

خطة بحث

الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني
بالمملكة العربية السعودية

Civil Obligations and Responsibilities of Cybersecurity Practitioners in the Kingdom of
Saudi Arabia

إعداد

منار فهد خلف التميمي

الرقم الجامعي: 243000751

أشرف

د. نور القلالي

الفصل الدراسي الثاني

2025م/1446هـ

المقدمة

يعد الأمن والتشريع القانوني من أهم ركائز نهضة الدول، حيث تقع على عاتق الدولة مسؤولية سن القوانين التي تضمن الأمن بمختلف أشكاله، ويبرز الأمن السيبراني كواحد من أهم مجالات الحماية في العصر الحديث، نظرًا لارتباطه الوثيق بالتطور التكنولوجي، ومع التقدم المستمر في عالم الإنترنت والمعلومات، يصبح من الضروري وجود تشريعات قانونية متخصصة في الأمن السيبراني، تساهم في الحد من الجرائم الرقمية وتقليل المخاطر المترتبة عليها، مما يعزز الأمان الرقمي ويحمي الأفراد والمؤسسات من التهديدات السيبرانية المتزايدة.

وحرصت المملكة العربية السعودية على الريادة في مجال الأمن السيبراني، حيث عملت على تطوير سياسات وتشريعات متقدمة لتعزيز الحماية الرقمية، ومواجهة التحديات السيبرانية، ومن أهمها: "تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله- وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ 1439/2/11هـ، لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه؛ حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية" (الهيئة الوطنية للأمن السيبراني، 1439). وإصدار المرسوم الملكي رقم 57231 في 1439/11/10هـ، بإسراع الجهات الحكومية في تطبيق متطلبات الأمن السيبراني (المنصة الوطنية الموحدة، 1439). كما تفوقت المملكة العربية السعودية سيبرانيًا، حيث حققت المرتبة الثانية عالميًا، من بين (193) دولة، والأولى على مستوى الوطن العربي والشرق الأوسط وقارة آسيا (الهيئة الوطنية للأمن السيبراني، 1439).

ويشمل الأمن السيبراني المجتمع بأكمله، حيث يتحمل كل فرد أو مؤسسة مسؤولية المساهمة في تحقيقه، وذلك لحماية الخصوصية، وضمان أمن أصول المؤسسات ومواردها من الجوانب التقنية والمعلوماتية والتنظيمية والبشرية والمالية (حبیباتنی، 2020، 606). ونظرًا للتحديات التي تواجه السيطرة القانونية على الجرائم السيبرانية في الوقت الحالي، تفرض بعض الهيئات القانونية في المملكة العربية السعودية، إلى جانب الاتفاقيات الدولية، التزامات قانونية على المنظمات لاتخاذ التدابير الأمنية اللازمة، ويأتي ذلك استجابة لاستغلال المجرمين للثغرات التشريعية في بعض الدول التي لم تضع قوانين واضحة تجرم الجرائم المعلوماتية، إضافة إلى وجود ثغرات رقمية آمنة تتيح ارتكاب الجرائم السيبرانية والتهرب من العقوبات القانونية (حسين، 2020، 20).

وترى الباحثة أن الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني في المملكة العربية السعودية لها دور في حماية الفضاء الرقمي من التهديدات المتزايدة، من خلال فرض التشريعات والقوانين على المتخصصين في هذا المجال لاتخاذ تدابير أمنية مشددة لضمان سرية المعلومات وسلامة البنية التحتية الرقمية، وهذه الالتزامات تساعد في تعزيز الأمن السيبراني والثقة في المعاملات الإلكترونية.

وفي ظل عدم وجود حماية قانونية واضحة وصريحة يمكن الاعتماد على القواعد العامة للمسؤولية المدنية، باعتبارها المظلة العامة التي تستظل بها كافة الحقوق المدنية، وذلك من خلال توضيح الأركان الواجب توافرها لقيام المسؤولية التقصيرية أو العقدية، والتي تشمل الخطأ والضرر وعلاقة السببية بينهما، وبذلك يمكن مساءلة القائمين على أعمال الأمن السيبراني عند الإخلال بواجباتهم أو التسبب في أضرار ناتجة عن إهمالهم أو تقصيرهم في تنفيذ التدابير الأمنية المطلوبة (قعدان، 2020، 40).

وبناءً على ما سبق تستعرض هذه الدراسة الأطر القانونية للمسؤولية المدنية التي يتحملها العاملون في مجال الأمن السيبراني عند عدم الوفاء بالتزاماتهم أو التقصير بمسئولياتهم.

مشكلة الدراسة:

المسؤولية المدنية في الأمن السيبراني قد تكون عقدية أو تقصيرية، وأنها جميعاً ترتبط بالجانب الإلكتروني والتكنولوجي، مما يجعل طبيعة الجرائم المعلوماتية الخاصة بالأمن السيبراني مختلفة، من حيث صعوبة تحديد المرتكب القائم بها، وعدم وضوح المصطلحات الخاصة بأمن المعلومات أو مرونتها، وصعوبة اكتشافها لعدم تركها أثراً ملموساً، وصعوبة إثباتها حيث إنها تقع في واقع غير ملموس، إضافة إلى أن الجرائم السيبرانية عابرة للحدود، لذلك فهي تحتاج إلى قوانين صارمة للتعامل معها، وتفعيل التعاون الدولي لمكافحتها.

وجاء الإحساس بمشكلة الدراسة الحالية بمجموعة من الشواهد، يمكن إيجازها على النحو التالي:

اهتمام المملكة العربية السعودية بالأمن السيبراني وإقامتها لمجموعة من المؤتمرات التي تعكس التزام المملكة بتطبيق الأمن السيبراني ومواكبة التطورات التقنية الحديثة، والتي من أهمها "المنتدى الدولي للأمن السيبراني، أكتوبر 2024" ويعقد هذا المنتدى بشكل دوري في الرياض، ويجمع صناع القرار وممثلي الحكومات والشركات، والقائمين على تقديم خدمات الأمن السيبراني، كذلك "مؤتمر الشرق الأوسط وشمال أفريقيا لأمن المعلومات (MENA ISC)، 2024"، يركز هذا المؤتمر على التحديات والتهديدات السيبرانية في المنطقة، ويعقد سنوياً في الرياض، و"مؤتمر

@Hack:2021" أطلق هذا المؤتمر لأول مرة في الرياض عام 2021، ويعد من أكبر الفعاليات في مجال الأمن السيبراني في المنطقة، حيث يجمع خبراء ومختصين من جميع أنحاء العالم لمناقشة أحدث التطورات والتحديات. وجميع هذه المؤتمرات أوصت بضرورة الاهتمام بالقوانين والتشريعات الخاصة بالأمن السيبراني، وإعداد الدراسات والأبحاث التي تدعم المجال القانوني للأمن السيبراني.

كذلك نتائج الدراسات السابقة التي أكدت ضعف التشريعات الخاصة بالأمن السيبراني كدراسة حسين (2021) التي أشارت إلى أن هناك حاجة إلى تنظيم تشريعي متكامل يحدد المركز القانوني لمقدمي خدمات الأمن السيبراني، ويبين مسؤولية والتزام كل منهم عما يرتكب من مخالفات عبر الشبكة، ويحدد ضوابط قانونية تضبط حقوق أطراف النشاط الإلكتروني والتزاماته.

وايضاً الأطر التشريعية التي قررتها المملكة العربية السعودية، حيث نظمت هيئة الاتصالات وتقنية المعلومات بالمملكة العربية السعودية إطار تنظيمي شامل للأمن السيبراني بغرض زيادة مستوى نضجه في قطاع الاتصالات وتقنية المعلومات والبريد، ويهتم بشكل أساسي بالجهات المرخصة أو المسجلة في الهيئة وتلك الخاضعة لها بصفقتها الجهة المنظمة لقطاع الاتصالات وتقنية المعلومات (القائمين على الخدمة) في المملكة العربية السعودية (هيئة الاتصالات وتقنية المعلومات، 2020).

وبالاستناد إلى ما سبق، ونظراً لغياب تشريع واضح يحدد نطاق المسؤوليات والالتزامات القانونية، وأن هذا الامر يؤثر على كفاءة الحماية السيبرانية، ومع تزايد الاعتماد على الخدمات الرقمية والتقنيات الحديثة، مما يستدعي تحقيق التوازن بين حماية الحقوق الرقمية ومساءلة المخالفين والمقصرين، إضافة إلى الجهود التنظيمية التي تبذلها المملكة العربية السعودية لتوفير منظومة تشريعية متكاملة لمواكبة التحديات الرقمية وتعزيز الحماية القانونية، يجعل موضوع الدراسة الحالية ذا أولوية بحثية، لتناوله الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني ويمكن تحديد مشكلة الدراسة الحالية في السؤال الرئيسي التالي: ما الالتزامات والمسؤوليات المدنية للقائمين على

أعمال الأمن السيبراني بالمملكة العربية السعودية؟

أسئلة الدراسة.

ويتفرع من السؤال الرئيس مجموعة من الأسئلة الفرعية التي تشمل ما يلي:

1. ما المقصود بالمسؤولية المدنية والأمن السيبراني؟

2. ما الالتزامات المدنية للقائمين على أعمال الخدمات المعلوماتية بالأمن السيبراني؟
3. ما الالتزامات المدنية للقائمين على أعمال الخدمات الفنية بالأمن السيبراني؟
4. ما شروط تحقق مسؤولية القائمين على أعمال خدمات الأمن السيبراني؟
5. ما الحماية النظامية للأمن السيبراني وفقاً للنظام السعودي؟

أهداف الدراسة.

1. التعرف على المقصود بالمسؤولية المدنية والأمن السيبراني.
2. توضيح الالتزامات المدنية للقائمين على أعمال الخدمات المعلوماتية بالأمن السيبراني.
3. بيان الالتزامات المدنية للقائمين على أعمال الخدمات الفنية بالأمن السيبراني.
4. تحديد شروط تحقق مسؤولية القائمين على أعمال خدمات الأمن السيبراني.
5. توضيح الحماية النظامية للأمن السيبراني وفقاً للنظام السعودي.

أهمية الدراسة:

أولاً: الأهمية العلمية (النظرية):

- مواكبة موضوع الدراسة لتوجهات المؤتمرات ورؤية المملكة العربية السعودية "2030"، حيث ركزت رؤية المملكة على الاهتمام بالتحول الرقمي، وتعزيز الأمن السيبراني.
- تعد الدراسة الحالية إضافة جديدة لأدبيات المكتبة السعودية في البحوث القانونية التي تناولت الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني.

ثانياً: الأهمية العملية (التطبيقية):

- تتبع الأهمية العملية للدراسة وتوضيح الأنظمة والتشريعات القانونية للأمن السيبراني السعودي الخاصة بالالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني.
- يؤمل استفادة المشرعين وأصحاب القرار في مجال الأمن السيبراني من نتائج الدراسة وتوصياتها.
- تفيد الدراسة الحالية الباحثين والمختصين في المجال القانوني، بتقديم مجموعة من المقترحات البحثية الجديدة التي يمكن دراستها مستقبلاً.

منهج الدراسة:

سوف تعتمد الدراسة المنهج الوصفي والتحليلي. ويعرف بأنه: "أسلوب من أساليب التحليل التي تركز على معلومات كافية ودقيقة عن ظاهرة أو موضوع محدد، أو فترة زمنية معلومة، من أجل الحصول على نتائج علمية، ثم تفسيرها بطريقة موضوعية"

مصطلحات الدراسة:

1. المسؤولية المدنية:

- يعرفها دبش (2019، 21) اصطلاحاً بأنها: "مؤاخذة المرء باعتباره مسؤولاً عما ارتكبه من أفعال، وتتراوح هذه المؤاخذة بين استهجان المجتمع لتصرفه، وبين الجزاء الذي يقرره القانون".
- تعرفها الباحثة إجرائياً: "الالتزامات القانونية التي تقع على القائمين على أعمال الأمن السيبراني في المملكة العربية السعودية، والتي تترتب عند الإخلال بواجباتهم أو التقصير في اتخاذ التدابير الأمنية اللازمة لحماية البيانات والمعلومات الرقمية، وتتحدد هذه المسؤولية وفق لأحكام القانون سواء كانت عقدية أو تقصيرية.

2. الأمن السيبراني:

- عرفه جبور (2018، 241) اصطلاحاً بأنه: "أمن الشبكات والأنظمة المعلوماتية، والبيانات المعلومات، والأجهزة المتصلة بالإنترنت، ويتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو الحد من آثارها في أقصى الأحوال وأسوأها".
- تعرفه الباحثة إجرائياً: مجموعة السياسات والإجراءات والتدابير التقنية والتنظيمية التي يتبناها القائمون على أعمال الأمن السيبراني في المملكة العربية السعودية لحماية الأنظمة الرقمية والشبكات والبيانات من التهديدات السيبرانية.

حدود الدراسة:

- الحدود الموضوعية: سوف تتناول الدراسة الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني بالمملكة العربية السعودية.

- الحدود المكانية: محددة بتشريعات المملكة العربية السعودية.

الخطـة البحثية:

المبحث الأول: الالتزامات والمسؤوليات المدنية للقائمين على أعمال الأمن السيبراني.

المطلب الأول: ماهية المسؤولية المدنية والأمن السيبراني.

الفرع الأول: مفهوم المسؤولية المدنية.

الفرع الثاني: مفهوم الأمن السيبراني.

المطلب الثاني: الالتزامات المدنية للقائمين على أعمال الأمن السيبراني.

الفرع الأول: الالتزامات المدنية لمقدمي الخدمات المعلوماتية.

الفرع الثاني: الالتزامات المدنية لمقدمي الخدمات الفنية.

المبحث الثاني: المسؤوليات المدنية للقائمين على أعمال الأمن السيبراني.

المطلب الأول: شروط المسؤولية المدنية لخدمات الأمن السيبراني.

الفرع الأول: الشروط الإجرائية للمسؤولية المدنية لخدمات الأمن السيبراني.

الفرع الثاني: الشروط الموضوعية للمسؤولية المدنية لخدمات الأمن السيبراني.

المطلب الثاني: الحماية النظامية للأمن السيبراني وفقاً للنظام السعودي

الفرع الأول: أركان قيام المسؤولية المدنية للأمن السيبراني.

الفرع الثاني: الحماية المدنية لجرائم انتهاك الأمن السيبراني.

الخاتمة

النتائج

التوصيات

قائمة المراجع

قائمة المصادر والمراجع

- جبور، منى الأشقر. (2018). *السيبرانية*. هاجس العصر. جامعة الدول العربية، 241.
- حبيباتي، بثينة. (2020). *الطبيعة الخاصة للجريمة المعلوماتية*. مجلة دراسات وأبحاث: جامعة الجلفة، 3(12)، 606.
- حسين. حنين جميل. (2021). *الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)*. رسالة ماجستير، قسم القانون الخاص. كلية الحقوق جامعة الشرق الأوسط.
- حسين، حنين جميل. (2021). *الإطار القانوني لخدمات الأمن السيبراني دراسة مقارنة*، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الأوسط، سوريا.
- دبش، عمرو أحمد. (2019). *أركان المسؤولية المدنية*. مجلة العلوم القانونية والاجتماعية: جامعة زيان عاشور الجلفة، 2(4)، 21.
- دويدري، رجاء وحيد. (2000). *البحث العلمي أساسياته النظرية وممارسته العملية*. دمشق: دار الفكر المعاصر، ص: 183
- قعدان، سرين مروان محمد صالح. (2020). *الحماية المدنية للمعلومات الإلكترونية: دراسة مقارنة*، رسالة ماجستير، جامعة النجاح الوطنية، كلية الدراسات العليا.
- منتدى الدولي للأمن السيبراني. (أكتوبر 2024). *اللقاء السنوي للمنتدى الدولي للأمن السيبراني* [/https://gcforum.org/ar](https://gcforum.org/ar)
- المنصة الوطنية الموحدة. (1439). <https://www.my.gov.sa/wps/portal/snp/main>
- مؤتمر "Hack@". (2021). [/https://www.gea.gov.sa/hack-blvd](https://www.gea.gov.sa/hack-blvd)
- مؤتمر الشرق الأوسط وشمال أفريقيا لأمن المعلومات (MENA ISC)، 2024، [/https://www.menaisc.com](https://www.menaisc.com)
- هيئة الاتصالات وتقنية المعلومات. (2020). *الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات والبريد*. www.citc.gov.sa
- الهيئة الوطنية للأمن السيبراني. (1439هـ). <https://nca.gov.sa/pages/about.html>