاق الجرائم المتعلقة بالأخبار الكاذبة والمعلومات المضللة. مع تحسين آليات التعاون الدولي لملاحقة المجرمين السيبرانيين خارج المملكة.

⁴⁵ أبو الرب، م. أ. ع. (2019). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. المجلة الجزائرية للأمن الإنساني.

3. نظام حماية البيانات الشخصية (صدر بموجب مرسوم ملكي عام 2021)

يهدف هذا النظام إلى حماية البيانات الشخصية للمواطنين والمقيمين، ومنع إساءة استخدامها من قبل الجهات التي تقوم بجمعها أو معالجتها. يتضمن النظام الأحكام التالية:

تحديد قواعد جمع البيانات الشخصية وتخزينها ومعالجتها. وفرض قيود صارمة على نقل البيانات خارج المملكة إلا وفق شروط معينة. أيضا منح الأفراد حقوقاً قانونية في التحكم في بياناتهم، مثل الحق في الوصول إلى البيانات، وتصحيحها، وحذفها. مع فرض غرامات كبيرة على الجهات التي تنتهك أحكام هذا النظام، خاصة إذا تسببت في تسريب بيانات حساسة⁴⁶.

4. نظام مكافحة الاحتيال المالي وخيانة الأمانة (صدر عام 2023)

نظرا لتزايد جرائم الاحتيال السيبراني، خاصة في القطاع المالي، تم إصدار هذا النظام لمواجهة عمليات الاحتيال التي تتم عبر الإنترنت. يتضمن القانون عقوبات صارمة على من يقومون بتنفيذ عمليات احتيال⁴⁷ إلكترونية، مثل انتحال الهوية المالية، أو التلاعب بالمعاملات الرقمية، أو استخدام بطاقات الدفع الإلكترونية بشكل غير قانوني.

⁴⁶ بني سلامة، م. ع. (2018). الجريمة السيبرانية في النظام القانوني الأردني. مجلة جامعة الزرقاء للبحوث والدراسات الإنسانية، ع34.

لمالكي، ر. ع. (2023). مكافحة الجرائم السيبرانية في السعودية: دراسة مقارنة. مجلة القانون الدولي، 9(1)، 40-55.⁴⁷

5. نظام الهيئة الوطنية للأمن السيبراني (صدر بموجب أمر ملكي عام 2017)

أنشأت المملكة الهيئة الوطنية للأمن السيبراني (NCA) لتكون الجهة المسؤولة عن وضع السياسات

العامّة لحماية البنية التحتية الرقمية للدولة. تعمل الهيئة على:

وضع معايير الأمن السيبراني للمؤسسات الحكومية والخاصة. ومراقبة الامتثال لهذه المعايير وضمان

تطبيق أفضل الممارسات في الأمن السيبراني. وتطوير استراتيجيات لمواجهة التهديدات الإلكترونية التي

تستهدف البنية التحتية الوطنية. أيضا تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وتبادل

المعلومات مع الدول والمنظمات المختصة⁴⁸.

6. نظام التجارة الإلكترونية (صدر عام 2019) ينظم هذا النظام التعاملات التجارية التي تتم عبر

الإنترنت، ويشمل حماية حقوق المستهلك، وضمان عدم استغلال المنصات الإلكترونية في تنفيذ عمليات

احتيال أو تلاعب بالبيانات المالية. كما يفرض النظام إجراءات أمنية على المتاجر الإلكترونية لحماية

بيانات العملاء ومنع تسريب المعلومات الشخصية.

⁴⁸ الحربي، ع. م. (2017). التحديات القانونية للأمن السيبراني في المملكة العربية السعودية. مجلة الدراسات القانونية المعاصرة، 6(1)، 55-70.

7. أنظمة ولوائح البنك المركزي السعودي (SAMA) للأمن السيبراني

نظرا لأن القطاع المصرفي والمالي من أكثر القطاعات عرضة للهجمات السيبرانية، وضع البنك المركزي السعودي مجموعة من القواعد واللوائح التي تُلزم البنوك وشركات التقنية المالية باتتباع معايير صارمة في الأمن السيبراني، تشمل:

- تطبيق بروتوكولات التشفير لحماية المعاملات المالية.
- فرض إجراءات تحقق مزدوجة لمنع الاحتيال الإلكتروني.
- وضع خطط استجابة لحوادث الأمن السيبراني والتعامل الفوري مع الاختراقات.

8. نظام مكافحة غسل الأموال وتمويل الإرهاب (آخر تعديل عام 2022)

يتضمن هذا النظام مواد تتعلق بمكافحة استخدام الإنترنت لتنفيذ عمليات غسل الأموال وتمويل الإرهاب، خاصة عبر العملات الرقمية والمنصات الإلكترونية. يفرض القانون رقابة صارمة على المعاملات المالية المشبوهة، ويوجب الإبلاغ عن أي عمليات إلكترونية غير اعتيادية قد تكون مرتبطة بجرائم

مالية.⁴⁹

⁴⁹ القصير، ي. ع. (2023). الجرائم الإلكترونية في السعودية: التحديات والحلول القانونية. مجلة القانون والمجتمع، 22(3)، 100-115.

ثالثاً: التعاون الدولي في مكافحة الجرائم الإلكترونية

تشارك السعودية بفعالية في الاتفاقيات الدولية لمكافحة الجرائم السيبرانية، وتعمل على التعاون مع الدول الأخرى لملاحقة مجرمي الإنترنت الذين ينفذون هجماتهم من خارج المملكة. كما أن المملكة تعتمد على تبادل المعلومات الاستخباراتية مع جهات دولية مختصة لتعزيز الأمن السيبراني على مستوى عالمي.

- تعكس هذه التشريعات والأنظمة مدى التزام السعودية بتعزيز الأمن السيبراني وحماية الأفراد والمؤسسات من التهديدات الرقمية. كما أن التطوير المستمر للقوانين يعكس إدراك المملكة للتغيرات السريعة في مجال الجرائم الإلكترونية، مما يجعل نظامها القانوني أكثر تكيفاً مع التحديات المستقبلية. ومع استمرار تقدم التكنولوجيا، من المتوقع أن تستمر السعودية في إصدار تحديثات جديدة تعزز الحماية الرقمية وتدعم بيئة إلكترونية آمنة لجميع المستخدمين⁵⁰.

رابعاً: العقوبات المفروضة على مرتكبي جرائم الأمن السيبراني وفقاً للنظام السعودي

تولي المملكة العربية السعودية اهتماماً بالغاً بمكافحة جرائم الأمن السيبراني، وذلك من خلال نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) لعام 1428هـ (2007م)، بالإضافة إلى تعديلات وتشريعات لاحقة تهدف إلى تعزيز الأمن السيبراني والحد من الجرائم الإلكترونية. يتضمن هذا النظام عقوبات صارمة تتراوح بين السجن والغرامات المالية، وذلك بحسب طبيعة الجريمة وخطورتها وتأثيرها على الأفراد أو المؤسسات أو الأمن الوطني.

⁵⁰ Kramer, F. D., & Starr, S. H. (2016). Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization. National Defense University Press

عقوبة الوصول غير المشروع إلى الأنظمة المعلوماتية

يعاقب كل من يقوم بالدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي دون تصريح، بالسجن لمدة تصل إلى سنة واحدة، أو غرامة مالية تصل إلى 500 ألف ريال سعودي، أو بكلا العقوبتين معا.

إذا كان الدخول غير المشروع بهدف الحصول على بيانات أو تغييرها أو إتلافها، فتتعدد العقوبة لتصل إلى السجن 3 سنوات وغرامة مالية تصل إلى مليوني ريال سعودي.

في حال أدى الاختراق إلى تعطيل الأنظمة الحكومية أو المنشآت الحيوية، فقد تصل العقوبة إلى السجن 10 سنوات وغرامة تصل إلى 5 ملايين ريال سعودي⁵¹.

عقوبة التجسس الإلكتروني واعتراض البيانات

يحظر النظام أي محاولة لاعتراض البيانات الإلكترونية أو التجسس على الاتصالات عبر الإنترنت، وتصل العقوبة إلى: السجن لمدة تصل إلى 4 سنوات. وغرامة تصل إلى 3 ملايين ريال سعودي. وفي

حال كان التجسس يستهدف جهات حكومية أو أنظمة حساسة، فقد تصل العقوبة إلى السجن 10 سنوات وغرامة مالية أقصاها 5 ملايين ريال سعودي⁵².

عقوبة الاحتيال الإلكتروني وسرقة المعلومات المصرفية

⁵¹ الحربي، ع. م. (2024). التحديات القانونية للأمن السيبراني في المملكة العربية السعودية. مجلة الدراسات القانونية المعاصرة، 6(1)، 55-70.

⁵² Almann, A. (2023). Cybercrime. In: Legal Translation between English and Arabic. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-14838-5_11

يعد الاحتيال المالي عبر الإنترنت، مثل سرقة بيانات البطاقات الائتمانية أو تنفيذ معاملات غير مشروعة عبر المنصات الرقمية، جريمة خطيرة، ويعاقب مرتكبها بـ: السجن لمدة تصل إلى 3 سنوات. وغرامة تصل إلى مليوني ريال سعودي. وإذا كان الجاني يعمل ضمن عصابة إجرامية أو استهدف عدة ضحايا، فقد تصل العقوبة إلى السجن 7 سنوات وغرامة مالية تصل إلى 5 ملايين ريال سعودي.⁵³

عقوبة نشر أو ترويج المحتوى الإباحي أو المخالف للقيم الإسلامية

يحظر النظام نشر أو توزيع المحتوى الذي يتعارض مع القيم الدينية والأخلاقية أو يحرض على الفسوق عبر الإنترنت، ويعاقب مرتكبها بـ: السجن لمدة تصل إلى 5 سنوات. وغرامة تصل إلى 3 ملايين ريال سعودي. وتشديد العقوبة في حال كان النشر يستهدف القاصرين أو يُستخدم في سياقات الابتزاز والاستغلال الجنسي.⁵⁴

عقوبة الابتزاز الإلكتروني والتشهير وانتهاك الخصوصية

يعاقب كل من يستخدم وسائل التقنية الحديثة لابتزاز شخص آخر أو تهديده أو التشهير به أو نشر معلوماته الشخصية دون إذنه، بالعقوبات التالية: السجن لمدة تصل إلى سنة واحدة. وغرامة تصل إلى

⁵³ National Research Council. (2014). Cybersecurity and cybepower: Defining the legal and policy framework. National Academies Press.

⁵⁴ العتيبي، م. خ. (2023). دور التشريعات السعودية في مواجهة الجرائم السيبرانية. مجلة الأمن والحياة، 19(3)، 45-60.

500 ألف ريال سعودي. وإذا كان الابتزاز ينطوي على تهديد خطير أو يؤدي إلى أضرار نفسية

واجتماعية جسيمة، فقد يتم تشديد العقوبة إلى السجن 3 سنوات وغرامة تصل إلى مليون ريال سعودي.

عقوبة تعطيل الخدمات الإلكترونية أو نشر الفيروسات والبرمجيات الضارة

تعتبر الهجمات الإلكترونية التي تستهدف البنية التحتية الرقمية للمملكة أو تعطل خدمات الإنترنت جريمة

خطيرة، وتصل عقوبتها إلى: السجن لمدة تصل إلى 4 سنوات. وغرامة تصل إلى 3 ملايين ريال

سعودي. وإذا كان الهجوم يستهدف منشآت حكومية أو بنية تحتية حيوية، فقد تصل العقوبة إلى السجن

10 سنوات وغرامة تصل إلى 5 ملايين ريال سعودي⁵⁵.

عقوبة تمويل الجرائم الإلكترونية أو تسهيلها

يحظر النظام تقديم أي دعم مالي أو تقني للأشخاص أو الجهات المتورطة في الجرائم الإلكترونية، مثل

تمويل الهجمات السيبرانية أو تزويد المجرمين بالبنية التحتية الرقمية. تصل العقوبة إلى: السجن لمدة

تصل إلى 5 سنوات. وغرامة تصل إلى 3 ملايين ريال سعودي. وفي حال كان التمويل يهدف إلى دعم

أنشطة إرهابية إلكترونية، فقد تصل العقوبة إلى السجن 15 عامًا وغرامة مالية ضخمة.

عقوبة نشر الأخبار الكاذبة والمعلومات المضللة عبر الإنترنت

⁵⁵ نفس المرجع السابق

نظرا لخطورة الشائعات على الأمن الوطني والسلم الاجتماعي، يعاقب النظام كل من ينشر أخبارًا كاذبة أو معلومات مضللة عبر الإنترنت بغرض إحداث فوضى أو إضرار بسمعة أشخاص أو مؤسسات، وذلك بـ: السجن لمدة تصل إلى 5 سنوات. وغرامة تصل إلى 3 ملايين ريال سعودي. وإذا كان النشر يتم عبر منصات إعلامية كبرى أو يستهدف جهات حكومية، فقد تصل العقوبة إلى السجن 10 سنوات وغرامة تصل إلى 5 ملايين ريال سعودي.

عقوبة انتحال الهوية الإلكترونية واستخدام الحسابات المزيفة

يمنع استخدام الحسابات المزيفة لانتحال شخصية أفراد أو مؤسسات أو جهات حكومية، وتصل العقوبة إلى: السجن لمدة تصل إلى 3 سنوات. وغرامة تصل إلى مليون ريال سعودي. وإذا تم استخدام الهوية المزورة في تنفيذ جرائم أخرى، مثل الاحتيال أو الابتزاز، فإن العقوبة قد تصل إلى السجن 7 سنوات وغرامة تصل إلى 5 ملايين ريال سعودي⁵⁶.

عقوبة المساس بالأمن الوطني عبر الإنترنت

تعد الجرائم الإلكترونية التي تستهدف الأمن القومي أو تحرض ضد الدولة أو تحاول التأثير على استقرارها السياسي من أخطر الجرائم السيبرانية، ويعاقب مرتكبها بـ: السجن لمدة تصل إلى 10 سنوات. وغرامة تصل إلى 5 ملايين ريال سعودي. وفي حال كان الفعل يُصنف ضمن الجرائم الإرهابية

⁵⁶ الشمري، ف. م. (2023). الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. مجلة القانون والعلوم السياسية، 15(1)، 95-110.

الإلكترونية، فقد تصل العقوبة إلى السجن المؤبد أو حتى الإعدام في بعض الحالات وفقاً للأنظمة الأمنية المعمول بها.

- تعكس هذه العقوبات مدى جدية المملكة العربية السعودية في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني. ومع التطور المستمر في تقنيات المعلومات، تقوم الجهات المعنية بتحديث الأنظمة والقوانين لضمان أقصى درجات الحماية الرقمية، سواء للأفراد أو المؤسسات أو الأمن الوطني بشكل عام. كما أن المملكة تتبنى سياسات صارمة لضمان تنفيذ هذه العقوبات بفعالية، مما يحد من الجرائم الإلكترونية ويجعل البيئة الرقمية أكثر أماناً واستقراراً.

خامساً: كيف تواجه المملكة العربية السعودية التحديات التقنية والقانونية المستجدة في مجال الأمن السيبراني

مع تزايد الاعتماد على التكنولوجيا الرقمية وتنامي التهديدات السيبرانية عالمياً، اتخذت المملكة العربية السعودية نهجاً شاملاً ومتعدد الجوانب لمواجهة التحديات التقنية والقانونية المستجدة في مجال الأمن السيبراني. يشمل هذا النهج تطوير الأطر التشريعية، تعزيز القدرات التقنية، التعاون الدولي، ورفع الوعي العام حول المخاطر السيبرانية. وفيما يلي هذه أبرز الاستراتيجيات التي تعتمدها المملكة لمجابهة هذه التحديات⁵⁷:

1. تعزيز الإطار القانوني والتنظيمي لمكافحة الجرائم السيبرانية

Almanna, A. (2023). Cybercrime. In: Legal Translation between English and Arabic. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-14838-5_11

تعمل المملكة بشكل مستمر على تطوير القوانين والتشريعات التي تحكم الأمن السيبراني لمواكبة التطورات التقنية المستجدة. ومن أبرز الجهود في هذا المجال⁵⁸:

- تحديث نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) لعام 1428هـ، بحيث يتضمن عقوبات صارمة لمكافحة جرائم الاختراق، الاحتيال الإلكتروني، التجسس، الابتزاز، ونشر الأخبار الكاذبة.

- إصدار اللائحة التنفيذية لنظام مكافحة الجرائم المعلوماتية، والتي تفصل الإجراءات التنفيذية لملاحقة المجرمين السيبرانيين وتعزيز آليات التحقيق في الجرائم الرقمية.

- إصدار قوانين لحماية البيانات الشخصية وفقاً لأحدث المعايير الدولية، والتي تلزم الجهات الحكومية والخاصة بضمان سرية وحماية بيانات المستخدمين⁵⁹.

- تفعيل أنظمة مكافحة الهجمات السيبرانية ضد البنية التحتية الحساسة، مثل أنظمة المصارف، الطاقة، الصحة، والاتصالات، لضمان استمرارية الخدمات الحيوية.

- إنشاء الهيئة الوطنية للأمن السيبراني (NCA)، وهي الجهة التنظيمية المسؤولة عن تطوير الاستراتيجيات والسياسات المتعلقة بالأمن السيبراني والإشراف على تنفيذها عبر القطاعات المختلفة.

⁵⁸ يونس، ي. ر. (2024). التحديات القانونية للجرائم السيبرانية في القانون الدولي. موسوعة ودق القانونية.

⁵⁹ Andreasson, K. J. (2012). Cybersecurity: Public sector threats and responses. CRC Press

2. الاستثمار في البنية التحتية التقنية لحماية الفضاء السيبراني تعمل المملكة على تعزيز بنيتها

البنية التحتية الرقمية لمواجهة التهديدات السيبرانية من خلال عدة إجراءات تقنية متقدمة⁶⁰:

تطوير أنظمة كشف الهجمات السيبرانية والاستجابة لها عبر تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة لتحديد أي أنشطة مشبوهة في الشبكات الرقمية. واستخدام أنظمة التشفير المتقدمة لحماية المعلومات والاتصالات الحساسة، مما يمنع الجهات غير المصرح لها من الوصول إلى البيانات. مع توسيع مراكز العمليات الأمنية (Security Operations Centers – SOC) لمراقبة التهديدات السيبرانية على مدار الساعة والاستجابة للهجمات في الوقت الفعلي. والاعتماد على الحوسبة السحابية الوطنية لضمان تخزين البيانات في بيئات محمية تخضع لأنظمة أمنية متطورة تمنع الاختراقات والتسريبات. مع تعزيز تقنيات الحماية ضد البرمجيات الخبيثة من خلال تطوير برامج مكافحة الفيروسات، الجدران النارية المتقدمة، وتقنيات كشف البرمجيات الضارة داخل المؤسسات الحكومية والخاصة.

3. تعزيز التعاون الدولي والإقليمي في مجال الأمن السيبراني نظرا للطبيعة العالمية للتهديدات

السيبرانية، تسعى المملكة إلى تعزيز التعاون مع الدول الأخرى والمنظمات الدولية لمكافحة الجرائم الإلكترونية من خلال: الانضمام إلى الاتفاقيات الدولية لمكافحة الجرائم السيبرانية، مثل اتفاقية بودابست

⁶⁰ كورنيش، ب. (2017). الأمن السيبراني: الجغرافيا السياسية، القانون والسياسة. دار نشر جامعة أكسفورد.

لمكافحة الجرائم الإلكترونية، والتي تهدف إلى تسهيل تبادل المعلومات بين الدول لملاحقة المجرمين السيبرانيين عبر الحدود⁶¹.

- التعاون مع الشركات العالمية المتخصصة في الأمن السيبراني، مثل مايكروسوفت، سيسكو، وبالو ألتو، لتعزيز البنية التحتية للأمن الرقمي داخل المملكة.

- إبرام اتفاقيات تبادل المعلومات حول التهديدات السيبرانية مع الدول الخليجية والعربية لتعزيز الجهود المشتركة في مواجهة الهجمات الإلكترونية.

- المشاركة في المؤتمرات الدولية للأمن السيبراني مثل المنتدى الدولي للأمن السيبراني (GCF) الذي تستضيفه المملكة لتعزيز التعاون وتبادل الخبرات في مجال الأمن السيبراني.

4. تطوير القدرات البشرية والتدريب المستمر للمتخصصين في الأمن السيبراني

تدرك المملكة أن مواجهة التحديات السيبرانية تتطلب كوادر وطنية مؤهلة، ولذلك استثمرت بشكل كبير في تطوير المهارات والقدرات البشرية من خلال:

إطلاق برامج تعليمية متخصصة في الأمن السيبراني بالتعاون مع الجامعات السعودية والعالمية، مثل برامج البكالوريوس والماجستير في الأمن السيبراني. وتدريب الموظفين الحكوميين في القطاعات

⁶¹ الهتاش، ن. م.، & مسعود، ص. ح. (2020). التعاون الأمني في دول حوض البحر الأبيض المتوسط: التهديدات الأمنية في ضوء الصراعات الإقليمية والدولية. دار الفكر العربي.

الحساسة على كيفية التعامل مع الهجمات السيبرانية، واتخاذ التدابير الأمنية اللازمة لحماية البيانات. وإنشاء مراكز تدريب متخصصة في الأمن السيبراني، مثل الأكاديمية الوطنية للأمن السيبراني، التي تقدم برامج متقدمة في مجال التصدي للهجمات الإلكترونية. مع تشجيع الشباب على دخول مجال الأمن السيبراني من خلال المسابقات والهاكاثونات التي تهدف إلى اكتشاف المواهب وتطوير مهارات الاختراق الأخلاقي والدفاع السيبراني.

5. رفع الوعي العام حول الأمن السيبراني وتعزيز الثقافة الرقمية

من أجل تقليل مخاطر الهجمات الإلكترونية، تعمل المملكة على نشر الوعي بأهمية الأمن السيبراني بين المواطنين والمؤسسات عبر: إطلاق حملات توعية مكثفة حول الأمن السيبراني، مثل حملة "كن واعيا"، والتي تهدف إلى توعية الأفراد بأساليب الاحتيال الإلكتروني وكيفية حماية بياناتهم. وتطوير سياسات الأمن السيبراني داخل الشركات والمؤسسات، بحيث يتم تدريب الموظفين على أساليب الحماية من التصيد الاحتيالي والاختراقات الرقمية. أيضا تعزيز ثقافة الحذر الرقمي بين الأفراد من خلال وسائل الإعلام ووسائل التواصل الاجتماعي، حيث يتم توضيح مخاطر مشاركة المعلومات الحساسة عبر الإنترنت. وفرض معايير أمنية إلزامية على الشركات لضمان تنفيذ سياسات حماية البيانات والامتثال للمعايير الأمنية الصارمة.

سادسا: استخدام الذكاء الاصطناعي والتحليلات المتقدمة في الأمن السيبراني

لمواجهة التهديدات المتطورة، تعتمد المملكة على الذكاء الاصطناعي في الأمن السيبراني من خلال:

تحليل الأنماط السيبرانية وتوقع الهجمات المحتملة، مما يساعد في التصدي للهجمات قبل وقوعها. وتطوير أنظمة أمنية ذاتية التعلم يمكنها الكشف عن السلوكيات غير الطبيعية داخل الشبكات الرقمية والاستجابة تلقائيًا لمنع أي اختراق. وتعزيز تقنيات المصادقة الحيوية، مثل التعرف على بصمات الأصابع والتعرف على الوجه، لضمان حماية أقوى للحسابات والبيانات.

- تظهر الجهود التي تبذلها المملكة العربية السعودية في مجال الأمن السيبراني التزامًا كبيرًا بحماية الفضاء الرقمي من التهديدات المتزايدة. فمن خلال تحديث التشريعات، الاستثمار في التكنولوجيا، تعزيز التعاون الدولي، وتطوير الكوادر البشرية، تعمل المملكة على بناء بيئة رقمية آمنة وموثوقة تواكب التطورات التقنية السريعة. ومع استمرار تطور التهديدات السيبرانية، من المتوقع أن تستمر المملكة في تبني استراتيجيات جديدة ومتقدمة للحفاظ على أمنها السيبراني وتعزيز مكانتها كواحدة من الدول الرائدة في هذا المجال⁶².

سابعاً: التحديات القانونية في المملكة العربية السعودية

⁶² المالكي، ر. ع. (2023). مكافحة الجرائم السيبرانية في السعودية: دراسة مقارنة. مجلة القانون الدولي، 19(1)، 40-55.

أ-تطور الأنظمة القانونية وحقوق الإنسان: في إطار رؤية المملكة 2030، تسعى السعودية إلى تطوير

أنظمتها القانونية لتعزيز حقوق الإنسان. ورغم الجهود المبذولة، إلا أن هناك حاجة إلى تحديد دقيق للأدوار بين السلطات التنظيمية وضمان وصول الأفراد إلى النظام القانوني بفعالية.⁶³

ب-ضمانات التحقيق التأديبي: تُعنى هذه الدراسة ببيان الضمانات التي كفلتها الأنظمة المقارنة في كل من الأردن والسعودية أثناء سير عملية التحقيق مع الموظف المتهم بارتكاب مخالفة معينة، وذلك بهدف الكشف عنها ومن ثم إقامة المسؤولية التأديبية عليه.

ثامناً: دور الحكومة السعودية في تعزيز الأمن السيبراني

أطلقت الحكومة السعودية الاستراتيجية الوطنية للأمن السيبراني بهدف تحقيق حوكمة متكاملة للأمن السيبراني على المستوى الوطني، وإدارة فعالة للمخاطر السيبرانية، وحماية الفضاء السيبراني، وتعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية، بالإضافة إلى تعزيز الشراكات والتعاون في هذا المجال، وبناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة. أنشأت المملكة الهيئة الوطنية للأمن السيبراني في عام 2017، لتكون الجهة المسؤولة عن حماية مصالح المملكة الحيوية والأمن القومي والبنية التحتية الحساسة.⁶⁴

بالإضافة إلى ذلك، أطلقت المملكة الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز تحت مظلة اللجنة الأولمبية السعودية، بهدف تقديم أنشطة وبرامج تساهم في زيادة وعي المجتمع بالأمن السيبراني والبرمجة والدرونز، ودعم وتشجيع الشباب للاحتراف في هذا المجال. نتيجة لهذه الجهود،

أبو حجر، حازم. (2023). تطور الرقابة على دستورية القوانين في الأردن: دراسة مقارنة. مجلة كلية الشريعة والقانون بتفهما الأشراف، (26)1

⁶⁴ الهيئة الوطنية للأمن السيبراني. (2025). الاستراتيجية الوطنية للأمن السيبراني

حققت المملكة العربية السعودية المرتبة الثانية عالمياً في مؤشر الأمن السيبراني من الاتحاد الدولي للاتصالات، مما يعكس التزامها بتعزيز أمنها السيبراني وحماية بنيتها التحتية الرقمية.⁶⁵

على الرغم من هذه الإنجازات، تواجه المملكة تحديات مستمرة في مجال الأمن السيبراني، مما يتطلب استمرار الجهود المشتركة بين الحكومة والمؤسسات لتطوير استراتيجيات استجابة فورية، وتعزيز التنسيق الإقليمي، وبناء بنية تحتية رقمية قوية ومستدامة.⁶⁶

بالإضافة إلى ذلك، أصدرت المملكة العربية السعودية أنظمة حديثة لتنظيم العقوبات وتحديدتها، مثل نظام مكافحة جرائم الإرهاب وتمويله، ونظام مكافحة جرائم المعلوماتية، ونظام مكافحة غسل الأموال. تهدف هذه الأنظمة إلى مواجهة التحديات الأمنية المستجدة وتوفير إطار قانوني واضح لتجريم ومعاقبة هذه الجرائم.

المبحث الثاني: القوانين الأردنية لمكافحة الجرائم السيبرانية

تمهيد:

تُعد المملكة الأردنية الهاشمية من الدول السبّاقة في تبني تشريعات لمكافحة الجرائم السيبرانية، حيث أصدرت عدة قوانين تهدف إلى حماية الفضاء الإلكتروني وتعزيز الأمن السيبراني. من أبرز هذه التشريعات قانون الجرائم الإلكترونية رقم 27 لعام 2015، الذي يستهدف مكافحة الأنشطة الإجرامية عبر الإنترنت، وقانون الأمن السيبراني رقم 16 لعام 2019، الذي يركز على حماية البنية التحتية المعلوماتية الوطنية. كما تبنت المملكة قوانين أخرى تتعلق بحماية البيانات الشخصية ومكافحة غسل

⁶⁵ البوابة الوطنية السعودية". (2025). الأمن السيبراني في المملكة العربية السعودية"

⁶⁶ المدونة العربية". (2024). إنجازات السعودية في مجال الأمن السيبراني ."

الأموال وتمويل الإرهاب، مما يعكس التزامها بتطوير إطار قانوني متكامل يعزز الأمان السيبراني ويحمي المجتمع الرقمي.

أولاً: القوانين الأردنية لمكافحة الجرائم السيبرانية

تبنت المملكة الأردنية الهاشمية عدة قوانين وتشريعات تهدف إلى مكافحة الجرائم السيبرانية وتعزيز الأمن السيبراني لحماية الأفراد والمؤسسات من التهديدات الرقمية. ومن أبرز هذه القوانين:

أ- قانون الجرائم الإلكترونية رقم 27 لعام 2015:

صدر قانون الجرائم الإلكترونية رقم 27 لعام 2015، الذي يهدف إلى مكافحة الجرائم المرتكبة باستخدام الوسائل الإلكترونية. يشمل القانون تعريفات للجرائم الإلكترونية والعقوبات المترتبة عليها، مثل الدخول غير المصرح به إلى أنظمة المعلومات، وإلغاء أو حذف أو تعديل البيانات دون إذن. بالإضافة إلى ذلك، تم إصدار قانون الأمن السيبراني رقم 16 لعام 2019 لتعزيز حماية البنية التحتية للمعلومات الوطنية.⁶⁷

يعتبر هذا القانون من أبرز التشريعات الأردنية في مجال مكافحة الجرائم السيبرانية. يتناول القانون تعريفات للجرائم الإلكترونية والعقوبات المترتبة عليها، مثل الدخول غير المصرح به إلى أنظمة المعلومات، وإلغاء أو حذف أو تعديل البيانات دون إذن.⁶⁸

ب- قانون الأمن السيبراني رقم 16 لعام 2019:

⁶⁷ المركز الوطني للأمن السيبراني. (2019). قانون الأمن السيبراني رقم 16 لعام 2019. تم استرجاعه في 5 فبراير 2025، من <https://ncsc.jo>

⁶⁸ المركز الوطني للأمن السيبراني. (2019). قانون الأمن السيبراني رقم 16 لعام 2019.

يهدف قانون الأمن السيبراني رقم 16 لعام 2019 إلى تعزيز حماية البنية التحتية للمعلومات الوطنية، وتحديد المسؤوليات والواجبات المتعلقة بالأمن السيبراني، لضمان بيئة رقمية آمنة وموثوقة. كما ينص القانون على إنشاء المركز الوطني للأمن السيبراني، والذي يتولى الإشراف على تنفيذ السياسات والمعايير الخاصة بالأمن السيبراني، والتصدي للتهديدات الإلكترونية التي تستهدف الأنظمة الحيوية في المملكة، مما يعكس التزام الأردن بتطوير استراتيجية متكاملة لحماية فضاءها الرقمي.⁶⁹

ج- قانون حماية البيانات الشخصية رقم 13 لعام 2018:

قانون حماية البيانات الشخصية رقم 13 لعام 2018 يهدف إلى حماية خصوصية الأفراد في الفضاء الإلكتروني وضمان سرية بياناتهم الشخصية. يتناول القانون كيفية جمع واستخدام وتخزين البيانات الشخصية، ويحدد الشروط الواجب اتباعها من قبل الجهات التي تتعامل مع هذه البيانات. كما ينص على إنشاء هيئة حماية البيانات الشخصية، التي تتولى مسؤولية الإشراف على تطبيق أحكام هذا القانون وضمان الامتثال لها من قبل المؤسسات والشركات. يهدف القانون إلى تحقيق توازن بين حماية الخصوصية وتحقيق أهداف التنمية الرقمية، مما يعزز الثقة في التعاملات الإلكترونية ويحد من المخاطر المرتبطة بالتحكم في البيانات الشخصية.

⁶⁹ هيئة تنظيم قطاع الاتصالات. (2015). قانون الجرائم الإلكترونية رقم 27 لعام 2015.

د-قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 46 لعام 2007:

يتناول هذا القانون مكافحة الجرائم المالية المرتبطة بالجرائم السيبرانية، مثل غسل الأموال وتمويل الإرهاب. يتناول هذا القانون كيفية كشف ومعالجة الأموال غير المشروعة التي قد يتم تحويلها عبر الأنظمة الرقمية أو الإنترنت. كما يحدد القانون العقوبات المترتبة على هذه الجرائم ويشمل آليات تفصيلية للتعاون بين المؤسسات المالية والجهات القانونية لمكافحة عمليات غسل الأموال واستخدامها في تمويل الأنشطة الإرهابية. يساهم هذا القانون في تعزيز الأمن المالي وحماية الاقتصاد الوطني من الجرائم الرقمية المرتبطة بالأموال.⁷⁰

ه-قانون مكافحة الإرهاب رقم 55 لعام 2006: يتناول هذا القانون الجرائم المرتبطة بالإرهاب في

الفضاء الإلكتروني، مثل التحريض على الإرهاب عبر الإنترنت، واستخدام وسائل الاتصال الرقمية لنشر الأفكار المتطرفة أو تنظيم الأعمال الإرهابية. يحدد هذا القانون العقوبات المترتبة على هذه الأنشطة، بما في ذلك السجن لفترات طويلة والغرامات المالية، ويعزز قدرة السلطات على مراقبة الأنشطة المشبوهة في الفضاء السيبراني. يبرز هذا القانون التزام المملكة الأردنية بتعزيز الأمن السيبراني وحماية الفضاء الإلكتروني من الجرائم المرتبطة بالإرهاب، ويعتبر جزءاً من استراتيجية أوسع لحماية الاستقرار الأمني في البلاد.⁷¹

ثانياً: التحديات القانونية التي تواجه تطبيق القوانين في الأردن

تواجه المملكة الأردنية الهاشمية تحديات قانونية متعددة تؤثر على فعالية تطبيق القوانين. فيما يلي تحليل مفصل لأبرز هذه التحديات:

⁷⁰ هيئة تنظيم قطاع الاتصالات. (2018). قانون حماية البيانات الشخصية رقم 13 لعام 2018.

⁷¹ وزارة الداخلية. (2006). قانون مكافحة الإرهاب رقم 55 لعام 2006.

1. **الثغرات القانونية:** تواجه التشريعات الأردنية بعض الثغرات القانونية التي تؤثر على فعالية

تطبيق القوانين. من أبرز هذه الثغرات غموض في الصياغة وافتقار إلى تعريفات دقيقة لبعض الجرائم أو الحقوق، مما يؤدي إلى تفسيرات متباينة من قبل المحاكم أو السلطات التنفيذية. هذه الثغرات تؤدي في بعض الأحيان إلى صعوبة تطبيق القوانين بشكل دقيق وعادل.

من الضروري تحديث وتطوير التشريعات بانتظام لتواكب التطورات السريعة في المجالات القانونية والتقنية والاقتصادية، وتوضيح المصطلحات والتعريفات لتجنب أي لبس في التنفيذ.

2. **تطور الرقابة على دستورية القوانين:** شهدت الأردن تطوراً في مجال الرقابة على دستورية

القوانين من خلال إنشاء المحكمة الدستورية التي تشرف على فحص القوانين للتأكد من توافقها مع الدستور. ورغم هذا التقدم، فإن هناك حاجة لتعزيز فعالية هذه الرقابة لضمان حماية الحقوق والحريات الأساسية للمواطنين، والتأكد من أن جميع التشريعات المعتمدة لا تتعارض مع المبادئ الدستورية.

يمكن تحسين آلية الرقابة على دستورية القوانين من خلال تمكين المحكمة الدستورية من مراجعة القوانين بشكل أوسع وضمان معايير صارمة تتماشى مع التطورات الاجتماعية والسياسية.

3. **التحديات القانونية والتشريعية التي تواجه البلديات:** تواجه البلديات في الأردن تحديات قانونية

تتعلق بالاستقلال المالي والإداري، حيث أن القانون الحالي لا يمنح البلديات الصلاحيات الكافية لتنفيذ مشاريعها بشكل فعال ولا يوفر لها الموارد المالية المستدامة لتحقيق أهداف التنمية المحلية.

يجب العمل على تعديل التشريعات الخاصة بالبلديات لتوسيع صلاحياتها، وتوفير آليات قانونية جديدة تضمن لها الاستقلال المالي والإداري، بالإضافة إلى تطوير الهيكل التنظيمي والموارد المالية الضرورية لدعم المشاريع المحلية.

إن هذه التحديات تتطلب تحركًا جادًا من قبل المشرعين والمجتمع المدني لتعزيز فعالية النظام القانوني في الأردن. من خلال تحسين الثغرات القانونية، تعزيز الرقابة على دستورية القوانين، وتوفير الدعم للبلديات، يمكن تحقيق بيئة قانونية أكثر عدالة وفعالية تدعم التنمية الشاملة في المملكة.

ثالثًا: أوجه القصور في التشريعات الأردنية المتعلقة بمكافحة الجرائم السيبرانية

رغم الجهود التي بذلتها المملكة الأردنية الهاشمية في تطوير منظومتها القانونية لمكافحة الجرائم السيبرانية، إلا أن هناك العديد من أوجه القصور التي تجعل التشريعات الحالية غير كافية لمواكبة التطورات السريعة في الفضاء الرقمي. ومن أبرز هذه القصور أن القوانين المتعلقة بالجرائم السيبرانية لا تزال تعتمد على قانون الجرائم الإلكترونية رقم 27 لسنة 2015، الذي تم تعديله عام 2023، ومع ذلك، فإن بعض مواد لا تزال تواجه انتقادات بسبب عدم وضوحها أو قابليتها للتطبيق الفعّال على أرض الواقع.⁷²

أحد أبرز أوجه القصور يتمثل في عدم شمولية القانون لجميع أنواع الجرائم السيبرانية الحديثة، حيث يركز القانون الأردني بشكل أساسي على بعض الجرائم التقليدية مثل الاختراق غير المصرح به وسرقة البيانات، لكنه لا يعالج بوضوح جرائم أكثر تعقيدًا مثل هجمات الذكاء الاصطناعي، التلاعب بالبيانات

⁷² محمد م. (2021). الأمن السيبراني. حُماة الحق - محامي الأردن.

باستخدام تقنية "التزييف العميق" (Deepfake)، والجرائم المتعلقة بالعملات الرقمية والاحتياز عبر البلوكتشين. هذا القصور يجعل الجهات المعنية تواجه صعوبات في تتبع هذه الجرائم أو تقديم مرتكبيها للعدالة، نظرًا لعدم وجود أطر قانونية واضحة تحكم هذه القضايا.

كذلك، يعاني القانون الأردني من ضعف في العقوبات المقررة لبعض الجرائم السيبرانية، حيث أن بعض الجرائم الإلكترونية تُعاقب بغرامات مالية منخفضة لا تشكل رادعًا حقيقيًا للمجرمين، خاصة أولئك الذين يحققون أرباحًا ضخمة من خلال عمليات الاحتياز الإلكتروني أو الابتزاز السيبراني. بالإضافة إلى ذلك، هناك جرائم خطيرة مثل الهجمات التي تستهدف البنية التحتية الرقمية للدولة أو المؤسسات المالية لا يتم تصنيفها كجرائم إرهابية بوضوح، مما يجعل العقوبات المطبقة عليها غير كافية لحجم التهديد الذي تمثله.

من ناحية أخرى، يواجه القانون الأردني تحديات قانونية في مجال التحقيق الجنائي السيبراني، خاصة فيما يتعلق بجمع الأدلة الرقمية وقانونية استخدامها في المحاكم. في العديد من الحالات، يكون من الصعب تتبع المجرمين السيبرانيين بسبب استخدامهم تقنيات تشفير متقدمة أو استضافتهم لمواقعهم على خوادم خارج الأردن، الأمر الذي يتطلب تعاونًا دوليًا مع مزودي الخدمة وشركات التكنولوجيا العالمية. ومع ذلك، فإن القوانين الأردنية الحالية لا تتيح بشكل كافٍ آليات واضحة تمكن الأجهزة الأمنية من الحصول على المعلومات الرقمية بطريقة سريعة دون الإخلال بحقوق الأفراد في الخصوصية.

هناك قصور في حماية البيانات الشخصية لمستخدمي الإنترنت، حيث لا يوجد في الأردن قانون متكامل لحماية البيانات والخصوصية الرقمية على غرار القوانين الأوروبية مثل اللائحة العامة لحماية البيانات (GDPR). هذا النقص يجعل المواطنين عرضة لاستغلال بياناتهم من قبل شركات خاصة أو حتى من

قبل مجرمي الإنترنت، حيث لا توجد إجراءات قانونية صارمة تلزم الشركات بالإفصاح عن كيفية تعاملها مع البيانات الشخصية أو معاقبتها في حالة إساءة استخدامها.⁷³

كما أن هناك افتقارًا واضحًا للإطار القانوني الذي ينظم التعاون بين القطاعين العام والخاص في مجال الأمن السيبراني، حيث لا توجد تشريعات تلزم الشركات الخاصة بالإبلاغ عن الهجمات السيبرانية التي تتعرض لها، مما يؤدي إلى تأخير اكتشاف التهديدات ومعالجتها. وعلى الرغم من وجود بعض المبادرات من قبل هيئة تنظيم قطاع الاتصالات في الأردن، إلا أن هذه الجهود لا تزال غير كافية لإنشاء نظام استجابة سريع ومنظم لحالات الطوارئ السيبرانية.

- فإن القانون الأردني يواجه انتقادات تتعلق بمدى تأثيره على حرية التعبير في الفضاء الرقمي، حيث أن بعض مواده تُستخدم في ملاحقة الأفراد بسبب تعبيرهم عن آرائهم عبر الإنترنت، مما يثير جدلاً حول مدى تحقيق التوازن بين مكافحة الجرائم السيبرانية وحماية حقوق الأفراد في استخدام الإنترنت بحرية.

بناءً على هذه القصور، فإن الحاجة إلى تطوير التشريعات الأردنية الخاصة بالأمن السيبراني أصبحت ضرورية، وذلك من خلال تحديث القوانين الحالية بحيث تشمل جميع الجرائم السيبرانية الحديثة، تشديد العقوبات على الجرائم الإلكترونية الخطيرة، تبني تشريعات واضحة لحماية البيانات الشخصية، وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.

رابعاً: التنسيق بين الجهات الأمنية والقضائية في الأردن لمكافحة الجرائم الإلكترونية

يتم التنسيق بين الجهات الأمنية والقضائية في الأردن لمكافحة الجرائم الإلكترونية من خلال إطار قانوني وتنظيمي يهدف إلى تعزيز التعاون بين مختلف المؤسسات المختصة، بما في ذلك وحدة الجرائم الإلكترونية التابعة للأمن العام، والنيابة العامة، والمحاكم المتخصصة، والجهات التنظيمية مثل هيئة

⁷³ سوداح، ف. (2024). الأمن السيبراني في الأردن: تحديات الحاضر، وإستراتيجيات للمستقبل. رقمنة.

تنظيم قطاع الاتصالات. يعتمد هذا التنسيق على آليات متعددة تضمن تكامل الأدوار بين هذه الجهات، وذلك بهدف التحقيق الفعّال في الجرائم الإلكترونية، ملاحقة الجناة، وتقديمهم للعدالة، إضافةً إلى الحد من انتشار الجرائم السيبرانية في المجتمع⁷⁴.

في البداية، يلعب الأمن العام ممثلاً بوحدة الجرائم الإلكترونية دوراً محورياً في استقبال الشكاوى والبلاغات من الأفراد أو المؤسسات حول الجرائم الإلكترونية، سواء كانت تتعلق بالاختراقات، الاحتيال الإلكتروني، الابتزاز السيبراني، أو التهديدات الأخرى التي تتم عبر الإنترنت. عند تلقي البلاغ، تقوم هذه الوحدة بالتحقق من المعلومات وجمع الأدلة الرقمية باستخدام أدوات متقدمة في تحليل البيانات واستعادة المعلومات المحذوفة، وذلك بالتعاون مع الخبراء التقنيين المتخصصين في الأمن السيبراني. هذا التنسيق التقني ضروري لضمان صحة الأدلة الرقمية وقانونية جمعها، حتى تكون مقبولة أمام المحاكم عند تقديمها كأدلة إثبات ضد المتهمين⁷⁵.

بعد جمع الأدلة الرقمية وتحليلها، يتم إحالة القضية إلى النيابة العامة التي تتولى مسؤولية توجيه الاتهام وتقديم القضية أمام القضاء. النيابة العامة تعتمد بشكل كبير على التقارير الفنية التي تقدمها وحدة الجرائم الإلكترونية، والتي تشمل تفاصيل حول طبيعة الجريمة، طرق تنفيذها، الأدلة التي تم جمعها، وتحديد هوية المشتبه بهم إن أمكن. وهنا يظهر التنسيق الوثيق بين الجهات الأمنية والنيابة العامة، حيث يتم عقد اجتماعات دورية بين المحققين الرقميين والمدعين العامين لضمان أن تكون التحقيقات متوافقة مع القوانين النافذة، ولا تشوبها أي ثغرات قانونية قد تؤثر على سير العدالة.

⁷⁴ العكاليك، ح. (2021). الضوابط القانونية للأمن السيبراني في الأردن. صحيفة الغد.

⁷⁵ اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (السنة). الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية. الأمم المتحدة.

عندما تصل القضايا إلى المحاكم، يتم التعامل معها من قبل قضاة مدربين ومتخصصين في الجرائم الإلكترونية، نظرًا للطبيعة المعقدة لهذا النوع من الجرائم التي تتطلب معرفة متقدمة بالتكنولوجيا والقوانين الرقمية. القضاء يعتمد على تقارير النيابة العامة والأمن العام، وفي بعض الحالات، يتم استدعاء خبراء أمن سيبراني للإدلاء بشهاداتهم حول طبيعة الجريمة وتفسير الأدلة التقنية للمحكمة. هذا الجانب من التنسيق يهدف إلى سد الفجوة بين الجوانب التقنية والقانونية، بحيث تكون الأحكام القضائية مبنية على فهم دقيق لطبيعة الجريمة الإلكترونية وطريقة ارتكابها.

علاوة على ذلك، هناك تنسيق على المستوى التشريعي والتنظيمي بين الجهات الأمنية والقضائية وهيئة تنظيم قطاع الاتصالات، التي تلعب دورًا مهمًا في تقديم الدعم الفني في القضايا المتعلقة بالمحتوى الرقمي، حجب المواقع المخالفة، وتعقب العناوين الإلكترونية (IP Addresses) للمجرمين الإلكترونيين. كما أن هذه الهيئة تعمل على وضع سياسات تنظيمية تساهم في منع الجرائم الإلكترونية قبل وقوعها، مثل فرض معايير أمنية على الشركات والمؤسسات التي تتعامل مع البيانات الحساسة، والتأكد من امتثالها لمتطلبات الأمن السيبراني.

إلى جانب ذلك، يتم تعزيز التنسيق بين الجهات الأمنية والقضائية من خلال التعاون الدولي مع الإنترنت والمنظمات الأمنية العالمية، نظرًا لأن العديد من الجرائم السيبرانية تتجاوز الحدود الوطنية، حيث يمكن أن يكون الجاني خارج الأردن بينما الضحية داخلها. هذا التعاون يشمل تبادل المعلومات، تسليم المجرمين، وتطبيق الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية، مما يزيد من فاعلية الملاحقة القانونية لهذه الجرائم⁷⁶.

⁷⁶ مجلس البحوث الوطني. (2014). الأمن السيبراني والقوة السيبرانية: تحديد الإطار القانوني والسياسي. دار الأكاديميات الوطنية للنشر.

- يشمل التنسيق بين الجهات الأمنية والقضائية برامج تدريب وتأهيل مشتركة تستهدف العاملين في هذه المجالات، بهدف تطوير قدراتهم القانونية والتقنية في التعامل مع الجرائم الإلكترونية. يتم تنظيم ورش عمل ودورات تدريبية لضباط الأمن والقضاة وأعضاء النيابة العامة، لتعريفهم بأحدث الأساليب في التحقيقات السيبرانية، القوانين الجديدة، وآليات التعامل مع الأدلة الرقمية بشكل قانوني يضمن حقوق الأفراد ويحفظ الأدلة من التلاعب أو الإتلاف.

بفضل هذه الآليات، يتم تعزيز التعاون بين الجهات الأمنية والقضائية في الأردن، مما يساهم في تطوير منظومة مكافحة الجرائم الإلكترونية، وتسريع عمليات التحقيق والمحاكمة، وضمان تحقيق العدالة في القضايا التي تتعلق بالأمن السيبراني، مع الحفاظ على حقوق الأفراد والمؤسسات في بيئة رقمية آمنة.

خامساً: أبرز القوانين الأردنية المنظمة لجرائم الأمن السيبراني

تسعى المملكة الأردنية الهاشمية إلى تطوير منظومتها التشريعية لمواكبة التطورات المتسارعة في مجال الأمن السيبراني، خاصة مع تزايد الجرائم الإلكترونية التي تهدد الأفراد والمؤسسات والبنية التحتية الرقمية للدولة. وعلى الرغم من أن التشريعات الأردنية لم تعتمد قانوناً شاملاً يغطي جميع جوانب الأمن السيبراني، إلا أن هناك مجموعة من القوانين التي تنظم هذا المجال، والتي يتم تحديثها بشكل دوري لضمان مواجهة التهديدات المستجدة.⁷⁷

أحد القوانين الأساسية في هذا المجال هو قانون الجرائم الإلكترونية رقم (27) لسنة 2015، والذي تم تعديله في عام 2023. يهدف هذا القانون إلى مكافحة الجرائم التي تُرتكب باستخدام الوسائل الإلكترونية، سواء كانت جرائم اختراق، احتيال إلكتروني، ابتزاز رقمي، أو نشر محتوى غير قانوني عبر الإنترنت.

⁷⁷ بني سلامة، م. ع. (2017). الجريمة السيبرانية في النظام القانوني الأردني. مجلة جامعة الزرقاء للبحوث والدراسات الإنسانية، 24(1)، 85-102.

يتضمن القانون مجموعة من العقوبات التي تتراوح بين الغرامات المالية والسجن، تبعاً لخطورة الجريمة وطبيعتها. ومن بين الأمور التي يعالجها هذا القانون تجريم الدخول غير المشروع إلى الأنظمة الإلكترونية، وتعطيل المواقع الإلكترونية، وسرقة البيانات أو إتلافها، والتجسس الإلكتروني، إضافة إلى مكافحة خطاب الكراهية والاحتفال عبر الإنترنت.

كما ينظم قانون الاتصالات رقم (13) لسنة 1995 بعض الجوانب المتعلقة بالأمن السيبراني، خاصة فيما يتعلق بتنظيم عمل مزودي خدمات الإنترنت، وحماية سرية الاتصالات. يمنح هذا القانون هيئة تنظيم قطاع الاتصالات صلاحيات واسعة في الرقابة على قطاع الاتصالات والإنترنت، مما يشمل إصدار التراخيص لمزودي الخدمة، وضمان امتثالهم للمعايير الأمنية المطلوبة، إضافة إلى إمكانية التدخل في بعض الحالات لحجب المواقع التي تُستخدم في تنفيذ الجرائم الإلكترونية أو نشر المحتوى المخالف للقانون.

أما قانون العقوبات الأردني رقم (16) لسنة 1960، فقد تم تعديله ليشمل مواد تتعلق بالجرائم الإلكترونية. قبل صدور قانون الجرائم الإلكترونية، كانت بعض الجرائم السيبرانية تُعاقب بموجب هذا القانون، خاصة فيما يتعلق بجرائم الدم والقذف الإلكتروني، وانتهاك الخصوصية، والاحتفال باستخدام وسائل إلكترونية. ومع ذلك، فإن التطورات السريعة في الجريمة السيبرانية فرضت الحاجة إلى قوانين أكثر تخصصاً، مما أدى إلى إصدار قانون الجرائم الإلكترونية كتشريع منفصل لمعالجة هذه القضايا بفعالية أكبر⁷⁸.

⁷⁸ سوداح، ف. (2024). الأمن السيبراني في الأردن: تحديات الحاضر، وإستراتيجيات للمستقبل. رقمنة.

ويعد قانون المعاملات الإلكترونية رقم (15) لسنة 2015 من القوانين المهمة التي تنظم استخدام التكنولوجيا في التعاملات المالية والتجارية، وتوفر إطاراً قانونياً للتوقيعات الإلكترونية، والمراسلات الرقمية، والعقود الإلكترونية. يهدف هذا القانون إلى تعزيز الثقة في المعاملات الرقمية، وضمان صحتها القانونية، مما يساهم في الحد من التزوير الإلكتروني والاحتيال الرقمي. كما يشمل القانون أحكاماً تتعلق بحماية بيانات المستخدمين في المعاملات الإلكترونية، وضمان عدم إساءة استخدامها من قبل الشركات أو الأفراد.

أما فيما يتعلق بحماية البيانات الشخصية، فلا يوجد حتى الآن قانون مستقل ينظم هذا الجانب بشكل شامل، لكن هناك بعض الأحكام المتفرقة في القوانين المختلفة التي توفر حماية جزئية لبيانات الأفراد، مثل قانون الاتصالات وقانون المعاملات الإلكترونية. ومع ذلك، فإن غياب قانون شامل لحماية البيانات الشخصية يعد أحد أوجه القصور في التشريعات الأردنية، حيث إن هذا النقص يجعل المستخدمين عرضة لانتهاك خصوصيتهم من قبل بعض الجهات التي تجمع بياناتهم دون وجود آليات قانونية صارمة لتنظيم ذلك.

بالإضافة إلى هذه القوانين، هناك العديد من التشريعات الأخرى التي تدعم جهود مكافحة الجرائم الإلكترونية، مثل قانون غسيل الأموال وتمويل الإرهاب، الذي يتعامل مع الجرائم المالية التي تتم عبر الإنترنت، وقانون حماية حق المؤلف، الذي يشمل حماية الحقوق الرقمية ومنع القرصنة الإلكترونية. كما أن هناك لوائح تنظيمية تصدرها الجهات المختصة، مثل هيئة تنظيم قطاع الاتصالات والبنك المركزي الأردني، والتي تضع معايير وإجراءات للأمن السيبراني في قطاعات محددة، مثل القطاع المصرفي والمالي.

بشكل عام، يمكن القول إن التشريعات الأردنية المتعلقة بالأمن السيبراني لا تزال في طور التطوير، حيث يتم تعديل القوانين القائمة بشكل دوري، لكن هناك حاجة إلى قانون أكثر شمولاً يُنظم الأمن السيبراني بشكل متكامل، بحيث يغطي جميع الجوانب المتعلقة بمكافحة الجرائم الإلكترونية، وحماية البيانات، والاستجابة للطوارئ السيبرانية، والتعاون الدولي في هذا المجال.

سادساً: دور الحكومة الأردنية في حماية الأمن السيبراني

تلعب الحكومة الأردنية دوراً محورياً في حماية الأمن السيبراني وتعزيز البنية التحتية الرقمية لمواجهة التهديدات المتزايدة في الفضاء الإلكتروني. من خلال وضع استراتيجيات وطنية وتطوير أطر تشريعية وتنظيمية متكاملة، تسعى الحكومة إلى ضمان بيئة رقمية آمنة تدعم التحول الرقمي المستدام، مما يعزز ثقة الأفراد والمؤسسات في استخدام التكنولوجيا، ويحمي البيانات والأنظمة الحيوية من الهجمات السيبرانية، لضمان استمرار النمو الاقتصادي والتطور التكنولوجي في المملكة.⁷⁹

أ- الاستراتيجية الوطنية للأمن السيبراني

أطلقت الحكومة الأردنية الاستراتيجية الوطنية للأمن السيبراني 2018-2023 بهدف تعزيز القدرات الوطنية في مجال الأمن السيبراني، إدارة المخاطر السيبرانية، وتشجيع الابتكار والشراكات بين القطاعين العام والخاص. تتضمن الاستراتيجية محاور رئيسية مثل بناء كوادر مؤهلة، تطوير آليات للتعقب بالتهديدات، ووضع خطط استجابة فعالة لمواجهة التهديدات السيبرانية المتزايدة وضمان أمان الفضاء الرقمي في المملكة.

⁷⁹ الجمال، قصي حمدان". (2025). الأردن الأول عربياً في الأمن السيبراني: قيادة رقمية تعزز الثقة والاستثمار. "جريدة الرأي".

ب-المركز الوطني للأمن السيبراني

أنشأت الحكومة المركز الوطني للأمن السيبراني بموجب قانون الأمن السيبراني رقم 16 لعام 2019، ليكون الجهة المسؤولة عن تنظيم وضمان بيئة رقمية آمنة، حيث يقوم المركز بإصدار أنظمة وتعليمات تُلزم الشركات والمؤسسات بتطبيق معايير الأمن السيبراني، ويعمل على تنسيق الجهود الوطنية لحماية الفضاء السيبراني.⁸⁰

بالإضافة إلى الاستراتيجية الوطنية، أصدرت الحكومة مجموعة من السياسات المؤسسية المتعلقة بالأمن السيبراني الوطني، بهدف حماية أصول المعلومات في المملكة، وخلق فرص استثمارية جديدة، وتطوير الأعمال مع زيادة فعاليتها وكفاءتها.⁸¹

نتيجة لهذه الجهود، حقق الأردن المركز الأول عربياً في مجال الأمن السيبراني، مما يعكس تطوراً نوعياً في حماية البنية التحتية الرقمية وتعزيز القدرات التقنية. هذا الإنجاز يعزز الثقة في البيئة الرقمية الأردنية ويدعم جذب الاستثمارات وتعزيز الاقتصاد الرقمي. على الرغم من هذه النجاحات، يواجه الأردن تحديات مستمرة في مجال الأمن السيبراني، تتطلب تكثيف الجهود المشتركة بين الحكومة والمؤسسات لتطوير استراتيجيات استجابة فورية، وتعزيز التنسيق الإقليمي، وبناء بنية تحتية رقمية قوية ومستدامة

تتسم الأنظمة القانونية في المملكة الأردنية الهاشمية والمملكة العربية السعودية بتطبيق عقوبات جنائية

⁸⁰ سوداح، فادي. (2024). الأمن السيبراني في الأردن: تحديات الحاضر، دروس مستفادة، وإستراتيجيات للمستقبل. "جريدة الغد

⁸¹ الهنادة، أحمد. (2022). القيادة العامة | القوات المسلحة الأردنية الجيش - العربي. "

تهدف إلى تحقيق الردع العام والخاص، والحفاظ على النظام العام. في الأردن، يُعتبر قانون العقوبات رقم 16 لسنة 1960، وتعديلاته اللاحقة، الإطار القانوني الأساسي لتحديد الجرائم والعقوبات المترتبة عليها. يشمل هذا القانون مجموعة متنوعة من العقوبات، تتراوح بين الإعدام، والأشغال الشاقة المؤبدة أو المؤقتة، والاعتقال المؤبد أو المؤقت، بالإضافة إلى الغرامات المالية. كما يتضمن القانون أحكاماً تتعلق بالعقوبات التكميلية، مثل الحبس التكميلي والغرامة⁸²

في السنوات الأخيرة، اتجه المشرع الأردني نحو تبني العقوبات البديلة كوسيلة للإصلاح والتأهيل، وتقليل الاكتظاظ في مراكز الإصلاح والتأهيل. تشمل هذه العقوبات الخدمة المجتمعية والمراقبة المجتمعية، والتي تهدف إلى إعادة دمج المحكوم عليهم في المجتمع وتعزيز دورهم الإيجابي⁸³.

بصفة عامة، تسعى كل من الأردن والسعودية إلى تحديث وتطوير أنظمتها القانونية لمواكبة المستجدات والتحديات المتسارعة، خاصة في مجالات الأمن السيبراني، وحماية البيانات، ومكافحة الجرائم الإلكترونية. يأتي هذا التطوير مع مراعاة القيم الدينية والاجتماعية السائدة في كلا البلدين، لضمان تحقيق التوازن بين التقدم القانوني والتكنولوجي وبين الحفاظ على المبادئ الثقافية والمجتمعية، مما يعزز بيئة قانونية متينة تدعم الاستقرار والتنمية المستدامة.

سابعاً: الفرق بين قوانين الجرائم السيبرانية في الأردن والسعودية

⁸² قانون العقوبات الأردني، المادة 16.

⁸³ حماة الحق (2020). العقوبات البديلة في التشريع الأردني.

تتفاوت التشريعات المتعلقة بالجرائم السيبرانية بين الأردن والمملكة العربية السعودية من حيث النطاق والتطبيق، حيث يمكن تحديد أوجه التشابه والاختلاف على النحو التالي:

أوجه التشابه والاختلاف بين النظامين السعودي والأردني في مكافحة جرائم الأمن السيبراني

النطاق والتعريفات: في الأردن والسعودية، تم وضع تشريعات متخصصة لمكافحة الجرائم الإلكترونية، حيث تحدد القوانين العقوبات المترتبة على مختلف الأنشطة غير القانونية في الفضاء الرقمي. يشمل كلا التشريعين تعريفاً شاملاً للجرائم السيبرانية، بما في ذلك اختراق الأنظمة، الاختيال الرقمي، الهجمات الإلكترونية على المؤسسات، وانتهاك الخصوصية، بالإضافة إلى أي سلوكيات غير قانونية تتم عبر الإنترنت. تهدف هذه القوانين إلى تعزيز الأمن السيبراني، وحماية البنية التحتية الرقمية، وضمان بيئة إلكترونية آمنة للمجتمع والأعمال.

يعد الأمن السيبراني أحد أهم التحديات التي تواجه الدول في العصر الحديث، مما دفع الحكومات إلى سن تشريعات خاصة لمكافحة الجرائم الإلكترونية. في هذا السياق، سنتناول مقارنة تفصيلية بين النظام السعودي والنظام الأردني من حيث الإطار القانوني، تعريف الجرائم السيبرانية، العقوبات المفروضة، آليات التحقيق، والتعاون الدولي.

أولاً: أوجه التشابه بين النظام السعودي والنظام الأردني

الإطار القانوني والتنظيمي:

في المملكة العربية السعودية، ينظم "نظام مكافحة الجرائم المعلوماتية" الصادر بالمرسوم الملكي رقم (م/17) لعام 1428 هـ (2007م) الجرائم السيبرانية.

في المملكة الأردنية الهاشمية، ينظم "قانون الجرائم الإلكترونية رقم 27 لسنة 2015" هذه الجرائم، وتم تعديله لاحقاً لمواكبة التطورات في الجرائم الإلكترونية⁸⁴.

- كلا النظامين يهدفان إلى الحد من الجرائم الإلكترونية، حماية الأفراد والمؤسسات، وتنظيم استخدام الإنترنت ووسائل التقنية الحديثة بطريقة آمنة.

- يتفق النظامان على تعريف الجرائم السيبرانية بأنها أي أفعال غير قانونية ترتكب باستخدام تقنية المعلومات أو تستهدف الأنظمة المعلوماتية.

تشمل الجرائم في كلا النظامين: الاحتيال الإلكتروني، اختراق الأنظمة، التشهير الإلكتروني، انتهاك الخصوصية، سرقة البيانات، ونشر المحتوى غير القانوني.

العقوبات المفروضة على الجرائم السيبرانية

⁸⁴ المالكي، ر. ع. (2018). مكافحة الجرائم السيبرانية في السعودية: دراسة مقارنة. مجلة القانون الدولي، 9(1)، 40-55.

يفرض كلا النظامين عقوبات مشددة تشمل السجن، الغرامات المالية، ومصادرة الأدوات المستخدمة في الجريمة.

على سبيل المثال، يعاقب القانون السعودي بالسجن حتى 10 سنوات وغرامة تصل إلى 5 ملايين ريال سعودي على الجرائم المتعلقة بالاختراقات وانتهاك الخصوصية. بينما يفرض القانون الأردني عقوبات تصل إلى 3 سنوات وغرامة مالية تصل إلى 7,000 دينار أردني على الجرائم الإلكترونية الخطيرة.

التصدي لجرائم الاحتيال الإلكتروني

يجرم كلا النظامين عمليات الاحتيال التي تتم عبر الإنترنت، مثل الاستيلاء غير المشروع على الأموال باستخدام وسائل إلكترونية، والتصيد الاحتيالي.

العقوبات في السعودية قد تصل إلى السجن 3 سنوات وغرامة مالية تصل إلى 2 مليون ريال سعودي، بينما تصل العقوبات في الأردن إلى السجن سنة أو غرامة مالية حسب خطورة الجريمة.

حماية الخصوصية والبيانات الشخصية

يحظر كلا النظامين الوصول غير المصرح به إلى المعلومات الشخصية، أو نشر بيانات الأفراد بدون موافقة، أو التنصت غير القانوني على الاتصالات الإلكترونية.

يعاقب القانون السعودي على هذا النوع من الجرائم بالسجن حتى 4 سنوات وغرامة تصل إلى 3

ملايين⁸⁵ ريال، بينما يعاقب القانون الأردني بالسجن حتى 3 سنوات وغرامة تصل إلى 5,000 دينار.

حظر نشر المحتوى غير القانوني

يجرم النظامان نشر المحتوى الذي يضر بالمجتمع، كالتحريض على العنف أو نشر الشائعات أو المواد الإباحية أو التشهير بالأشخاص.

في السعودية، تصل العقوبة إلى 5 سنوات سجن وغرامة تصل إلى 3 ملايين ريال، بينما في الأردن

تصل إلى 3 سنوات سجن أو غرامة مالية حسب نوع الجريمة.

يتشابه النظامان السعودي والأردني في الأهداف العامة لمكافحة الجرائم السيبرانية، من خلال فرض عقوبات على الجرائم الإلكترونية وحماية الأمن السيبراني. لكن يختلفان في بعض الجوانب مثل مدى شمولية القوانين، شدة العقوبات، آليات التحقيق، والتعاون الدولي. يمكن لكلا البلدين تطوير منظومتهما القانونية عبر تعزيز التعاون الإقليمي، تبادل الخبرات، وتشديد القوانين على الجرائم الإلكترونية الخطيرة لضمان بيئة رقمية أكثر أماناً.

⁸⁵ الأنصاري، خ. س. (2022). الأمن السيبراني في المملكة العربية السعودية: الإطار القانوني والتحديات المستقبلية. مجلة الدراسات الإستراتيجية، 14(2)، 65-80.

ثامناً: أبرز التحديات المشتركة التي تواجه المملكة العربية السعودية والمملكة الأردنية الهاشمية في مجال الأمن السيبراني

مع التطور المتسارع في التكنولوجيا وانتشار الخدمات الرقمية، أصبحت المملكة العربية السعودية والمملكة الأردنية الهاشمية تواجهان تحديات متزايدة في مجال الأمن السيبراني. ورغم الجهود الكبيرة التي تبذلها الحكومتان لحماية الأنظمة المعلوماتية والبنية التحتية الرقمية، إلا أن هناك العديد من التحديات المشتركة التي تعيق التصدي الفعال للهجمات السيبرانية والتعامل مع المخاطر المتزايدة في الفضاء الرقمي. وفيما يلي أبرز هذه التحديات بالتفصيل⁸⁶.

1. تصاعد وتطور الجرائم السيبرانية ووسائل الهجوم

يشهد العالم تطوراً مستمراً في أساليب الهجمات السيبرانية، حيث أصبحت الهجمات أكثر تعقيداً واحترافية مع استخدام تقنيات جديدة مثل الذكاء الاصطناعي، والتعلم الآلي، وتقنيات الهندسة الاجتماعية. وتعاني كل من السعودية والأردن من هجمات سيبرانية متقدمة تستهدف البنية التحتية الحساسة مثل القطاعات المصرفية، الحكومية، والعسكرية.

على سبيل المثال، زادت الهجمات التي تعتمد على برامج الفدية (Ransomware) والهجمات التي تستهدف شبكات المؤسسات الكبرى لتعطيل الخدمات أو سرقة البيانات. أيضاً، تشهد الدولتان هجمات

⁸⁶ القصير، ي. ع. (2023). الجرائم الإلكترونية في السعودية: التحديات والحلول القانونية. مجلة القانون والمجتمع، 22(3)، 115-100.

الاحتيال الإلكتروني والتصيد الاحتيالي (Phishing) ، حيث يتم خداع المستخدمين للإفصاح عن

معلومات حساسة مثل بيانات الحسابات البنكية.

2. نقص الكفاءات والخبرات المتخصصة في الأمن السيبراني

على الرغم من الجهود المبذولة في تدريب الكوادر الوطنية في مجال الأمن السيبراني، إلا أن الطلب

على المتخصصين في الأمن السيبراني يفوق عدد الكفاءات المتاحة في السوقين السعودي والأردني.

هناك حاجة ماسة لمزيد من المتخصصين في مجال تحليل البيانات السيبرانية، التحقيق الرقمي، اختبار

الاختراق، وتقنيات التشفير. ويعد استقطاب الكفاءات المؤهلة تحدياً صعباً بسبب المنافسة العالمية على

الخبرات في هذا المجال، حيث تقدم العديد من الدول المتقدمة حوافز مالية مغرية لجذب خبراء الأمن

السيبراني. أيضاً، لا تزال الجامعات في البلدين بحاجة إلى تطوير برامج أكاديمية أكثر تركيزاً على

الأمن السيبراني لمواكبة التطورات السريعة في هذا المجال.

3. عدم كفاية التعاون الدولي والإقليمي في مواجهة التهديدات السيبرانية تعتبر الجرائم السيبرانية من

الجرائم العابرة للحدود، مما يتطلب تعاوناً دولياً وإقليمياً فعالاً لمواجهتها.

تعاني **السعودية** والأردن من تحديات في تبادل المعلومات الأمنية مع الجهات الدولية بسبب القوانين السيادية والقيود المفروضة على مشاركة البيانات الحساسة. الأردن ليس عضواً في اتفاقية بودابست لمكافحة الجرائم السيبرانية، مما قد يعيق تعاونه مع بعض الدول في ملاحقة الجرائم الإلكترونية.

السعودية، رغم امتلاكها هيئات متخصصة مثل الهيئة الوطنية للأمن السيبراني، لا تزال بحاجة إلى توسيع شبكة التعاون مع الدول الإقليمية لتعزيز الأمن السيبراني المشترك.

4. الاستهداف المتزايد للبنية التحتية الحيوية تعتمد المملكة العربية السعودية والمملكة الأردنية الهاشمية بشكل كبير على التكنولوجيا الرقمية في تشغيل القطاعات الحيوية مثل الطاقة، النقل، الصحة، والخدمات المالية، مما يجعلها أهدافاً رئيسية للهجمات السيبرانية⁸⁷.

في السعودية، تعرضت بعض المنشآت النفطية سابقاً لهجمات سيبرانية تهدف إلى تعطيل الإنتاج أو سرقة البيانات الاستراتيجية، مما يشكل تهديداً كبيراً على الاقتصاد الوطني.

في الأردن، هناك مخاوف من استهداف البنوك والأنظمة الحكومية بهجمات تهدف إلى تعطيل الخدمات وسرقة المعلومات الحساسة.

يمثل تأمين هذه البنية التحتية تحدياً كبيراً بسبب التعقيد التكنولوجي المتزايد والاحتياج إلى استثمارات ضخمة في الأمن السيبراني⁸⁸.

⁸⁷ حماة الحق. (2020). العقوبات البديلة في التشريع الأردني.

5. تحديات تشريعية وقانونية في مكافحة الجرائم السيبرانية

على الرغم من وجود قوانين لمكافحة الجرائم السيبرانية في السعودية والأردن، إلا أن هناك عدة تحديات تشريعية تحد من فاعلية هذه القوانين:

- عدم مواكبة بعض القوانين للتطورات التقنية الحديثة، حيث يتم استحداث تقنيات جديدة في الجريمة السيبرانية بوتيرة أسرع من تحديث القوانين⁸⁹.

- صعوبة إثبات الجرائم الإلكترونية، خاصة في الحالات التي تعتمد على تقنيات إخفاء الهوية مثل الشبكة المظلمة (Dark Web) والتشفير المتقدم.

- تفاوت العقوبات بين الجرائم المختلفة، حيث أن بعض الجرائم الخطيرة مثل الهجمات السيبرانية المنظمة قد لا تحظى بعقوبات كافية في بعض الحالات.

6. نقص الوعي المجتمعي بمخاطر الأمن السيبراني

لا يزال هناك ضعف في الوعي المجتمعي حول أهمية الأمن السيبراني وطرق الحماية من الهجمات الإلكترونية، مما يجعل الأفراد والمؤسسات عرضة للاختراقات.

⁸⁸ الحربي، ع. م. (2024). التحديات القانونية للأمن السيبراني في المملكة العربية السعودية. مجلة الدراسات القانونية المعاصرة، 6(1)، 55-70.

⁸⁹ الشمري، ف. م. (2023). الجرائم السيبرانية في المملكة العربية السعودية: دراسة تحليلية. مجلة القانون والعلوم السياسية، 15(1)، 95-110.

يواجه كل من السعودية والأردن تحدياً في تعزيز الثقافة السيبرانية بين الأفراد، خاصة في الشركات الصغيرة والمتوسطة التي قد لا تمتلك إجراءات أمنية قوية. تشير التقارير إلى أن أغلب الهجمات الناجحة تعتمد على استغلال الأخطاء البشرية، مثل استخدام كلمات مرور ضعيفة، أو تحميل ملفات مجهولة المصدر. وهناك حاجة إلى حملات توعية مستمرة وبرامج تدريبية موجهة للجمهور لتعزيز الحماية الذاتية ضد المخاطر السيبرانية⁹⁰.

7. ارتفاع التكاليف المالية لمكافحة الجرائم السيبرانية

يتطلب تطوير الأنظمة الأمنية السيبرانية استثمارات مالية كبيرة، سواء من قبل الحكومات أو القطاع الخاص.

- تحتاج البنوك، المؤسسات المالية، والجهات الحكومية إلى تقنيات حديثة ومتطورة مثل الذكاء الاصطناعي، التحليل الجنائي الرقمي، وتقنيات الحماية من الاختراقات، مما يشكل عبئاً مالياً كبيراً.

في الأردن، قد يشكل التمويل المحدود تحدياً في تطوير البنية التحتية السيبرانية، خاصة في المؤسسات الصغيرة والمتوسطة.

في السعودية، رغم وجود استثمارات ضخمة في الأمن السيبراني، إلا أن ارتفاع تكلفة الاستعداد للهجمات السيبرانية يشكل تحدياً مستمراً، خاصة مع تزايد تعقيد الهجمات وتطورها.

⁹⁰ العمارة، م.، & عبدالرزاق، م. (2020). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. مجلة طبنة للدراسات العلمية الأكاديمية، 7(1)، 1337-1353.

يواجه كل من السعودية والأردن تحديات مشتركة في الأمن السيبراني تتطلب استراتيجيات متطورة لمواجهتها. ومن أهم الحلول الممكنة:

- زيادة الاستثمار في تدريب الكوادر المحلية وتأهيلها في مجال الأمن السيبراني.
- تعزيز التعاون الدولي والإقليمي لتبادل المعلومات حول الجرائم السيبرانية.
- تحديث القوانين بشكل دوري لمواكبة التطورات التقنية السريعة.
- رفع مستوى الوعي المجتمعي بالأمن السيبراني لحماية الأفراد والمؤسسات من الهجمات الإلكترونية.
- تعزيز الحماية للبنية التحتية الحيوية وتطوير أنظمة دفاع إلكترونية متقدمة.
- إن نجاح الدولتين في مواجهة هذه التحديات يعتمد على التعاون المشترك، الاستثمارات الذكية، وتطوير سياسات مرنة تستطيع التعامل مع التهديدات السيبرانية المتغيرة باستمرار.

تاسعا: الدروس المستفادة وأفضل الممارسات لتطوير التشريعات الخاصة بالأمن السيبراني

مع التطور المستمر للفضاء الرقمي، أصبحت الجرائم السيبرانية أكثر تعقيدا، مما يستدعي تطوير التشريعات القانونية لمكافحة هذه الجرائم بفاعلية. وتعد المملكة العربية السعودية والمملكة الأردنية الهاشمية من الدول التي تواجه تحديات في هذا المجال، حيث تعملان على تعزيز أطرها القانونية لمواكبة التطورات التقنية السريعة. بناءً على التجارب العالمية والدروس المستفادة من الدول الرائدة في

مجال الأمن السيبراني، يمكن تحديد مجموعة من أفضل الممارسات التي يمكن تبنيها لتطوير التشريعات الخاصة بالأمن السيبراني.

1. تبني نهج تشريعي استباقي ومرن

تعتبر القوانين التقليدية في العديد من الدول بطيئة في مواكبة التطورات التكنولوجية، مما يخلق فجوة قانونية يستغلها مجرمو الإنترنت. لذلك، يجب أن تكون التشريعات الخاصة بالأمن السيبراني استباقية ومرنة بحيث تتكيف مع التغيرات السريعة في التقنيات السيبرانية⁹¹. يجب أن تتضمن القوانين مواد عامة وشاملة تحدد المبادئ الأساسية لحماية الأمن السيبراني، بدلاً من التركيز على حالات محددة قد تصبح غير ذات صلة مع مرور الوقت. وضرورة تضمين بنود قانونية تسمح بتحديث التشريعات دورياً وفقاً للتطورات التقنية الجديدة، مثل تقنيات الذكاء الاصطناعي، التشفير المتقدم، وإنترنت الأشياء (IoT). استخدام إطار تنظيمي ديناميكي يسمح بإدخال لوائح تنظيمية جديدة بسرعة عند ظهور تهديدات سيبرانية جديدة دون الحاجة إلى تعديل القانون الأساسي بشكل متكرر.

2. تعزيز التعاون الدولي والإقليمي في مجال الأمن السيبراني

تعد الجرائم السيبرانية جرائم عابرة للحدود، مما يجعل التعاون بين الدول أمراً ضرورياً لتتبع المجرمين السيبرانيين ومكافحتهم بفاعلية.

⁹¹ المالكي، ر. ع. (2023). مكافحة الجرائم السيبرانية في السعودية: دراسة مقارنة. مجلة القانون الدولي، (1)9، 40-55.

يجب على الدول العربية، بما في ذلك السعودية والأردن، الانضمام إلى الاتفاقيات الدولية المتعلقة بالأمن السيبراني، مثل اتفاقية بودابست لمكافحة الجرائم السيبرانية، التي تسهل تبادل المعلومات والتعاون في ملاحقة الجناة. وتطوير اتفاقيات تعاون إقليمية بين الدول العربية تضمن تبادل البيانات الأمنية، والتعاون في التحقيقات الجنائية السيبرانية، ومشاركة الخبرات التقنية. أيضا تعزيز التعاون مع شركات التكنولوجيا العالمية مثل جوجل، مايكروسوفت، وفيسبوك، لضمان إزالة المحتوى الضار بسرعة، والمساعدة في التحقيقات الجنائية عند الحاجة⁹².

3. وضع عقوبات قانونية رادعة للجرائم السيبرانية

يعد تشديد العقوبات من أهم الوسائل لردع الجرائم السيبرانية، حيث يجب أن تتضمن التشريعات عقوبات صارمة ضد الجرائم الإلكترونية الخطيرة، مثل:

الاختراق غير المشروع للأنظمة الحكومية والخاصة، والتي يجب أن تصل عقوباتها إلى السجن المشدد والغرامات الكبيرة. وسرقة البيانات الشخصية واستخدامها في عمليات الاحتيال الإلكتروني، وهي جريمة تتطلب عقوبات صارمة تشمل التعويضات المالية الكبيرة للضحايا. أيضا هجمات تعطيل الخدمات (DDoS) وبرامج الفدية (Ransomware)، حيث يمكن أن تؤدي هذه الهجمات إلى خسائر مالية ضخمة، مما يستوجب فرض عقوبات مشددة على مرتكبيها. ونشر نشر البرمجيات الخبيثة

⁹² العمارة، م.، & عبدالرزاق، م. (2020). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. مجلة طنبه للدراسات العلمية الأكاديمية، 7(1)، 1337-1353.

والفيروسات، وهي جريمة يجب أن يعاقب عليها القانون بشكل واضح لتجنب انتشار أدوات الاختراق بين الأفراد غير المتخصصين.

4. تطوير إطار قانوني واضح لحماية البيانات الشخصية

مع تزايد استخدام الخدمات الرقمية، أصبح من الضروري وضع قوانين واضحة لحماية خصوصية الأفراد وتأمين بياناتهم من الانتهاكات السيبرانية⁹³.

إصدار قوانين تلزم الشركات والمؤسسات الحكومية بتطبيق إجراءات صارمة لحماية البيانات الشخصية، مثل استخدام تقنيات التشفير وإجراءات المصادقة الثنائية. ووضع قيود واضحة على جمع البيانات واستخدامها، بحيث يتم منع الشركات من تخزين بيانات المستخدمين لفترات طويلة دون مبرر قانوني. إلزام الشركات بالإبلاغ عن أي اختراق أمني يؤثر على بيانات المستخدمين خلال فترة زمنية قصيرة، لضمان الشفافية وحماية الضحايا المحتملين.

5. إنشاء هيئات متخصصة للإشراف على تطبيق قوانين الأمن السيبراني

تحتاج كل دولة إلى هيئة متخصصة تشرف على تنفيذ قوانين الأمن السيبراني وتراقب الامتثال للأنظمة.

⁹³ اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (2023). الأمن في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية. الأمم المتحدة.

في السعودية، تعتبر الهيئة الوطنية للأمن السيبراني مثالا ناجحا على إنشاء جهة مختصة بتنظيم ومراقبة الأمن السيبراني على المستوى الوطني.

في الأردن، هناك حاجة إلى تعزيز دور المؤسسات المختصة، مثل وحدة مكافحة الجرائم الإلكترونية، لضمان وجود جهة إشرافية قوية تمتلك صلاحيات واضحة لإنفاذ القوانين واتخاذ إجراءات فورية ضد التهديدات السيبرانية. يجب أن تكون هذه الهيئات مستقلة ولديها إمكانيات تقنية متقدمة تمكنها من التعامل مع التهديدات السيبرانية بكفاءة عالية.

6. تعزيز الوعي المجتمعي حول الأمن السيبراني لا يمكن للتشريعات وحدها أن تحقق الأمن السيبراني دون نشر الوعي بين المواطنين والشركات حول مخاطر الجرائم الإلكترونية⁹⁴.

- يجب أن تتبنى الحكومات حملات توعوية وطنية لتثقيف الأفراد حول أساليب الحماية من الهجمات السيبرانية، مثل تجنب التصيد الاحتيالي، استخدام كلمات مرور قوية، وتحديث البرمجيات بانتظام. مع إدراج مناهج دراسية متخصصة في المدارس والجامعات حول الأمن السيبراني، لضمان أن الأجيال القادمة تمتلك المهارات الأساسية لحماية نفسها من التهديدات السيبرانية. وإطلاق دورات تدريبية مجانية عبر الإنترنت تساعد الشركات الصغيرة والمتوسطة في تبني أفضل ممارسات الأمن السيبراني لحماية بياناتها وأنظمتها.

⁹⁴ العمارة، م.، & عبدالرزاق، م. (2024). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. مجلة طبنة للدراسات العلمية الأكاديمية، 7(1)، 1337-1353.

7. تسهيل عمليات التحقيق الجنائي الرقمي وتطوير الأدلة الإلكترونية

التحقيق في الجرائم السيبرانية يواجه تحديات كبيرة بسبب طبيعة الجرائم الإلكترونية التي تعتمد على إخفاء الهوية واستخدام تقنيات التشفير. يجب أن تتيح القوانين للجهات الأمنية إمكانية الوصول إلى الأدلة الرقمية وتحليلها بطرق قانونية تحافظ على خصوصية المستخدمين. ووضع تشريعات تنظم كيفية جمع الأدلة الإلكترونية وقبولها في المحاكم، بحيث يتم الاعتراف بالأدلة الرقمية كأدلة قانونية صالحة أمام القضاء. أيضا التعاون مع شركات الاتصالات ومزودي خدمات الإنترنت لضمان إمكانية تتبع الأنشطة الإجرامية دون انتهاك حقوق المستخدمين الأبرياء⁹⁵.

- إن تطوير التشريعات الخاصة بالأمن السيبراني يتطلب نهجاً شاملاً يجمع بين التشريعات القانونية الصارمة، التعاون الدولي، تعزيز الوعي المجتمعي، والاستثمار في البنية التحتية السيبرانية. ومن خلال تبني هذه الدروس المستفادة وأفضل الممارسات، يمكن للدول تحقيق مستوى عالٍ من الحماية السيبرانية، مما يساهم في تأمين البنية الرقمية وحماية البيانات الوطنية والمجتمعية من التهديدات المتزايدة.

عاشرا: كيف يمكن تعزيز التعاون الإقليمي والدولي بين المملكة العربية السعودية والأردن لمواجهة التهديدات السيبرانية العابرة للحدود

تعد التهديدات السيبرانية العابرة للحدود من أخطر التحديات التي تواجه الدول اليوم، حيث لم تعد الهجمات الإلكترونية محصورة داخل نطاق دولة واحدة، بل أصبحت شبكات الجرائم السيبرانية تعمل

⁹⁵ نفس المرجع السابق

على مستوى عالمي، مستهدفة الحكومات، المؤسسات المالية، الشركات الكبرى، وحتى الأفراد. وفي هذا السياق، يبرز التعاون الإقليمي والدولي بين الدول كعنصر أساسي لتعزيز الأمن السيبراني وتقليل المخاطر المرتبطة بالهجمات الإلكترونية. وبالنسبة للمملكة العربية السعودية والأردن، فإن تعزيز هذا التعاون يمكن أن يسهم بشكل كبير في الحد من الجرائم الإلكترونية ومكافحة الهجمات التي تستهدف البنية التحتية الرقمية في كلا البلدين.

أولاً: أهمية التعاون الإقليمي والدولي في مكافحة التهديدات السيبرانية

التعاون بين الدول في مجال الأمن السيبراني لم يعد خياراً، بل أصبح ضرورة حتمية في ظل تصاعد الهجمات الإلكترونية التي تستهدف مؤسسات حكومية، قطاعات اقتصادية، وشبكات الاتصالات. تتطلب مواجهة هذه التهديدات استراتيجيات موحدة وتنسيقاً عالي المستوى بين الدول، خاصةً تلك التي تمتلك مصالح مشتركة وتواجه تحديات سيبرانية متشابهة، كما هو الحال بين السعودية والأردن⁹⁶.

يتيح التعاون الإقليمي والدولي تبادل المعلومات حول أحدث الهجمات الإلكترونية، تبني سياسات وقائية موحدة، تحسين الاستجابة السريعة للهجمات، وتطوير تقنيات دفاعية مشتركة. كما أنه يعزز من قدرة الدول على تعقب المجرمين السيبرانيين الذين قد ينفذون هجماتهم من خارج الحدود الوطنية.

ثانياً: مجالات التعاون بين المملكة العربية السعودية والأردن في مجال الأمن السيبراني

يمكن أن يتخذ التعاون بين السعودية والأردن عدة أشكال لمواجهة التهديدات السيبرانية العابرة للحدود، ومن أبرزها:

⁹⁶ العكاليك، ح. (2022). الضوابط القانونية للأمن السيبراني في الأردن. صحيفة عمون الإخبارية.

1. تبادل المعلومات والتنسيق في التصدي للهجمات الإلكترونية

من أهم الجوانب التي تسهم في تعزيز الأمن السيبراني هو تبادل المعلومات حول التهديدات والهجمات الإلكترونية بين الجهات المختصة في كلا البلدين. يمكن إنشاء منصات مشتركة لمشاركة البيانات حول الهجمات المحتملة، برمجيات الفدية، التصيد الاحتيالي، والهجمات المستهدفة للبنية التحتية الحيوية. ويساعد هذا التنسيق في رفع جاهزية كل من السعودية والأردن لمواجهة الهجمات بسرعة وفعالية، حيث إن التعرف المبكر على التهديدات يقلل من تأثيرها السلبي⁹⁷.

2. تطوير إطار قانوني مشترك لمكافحة الجرائم السيبرانية

- نظرا لاختلاف التشريعات بين الدول، يمكن للسعودية والأردن العمل على مواءمة قوانين مكافحة الجرائم السيبرانية لتسهيل عمليات التحقيق والملاحقة القانونية للمجرمين السيبرانيين الذين يعملون عبر الحدود.

- يمكن إبرام اتفاقيات تعاون قضائي تتيح تبادل المعلومات حول المشتبه بهم في القضايا السيبرانية، وتسهيل إجراءات تسليم المطلوبين في قضايا الجرائم الإلكترونية.

⁹⁷ العتيبي، م. خ. (2023). دور التشريعات السعودية في مواجهة الجرائم السيبرانية. مجلة الأمن والحياة، 19(3)، 45-60.

- تعزيز التعاون في تطوير تشريعات موحدة لحماية البيانات الشخصية، خاصة مع تزايد عمليات سرقة البيانات واختراق الأنظمة المالية.

3. التعاون في بناء القدرات والتدريب الأمني

- يمكن تعزيز التعاون بين الجهات المختصة في كلا البلدين من خلال تبادل الخبرات وتنظيم ورش عمل ودورات تدريبية حول أحدث تقنيات الدفاع السيبراني وأساليب التصدي للهجمات المتطورة.

- إنشاء برامج تدريب مشتركة للكوادر الأمنية والقضائية لتعزيز مهارات التحقيق في الجرائم السيبرانية، وتطوير الأدلة الرقمية التي يمكن استخدامها في المحاكم⁹⁸.

- إقامة تدريبات محاكاة لهجمات سيبرانية افتراضية بين المؤسسات الأمنية في البلدين لاختبار قدرات الاستجابة الفورية لأي تهديدات طارئة.

4. تعزيز التعاون مع المنظمات الدولية والإقليمية

يمكن للسعودية والأردن توحيد جهودهما في التعاون مع المنظمات الدولية مثل الاتحاد الدولي للاتصالات (ITU) والمنتدى العالمي للأمن السيبراني (GCF) لتعزيز أمنهما الرقمي. والانضمام إلى الاتفاقيات الدولية التي تسهل تبادل المعلومات والتحقيقات في الجرائم السيبرانية، مثل اتفاقية بودابست لمكافحة الجرائم الإلكترونية، والتي تتيح تبادل الأدلة الرقمية بين الدول. أيضا المشاركة في المبادرات

⁹⁸ حسن، ك. (2021). الجهود الدولية في مواجهة الجرائم السيبرانية. منشورات الحلبي الحقوقية.

الخليجية والعربية لتعزيز الأمن السيبراني، مثل التعاون مع مجلس التعاون الخليجي في وضع استراتيجيات موحدة لمكافحة الجرائم الإلكترونية⁹⁹.

5. إنشاء مركز مشترك للأمن السيبراني يمكن للمملكة العربية السعودية والأردن إنشاء مركز أمني سيبراني مشترك يعمل على تحليل التهديدات، مشاركة المعلومات الاستخباراتية، وتطوير استراتيجيات استباقية للتصدي للهجمات الإلكترونية المتزايدة. يمكن لهذا المركز أن يكون منصة لتبادل التقارير الأمنية، دراسة الاتجاهات الجديدة في الجرائم السيبرانية، وتطوير حلول مبتكرة لمكافحة التهديدات المتطورة¹⁰⁰.

ثالثاً: التحديات التي قد تواجه التعاون بين البلدين في مجال الأمن السيبراني

على الرغم من الفوائد الكبيرة التي يمكن تحقيقها من التعاون السيبراني بين السعودية والأردن، إلا أن هناك بعض التحديات التي قد تعرقل هذا التعاون، ومنها:

الاختلافات في السياسات والتشريعات المتعلقة بحماية البيانات والجرائم السيبرانية، مما قد يؤدي إلى عقبات في تنسيق التحقيقات والملاحقات القانونية.

⁹⁹ حسن، ك. (2021). الجهود الدولية في مواجهة الجرائم السيبرانية. منشورات الحلبي الحقوقية.

¹⁰⁰ Kramer, F. D., & Starr, S. H. (2016). Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization. National Defense University Press

- التحديات التقنية والتفاوت في مستوى البنية التحتية السيبرانية بين البلدين، حيث قد تتطلب بعض أشكال التعاون استثمارات إضافية في تطوير الأنظمة الأمنية السيبرانية.

- القيود على تبادل المعلومات الحساسة، حيث إن بعض البيانات المتعلقة بالأمن السيبراني قد تكون سرية، مما يستدعي وضع آليات موثوقة لحماية المعلومات المشتركة.

- الهجمات السيبرانية المدعومة من جهات خارجية، والتي قد تستهدف إضعاف التعاون بين الدول من خلال تنفيذ عمليات قرصنة وتجسس إلكتروني معقدة.

رابعاً: التوصيات لتعزيز التعاون بين السعودية والأردن في مجال الأمن السيبراني

لتجاوز التحديات وتعزيز التعاون الفعال بين البلدين، يمكن اتخاذ الخطوات التالية: توقيع اتفاقيات ثنائية تشمل جميع جوانب الأمن السيبراني، من تبادل المعلومات إلى التعاون القانوني والتقني. وإطلاق مبادرات مشتركة للأبحاث والتطوير في مجال الأمن السيبراني لتطوير حلول متقدمة لمكافحة التهديدات السيبرانية. أيضاً تعزيز مشاركة القطاع الخاص في الجهود الأمنية السيبرانية، حيث يمكن للشركات الكبرى المساهمة في تطوير تقنيات الحماية والاستجابة للهجمات. مع الاستثمار في الذكاء الاصطناعي والتحليلات الأمنية لإنشاء أنظمة سيبرانية ذكية قادرة على التنبؤ بالهجمات قبل حدوثها.

- يمثل التعاون السيبراني بين المملكة العربية السعودية والأردن خطوة ضرورية لمواجهة التهديدات السيبرانية المتزايدة التي تتجاوز الحدود الوطنية. ومن خلال تعزيز تبادل المعلومات، توحيد القوانين، بناء القدرات، والتنسيق مع المنظمات الدولية، يمكن للبلدين تحقيق بيئة رقمية أكثر أماناً وفعالية. وعلى

الرغم من التحديات التي قد تواجه هذا التعاون، فإن العمل المشترك والتخطيط الاستراتيجي يمكن أن يسهم في بناء درع سيبراني قوي يحمي الأصول الرقمية الحيوية لكل من السعودية والأردن.

التحديث والتطوير:

الأردن: شهدت التشريعات الأردنية تطورًا ملحوظًا، حيث تم تحديث قانون الجرائم الإلكترونية في عام 2023 بهدف مواكبة التطورات التقنية السريعة والتهديدات المتزايدة في مجال الأمن السيبراني. هذا التحديث شمل تشديد العقوبات وتوضيح الأطر القانونية التي تتعلق بالجرائم المرتكبة عبر الإنترنت.

السعودية: في المقابل، لم تتوفر معلومات تشير إلى تحديثات مشابهة في التشريعات السعودية منذ إصدار نظام مكافحة الجرائم المعلوماتية في عام 2007. ورغم أن هذا النظام يتضمن مجموعة من العقوبات ضد الجرائم السيبرانية، إلا أنه لم يتم تحديثه بشكل كبير لمواكبة التطور السريع في مجال التقنية والتهديدات الرقمية الحديثة.

بناءً على ذلك، يمكن القول إن التشريعات الأردنية في مجال الأمن السيبراني تُظهر مرونة أكبر في التكيف مع التغيرات التقنية، بينما تظل التشريعات السعودية في هذا المجال دون تحديثات تواكب التطورات الحديثة بشكل كافٍ.

الهيئات التنظيمية: أنشأ الأردن المركز الوطني للأمن السيبراني للإشراف على تنفيذ السياسات والمعايير المتعلقة بالأمن السيبراني. بينما في السعودية، تتولى الهيئة الوطنية للأمن السيبراني مسؤولية حماية الأمن السيبراني وتعزيز القدرات الوطنية في هذا المجال.

في المملكة العربية السعودية، فيستند النظام القانوني إلى الشريعة الإسلامية، مع تطبيق العقوبات التعزيرية والحدود والقصاص بناءً على نوع الجريمة وظروفها. تشمل العقوبات التعزيرية مجموعة واسعة من التدابير، مثل السجن، والجلد، والغرامات المالية، والتوبيخ، والمنع من السفر، وغيرها من العقوبات التي يحددها القاضي بناءً على تقديره وحسب ما تقتضيه مصلحة المجتمع¹⁰¹.

بصفة عامة، بينما تشترك الدولتان في الهدف العام المتمثل في مكافحة الجرائم السيبرانية، إلا أن هناك اختلافات في هيكلة التشريعات وتحديثها، بالإضافة إلى المؤسسات المسؤولة عن تنفيذ هذه القوانين¹⁰².

مع التقدم السريع في التكنولوجيا والتحول الرقمي المتزايد، أصبح الأمن السيبراني أحد التحديات الكبرى التي تواجه الأفراد والشركات والدول على حد سواء. تتطور التهديدات السيبرانية بشكل مستمر، مما يستدعي تطوير استراتيجيات متقدمة لحماية البيانات والأنظمة الحساسة. يُعد الذكاء الاصطناعي أحد الحلول الفعالة في التصدي لهذه التهديدات، حيث يتيح تقنيات جديدة للكشف عن الهجمات والتفاعل معها بطرق أكثر سرعة وكفاءة. ومع ذلك، يواجه الأمن السيبراني تحديات كبيرة، مثل نقص الوعي والتدريب، وتطور الهجمات السيبرانية باستخدام تقنيات متقدمة، بالإضافة إلى الحاجة إلى تشريعات موحدة لضبط الأمن الرقمي على مستوى عالمي.

¹⁰¹ الهيئة السعودية لحقوق الإنسان. (2021).

¹⁰² هيئة الخبراء بمجلس الوزراء. (2007). نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم م/17. تم استرجاعه في 5 فبراير 2025، من <https://laws.boe.gov.sa>

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون

الأردني والسعودي

مشعل خضر روجان العنزي

أشرف عليها

الاستاذ الدكتور : أكرم الفايز

الملخص

تهدف هذه الدراسة إلى تحليل الإطار القانوني لمكافحة جرائم الأمن السيبراني في كل من الأردن والسعودية، من خلال مقارنة التشريعات القانونية في كلا البلدين. تتمثل مشكلة الدراسة في الحاجة إلى تطوير وتحسين الإطار التشريعي لمكافحة الجرائم السيبرانية التي تزداد تطوراً مع تسارع الثورة الرقمية. وتستعرض الدراسة أبرز أوجه التشابه والاختلاف بين القوانين الأردنية والسعودية، مع التركيز على كيفية التصدي للتهديدات السيبرانية وحماية البنية التحتية الرقمية للدوائر الحكومية في كل من البلدين. تسعى الدراسة إلى تحليل دور التشريعات في تعزيز الأمن الرقمي، ومدى كفاءتها في التصدي للتهديدات المتزايدة مثل الاختراقات السيبرانية، وسرقة البيانات، والهجمات الإلكترونية. كما تتناول العقوبات والإجراءات الوقائية المتبعة في كل قانون، وتبحث في قدرة هذه التشريعات على مواجهة الجرائم السيبرانية الحديثة. كما تقدم الدراسة توصيات لتحسين التشريعات القانونية وتعزيز التعاون بين الأردن والسعودية في مجال الأمن السيبراني لمواجهة التحديات المشتركة. وتعتمد الدراسة على المنهج الوصفي التحليلي ومنهج المقارنة بين القوانين الأردنية والسعودية، مستندة إلى النصوص القانونية والتفسيرات الفقهية دون إجراء دراسات ميدانية. من خلال هذا التحليل، تهدف الدراسة إلى سد الفجوات التشريعية الحالية، ورفع كفاءة الاستجابة للتحديات السيبرانية، وتحقيق حماية فعالة للأمن السيبراني على مستوى دوائر الدولة في كلا البلدين.

الكلمات المفتاحية: الأمن السيبراني، جرائم الأمن السيبراني، التشريعات القانونية، الجرائم الإلكترونية.



Legal Challenges in Combating Cybersecurity Crimes in Government Agencies: A Comparative Study Between Jordanian and Saudi Law

By: Meshal Khader Alenzi

Supervised by

Akram Al Fayez

Abstract

This study aims to analyze the legal framework for combating cybersecurity crimes in both Jordan and Saudi Arabia by comparing the legal legislations in both countries. The problem of the study lies in the need to develop and improve the legislative framework to combat the increasingly sophisticated cybercrimes, accelerated by the digital revolution. The study reviews the main similarities and differences between Jordanian and Saudi laws, focusing on how to confront cyber threats and protect the digital infrastructure of government agencies in both countries. The study seeks to analyze the role of legislation in enhancing digital security and its effectiveness in addressing growing threats such as cyber breaches, data theft, and cyber-attacks. It also covers the penalties and preventive measures outlined in each law, examining the ability of these legislations to face modern cybersecurity crimes. Furthermore, the study provides recommendations to improve legal

frameworks and enhance cooperation between Jordan and Saudi Arabia in the field of cybersecurity to address shared challenges. The study relies on a descriptive–analytical approach and a comparative method between Jordanian and Saudi laws, based on legal texts and jurisprudential interpretations without conducting field studies. Through this analysis, the study aims to fill the current legislative gaps, improve the effectiveness of responses to cybersecurity challenges, and achieve effective protection of cybersecurity at the level of government agencies in both countries.

Keywords: Cybersecurity, Cybersecurity Crimes, Legal Legislations, Cybercrimes.

•

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

قائمة المحتويات

الصفحة	الموضوع
ب	التفويض
ج	قرار لجنة المناقشة
د	إهداء
هـ	شكر وتقدير
و	قائمة المحتويات
ح	قائمة الجداول
ط	قائمة الملحقات
ي	الملخص باللغة العربية
ك	الملخص باللغة الإنجليزية
الفصل التمهيدي: الإطار العام للدراسة	
1	المقدمة
2	مشكلة الدراسة
2	أسئلة الدراسة
3	أهداف الدراسة
4	أهمية الدراسة
4	مصطلحات الدراسة
الدراسات السابقة	
7	الدراسات العربية
13	الدراسات الأجنبية
الفصل الأول: الإطار المفاهيمي للجرائم السيبرانية والأمن السيبراني	
16	تمهيد
المبحث الأول: الجرائم السيبرانية والأمن السيبراني	
16	المطلب الأول: تعريف جرائم الأمن السيبراني وخصائصها

16	أولاً: مفهوم جرائم الأمن السيبراني
17	ثانياً: خصائص الجرائم السيبرانية
19	ثالثاً: أنواع الجرائم السيبرانية المختلفة
21	المطلب الثاني: الأمن السيبراني
21	أولاً: مفهوم الأمن السيبراني
21	ثانياً: تطور التكنولوجيا وتأثيرها على الأمن السيبراني
24	ثالثاً: دور التكنولوجيا في تعزيز الأمن السيبراني
المبحث الثاني: التأثيرات والتحديات في الأمن السيبراني	
25	المطلب الأول: الآثار المترتبة على جرائم الأمن السيبراني
25	أولاً: الآثار القانونية والاقتصادية المترتبة على جرائم الأمن السيبراني
27	ثانياً: الآثار الاجتماعية والنفسية المترتبة على جرائم الأمن السيبراني
30	المطلب الثاني: التحديات الحديثة التي تواجه الأمن السيبراني
30	أولاً: التحديات المتعلقة بالتكنولوجيا السريعة والاعتماد المتزايد على التقنيات الرقمية
34	ثانياً: تأثير الجرائم السيبرانية على الأمن الوطني
المبحث الثالث: استراتيجيات وتطوير التشريعات لمكافحة الجرائم السيبرانية	
36	المطلب الأول: استراتيجيات مواجهة الجرائم السيبرانية
36	أولاً: تعزيز الأمن السيبراني والتعاون الدولي
37	ثانياً: التوعية والتدريب في مجال الأمن السيبراني
38	ثالثاً: العلاقة بين الجرائم السيبرانية وحماية البيانات الشخصية
39	المطلب الثاني: تطور التشريعات القانونية وتحليل فعاليتها
39	أولاً: تطور التشريعات القانونية لمكافحة الجرائم السيبرانية
41	ثانياً: تحليل فعالية التشريعات الوطنية في مواجهة الجرائم السيبرانية
الفصل الثاني: التحديات القانونية في كل من المملكة العربية السعودية والمملكة الأردنية الهاشمية	
43	تمهيد
المبحث الأول: التحديات القانونية من المملكة العربية السعودية	

43	أولاً: القوانين السعودية لمكافحة الجرائم السيبرانية
45	ثانياً: القوانين والتشريعات المعمول بها في المملكة العربية السعودية لمكافحة جرائم الأمن السيبراني
51	ثالثاً: التعاون الدولي في مكافحة الجرائم الإلكترونية
51	رابعاً: العقوبات المفروضة على مرتكبي جرائم الأمن السيبراني وفقاً للنظام السعودي
57	خامساً: كيف تواجه المملكة العربية السعودية التحديات التقنية والقانونية المستجدة في مجال الأمن السيبراني
61	سادساً: استخدام الذكاء الاصطناعي والتحليلات المتقدمة في الأمن السيبراني
62	سابعاً: التحديات القانونية في المملكة العربية السعودية
62	ثامناً: دور الحكومة السعودية في تعزيز الأمن السيبراني
المبحث الثاني: القوانين الأردنية لمكافحة الجرائم السيبرانية	
64	تمهيد
64	أولاً: القوانين الأردنية لمكافحة الجرائم السيبرانية
67	ثانياً: التحديات القانونية التي تواجه تطبيق القوانين في الأردن
69	ثالثاً: أوجه القصور في التشريعات الأردنية المتعلقة بمكافحة الجرائم السيبرانية
71	رابعاً: التنسيق بين الجهات الأمنية والقضائية في الأردن لمكافحة الجرائم الإلكترونية
74	خامساً: أبرز القوانين الأردنية المنظمة لجرائم الأمن السيبراني
77	سادساً: دور الحكومة الأردنية في حماية الأمن السيبراني
80	سابعاً: الفرق بين قوانين الجرائم السيبرانية في الأردن والسعودية
84	ثامناً: أبرز التحديات المشتركة التي تواجه المملكة العربية السعودية والمملكة الأردنية الهاشمية في مجال الأمن السيبراني
89	تاسعاً: الدروس المستفادة وأفضل الممارسات لتطوير التشريعات الخاصة بالأمن السيبراني

96	عاشراً: كيف يمكن تعزيز التعاون الإقليمي والدولي بين المملكة العربية السعودية والأردن لمواجهة التهديدات السيبرانية العابرة للحدود
103	الخاتمة
105	النتائج
107	التوصيات
المراجع	
109	المراجع العربية
111	المراجع الأجنبية

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>



التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة:

دراسة مقارنة بين القانون الأردني والسعودي

أعدت من قبل

مشعل خضر روجان الغنزي

أشرف عليها

الأستاذ الدكتور أكرم الفايز

قدمت هذه الرسالة إلى كلية الحقوق كجزء من متطلبات الحصول على درجة الماجستير

في القانون

حزيران 2025



نموذج التفويض

أنا الطالب: مشعل خضر روجان العنزي أفوض جامعة الاسراء تزويد نسخ من رسالتي "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" للمكتبات، والمؤسسات، أو الهيئات، أو الأشخاص عند طلبها

الاسم: مشعل خضر روجان العنزي

التوقيع:

التاريخ: 2025

Al-Isra University

Authorization Form

I am Meshal khader alenzi authorize the Isra University to supply copies of my thesis to libraries or establishments or individuals on request.

Signature:.....

Date: ..15/6/2025

نموذج (4) صفحة لجنة المناقشة

نوقشت هذه الرسالة ("التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة" دراسة مقارنة بين القانونين الأردني والسعودي)

وأجيزت بتاريخ 29 / 5 / 2025.

أعضاء لجنة المناقشة:

التوقيع

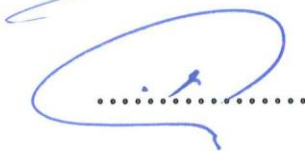
اسم العضو

.....


الأستاذ الدكتور: اكرم طراد الفايز / مشرفاً ومشرفاً

.....


الدكتورة: أمل خلف الحباشنه / عضواً داخلياً

.....


الدكتور: منير محمد العفشيات / عضواً خارجياً

" الإهداء "

إلى حبيبي، وتاج رأسي ومصدر فخري، إلى من بذل الغالي والنفيس في سبيل وصولي إلى درجة علمية عالية، وشجّعني على حب العلم والطموح وتحدي الصعاب.. والذي الغالي.

إلى من تسر العين برؤيته العين عمي الغالي عبد العزيز
إلى حبيبي، وملهمتي ونور عيني وبهجة حياتي، إلى معنى الحب وينبوع الخنان، إلى معلمتي الأول،
إلى من منحتني حب التفوق والنجاح والتميز والمثابرة وعدم اليأس، وغمرتني بنصائحها، وكانت
دعواتها لي بالتوفيق كالنسمة التي تذلل الصعاب في كل خطوة أخطوها.. والدتي العظيمة.

حفظهما الله لي من كل مكروه، ومتعني ببرهما ورد جميلهما.

إلى سندي وعوني بعد الله إخوتي وأخواتي (نوف ، ساره ، ريان ، إيثار ، محمد ، أنس)
إلى من كانت لي الرفيقة المساندة.. رفيقة دربي (وجدان بنت فالح الرويلي)
إلى أجمل هدية حباني الله إياها، إلى قرة العين وبهجة الفؤاد (ريان) وإلى أنيس القلب أبن أخي
الغالي أنس بن ريان ووالدته الكريمه ..

إليكم جميعاً أهدي ثمرة جهدي المتواضع، الذي أرجو من الله أن يجعله علماً يُنتفع به.

" شكر وتقدير "

لا يسعني وقد شارفت هذه الرسالة على الانتهاء إلا أن أتقدم بجزيل الشكر وخالص العرفان إلى المربي الفاضل الأستاذ الدكتور: أكرم الفايز، الذي كان لتوجيهاته وآرائه الدور الأكبر في إخراج هذا الجهد إلى حيز الوجود.

كما أتقدم بالشكر للأساتذة أعضاء لجنة المناقشة الأستاذ الدكتور أكرم الفايز والدكتور منير العفيشات والدكتورة أمل الحباشنة على تفضلهم بقبول مناقشة الرسالة، وإلى كل الأساتذة الذين أضافوا بصمتهم في هذه الرسالة، وإلى جميع أفراد مجتمع الدراسة. والشكر الجزيل لمن ساهم في تطبيق إجراءات هذه الرسالة.

قائمة المحتويات

الصفحة	الموضوع
ب	التفويض
ج	قرار لجنة المناقشة
د	إهداء
هـ	شكر وتقدير
و	قائمة المحتويات
ح	قائمة الجداول
ط	قائمة الملحقات
ي	الملخص باللغة العربية
ك	الملخص باللغة الإنجليزية
الفصل التمهيدي: الإطار العام للدراسة	
1	المقدمة
2	مشكلة الدراسة
2	أسئلة الدراسة
3	أهداف الدراسة
4	أهمية الدراسة
4	مصطلحات الدراسة
الدراسات السابقة	
7	الدراسات العربية
13	الدراسات الأجنبية
الفصل الأول: الإطار المفاهيمي للجرائم السيبرانية والأمن السيبراني	
16	تمهيد
المبحث الأول: الجرائم السيبرانية والأمن السيبراني	
16	المطلب الأول: تعريف جرائم الأمن السيبراني وخصائصها

16	أولاً: مفهوم جرائم الأمن السيبراني
17	ثانياً: خصائص الجرائم السيبرانية
19	ثالثاً: أنواع الجرائم السيبرانية المختلفة
21	المطلب الثاني: الأمن السيبراني
21	أولاً: مفهوم الأمن السيبراني
21	ثانياً: تطور التكنولوجيا وتأثيرها على الأمن السيبراني
24	ثالثاً: دور التكنولوجيا في تعزيز الأمن السيبراني
المبحث الثاني: التأثيرات والتحديات في الأمن السيبراني	
25	المطلب الأول: الآثار المترتبة على جرائم الأمن السيبراني
25	أولاً: الآثار القانونية والاقتصادية المترتبة على جرائم الأمن السيبراني
27	ثانياً: الآثار الاجتماعية والنفسية المترتبة على جرائم الأمن السيبراني
30	المطلب الثاني: التحديات الحديثة التي تواجه الأمن السيبراني
30	أولاً: التحديات المتعلقة بالتكنولوجيا السريعة والاعتماد المتزايد على التقنيات الرقمية
34	ثانياً: تأثير الجرائم السيبرانية على الأمن الوطني
المبحث الثالث: استراتيجيات وتطوير التشريعات لمكافحة الجرائم السيبرانية	
36	المطلب الأول: استراتيجيات مواجهة الجرائم السيبرانية
36	أولاً: تعزيز الأمن السيبراني والتعاون الدولي
37	ثانياً: التوعية والتدريب في مجال الأمن السيبراني
38	ثالثاً: العلاقة بين الجرائم السيبرانية وحماية البيانات الشخصية
39	المطلب الثاني: تطور التشريعات القانونية وتحليل فعاليتها
39	أولاً: تطور التشريعات القانونية لمكافحة الجرائم السيبرانية
41	ثانياً: تحليل فعالية التشريعات الوطنية في مواجهة الجرائم السيبرانية
الفصل الثاني: التحديات القانونية في كل من المملكة العربية السعودية والمملكة الأردنية الهاشمية	
43	تمهيد
المبحث الأول: التحديات القانونية من المملكة العربية السعودية	

43	أولاً: القوانين السعودية لمكافحة الجرائم السيبرانية
45	ثانياً: القوانين والتشريعات المعمول بها في المملكة العربية السعودية لمكافحة جرائم الأمن السيبراني
51	ثالثاً: التعاون الدولي في مكافحة الجرائم الإلكترونية
51	رابعاً: العقوبات المفروضة على مرتكبي جرائم الأمن السيبراني وفقاً للنظام السعودي
57	خامساً: كيف تواجه المملكة العربية السعودية التحديات التقنية والقانونية المستجدة في مجال الأمن السيبراني
61	سادساً: استخدام الذكاء الاصطناعي والتحليلات المتقدمة في الأمن السيبراني
62	سابعاً: التحديات القانونية في المملكة العربية السعودية
62	ثامناً: دور الحكومة السعودية في تعزيز الأمن السيبراني
المبحث الثاني: القوانين الأردنية لمكافحة الجرائم السيبرانية	
64	تمهيد
64	أولاً: القوانين الأردنية لمكافحة الجرائم السيبرانية
67	ثانياً: التحديات القانونية التي تواجه تطبيق القوانين في الأردن
69	ثالثاً: أوجه القصور في التشريعات الأردنية المتعلقة بمكافحة الجرائم السيبرانية
71	رابعاً: التنسيق بين الجهات الأمنية والقضائية في الأردن لمكافحة الجرائم الإلكترونية
74	خامساً: أبرز القوانين الأردنية المنظمة لجرائم الأمن السيبراني
77	سادساً: دور الحكومة الأردنية في حماية الأمن السيبراني
80	سابعاً: الفرق بين قوانين الجرائم السيبرانية في الأردن والسعودية
84	ثامناً: أبرز التحديات المشتركة التي تواجه المملكة العربية السعودية والمملكة الأردنية الهاشمية في مجال الأمن السيبراني
89	تاسعاً: الدروس المستفادة وأفضل الممارسات لتطوير التشريعات الخاصة بالأمن السيبراني

96	عاشرا: كيف يمكن تعزيز التعاون الإقليمي والدولي بين المملكة العربية السعودية والأردن لمواجهة التهديدات السيبرانية العابرة للحدود
103	الخاتمة
105	النتائج
107	التوصيات
المراجع	
109	المراجع العربية
111	المراجع الأجنبية

التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون

الأردني والسعودي

مشعل خضر روجان العنزي

أشرف عليها

الاستاذ الدكتور : أكرم الفايز

الملخص

تهدف هذه الدراسة إلى تحليل الإطار القانوني لمكافحة جرائم الأمن السيبراني في كل من الأردن والسعودية، من خلال مقارنة التشريعات القانونية في كلا البلدين. تتمثل مشكلة الدراسة في الحاجة إلى تطوير وتحسين الإطار التشريعي لمكافحة الجرائم السيبرانية التي تزداد تطوراً مع تسارع الثورة الرقمية. وتستعرض الدراسة أبرز أوجه التشابه والاختلاف بين القوانين الأردنية والسعودية، مع التركيز على كيفية التصدي للتهديدات السيبرانية وحماية البنية التحتية الرقمية للدوائر الحكومية في كل من البلدين. تسعى الدراسة إلى تحليل دور التشريعات في تعزيز الأمن الرقمي، ومدى كفاءتها في التصدي للتهديدات المتزايدة مثل الاختراقات السيبرانية، وسرقة البيانات، والهجمات الإلكترونية. كما تتناول العقوبات والإجراءات الوقائية المتبعة في كل قانون، وتبحث في قدرة هذه التشريعات على مواجهة الجرائم السيبرانية الحديثة. كما تقدم الدراسة توصيات لتحسين التشريعات القانونية وتعزيز التعاون بين الأردن والسعودية في مجال الأمن السيبراني لمواجهة التحديات المشتركة. وتعتمد الدراسة على المنهج الوصفي التحليلي ومنهج المقارنة بين القوانين الأردنية والسعودية، مستندة إلى النصوص القانونية والتفسيرات الفقهية دون إجراء دراسات ميدانية. من خلال هذا التحليل، تهدف الدراسة إلى سد الفجوات التشريعية الحالية، ورفع كفاءة الاستجابة للتحديات السيبرانية، وتحقيق حماية فعالة للأمن السيبراني على مستوى دوائر الدولة في كلا البلدين.

الكلمات المفتاحية: الأمن السيبراني، جرائم الأمن السيبراني، التشريعات القانونية، الجرائم الإلكترونية.

الفصل التمهيدي

المقدمة:

لقد أصبحت جرائم الأمن السيبراني واحدة من أخطر التحديات التي تواجه الدول الحديثة مع استمرار الثورة الرقمية في تغيير جميع جوانب الحياة. حيث بات الاعتماد على التكنولوجيا الرقمية والبنية التحتية الإلكترونية ضرورة لا غنى عنها في إدارة مختلف القطاعات الحكومية والخاصة، إلا أن هذا التحول الرقمي صاحبه ظهور تهديدات سيبرانية متطورة تهدد الأمن الوطني وسلامة الأفراد والمؤسسات. تشمل هذه التهديدات الاختراقات السيبرانية، وسرقة البيانات، والهجمات الإلكترونية الموجهة ضد البنى التحتية الحيوية¹.

وفي مواجهة هذه التحديات، ظهرت الحاجة الماسة لوضع أطر قانونية وتشريعات فعّالة قادرة على مكافحة هذه الجرائم وتعزيز الحماية القانونية للبيانات والمعلومات. يمثل هذا النهج خطوة جوهريّة نحو حماية الأمن الداخلي للدول واستقرارها الاقتصادي، فضلاً عن حماية خصوصية الأفراد في الفضاء الرقمي. في هذا السياق، تعكس التشريعات في كل من الأردن والسعودية اهتماماً ملحوظاً بوضع قوانين متخصصة لمكافحة الجرائم السيبرانية، بما يدل على إدراك واضح لأهمية تعزيز الأمن السيبراني على المستوى الوطني².

ومع التطورات التقنية السريعة التي يشهدها العالم، بات من الضروري دراسة ومقارنة هذه التشريعات لفهم مدى فعاليتها في مواجهة التحديات السيبرانية المتزايدة. من هنا، تأتي أهمية هذه الدراسة التي تهدف إلى مقارنة الأطر القانونية الأردنية والسعودية في مكافحة جرائم الأمن السيبراني. تسلط الدراسة الضوء

¹ برادة، عبد الرازق. (2024). الأمن السيبراني ودوره في الحد من الهجمات الإلكترونية. في الجريمة

الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، المركز المغاري-شرق أدنى للدراسات الإستراتيجية.

² مسلم، نيراس، (2021). الجرائم السيبرانية وأثرها على الأمن السيبراني، كلية القانون، جامعة بغداد.

على نقاط القوة والتحديات في كل نظام قانوني، وتحلل مدى تكامل هذه التشريعات مع التطورات التكنولوجية الحديثة. كما تقدم الدراسة اقتراحات لتحسين الأطر القانونية وتعزيز التعاون بين البلدين في هذا المجال الحيوي، من أجل مواجهة التهديدات السيبرانية بشكل أكثر شمولية وكفاءة³.

مشكلة الدراسة

مع التطور التكنولوجي السريع، أصبحت جرائم الأمن السيبراني تمثل تهديدًا خطيرًا على دول العالم، بما في ذلك الأردن والمملكة العربية السعودية. ورغم وجود تشريعات قانونية متقدمة في كلا البلدين، إلا أن هناك فجوات تشريعية تعيق التصدي لبعض الجرائم السيبرانية المستحدثة، مما يثير الحاجة إلى تحسين الإطار القانوني لمواكبة هذه التحديات. لذا، تتمثل مشكلة الدراسة في:

. كيف يمكن تطوير وتحسين الإطار التشريعي لكل من الأردن والمملكة العربية السعودية لمكافحة

جرائم الأمن السيبراني بشكل أكثر فعالية وشمولية؟

. ما هي أوجه التشابه والاختلاف بين التشريعات الأردنية والسعودية في كيفية التصدي للجرائم

السيبرانية وحماية الأمن الرقمي؟

تعالج الدراسة هذه الأسئلة من خلال تحليل مقارنة بين التشريعات في البلدين، مع التركيز على دور هذه القوانين في حماية دوائر الدولة من التهديدات السيبرانية.

أسئلة الدراسة

1. ما هي الإطار القانوني لجرائم الأمن السيبراني في الأردن والسعودية؟

2. ما هي أبرز الجرائم السيبرانية التي تواجه دوائر الدولة؟

³ محيدين، علي، وحامي، عادل. (2022). الآليات القانونية لحماية الأمن السيبراني. في مؤتمر الآليات القانونية لحماية الأمن السيبراني. جامعة غرداية، الجزائر.

3. كيف تختلف العقوبات والإجراءات الوقائية بين القانون الأردني والقانون السعودي؟

أهداف الدراسة

1. تحليل الإطار القانوني لمكافحة جرائم الأمن السيبراني في التشريعات الأردنية والسعودية:

يتناول هذا التحليل الأنظمة القانونية المعتمدة في كل من الأردن والسعودية لمكافحة الجرائم السيبرانية مثل نظام مكافحة جرائم المعلوماتية في السعودية وقانون الجرائم الإلكترونية في الأردن. يركز التحليل على كيفية تحديد هذه التشريعات للجرائم السيبرانية وتحديد العقوبات المترتبة عليها.

2. تحديد أوجه التشابه والاختلاف بين القانونين في مواجهة الجرائم السيبرانية:

تتشترك التشريعات الأردنية والسعودية في الكثير من الأهداف والمبادئ لمكافحة الجرائم الإلكترونية، ولكن تختلف في تفاصيل التطبيق والعقوبات. يتمثل الاختلاف في مرونة التشريعات الأردنية التي تجدد بشكل مستمر لمواكبة التهديدات الجديدة، بينما تفتقر التشريعات السعودية إلى التحديث المستمر في هذا المجال.

3. تقديم توصيات لتحسين التشريعات القانونية في الأردن والسعودية وتعزيز التعاون المشترك:

يوصى بتطوير التشريعات في كلا البلدين لمواكبة التطورات السريعة في تكنولوجيا المعلومات وأمنها السيبراني. بالإضافة إلى ذلك، يجب تعزيز التعاون بين الدولتين لتبادل المعلومات والأبحاث المتعلقة بالأمن السيبراني وتحقيق التنسيق المشترك لمكافحة الجرائم السيبرانية العابرة للحدود.

أهمية الدراسة

تتبع أهمية هذه الدراسة من تسليطها الضوء على القضايا الأمنية والقانونية الحساسة المرتبطة بحماية المعلومات الحكومية ومكافحة الجرائم السيبرانية، حيث تعكس التحديات المتزايدة التي تواجه الأنظمة الرقمية في العصر الحديث. كما تكتسب الدراسة أهمية إضافية من خلال تحليلها المقارن بين التشريعات الأردنية والسعودية، وهو تحليل نادر يسهم في تحسين الإطار القانوني في البلدين وتعزيز قدرتهما على مواجهة التهديدات السيبرانية بفعالية. بالإضافة إلى ذلك، تقدم الدراسة توصيات عملية للمشرعين وجهات إنفاذ القانون، بهدف سد الثغرات القانونية، وتعزيز الاستراتيجيات الوقائية، وتوفير إطار قانوني قوي ومرن قادر على التصدي للتحديات السيبرانية المستجدة.

منهجية الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التحليلي لفهم القوانين المتعلقة بجرائم الأمن السيبراني وتحليلها، حيث يتم استعراض التشريعات الحالية وتقييم مدى فعاليتها في مواجهة التحديات السيبرانية. كما تستعين الدراسة بالمنهج المقارن للكشف عن أوجه التشابه والاختلاف بين التشريعات الأردنية والسعودية، مما يساعد في تقديم توصيات بناءة تساهم في تحسين هذه التشريعات وتعزيز الإطار القانوني لمكافحة الجرائم السيبرانية بشكل أكثر كفاءة وفعالية.

مصطلحات الدراسة

1. **التحديات القانونية (Legal Challenges) :** يشير المصطلح إلى العقبات التي تواجه

المشرعين والقضاة والمحامين في صياغة وتطبيق القوانين التي تنظم مجال معين، مثل قوانين

مكافحة الجرائم السيبرانية، والتي قد تشمل تعقيدات تقنية، عدم وضوح النصوص القانونية، أو تضارب القوانين بين الدول المختلفة⁴.

2. مكافحة الجرائم (Crime Prevention) : مجموعة الإجراءات والسياسات التي تتخذها الدولة

أو المؤسسات القانونية بهدف الحد من وقوع الجرائم، سواءً من خلال تشديد العقوبات، أو تحسين نظم الرقابة الإلكترونية، أو تعزيز الوعي القانوني والتقني لدى المؤسسات الحكومية والمجتمع⁵.

3. جرائم الأمن السيبراني (Cybersecurity Crimes) : الجرائم التي تستهدف أو تُرتكب

باستخدام التقنيات الحديثة والشبكات الإلكترونية، وتشمل جرائم مثل الاختراق (Hacking) ،

التجسس الإلكتروني (Cyber Espionage) ، سرقة البيانات (Data Breach) ، والهجمات

الإلكترونية (Cyber Attacks) مثل هجمات الحرمان من الخدمة (DDoS)⁶.

4. دوائر الدولة (Government Sectors) : تشمل المؤسسات والإدارات الحكومية التي تعمل

على تقديم الخدمات العامة وتنفيذ القوانين. في سياق الأمن السيبراني، تشمل دوائر الدولة

⁴ رفاعي، محمد، (2023). التحديات القانونية والإدارية لخصخصة المرافق العامة: دراسة مقارنة. مجلة البحوث القانونية والاقتصادية (المنصورة)، المجلد 13(84).

⁵ الصبحي، شهد، والربابغ، ريم، (2022). مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة 2030: دراسة مسحية لدى طلبة كلية الآداب والعلوم الإنسانية بجامعة الملك عبد العزيز بجدة، العدد (40).

⁶ مصطفى، إسلام، (2022). جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري. المجلة القانونية، المجلد 12(3).

الجهات المسؤولة عن حماية البنية التحتية الرقمية، مثل الوزارات والهيئات الحكومية ومراكز البيانات الوطنية⁷.

5. القانون الأردني (Jordanian Law) : الإطار القانوني الذي يحكم المملكة الأردنية الهاشمية، والذي يستمد أصوله من الشريعة الإسلامية والقانون المدني الفرنسي. يتضمن القانون الأردني مجموعة من التشريعات التي تنظم الجرائم السيبرانية، مثل قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015⁸.

6. القانون السعودي (Saudi Law) : الإطار القانوني الذي يحكم المملكة العربية السعودية، ويستمد أصوله من الشريعة الإسلامية. يحتوي القانون السعودي على أنظمة تنظم الأمن السيبراني ومكافحة الجرائم السيبرانية، مثل نظام مكافحة الجرائم المعلوماتية الصادر عام 2007، والذي يهدف إلى حماية البيانات الرقمية والبنية التحتية الإلكترونية⁹.

⁷ الحصري، طارق، (2019). الجهاز الإداري للدولة في مصر: المفهوم، التحديات، ورؤية التطوير، الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري.

⁸ الوصيف، آية، (2018). نص قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. تشريعات أردنية - قانون الجرائم الإلكترونية.

⁹ المركز الوطني للتنافسية. (2024). الاستراتيجية الوطنية للأمن السيبراني.

الدراسات السابقة:

أولاً: الدراسات العربية:

1-دراسة نصار (2024) بعنوان: واقع الحماية الجزائية للأمن السيبراني دراسة مقارنة: الأردن-

قطر

تهدف هذه الدراسة المقارنة بين الأردن وقطر إلى تقييم واقع الحماية الجزائية للأمن السيبراني في كلا البلدين وتحليل استراتيجياتهما في مواجهة التهديدات السيبرانية. تعتمد الدراسة على تحليل القوانين والتشريعات، بالإضافة إلى مراجعة السياسات الأمنية وأدوار المؤسسات المعنية. توصلت النتائج إلى أن الأردن قد اتخذ خطوات مهمة في تعزيز الحماية الجزائية من خلال إقرار قوانين جديدة وتطوير قدرات الأجهزة الأمنية والقضائية، بينما برزت قطر كرائدة إقليمية بتنفيذ استراتيجية وطنية متكاملة، وتعزيز التعاون بين القطاعين العام والخاص. توصي الدراسة بضرورة تحديث التشريعات في كلا البلدين لمواكبة تطور الجرائم السيبرانية، وتكثيف التدريب للكوادر المتخصصة، وتعزيز التعاون المشترك وتبادل الخبرات في مجال الأمن السيبراني.¹⁰

التعقيب: تسلط هذه الدراسة الضوء على الجهود المبذولة في الأردن وقطر لتعزيز الحماية القانونية للأمن السيبراني، مع التركيز على التشريعات الحديثة التي تم إدخالها في كلا البلدين. بينما قدمت قطر نموذجاً رائداً في التعاون بين القطاعين العام والخاص لتعزيز الأمن السيبراني، تبرز الحاجة إلى تحديث القوانين والتشريعات بشكل مستمر لضمان فعالية الاستجابة للتحديات السيبرانية المتجددة، وهو ما يعد محوراً أساسياً في توصيات الدراسة.

¹⁰ الوصيف، آية، (2018). نص قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. تشريعات أردنية – قانون الجرائم الإلكترونية.

2-دراسة الخضيرى (2024) بعنوان: سبل مكافحة الجرائم السيبرانية العابرة للحدود

تناولت هذه الدراسة الجرائم السيبرانية باعتبارها من أخطر التهديدات التي تواجه الأمن القومي للدول، حيث تتميز بقدرتها على تجاوز الحدود الجغرافية والسياسية والثقافية. يزداد خطر هذه الجرائم مع التطور المستمر لتكنولوجيا المعلومات والاتصالات، مما أدى إلى تهديد السيادة الوطنية وأثر سلباً على الاقتصاد والأمن الوطني. وتشمل الجرائم السيبرانية تهديدات متنوعة، أبرزها الإرهاب السيبراني الذي لا يعترف بالحدود، مما يتطلب استجابة دولية ومحلية عاجلة. توصي الدراسة بضرورة تعزيز التدابير الوقائية من خلال تحديث التشريعات، تطوير القدرات التقنية، وزيادة الوعي المجتمعي بخطورة هذه الجرائم، إلى جانب تعزيز التعاون الدولي لمواجهتها والحد من آثارها السلبية.

التعقيب: تؤكد هذه الدراسة على أهمية التعاون الدولي في مكافحة الجرائم السيبرانية العابرة للحدود، حيث تتطلب هذه التهديدات جهوداً منسقة بين الدول لضمان استجابة فعالة. كما تسلط الدراسة الضوء على الحاجة الملحة لتحديث التشريعات باستمرار لمواكبة التطورات السريعة في الفضاء الإلكتروني. بالإضافة إلى ذلك، يظهر بوضوح أهمية تطوير القدرات التقنية وتعزيز البنية التحتية الرقمية، لضمان قدرة الدول على التصدي للهجمات السيبرانية المعقدة، مما يعزز الأمن الرقمي على المستويين الوطني والدولي.¹¹

11 الصبحي، شهد، والرابع، ريم، (2022). مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة 2030: دراسة مسحية لدى طلبة كلية الآداب والعلوم الإنسانية بجامعة الملك عبد العزيز بجدة، العدد (40).

3- دراسة الخالدي وآخرون (2023) بعنوان: دور الأمن العام في مكافحة الجرائم الإلكترونية عبر

شبكات التواصل الاجتماعي: دراسة تحليلية

هدفت الدراسة إلى التعرف على دور الأمن العام في مكافحة الجرائم الإلكترونية عبر شبكات التواصل الاجتماعي، وتحليل أهم الموضوعات التي يتم نشرها وأساليب التوعية التي يعتمد عليها الأمن العام عبر هذه الشبكات. اعتمدت الدراسة على المنهج الوصفي التحليلي، وتوصلت إلى نتيجة مفادها أن الجمهور الأردني يعتمد بشكل مباشر على الحملات التوعوية المتعلقة بالجرائم الإلكترونية التي ينشرها الأمن العام عبر موقعه الرسمي على وسائل التواصل الاجتماعي. كما أشارت الدراسة إلى الدور البارز والفعال لجهاز الأمن العام في مكافحة الجرائم الإلكترونية وتعريف الجمهور بمخاطرها والعقوبات المترتبة عليها. وفي ضوء هذه النتائج، أوصت الدراسة بتكثيف الجهود الأمنية في نشر الحملات التوعوية عبر شبكات التواصل الاجتماعي التي تهدف إلى مكافحة الجرائم الإلكترونية بمختلف أنواعها، بالإضافة إلى تغليظ العقوبات القانونية على مرتكبي هذه الجرائم للحد من انتشارها.

التعليق: تعد الدراسة التي تناولت دور الأمن العام في مكافحة الجرائم الإلكترونية عبر شبكات التواصل الاجتماعي خطوة هامة لفهم كيفية التصدي لهذه الجرائم التي تهدد الأفراد والمجتمع. تظهر الدراسة فعالية الحملات التوعوية التي يبثها الأمن العام عبر الوسائل الاجتماعية في توعية الجمهور الأردني بمخاطر الجرائم الإلكترونية وعواقبها. ومع ذلك، يمكن تعزيز هذه الجهود من خلال تنويع أساليب التوعية لتشمل فئات أوسع من المجتمع، بما في ذلك الذين لا يستخدمون الشبكات الاجتماعية بشكل كبير. كما أن تغليظ العقوبات يمكن أن يكون رادعاً، لكنه يجب أن يكون موازناً مع سياسات وقائية وتعليمية تركز على الحد من الجرائم قبل وقوعها. في النهاية، تعتبر هذه الدراسة أساساً مهماً للتطوير المستقبلي في مجال الأمن السيبراني من خلال التعاون بين القطاعين العام والخاص وتوسيع نطاق التوعية.

4- دراسة حميدة (2021) بعنوان: الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي: نحو تفعيل

دور الأمن السيبراني المعلوماتي

تهدف هذه الدراسة إلى تحذير الجيل الجديد من الجرائم السيبرانية التي تتسم بخطورتها وصعوبة إثباتها، مع التركيز على الجرائم التي تُرتكب عبر مواقع التواصل الاجتماعي وتأثيرها على الأمن القومي للدول. اعتمدت الدراسة على المنهج الوصفي التحليلي لاستعراض وتحليل مظاهر الجرائم الإلكترونية وأساليب الحماية السيبرانية المتاحة لمواجهتها. توصلت الدراسة إلى أن الانتشار العشوائي لمواقع التواصل الاجتماعي وضعف التشريعات القانونية والرقابة يزيد من خطورة هذه الجرائم، مما يهدد البيانات الشخصية وأمن المؤسسات الوطنية. توصي الدراسة بضرورة تطوير تشريعات متخصصة لمكافحة الجرائم السيبرانية، تعزيز وسائل الحماية المعلوماتية، ورفع مستوى الوعي المجتمعي بأهمية الأمن السيبراني.

التعليق: تسلط هذه الدراسة الضوء على حجم المخاطر المتزايدة التي تشكلها الجرائم الإلكترونية عبر منصات التواصل الاجتماعي، حيث أصبحت هذه المنصات بيئة خصبة للاختراقات، والاحتيال الإلكتروني، وانتهاك الخصوصية. تؤكد الدراسة على أهمية وجود تشريعات متخصصة تنظم الاستخدام الآمن لهذه المنصات، وتحمي المستخدمين من الاستغلال السيبراني. كما تشدد على ضرورة زيادة الوعي المجتمعي حول حماية المعلومات الشخصية، وتعزيز الثقافة الرقمية التي تساعد الأفراد على تجنب الوقوع ضحية لهذه الجرائم، مما يساهم في بناء فضاء إلكتروني أكثر أمانًا وثقة.

5-دراسة مهدي (2021) بعنوان: الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري

تهدف هذه الدراسة إلى تحليل التحولات العميقة التي شهدتها العالم نتيجة للتطور التكنولوجي، مع التركيز على الجرائم السيبرانية باعتبارها أحد التحديات الرئيسية الناتجة عن هذه التحولات. اعتمدت الدراسة على المنهج الوصفي التحليلي لفهم طبيعة هذه الجرائم وتأثيرها على المجتمع الجزائري، في ظل كونها جرائم عابرة للحدود الجغرافيا لا تميز بين المجتمعات. توصلت الدراسة إلى أن الجزائر شهدت في السنوات الأخيرة ارتفاعاً ملحوظاً في مؤشر الجرائم السيبرانية، مما دفع المشرع إلى سن تشريعات تهدف إلى الحد من هذه الظاهرة. توصي الدراسة بضرورة تعزيز الإطار القانوني لمكافحة الجرائم السيبرانية، وتطوير قدرات الجهات الأمنية، مع نشر الوعي المجتمعي حول مخاطر الجرائم السيبرانية وسبل الوقاية منها.

التعليق: تقدم هذه الدراسة تحليلاً هاماً للتهديدات السيبرانية في الجزائر، حيث تسلط الضوء على التحديات القانونية والتقنية التي تفرضها هذه الجرائم على التشريع الجزائري. يبرز في الدراسة الحاجة إلى تعزيز التشريعات الوطنية وتطوير القوانين لتواكب التطورات السريعة في الجريمة السيبرانية، بما يضمن حماية فعالة للبنية التحتية الرقمية والمعلومات الحساسة، ويساهم في تحسين قدرة الدولة على التصدي للهجمات الإلكترونية بفعالية وكفاءة أكبر.

6- دراسة المرداس (2021) بعنوان: الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)

يهدف البحث إلى التعرف على واقع الأمن السيبراني في المملكة العربية السعودية مع التركيز على الوضع الحالي والمستقبلي لهذا المجال المهم، في ظل التحديات الاقتصادية والسياسية. اعتمدت الدراسة على المنهج الوصفي من خلال مراجعة الأدبيات السابقة، حيث تم شرح مفهوم أمن المعلومات

والأمن السيبراني وأهمية هذا المجال في حماية المعلومات. كما تم استعراض جهود المملكة في مكافحة الجرائم السيبرانية، وأشارت النتائج إلى أن مكافحة الجرائم الإلكترونية العابرة للحدود تعد من أكبر التحديات التي تواجه الدول، وتستدعي التعاون الدولي والإقليمي لمواجهتها. أوصى البحث بعدد من التوصيات المهمة، أبرزها نشر ثقافة الأمن السيبراني في المجتمع، توفير البنية التحتية اللازمة، تدريب الكوادر البشرية في هذا المجال، تمكين المرأة في العمل في الأمن السيبراني، بالإضافة إلى حماية الأطفال من الجرائم السيبرانية أثناء استخدام الإنترنت.

التعليق: تعتبر هذه الدراسة خطوة مهمة لفهم التحديات التي تواجه الأمن السيبراني في المملكة العربية السعودية، وخاصة فيما يتعلق بـ الجرائم الإلكترونية العابرة للحدود. التوصيات التي تم طرحها تعتبر أساسية لضمان حماية المعلومات وتعزيز الأمن الرقمي. من المهم أن تتبّع المملكة هذه التوصيات بشكل عاجل، خاصة في مجالات التدريب والتأهيل للكوادر، بالإضافة إلى تمكين المرأة في هذا القطاع لتعزيز التنوع. كما أن حماية الأطفال يجب أن تكون أولوية في مواجهة التهديدات المتزايدة على الإنترنت.

ثانياً: الدراسات الأجنبية

1-دراسة (Yousfi, 2024) بعنوان:

Cybersecurity Challenges and International Cooperation

تهدف هذه الدراسة إلى تعريف الأمن السيبراني وتقنياته، وتحديد مخاطر الجرائم الإلكترونية، مع إبراز الجهود الوطنية والدولية لمكافحة هذه الجرائم وتقييم مدى فعاليتها، مع التركيز على استجابة المشرع الجزائري لهذه المخاطر التي تهدد الأمن والمصالح الفردية. اعتمدت الدراسة على

المنهج الاستنباطي (التحليلي) والمقارن لتوضيح مفهوم الأمن السيبراني وحماية البيانات الشخصية، إضافة إلى تناول الآليات القانونية المتاحة لحمايتها ضد التهديدات الرقمية. توصلت الدراسة إلى أن النصوص التشريعية الجنائية الحالية بحاجة إلى تعزيز لضمان حماية فعالة للأمن السيبراني. توصي الدراسة بتطوير الأطر القانونية الوطنية لتحقيق توازن بين تبادل المعلومات في إطار التعاون الدولي وحماية البيانات الشخصية، مع تعزيز التعاون الدولي لمواجهة الجرائم الرقمية المتزايدة.

التعليق: تسلط هذه الدراسة الضوء على أهمية تعزيز الأطر القانونية في الجزائر لمواجهة الجرائم السيبرانية المتزايدة، حيث تتطلب التطورات الرقمية المتسارعة تحديث التشريعات الوطنية لضمان استجابة فعالة لهذه التهديدات. كما توصي الدراسة بتطوير التعاون الدولي بين الجزائر والدول الأخرى لمكافحة الجرائم الرقمية العابرة للحدود، والتي تشكل خطرًا على الأمن الفردي والمؤسسي، مما يستدعي جهودًا منسقة لتعزيز الأمن السيبراني على المستويين الوطني والدولي.

2-دراسة (Al-Kasassbeh1 at el., 2024) بعنوان:

Digital Human Rights in Jordanian Legislation and International Agreement

تهدف هذه الدراسة إلى تحليل واقع حقوق الإنسان الرقمية في التشريعات الأردنية والاتفاقيات الدولية، حيث تشمل هذه الحقوق الحريات المرتبطة بالتواصل، وتبادل المعرفة، وحرية الرأي، وحماية الخصوصية والبيانات، بالإضافة إلى ضمان الوصول العادل إلى البنية التحتية والخدمات التكنولوجية. استخدمت الدراسة منهجًا قانونيًا نوعيًا يعتمد على تحليل النصوص القانونية والبيانات المتاحة عبر المنصات الإلكترونية. توصلت الدراسة إلى أن الحقوق الرقمية تُعد جزءًا لا يتجزأ من حقوق الإنسان

الأساسية، حيث ظهر مفهوم "الحقوق الرقمية" بالتزامن مع تطور خطاب حقوق الإنسان المعاصر. وقد أكدت المنظمات الدولية على ضرورة الاعتراف بهذه الحقوق وضمان حمايتها. ومع ذلك، تواجه الحقوق الرقمية تحديات معقدة تشمل الجوانب التشريعية، والاستراتيجية، والتقنية، حيث أصبح استغلال البيانات الشخصية من قبل الشركات التكنولوجية الكبرى وتوظيفها لأغراض تجارية أو أمنية مصدر قلق كبير. توصي الدراسة بضرورة تعزيز الآليات التنظيمية لحماية الحقوق الرقمية، مع مراعاة التوازن بين حماية هذه الحقوق واحترام النظام العام والأخلاقيات المجتمعية.

التعقيب: تبرز هذه الدراسة أهمية حقوق الإنسان الرقمية في التشريع الأردني في ظل التحول الرقمي السريع، حيث تسلط الضوء على الحاجة إلى تعزيز آليات حماية هذه الحقوق وضمان توازنها مع النظام العام. كما تؤكد الدراسة على أهمية تطوير القوانين لضمان الخصوصية، حرية التعبير، وحماية البيانات الشخصية، بما يواكب التحديات الرقمية الحديثة ويحفظ حقوق الأفراد في البيئة الرقمية.

3-دراسة (Rawindaran et al., 2023) بعنوان:

Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom

تتناول هذه الدراسة مقاومة الشركات الصغيرة والمتوسطة في السعودية والمملكة المتحدة لتدابير الأمن السيبراني ضمن سياق الصناعة 5.0، مع التركيز على الحوكمة والسياسات المؤثرة. تبحث الدراسة في العوامل الثقافية والاقتصادية التي تسهم في هذه المقاومة، مثل ضعف الوعي بمخاطر الأمن السيبراني، والقيود المالية، والأولويات المتنافسة. اعتمدت الدراسة على منهج الأساليب المختلطة، بما

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

إسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

إسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

الخاتمة

تعتبر الجرائم السيبرانية من التحديات الكبيرة في العصر الرقمي، حيث تزداد تعقيداً نتيجة للتطورات التكنولوجية السريعة. في هذه الدراسة، تم تحليل التشريعات الأردنية والسعودية لمكافحة الجرائم السيبرانية، مع التركيز على أوجه التشابه والاختلاف بينهما. يشترك البلدان في التشريعات المتعلقة بحماية البيانات وفرض عقوبات صارمة على الجرائم السيبرانية، ولكن الأردن قام بتحديث قوانينه بشكل أسرع مقارنةً بالسعودية. كما تم التركيز على أهمية الذكاء الاصطناعي في الكشف المبكر عن التهديدات، والتأكيد على نقص الوعي والتدريب كأحد أكبر التحديات. تتضمن التوصيات تعزيز الوعي السيبراني، استثمار الذكاء الاصطناعي، وتحديث التشريعات لمواكبة التطورات. بوجه عام، يتطلب الأمر تعاوناً دولياً مستمراً لمكافحة الجرائم السيبرانية وحماية الفضاء الإلكتروني.

يعد الأمن السيبراني اليوم واحداً من أهم المجالات التي تتطلب تعاوناً دولياً وإقليمياً واسع النطاق، خاصة في ظل تزايد الهجمات الإلكترونية العابرة للحدود، والتي تستهدف المؤسسات الحيوية، القطاعات الاقتصادية، والبنى التحتية الرقمية. في هذا السياق، يصبح التعاون بين المملكة العربية السعودية والمملكة الأردنية الهاشمية ضرورة حتمية لتعزيز القدرات السيبرانية لكل من البلدين، ومواجهة التهديدات التي قد تؤثر على أمنهما الوطني والاقتصادي.

يتطلب تحقيق هذا التعاون تبادل المعلومات الأمنية حول الهجمات السيبرانية والبرمجيات الخبيثة بين الجهات المختصة، مما يسهم في سرعة الاستجابة للهجمات والحد من تأثيرها. كما أن توحيد القوانين والتشريعات المتعلقة بجرائم الأمن السيبراني بين السعودية والأردن يمكن أن يسهل عملية ملاحقة مرتكبي هذه الجرائم، خاصة مع تعقيد قضايا الجرائم السيبرانية التي غالبًا ما تمتد عبر دول متعددة. بالإضافة إلى ذلك، فإن بناء القدرات السيبرانية المشتركة من خلال التدريب وتطوير المهارات الفنية للجهات الأمنية والقضائية سيسهم في تحسين آليات التصدي للجرائم الإلكترونية وتعزيز الأمن الرقمي في كلا البلدين.

رغم الفوائد الكبيرة لهذا التعاون، إلا أن هناك تحديات تواجهه، مثل اختلاف التشريعات، القيود على تبادل المعلومات الحساسة، والتفاوت في مستوى البنية التحتية الرقمية. لذلك، من الضروري وضع استراتيجيات واضحة تتضمن إنشاء منصات تنسيق مشتركة، توقيع اتفاقيات تعاون ثنائية، وتعزيز الاستثمارات في تقنيات الذكاء الاصطناعي والتحليل الأمني المتقدم لمكافحة التهديدات السيبرانية بشكل أكثر كفاءة.

في النهاية، يمثل التعاون بين المملكة العربية السعودية والأردن في مجال الأمن السيبراني خطوة استراتيجية لتعزيز الحماية الرقمية وتحقيق بيئة إلكترونية أكثر أمانًا. ومن خلال تطوير السياسات المشتركة، تعزيز البحث والتطوير، والانضمام إلى الاتفاقيات الدولية المتخصصة في مكافحة الجرائم السيبرانية، يمكن للبلدين بناء منظومة سيبرانية قوية قادرة على مواجهة التحديات المستقبلية وضمان استقرار وأمن الفضاء الرقمي في المنطقة.

النتائج:

1. **التحول الرقمي وتوسيع نطاق الحماية** : يتطلب التحول الرقمي من الشركات تحديث

استراتيجيات الحماية لتشمل الحماية أثناء انتقال البيانات عبر الشبكات المتنوعة وأثناء اتصال الأجهزة الطرفية بالشبكة. تحتاج الشركات إلى استخدام تقنيات متطورة لضمان حماية البيانات في هذه البيئة المتغيرة.

2. **الذكاء الاصطناعي في مواجهة التهديدات السيبرانية** : يُعد الذكاء الاصطناعي أداة فعالة للكشف

عن التهديدات السيبرانية وتحليل البيانات بسرعة أكبر من الطرق التقليدية، مما يتيح التحكم بشكل أفضل في التهديدات المستقبلية من خلال التنبؤ بها والتفاعل معها بفاعلية.

3. **التحديات المرتبطة بتقدم الذكاء الاصطناعي** : مع تطور الذكاء الاصطناعي، يمكن للمهاجمين

استخدام هذه التكنولوجيا لزيادة تعقيد الهجمات السيبرانية، مما يجعل من الضروري تحديث استراتيجيات الدفاع لتتناسب مع التهديدات المعقدة والمتطورة.

4. **دور الذكاء الاصطناعي في تعزيز الأمن السيبراني خلال التحول الرقمي** : يلعب الذكاء

الاصطناعي دورًا حيويًا في تعزيز الأمن السيبراني من خلال مراقبة الأنماط المشبوهة في البيانات، مما يسمح بالتنبؤ بالتهديدات المستقبلية والاستجابة لها بشكل أسرع وأكثر كفاءة.

5. **الهجمات الإلكترونية المتطورة**: مع تطور التكنولوجيا، أصبحت الهجمات الإلكترونية أكثر

تعقيدًا باستخدام تقنيات مثل الذكاء الاصطناعي والتعلم الآلي، مما يزيد من صعوبة اكتشافها والتصدي لها في الوقت المناسب.

6. **نقص الوعي والتدريب**: يُعد نقص الوعي والتدريب في مجال الأمن السيبراني من التحديات

الكبيرة، حيث أن العديد من الأفراد والمؤسسات لا يملكون المعرفة الكافية لحماية بياناتهم من التهديدات الرقمية، مما يعرضهم لمخاطر كبيرة.

7. **التهديدات الداخلية**: تشمل التهديدات السيبرانية الداخلية من موظفين أو متعاونين لديهم

صلاحيات للوصول إلى المعلومات الحساسة، مما يجعلهم قادرين على استغلال هذه الصلاحيات لأغراض ضارة أو خبيثة.

8. **نقص التشريعات الموحدة**: تفتقر العديد من الدول إلى تشريعات موحدة تنظم معايير الأمن

السيبراني، مما يصعب تطبيق قوانين فعالة لمكافحة الجرائم السيبرانية ويعطل الجهود الدولية في مكافحة هذه التهديدات.

التوصيات لتعزيز الأمن السيبراني

1. تعزيز الوعي السيبراني: من الضروري زيادة الوعي لدى الأفراد والشركات حول أهمية الأمن السيبراني وكيفية حماية البيانات الشخصية والنظام المعلوماتي، من خلال حملات توعية تدريبية وبرامج توجيهية تساهم في مكافحة الجريمة الرقمية والحد من الثغرات الأمنية.
2. استثمار في الذكاء الاصطناعي: يجب استثمار التكنولوجيا المتقدمة مثل الذكاء الاصطناعي لتحليل البيانات والتنبؤ بالتهديدات المستقبلية، مما يساعد في الكشف المبكر عن الهجمات والتفاعل معها بسرعة، بما يساهم في تعزيز الدفاعات الإلكترونية.
3. تطوير استراتيجيات دفاعية متقدمة: من الضروري تطوير استراتيجيات دفاعية لحماية الأنظمة من الهجمات السيبرانية المعقدة والمتطورة، باستخدام تقنيات جديدة مثل التعلم الآلي والتقنيات التنبؤية التي تعزز قدرة الأنظمة على التكيف مع الهجمات الجديدة.
4. التعاون الدولي: تعزيز التعاون بين الدول في مكافحة الجرائم السيبرانية من خلال تبادل المعلومات المتعلقة بالتهديدات والجرائم الإلكترونية، لضمان استجابة منسقة وأكثر فاعلية على مستوى عالمي لمواجهة التهديدات العابرة للحدود.
5. تحديث التشريعات الوطنية: يجب تحديث القوانين الوطنية بانتظام لتواكب التطورات السريعة في التكنولوجيا، وضمان فعالية محاكمة الجرائم السيبرانية عبر تطوير أنظمة قانونية مرنة قادرة على مواكبة الابتكارات التقنية ومواجهة التهديدات المتجددة.

6. **التدريب المستمر للمختصين:** من الضروري توجيه المزيد من الاستثمارات في تدريب فرق

الأمن السيبراني لضمان جاهزيتهم في مواجهة التهديدات المتزايدة، بما يشمل التدريب على تقنيات حديثة وتطوير مهارات متقدمة في مجال الحماية من الهجمات.

7. **توسيع الحماية للبنية التحتية الحيوية:** يجب تطوير تقنيات إضافية لحماية البنية التحتية الحيوية

مثل قطاع الطاقة، والاتصالات، وغيرها من القطاعات الحيوية، من خلال أنظمة دفاع سيبراني متقدمة تضمن حماية الخدمات الأساسية من أي هجمات سيبرانية.

8. **تعزيز التعاون بين القطاعين العام والخاص:** يجب خلق شراكات استراتيجية بين الحكومة

والشركات الخاصة لتعزيز قدرات الدفاع السيبراني والتصدي للهجمات، مما يساهم في تعزيز الأمن الوطني وضمان استقرار الاقتصاد الرقمي في مختلف القطاعات.

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

أسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

أسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>

المراجع:

أولاً: الكتب المتخصصة:

- العتيبي، زياد. (2021). جرائم السيبرانية المرتكبة عبر الوسائط الرقمية. المجلة الأكاديمية العالمية للدراسات القانونية.
- الهيئة الوطنية للأمن السيبراني. (2025). الاستراتيجية الوطنية للأمن السيبراني
- يونس، ي. ر. (2024). التحديات القانونية للجرائم السيبرانية في القانون الدولي. موسوعة ودق القانونية.
- البوابة الوطنية السعودية. (2025). الأمن السيبراني في المملكة العربية السعودية
- اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (2023). الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسته. الأمم المتحدة
- المدونة العربية. (2024). إنجازات السعودية في مجال الأمن السيبراني .
- حازر الله، محمد. (2020). جرائم الأنترنت وتحديات الأمن السيبراني: دراسة في متغيرات الجريمة ومقارباتها العلاجية. مجلة المفكر.

- الربيعي، نورهان محمد. (2024). الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة). مجلة الفارابي للعلوم الإنسانية، 3(1)
- البهي، رغبة. (2021). الأمن السيبراني في 2020: بين الفرص والتحديات والحماية. المركز المصري للفكر والدراسات الاستراتيجية
- المطيري، سعد. (2023). مفهوم الجرائم الإلكترونية وسماتها. المجلة القانونية 16(5).
- بريدة، عبد الرزاق. (2024). الأمن السيبراني ودوره في الحد من الهجمات الإلكترونية. في الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، المركز المغربي-شرق أدنى للدراسات الإستراتيجية.
- مسلم، نبراس، (2021). الجرائم السيبرانية وأثرها على الأمن السيبراني، كلية القانون، جامعة بغداد.
- محيدين، علي، وحامي، عادل. (2022). الآليات القانونية لحماية الأمن السيبراني. في مؤتمر الآليات القانونية لحماية الأمن السيبراني. جامعة غرداية، الجزائر.

- Garrison, S. (2020, July 16). Challenges and solutions in cybersecurity. Stellar Cyber.
- Almann, A. (2023). Cybercrime. In Legal Translation between English and Arabic (pp. 197–212). Springer Nature.
- Gotelaere, S., & Paoli, L. (2022). Prevention and control of financial fraud: A scoping review. European Journal on Criminal Policy and Research. Springer Nature.
- teodor, F. (2018). Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU. Routledge.

- Kramer, F. D., & Starr, S. H. (2016). Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization. .National Defense University Press
- Andreasson, K. J. (2012). Cybersecurity: Public sector threats and responses. .CRC Press
- Cornish, P. (2017). Cybersecurity: Geopolitics, law, and policy. .Oxford University Press

ثالثا القوانين:

- الوصيف، آية، (2018). نص قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015. تشريعات أردنية – قانون الجرائم الإلكترونية.
- عالم القانون، (2024). الأمن السيبراني: تحديات معاصرة وتشريعات متجددة.
- المركز الوطني للأمن السيبراني. (2019). قانون الأمن السيبراني رقم 16 لعام 2019. تم استرجاعه في 5 فبراير 2025، من <https://ncsc.jo>

- هيئة الخبراء بمجلس الوزراء. (2007). نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم م/17. تم استرجاعه في 5 فبراير 2025، من <https://laws.boe.gov.sa>
- المركز الوطني للأمن السيبراني. (2019). قانون الأمن السيبراني رقم 16 لعام 2019.
- هيئة تنظيم قطاع الاتصالات. (2015). قانون الجرائم الإلكترونية رقم 27 لعام 2015.
- هيئة تنظيم قطاع الاتصالات. (2018). قانون حماية البيانات الشخصية رقم 13 لعام 2018.
- قانون العقوبات الأردني، المادة 16.
- حماة الحق. (2020). العقوبات البديلة في التشريع الأردني.
- الهيئة السعودية لحقوق الإنسان (2021).
- العمارة، م.، وعبد الرزاق م. (2024). الأصول القانونية لإجراءات الضابطة العدلية لجرائم الأمن السيبراني في الأردن. مجلة طبنة للدراسات العلمية الأكاديمية، 7(1)، 1337-1353.

- وزارة الداخلية. (2006). قانون مكافحة الإرهاب رقم 55 لعام 2006.
- هيئة الخبراء بمجلس الوزراء. (2007). نظام مكافحة جرائم المعلوماتية بالمرسوم الملكي رقم م/17.
- هيئة الخبراء بمجلس الوزراء. (2003). نظام مكافحة غسل الأموال بالمرسوم الملكي رقم م/39.
- هيئة الخبراء بمجلس الوزراء. (2018). نظام مكافحة الإرهاب وتمويله بالمرسوم الملكي رقم م/21.
- هيئة الخبراء بمجلس الوزراء. (2022). نظام حماية البيانات الشخصية بالمرسوم الملكي رقم م/19.

ثالثاً: رسائل الدكتوراه والماجستير

- محمد، م. (2020). القانون الدولي والتحديات المعاصرة: الجريمة السيبرانية نموذجاً. مجلة كلية الحقوق للبحوث القانونية والاقتصادية، 2(1)، 809-850.
- لحربي، ع. م. (2020). التحديات القانونية للأمن السيبراني في المملكة العربية السعودية. مجلة الدراسات القانونية المعاصرة، 6(1)، 55-70.

- القصير، ي. ع. (2017). الجرائم الإلكترونية في السعودية: التحديات والحلول القانونية. مجلة القانون والمجتمع، 22(3)، 100-115.
- مرزوق، بن مهدي.. (2021). الذكاء الاصطناعي كتوجه حتمي في حماية الأمن السيبراني (واقع اليوم ورهان المستقبل). مجلة السلام للعلوم الإنسانية والاجتماعية، 12(3)
- مجبل، هالة. (2021). الذكاء الاصطناعي ودوره في إدارة مخاطر الأمن السيبراني. مجلة كربلاء للعلوم الإنسانية 8(2)
- طارق، سارة. (2020). كيف يؤثر الذكاء الاصطناعي في الأمن السيبراني؟ مجلة عالم التكنولوجيا، 5(4)
- طالة، لامية. (2020). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. معالم للدراسات القانونية والسياسية، 4(2)
- القاضي، مروء، وسلطان، سوزان. (2024). واقع الأمن السيبراني للحوسبة السحابية لدى جامعة طيبة: دراسة حالة. المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، 4(2)

- العمارات، فارس. (2023). إشكالية الاستقرار والأمن الوطني في ظل الجريمة السيبرانية. آفاق سياسية، 104.
- عبد الجواد، نجوان. (2023). الجريمة السيبرانية وتأثيرها على الأمن القومي المصري: دراسة سوسيو تحليلية. مجلة كلية الآداب جامعة الفيوم، 15(1).
- دحماني، محمد. (2023). الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني. مجلة الفكر القانوني والسياسي، 7(2)،
- الأنصاري، خ. س. (2022). الأمن السيبراني في المملكة العربية السعودية: الإطار القانوني والتحديات المستقبلية. مجلة الدراسات الإستراتيجية، 14(2)، 65-80.
- المالكي، ر. ع. (2019). مكافحة الجرائم السيبرانية في السعودية: دراسة مقارنة. مجلة القانون الدولي، 9(1)، 40-55.
- رفاعي، محمد، (2023). التحديات القانونية والإدارية لخصخصة المرافق العامة: دراسة مقارنة. مجلة البحوث القانونية والاقتصادية (المنصورة)، المجلد 13(84).
- الصبحي، شهد، والربابغ، ريم، (2022). مدى وعي طلبة الدراسات العليا بنظام مكافحة الجرائم المعلوماتية في ظل التحول الرقمي ضمن رؤية المملكة 2030: دراسة

مسحية لدى طلبة كلية الآداب والعلوم الإنسانية بجامعة الملك عبد العزيز بجدة، العدد (40).

- مصطفى، إسلام، (2022). جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري. المجلة القانونية، المجلد 12(3).
- الحصري، طارق، (2019). الجهاز الإداري للدولة في مصر: المفهوم، التحديات، ورؤية التطوير، الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري.
- فياله، محمد. (2024). القانون الدولي والتحديات المعاصرة الجريمة السيبرانية نموذجاً. مجلة الحقوق للبحوث القانونية والاقتصادية، 2(1).
- الزهراني، ع. س. (2022). التحديات القانونية لمكافحة الجرائم الإلكترونية في المملكة العربية السعودية. مجلة الدراسات القانونية، 34(2)، 215-240.
- بني سلامة، م. ع. (2019). الجريمة السيبرانية في النظام القانوني الأردني. مجلة جامعة الزرقاء للبحوث والدراسات الإنسانية، 24(1)، 85-102.
- بطيخ، حاتم. (2021). تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات: دراسة تحليلية مقارنة. مجلة الدراسات القانونية والاقتصادية، 7

- أبو حجر، حازم. (2023) تطور الرقابة على دستورية القوانين في الأردن: دراسة

مقارنة. مجلة كلية الشريعة والقانون بتفهما الأشراف، (1)26

رابعاً: المواقع الإلكترونية

- المركز الوطني للتنافسية. (2024). الاستراتيجية الوطنية للأمن السيبراني.
- عبد المجيد، داليا. (2024). خمس توجهات للأمن السيبراني عام 2025: استشراف مستقبل الدفاع الرقمي. كوكب العلم.

https://www.bibalex.org/SCIplanet/ar/Article/Details?id=18061&utm_s

[source=chatgpt.com](https://www.bibalex.org/SCIplanet/ar/Article/Details?id=18061&utm_source=chatgpt.com)

- الهنادة، أحمد. (2022). القيادة العامة للقوات المسلحة الأردنية الجيش -العربي ."
- عالم القانون. (2024، 19 نوفمبر). تعزيز الأمن السيبراني: تحديات الحاضر وحلول المستقبل. عالم القانون

<https://alamalkanoun.com/featured-cybersecurity-challenges>

- بوزرار، عائشة. (2024). تأثير ثورة تكنولوجيا الإنترنت على الأمن القومي والدفاع السيبراني. أنفاس رقمية. استرجاع من <https://www.anfasse.org>

- العكايلك، ح. (2018). الضوابط القانونية للأمن السيبراني في الأردن. صحيفة الغد.

- سوداح، ف. (2017). الأمن السيبراني في الأردن: تحديات الحاضر، وإستراتيجيات للمستقبل.
- الجمال، قصي حمدان". (2025). الأردن الأول عربياً في الأمن السيبراني: قيادة رقمية تعزز الثقة والاستثمار. "جريدة الرأي.
- سوداح، فادي". (2024). الأمن السيبراني في الأردن: تحديات الحاضر، دروس مستفادة، وإستراتيجيات للمستقبل. "جريدة الغد

العنوان:	التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي
المؤلف الرئيسي:	العنزي، مشعل خضر روجان
مؤلفين آخرين:	الفايز، أكرم طراد مسلط(مشرف)
محكمة:	نعم
التاريخ الميلادي:	2025
موقع:	عمان
الصفحات:	1 - 118
رقم MD:	1588637
نوع المحتوى:	رسائل جامعية
اللغة:	Arabic
الدرجة العلمية:	رسالة ماجستير
الجامعة:	جامعة الاسراء الخاصة
الكلية:	كلية الحقوق
الدولة:	الاردن
قواعد المعلومات:	Dissertations
مواضيع:	الجرائم الإلكترونية، الأمن السيبراني، البيانات الشخصية، التشريعات الأردنية
رابط:	http://search.mandumah.com/Record/1588637

للاستشهاد بهذا البحث قم بنسخ البيانات التالية حسب أسلوب الاستشهاد المطلوب:

إسلوب APA

العنزي، مشعل خضر روجان، و الفايز، أكرم طراد مسلط. (2025). التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي (رسالة ماجستير غير منشورة). جامعة الاسراء الخاصة، عمان. مسترجع من <http://1588637/Record/com.mandumah.search/>

إسلوب MLA

العنزي، مشعل خضر روجان، و أكرم طراد مسلط الفايز. "التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة: دراسة مقارنة بين القانون الأردني والسعودي" رسالة ماجستير. جامعة الاسراء الخاصة، عمان، 2025. مسترجع من <http://1588637/Record/com.mandumah.search/>



التحديات القانونية لمكافحة جرائم الأمن السيبراني في دوائر الدولة:

دراسة مقارنة بين القانون الأردني والسعودي

أعدت من قبل

مشعل خضر روجان الغنزي

أشرف عليها

الأستاذ الدكتور أكرم الفايز

قدمت هذه الرسالة إلى كلية الحقوق كجزء من متطلبات الحصول على درجة الماجستير

في القانون

حزيران 2025