مجلة دراسات إنسانية واجتماعية / جامعة وهران02/ المجلد 14 ع 02.
ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري: دراسة مقارنة

The Legal Framework of Cybersecurity in Maintaining Public Health in Qatari Law: A Comparative Study

محمد حسن المهندي Mohammed Hassan Al-Mahendi
ماجستير دراسات أمنية قوة الأمن الداخلي/ قطر
ahmad_zarer7@yahoo.com

DOI : 10.46315/1714-014-002-015
الإرسال: 2025/01/31 **القبول**: 2025/03/11 **النشر**: 16/ 06/ 2025

**

ملخص: ترمي هذه الدراسة إلى معرفة فاعلية الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري، وقد اعتمدت الدراسة على المنهج التحليلي، والمنهج القانوني، والمنهج الاستقرائي، وتوصلت الدراسة إلى عدة نتائج، أهمها: ترتبط قدرة الدولة في مواجهة الجرائم السيبرانية بوجود استراتيجيات ورؤية واضحة في هذا الصدد، ومراجعة مستمرة لما يواكب الفضاء السيبراني من تطور في الأساليب والأدوات المستخدمة، حيث أن تلك الجرائم في تطور مستمر بالتزامن مع التطور التكنولوجي الهائل الذي يشهده العالم، وأنَّ قطعت دولة قطر شوطًا مميزًا في مجال الحفاظ على الأمن السيبراني سواءٌ في تطوير التشريعات أو إعداد الاستراتيجيات والوكالات المتعلقة بالأمن السيبراني، إدراكًا منها لحجم تأثير الجرائم السيبرانية في منظومة الأمن الوطني، مما جعلها قادرة على مواجهة تحديات ومخاطر الجرائم السيبرانية.

وأوصت الدراسة بضرورة تدريب العاملين في القطاع الصحي على ممارسات الأمن السيبراني لحماية خصوصية الأفراد، وضرورة المراجعة المستمرة لاستخدامات المواقع الإلكترونية، ووضع القيود اللازمة في إطار ضبطها والحيلولة دون استخداماتها السلبية التي تؤثر في الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني، الجرائم السيبراني، الإرهاب السيبراني، الردع السيبراني، الصحة العامة.

Abstract: (English)

This study aims to identify the effectiveness of the legal framework for cybersecurity in maintaining public health in Qatari law. The study relied on the analytical approach, the legal approach, and the inductive approach. The study reached several results, the most important of which are: The state's ability to confront cybercrimes is linked to the existence of clear strategies and vision in this regard, and a continuous review of the developments in cyberspace in terms of methods and tools used, as these crimes are constantly evolving in conjunction with the tremendous technological development witnessed by the world, and that the State of Qatar has made significant progress in the field of maintaining cybersecurity, whether in developing legislation or preparing strategies and agencies related to cybersecurity, in recognition of the extent of the impact of cybercrimes on the national security system, which made it capable of facing the challenges and risks of cybercrimes.

The study recommended the necessity of training workers in the health sector on cybersecurity practices to protect the privacy of individuals, and the necessity of continuous review of the uses of websites, and setting the necessary restrictions within the framework of controlling them and preventing their negative uses that affect cybersecurity.

Keywords: Cybersecurity, Cybercrime, Cyberterrorism, Cyberdeterrence, Public Health.

**

***- مقدمة:**

بات الانتشار الواسع والتطور التقني والإنترنت في مختلف أنحاء العالم، والاستخدام المتزايد لتطبيقات الذكاء الاصطناعي من الأمور المهمة في الحياة وأداة مساعدة وفاعلة في تطوير وتنمية استراتيجيات الدول بشكل عام والأفراد على وجه الخصوص، وقد كانت الدول المتقدمة سباقة في الاستفادة منها ومواكبتها، وأصبح من الصعوبة الاستغناء عنها.

أدى استخدام التكنولوجيا الرقمية في مجال الرعاية الصحية إلى إحداث تحول كبير في النظم الصحية على مستوى العالم، مما أثمر فوائد ومنافع لا تعد ولا تحصى، من بينها على سبيل المثال زيادة في تبادل البيانات وتحليلها، واستحداث أساليب إدارة جديدة لرعاية المرضى، وتعزيز إمكانية وصول المرضى للخدمات، كما قللت من تكاليف الخدمات في أغلب الأحيان.

وقد بذلت دولة قطر جهودها في تحقيق الأمن السيبراني؛ حيث أصدر المشرع القطري قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة (2014م)، شأنهم في ذلك شأن باقي الدول في العالم التي تأثرت بموجة من التطور والتقدم التقني، إضافة إلى إصدار قانون حماية البيانات الشخصية رقم (13) لسنة (2016م)، وذلك لضمان خصوصية البيانات الشخصية، وفي إطار جهود دولة قطر لمواجهة هذه التحديات ومجابهة المخاطر والتهديدات الحالية والناشئة، أُنشِأَت الوكالة الوطنية للأمن السيبراني بموجب القرار الأميري رقم (1) لسنة (2021م)؛ حيث تتولى الوكالة مسؤولية تنفيذ الإجراءات التي تهدف إلى الحدّ من المخاطر السيبرانية الوطنية، والاشراف عليها، والجاهزية والاستعداد لمواجهة الأزمات والجرائم السيبرانية، وتوفير الحماية اللازمة للبنية التحتية الحيوية، وغيرها من المهام والواجبات التي تهدف في مجملها إلى تحقيق الأمن السيبراني.

وللمحافظة على الصحة أطلقت وزارة الصحة القطرية برنامج الصحة الإلكترونية الوطني الذي يهدف إلى تطوير نظام صحي إلكتروني آمن ومتكامل يشمل هذه البرنامج حماية البيانات الصحية، وضمان الامتثال للمعايير الوطنية وتحسين فعالية وجودة الخدمات الصحية.

بناءً على ما تقدم؛ تتناول هذه الدراسة بالتحليل والاستنتاج الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة، ودراسة فائدتها وأهميتها في وضع السياسات والاستراتيجيات للحدّ من المخاطر الصحية.

أسباب اختيار الموضوع:

إنَّ من أهم الأسباب التي دعت إلى دراسة هذا الموضوع في ظل ما شهدته دولة قطر من تحولاً رقميًا واسعًا في الرعاية الصحية مع الاعتماد على أنظمة حديثة لإدارة السجلات الصحية، وتشغيل الخدمات الصحية عبد بُعد، وتطبيق التكنولوجيا في المؤسسات الطبية ومراكز الرعاية الصحية؛ حيث أن هذه الأنظمة الحديثة قد تكون هدفًا للتهديدات السيبرانية.

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

كما أن بيانات المرضى من أكثر البيانات حساسية وأي اختراق للأنظمة الصحية الإلكترونية في دولة قطر قد يؤدي إلى مشكلات قانونية واخلاقية خطيرة، ففي هذا النوع من الدراسات المرتبطة بالأمن السيبراني يساعد في تعزيز حماية هذه البيانات بما يتماشى مع قانون حماية البيانات القطري رقم (13) لسنة (2016م).

مشكلة الدراسة:

إنَّ تصاعد الهجمات السيبرانية على المؤسسات الصحية عالميًا خصوصًا خلال جائحة كورونا، جعل دراسة الإطار القانوني للأمن السيبراني في دولة قطر أولوية لضمان استمرارية تدفق الخدمات الصحية دون انقطاع أو تهديد؛ حيث أنَّ برنامج قطر الوطني للصحة الإلكترونية والبيانات" ضمن الاستراتيجية الوطنية للصحة الإلكترونية وإدارة البيانات، ويأتي الهدف من الصحة الإلكترونية التحسين التحولي والمستمر للرعاية الصحية من خلال استخدام المعلومات والتقنيات التي تدعم تقديم الرعاية الصحية والبحوث السريرية، بالتنسيق والتعاون مع أصحاب المصلحة الرئيسيين في مجال الصحة، وهذه الاستراتيجية ستحقق رغبة الدولة في أن تصبح رائدة حول العالم في اعتماد واستخدام وتطوير حلول مبتكرة، لذا تطرح هذه الدراسة التساؤل الرئيس الآتي: ما فاعلية الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري؟

تساؤلات الدراسة:

تسعى هذه الدراسة الإجابة على التساؤلات التالية:

1. ما فاعلية الأمن السيبراني في تحقيق الأمن الصحي في دولة قطر؟
2. ما مدى فاعلية التشريعات القطرية في تحقيق الأمن السيبراني؟
3. كيف يمكن المحافظة على الصحة العامة في دولة قطر في ظل التشريعات القانونية والتنظيمية، ودورها في حماية البيانات الشخصية للأفراد في المؤسسات الصحية القطرية؟

أهداف الدراسة:

ترمي هذه الدراسة إلى معرفة فاعلية الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في التشريعات القطرية، وذلك من خلال تحقيق الأهداف الفرعية التالية:

1. بيان فاعلية الأمن السيبراني في تحقيق الأمن الصحي في دولة قطر.
2. التعرف على مدى فاعلية التشريعات القطرية في تحقيق الأمن السيبراني.

3. تسليط الضوء على الآليات التشريعية والتنظيمية في المحافظة على الصحة العامة ودورها في حماية البيانات الشخصية للأفراد في المؤسسات الصحية القطرية.
4. التوصل إلى النتائج والتوصيات المناسبة لموضوع هذه الدراسة.

أهمية الدراسة:

تكمن أهمية دراسة دور الأمن السيبراني في حماية الصحة العامة في دولة قطر من أهمية الموضوع الذي نتناوله في ظل ما يشكله قطاع الصحة في الدولة من أهمية خاصة في تعزيز الأمن السيبراني، وحماية البيانات الشخصية للطواقم الطبية والإدارية ومتلقي الخدمات الطبية في المؤسسات الصحية في دولة قطر.

الدراسات السابقة:

ركزت دراسة المطيري (2022) على دور التشريعات الجزائية في حماية الأمن السيبراني في دول الخليج العربية، وبينت بشكل متعمق التحديات التي تواجه الأمن السيبراني في دول الخليج نظرًا لأن طبيعة هذه الجرائم خاصة، والوقوف على مدى قدرة التشريعات في دولة قطر على مواجه التحديات، واوصت بأنه بضرورة أن تنص تشريعات دول الخليج على مفهوم موحد للأمن السيبراني ويكون متفق عليه ومقبول لدى دول الخليج العربية.

وفي سياق آخر بين الهزاني (2023) بشكل متعمق ضوابط الأمن السيبراني في حماية البيانات، والكشف عن متطلبات تطبيق الأمن السيبراني في السعودية؛ حيث أولت اهتمامًا كبيرًا في تعزيز حماية بنيتها التحتية والرقمية من مخاطر التهديدات السيبرانية؛ حيث أكدت رؤية المملكة (2030م) على ضرورة تنمية البنية التحتية والرقمية ضمن مستهدافاتها، وأوصت الدراسة بضرورة تأهيل الكوادر البشرية في مجال الأمن السيبراني وتعزيز العلاقات المهنية والمجتمعية لتحقيق الأمن السيبراني.

أما دراسة عبد الرحمن (2023)، فقد ركزت على واقع القوانين الدولية والخليجية المنظمة للأمن السيبراني، وبينت دراسته أنه لا يوجد تعريف دولي موحد لمفهوم الأمن السيبراني، وعدم وجود تعريفات مصطلحات محددة لكل من الجريمة السيبرانية والهجوم السيبراني والفرق بينهما، وأنَّ غياب قانون خليجي موحد للأمن السيبراني في دول مجلس التعاون يضعف من قدراتها على مواجهة الهجمات السيبرانية.

ما يميز هذه الدراسة عن الدراسة السابقة في تناولها موضوع حديث نسبيًا يتمثل في دور الأمن السيبراني في حماية الصحة في دولة قطر؛ حيث لم تتناول أي من الدراسات السابقة دور الأمن السيبراني في حماية الصحة العامة، وإنما جاءت عامة لحماية الخصوصية، كما أنَّ هذه الدراسة على حد علم الباحث تناولت موضوع الأمن السيبراني وحماية الصحة العامة.

منهجية الدراسة:

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

تقتضي طبيعة الدراسة استخدام عدد من المناهج البحثية في هذا المقام، بأسلوب منضبط يمر بمراحل عدة، تبدأ بتحديد المشكلة، ثم وضع المعطيات، يليها تجميع المعلومات، وتنتهي بالوصول إلى الاستنتاجات المترتبة في المعالجة البحثية، ومن أهم تلك المنهجيات التي تستند إليها هذه الدراسة، هي:

- المنهج التحليلي: وهو المنهج القائم على تفسير وتحليل لجزئيات البحث، وذلك من خلال تأصيل الفكرة وردها إلى أصلها.
- المنهج القانوني: الذي يقوم على مقارنة التشريعات وتحليلها، على أن يكون التشريع القطري الأساس.
- المنهج الاستقرائي: الذي يقوم على الاستقراء، من خلال ما ورد في المصادر الثانوية، والدراسات والأبحاث والكتب، والمراجع العربية والأجنبية حول الأمن السيبراني وأهميته.

تقسيم خطة الدراسة:

لتحقيق الهدف الرئيس من هذا البحث ولمعالجة الاشكالية المطروحة تم تقسيم الخطة إلى المباحث التالية:

المبحث الأول: التأصيل النظري للأمن السيبراني والتهديدات السيبرانية

المطلب الأول: مفهوم الأمن السيبراني وأهميته

المطلب الثاني: أهداف وأبعاد الأمن السيبراني

المبحث الثاني: النظم القانونية للأمن السيبراني والمحافظة على الصحة العامة

المطلب الأول: التنظيم القانوني للأمن السيبراني في حماية الصحة العامة

المطب الثاني: الأمن السيبراني في حماية الصحة في سلطنة عُمان ودولة الإمارات

الخاتمة: (النتائج والتوصيات).

المبحث الأول: التأصيل النظري للأمن السيبر اني والتهديدات السيبر انية

يُعَدُّ مصطلح السيبرانية من المصطلحات الحديثة؛ حيث ارتبط هذا المصطلح بالجرائم والتهديدات السيبرانية التي ظهرت نتيجة لظهور أنظمة المعلومات ذاتها، ويعتبر ذلك أمرًا طبيعيًا نتيجة لتطور شتى مجالات الحياة بشكل عام، ومع الاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات وشبكة الإنترنت في العصر الحديث من قبل الحكومات والشركات والمؤسسات والأفراد، ولا سيما القطاعات الحيوية مثل القطاع المالي وقطاعات الطاقة والأمن والجيش لتقديم خدمات فعالة وعالية الجودة والكفاءة، للبحث في التأصيل النظري للأمن السيبراني والتهديدات

السيبرانية، تم تقسيم هذا المبحث إلى ثلاثة مطالب، نتناول مفهوم الأمن السيبراني وأهميته في (المطلب الأول)، ومن ثم البحث في أهداف وأبعاد الأمن السيبراني وإدارته في (المطلب الثاني).

المطلب الأول: مفهوم الأمن السيبراني وأهميته

الأمن ضرورة أساسية وعنصر رئيس للأفراد والمجتمع ككل، ومن ضرورات بناء وتطور المجتمع وصمام أمان لبقائه، ومرتكز من مرتكزات البناء والازدهار الحضاري في الدول؛ حيث تعمل الدول بكل مؤسساتها كل في مجال اختصاصها بفرض النظام وتعزيز سيادة القانون بواسطة أجهزتها الإدارية والقضائية والأمنية، وللبحث في موضوع الأمن السيبراني وأهميته، تم تقسيم هذا المطلب إلى فرعين، نتناول في (الفرع الأول) مفهوم الأمن السيبراني، ومن ثم البحث في أهمية الأمن السيبراني في (الفرع الثاني).

الفرع الأول: مفهوم الأمن السيبراني

يُعَدُّ الأمن إحدى أهم مبادئ ومرتكزات الحياة البشرية، لقوله عز وجل: {لِإِيلَافِ قُرَيْشٍ{1} إِيلَافِهِمْ رِحْلَةَ الشِّتَاء وَالصَّيْفِ{2} فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ{3} الَّذِي أَطْعَمَهُم مِّن جُوعٍ وَآمَنَهُم مِّنْ خَوْفٍ{4} (سورة قريش)، ويعني مصطلح الأمن عدم الخوف والطمأنينة، وفي لسان العرب لأبن منظور: الأمان والأمانة، وقد أمنت فأنا آمن وأمنت غيري من الأمن والأمان (أبن منظور: 13-22)، وقد عُرّف الأمن اصطلاحًا بأنَّه الإجراءات الأمنية التي تتخذها الدولة لحفظ أسرارها وتأمين أفرادها ومؤسساتها ومصالحها الحيوية في الداخل والخارج، إضافةً إلى القدرة على مواجهة الأحداث الأمنية والطوارئ دون اضطراب (محمد، 2012: 41)، ومع تطور المجتمعات والحياة الإنسانية دخلت العديد من التطورات والمتغيرات على مفهوم الأمن، ولم يجمع الباحثون على إعطاء مفهوم واحد للأمن، بل كان هنالك اتجاهين رئيسين هما (Tasoulla & Jain, 2014: 12):

الاتجاه الأول: يعطي مفهومًا ضيقًا للأمن بحيث يقصره على كل ما يتعلق بالحفاظ على السيادة الوطنية وعلى الوضع القانوني الطبيعي القائم للدولة والمجتمع في حدود الإطار الإقليمي للدولة.

الاتجاه الثاني: هذا الاتجاه يعطي مفهومًا أوسع للأمن؛ حيث أدى تطور الفكر الإنساني إلى تطور مفهوم الأمن، وأنَّ هذا التطور قد وصل بفلسفة الأمن إلى درجة الإحاطة بكل جوانب الحياة الإنسانية، والدور المعاصر للمنظومة الأمنية مفاده تحقيق الأمن على المستوى الداخلي والخارجي، وهذا الاتجاه في تناوله للأمن الشامل يأخذ بتصورات وطرق عمل جديدة في تعامله مع قضايا الأمن.

كما حددت منظمة الأمم المتحدة أبعاد الأمن بِـ: (الأمن الاقتصادي، الأمن الغذائي، الأمن الصحي، الأمن البيئي، الأمن الشخصي، وأمن المجتمع)، ويضيف الباحث إلى تلك الأبعاد أيضًا الأمن الفكري، والأمن السيبراني (Cyber Security) والذي نحن في صدد دراسته الآن؛ حيث يعتبر هذا المصطلح من المصطلحات شائعة الاستخدام وجزء لا يتجزأ من أبعاد الأمن الشامل، وقد

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

تعددت التعريفات التي تناولت هذا المصطلح؛ حيث يستخدم مصطلح السيبرانية لوصف مفاهيم وأنواع مختلفة من الجرائم التي تتم من خلال الإنترنت وأجهزة الحاسوب، فهنالك من عرّفه بأنَّه مجموعة من الأساليب الدفاعية التي تستخدم للكشف عن المتسللين المحتملين وإحباط عملياتهم (Canongia & Mandarino, 2014: 68)، وعرّف أيضًا بأنه مجموعة المعارف والتكنولوجيا والمؤسسات والأنشطة التي تحمي وتحافظ الوجود البيولوجي للحياة البشرية، والسلام الجماعي والازدهار لتعزيز حرية الأنسان (James, 2014: 13)، ويشير Donalds & Kweku (2019) إلى أنَّ الأمن السيبراني يتضمن الحد من مخاطر الهجمات الضارة على البرامج وأجهزة الحاسوب والشبكات، وعرفه آخر بأنَّه مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم أو وقوع الضرر أو الوصول غير المصرح به (بانقا، 2019: 16)، ويرى آخرون أنَّ الأمن السيبراني تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء السيبراني والأنظمة التي تدعم الفضاء الإلكتروني (Kure et al, 2018: 89)، وعرّفه الحيدري (2019: 26) بأنَّه النشاط الذي يعمل على تأمين الحماية اللازمة للموارد البشرية والمالية المتعلقة بتقنيات المعلومات والاتصالات؛ حيث يضمن آليات للحدّ من الخسائر والأضرار التي تترتب عن المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.

ويرتبط مصطلح الأمن السيبراني بالعديد من المصطلحات ذات العلاقة بالسيبرانية، ومن هذه المصطلحات ما يلي (السمحان، 2020: 11):

- الفضاء السيبراني: يتعلق في التواصل عبر الربط بين التقنيات الرقمية المختلفة؛ حيث تشمل مجموعة من العناصر المادية وغير المادية، وتتكون من البرمجيات وشبكات التواصل، والتطبيقات الاجتماعية والمستخدمين سواءٌ أكانوا مشغلين أو مستعملين.
- الردع السيبراني: يتعلق الردع السيبراني بتوفير الحماية ومنع الأعمال التي تهدف إلى الأضرار في أصول الدولة في الفضاء السيبراني، إضافةً إلى تلك التي تدعم العمليات الفضائية.
- الهجمات السيبرانية: يقصد بها أي فعل يعرض وظائف وقدرات شبكة الحاسوب لهدف سياسي أو أمني، من خلال استغلال ثغرات أمنية معينة تُمكّن المستهدف من التخريب، وتعريض النظام إلى الخطر.

- الجريمة السيبرانية: نشاط غير مشروع (محلة معطيات الحاسوب) أو كل فعل أو امتناع عن فعل مخالف للقانون صادر عن إرادة آثمة يعاقب عليه القانون.

بناءً على ما تقدم؛ يُعرّف الباحث الأمن السيبراني بأنَّه مجموعة من الأدوات والسياسات والمبادئ التوجيهية والتقنيات التي يمكن أن تستخدم لحماية البيئة السيبرانية وأصول المنظمة للحدّ من المخاطر والتهديدات السيبرانية.

ونطاق عمليات الأمن السيبراني يشمل حماية المعلومات والأنظمة من التهديدات السيبرانية الكبرى، وتأخذ هذه التهديدات أشكالًا مختلفة ومتنوعة، وغالبًا ما تستهدف التهديدات السيبرانية الأصول السرية والسياسية والعسكرية والأمنية لدولة ما، ومن التهديدات السيبرانية الشائعة ما يلي (Taveras, 2019):

- الإرهاب السيبراني: هو الاستخدام المبتكر لتكنولوجيا المعلومات من قبل الجماعات الإرهابية لتعزيزه أجندة سياسية، وقد اتخذ شكل هجمات على الشبكات وأنظمة الكمبيوتر والاتصالات، والبنى التحتية.

- الحرب السيبرانية: تنطوي على استخدام تكنولوجيا المعلومات لإحداث أضرار، ويتم تنفيذ هجمات الحرب الإلكترونية من قبل المتسللين الذين تلقوا تدريبًا على استخدام تكنولوجيا المعلومات، والدخول إلى البيانات، وتعطيل خدمات البنية التحتية، مثل وسائل النقل والخدمات الطبية، أو تعطيل التجارة.

- التجسس السيبراني: هي ممارسة استخدام تقنية المعلومات للحصول على معلومات سرية بدون إذن من أصحابها، وغالبًا ما تستخدم في العمليات العسكرية والأمنية.

كما يمكن إضافة إلى التهديدات السيبرانية المخاطر الصحية، وتهديد البيانات والمعلومات المتعلقة بالمرضى، لا سيما في ظل اعتماد القطاعات الحصية على الأنظمة الرقمية والإلكترونية في إدارة المجالات الصحية..

الفرع الثاني: أهمية الأمن السيبراني

تبرز أهمية الأمن السيبراني من خلال تعزيز حماية جميع ما يتعلق بالدولة إلكترونيًا، كحماية الأنظمة الإلكترونية، وأنظمة تقنية المعلومات، وحماية جميع مكونات أنظمة التقنيات التشغيلية المحيطة بالمجتمع من أجهزة، وبرمجيات، فأصبحت هذه من أهم الأولويات المهمة لدول العالم للحفاظ على بيانات مواطنيها، وحفظ ممتلكاتهم وبياناتهم الإلكترونية، فقد أنشأت الدول الكليات والمعاهد ومراكز البحوث للتعمق في دراسة الأمن السيبراني حتى يتم التوصل إلى ما يوفر ويحقق الحماية للمواطنين، والمجتمع بشكل عام (أبو حسين، 2021: 39)، كما أوضح Kure et al (2018: 881) أنَّ الأمن السيبراني يوفر الحماية من المتسللين ومجرمي الإنترنت والاحتيال الإلكتروني وغيرهما، وهو أحد المجالات التكنولوجية سريعة التطور، ليس فقط في قطاعات

تكنولوجيا المعلومات ولكن أيضًا في قطاعات الصحة والبنوك والتعليم والجيش والأمن والحكومة، وتكمن أهمية الأمن السيبراني أيضًا في فهم المخاطر وإدارتها والتحكم في التداعيات التنظيمية والقانونية وغيرها من التداعيات المرتبطة في مخاطر الأمن السيبراني، ومواجهتها والتقليل من الآثار الناجمة عن الهجمات السيبرانية (الحيدري، 2019: 32). وهنالك من أشار إلى أهمية الأمن السيبراني بما يلي (السمحان، 2020: 12-13):

- المحافظة على سرية البيانات وسلامتها، وذلك من خلال منع العبث بها، إضافةً إلى ذلك جاهزية المعلومات والبيانات عند الحاجة.
- توفير الحماية اللازمة للأجهزة والمواقع والشبكات من أية اختراقات لتحقيق منظومة الدرع الأمني الواقي للبيانات والمعلومات.
- التعرف على الثغرات ونقاط الضعف في الأنظمة الإلكترونية، والعمل على معالجتها.
- استغلال الوسائل والأدوات اللازمة، والعمل على تطويرها لتحقيِق الغاية من الأمن السيبراني.
- يسهم الأمن السيبراني في توفير بيئة آمنة من خلال شبكة اتصالات محصنة.

يرى الباحث أيضًا أنَّ أهمية الأمن السيبراني تتمثل في حماية شبكة المعلومات والاتصالات التي تلعب دورًا رئيسًا في تدفق البيانات بين المواطنين والمقيمين والدولة من الأخطار التي قد تتعرض لها؛ كالتخريب أو التدمير أو الاختراقات التي من الممكن أن تؤثر بشكل مباشر أو غير مباشر على شبكة الاتصالات وتقوم بفصلها وتوقف الخدمات، وكشف أهداف العدو والتعرف على طبيعة المهاجم، من خلال معرفة تكتيكاته وأساليبه المستخدمة، لكي يتم التصدي لأي اعتداء بشكل علمي وتقني، وتشفير التعاملات الإلكترونية؛ حيث يُعَد التشفير من أهم أساليب الحماية التي يصعب فك رموزها.

المطلب الثاني: أهداف و أبعاد الأمن السيبراني

تتعدد أهداف الأمن السيبراني، والتي تهدف في مجملها إلى حماية الأنظمة والشبكات في أي دولة من الاختراق وسرقة البيانات والمعلومات المهمة، كما أنَّ هنالك أبعاد اقتصادية، وسياسية، وأمنية وعسكرية للأمن السيبراني، ولبحث أهداف وأبعاد الأمن السيبراني، تم تقسيم هذا المطلب إلى فرعين، نتناول في (الفرع الأول) أهداف الأمن السيبراني، ومن ثم البحث في أبعاد الأمن السيبراني في (الفرع الثاني)، وفي الفرع الثالث (إدارة مخاطر الأمن السيبراني).

الفرع الأول: أهداف الأمن السيبراني

يشير كل من Donalds & Kweku (2019: 403-418) إلى أنَّ الأمن السيبراني يهدف إلى استخدام جميع الأساليب والأدوات التي تهدف إلى حماية البيانات والأنظمة والشبكات من الهجمات المتعمدة والعرضية من خلال استخدام مجموعة من الأدوات والسياسات ومفاهيم الأمان والضمانات، إضافةً إلى المبادئ التوجيهية، وإدارة المخاطر، وأفضل الممارسات والتقنيات التي يمكن أن تستخدم لحماية البيئة السيبرانية، وكذلك أصول المستخدمين والمنظمات، كما يهدف الأمن السيبراني إلى توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات، وتوفير المتطلبات اللازمة للحدّ من الجرائم السيبرانية التي تستهدف المستخدمين، وسد الثغرات في أنظمة أمن المعلومات، والتصدي للبرمجيات الخبيثة ومقاومة ما تستهدفه من احداث أضرار بالغة الخطورة، واتخاذ مجموعة من التدابير اللازمة لحماية المواطنين من المخاطر في مجالات استخدام الإنترنت المختلفة، وتدريب الأفراد على آليات جديدة لمواجهة التحديات الخاصة باختراق الأجهزة التقنية بقصد الضرر بمعلوماتهم الشخصية سواءٌ بالإتلاف أو بقصد السرقة (السمحان،2020 :12)، يرى آخر أنَّ الأمن السيبراني يركز على ما يجب أن تقوم فيه المنظمات لإدارة أمن المعلومات؛ حيث يتم تحليل مستوى استعداد المنظمة للأمن السيبراني من خلال المنهج التكامل الاستراتيجي، والتوسع في استراتيجية الأمن السيبراني خارج البيئة التنظيمية، وتخفيف المخاطر، والقدرة على التكيف، والمرونة في اتخاذ القرار لمواجهة الهجمات السيبرانية (الحيدري، 2019: 37).

كما أنَّ من أهداف الأمن السيبراني ما يلي:(Leukfeldt & Majid, 2016: 263-268)

1. مراقبة المخاطر المرتبطة بالكوارث الطبيعية والبشرية.
2. مراقبة البيئة السيبرانية.
3. مراقبة المخاطر التشغيلية التي قد تؤدي إلى تدمير الإنترنت، وذلك من خلال وضع استراتيجيات لإدارة مخاطر الأمن السيبراني.
4. الحد من التجسس والتخريب الإلكتروني على مستوى أجهزة الدولة والأفراد.
5. اتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمقيمين على حدٍ سواء من المخاطر المحتملة في مجال استخدام الإلكترونيات.

يضيف الباحث أيضًا إلى أنَّ الأمن السيبراني يساهم في سد الفجوات والثغرات في الشبكات وأنظمة المعلومات، وتوفير الحماية اللازمة والضرورية من أي اختراق في النظم الإلكترونية.

الفرع الثاني: أبعاد الأمن السيبراني

تتباين أبعاد الأمن السيبراني فهنالك البعد العسكري والأمني؛ حيث تنشأ أهمية الأمن السيبراني في هذا البُعد من خطورة الهجمات السيبرانية التي تؤدي إلى نشأة الصراعات المسلحة، والحروب، واختراق الأنظمة للمنشأة النووية، فينتج عنها تهديدات لأمن الدول والحكومات، وتؤدي هذه

الهجمات إلى الكوارث، وتتراكم الأمثلة التي يمكن ذكرها في هذا المجال، لتوضيح الأبعاد العسكرية والأمنية للأمن السيبراني (الدوسري، 2019: 11).

يكمن البُعد الآخر من أبعاد الأمن السيبراني في الأبعاد السياسية؛ حيث تقوم الأبعاد السياسية على أساس حماية نظام الدولة السياسي من استخدام التقنيات في بث المعلومات والبيانات لزعزعة استقرار أمن الدول والحكومات، وتتمثل الأبعاد السياسية في الأمن السيبراني في حق الدولة في حماية أنظمتها وواجبها في السعي لتحقيق استقرار وأمن شعبها، وقد أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي، في اللعبة السياسية. فأصبح بإمكانه الاطلاع على مبررات القرارات السياسية، التي تتخذها الحكومة في دولته من خلال الكم الهائل من المعلومات، التي يمكنه الوصول إليها عبر الإنترنت (الشريف، 2013: 198-201).

يرتبط الأمن السيبراني أيضًا ارتباطًا وثيقًا بالبعد الاقتصادي، المتعلق بالحفاظ على اقتصاد كل دولة فتتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لدول كثيرة، عبر إفادتها من فرص الاستخدام، التي تقدمها الشركات الدولية والكبيرة التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط، إلا أنَّ هذا يطرح مسائل عديدة منها ما يتعلق بحماية العمل وحماية المستهلك على شبكات الإنترنت، وقد دخل العالم العصر المالي الإلكتروني بعد إطلاق خدمات المحفظة الإلكترونية، وتزايد استخدام المصارف، والمؤسسات المالية؛ حيث تتنافس الشركات على إصدار التقارير التي تسمح باستخدام آليات دفع آمنه للأفراد، وقد وضعت بعض الدول تشريعات خاصة بهذه الأموال للحدّ من بعض الجرائم الاقتصادية والمالية الخطيرة، كتبييض وغسل الأموال (زروقة، 2018: 102).

أما البُعد القانوني فيترتب على النشاط الفردي والمؤسسي والحكومي في الأمن السيبراني نتائج قانونية، تستدعي إيجاد قواعد خاصة وهامه لحل النزاعات التي تنشأ عنها؛ حيث لابد من مراعاة التحولات التقنية التي رافقت ظهور مجتمع المعلومات، فقد تم إضافة حقوق جديدة غير الحقوق الأساسية، والحريات الإنسانية المعترف بها في الدساتير، والتشريعات الوطنية والدولية، كحق النفاذ إلى الشبكة العالمية للمعلومات (Canongia & Mandarino, 2014: 71).

الفرع الثالث: مفهوم وعناصر إدارة الأمن السيبراني

كما ذكرنا سابقًا الأمن السيبراني يتمثل في استخدام التقنيات الحديثة التنظيمية، والإدارية لمنع سوء استغلال المعلومات الإلكترونية، وحمايتها واتخاذ التدابير اللازمة لحماية المواطنين والمقيمين من المخاطر والتهديدات السيبرانية، ويشير مصطلح إدارة الأمن السيبراني في قدرة المؤسسات الحكومية على وضع ورسم السياسات الاستراتيجية، وتوفير الحماية للموارد والمنشآت

الحيوية في بيئة أمنية ديناميكية للمحافظة على أصولها، والتحفيف من المخاطر السيبرانية باستخدام مجموعة من الضوابط الإدارية والقانونية والتكنولوجية والعملية والاجتماعية (Kure et al, 2018: 89)

وقد أشارت استراتيجية دولة قطر للأمن السيبراني أنَّ إدارة الأمن السيبراني تتمثل في الحاجة لحماية خدمات تكنولوجيا المعلومات والاتصالات، والحاجة لتوفير فرص للاستفادة بشكل كامل من المزايا والكفاءات التي تقدمها تكنولوجيا المعلومات والاتصالات المتطورة، وتعمل الحكومة الدفاع عن مصالح دولة قطر في الفضاء الإلكتروني من التهديدات التي قد تلحق ضرارًا في أمنها الوطني، وذلك من خلال استغلال كافة الإمكانات المتاحة ابتداءً من ممارسة الدبلوماسية ومرورًا في المشاركة في سن التشريعات الدولية وصولاً إلى استقطاب وجذب الخبراء الأمنيين والعسكريين والاستخباراتيين لإدارة عمليات الفضاء الإلكتروني، وذلك لحماية مكونات الدولة من الهجمات السيبرانية (الاستراتيجية الوطنية للأمن السيبراني في دولة قطر، 2013).

يرى الباحث أنَّ إدارة الأمن السيبراني تتعلق في إدارة المعلومات والبيانات بشكل آمن من خلال وضع السياسات والإجراءات وتطبيق التكنولوجيا الحديثة، وذلك لتعزيز الأمن السيبراني للجهات الحكومية والشركات والأفراد على حدٍ سواء.

يشير stitilis et al (2016: 197-210) أنَّ عناصر إدارة الأمن السيبراني تتمثل في ما يلي:

- أمان التطبيق: تلعب التطبيقات دورًا أساسيًا في المشاريع التجارية؛ لهذا السبب تحتاج الشركات التركيز على أمان تطبيقات الويب.
- أمن المعلومات: تتضمن المعلومات سجلات الأعمال والبيانات الشخصية وبيانات العملاء والملكية الفكرية، وبالتالي من الضروري أن يكون لأي مؤسسة أمن إلكتروني مناسب.
- أمن الشبكة: يتم إجراء اختبار اختراق الشبكة لتقييم نقاط الضعف في النظام ومشكلات الأمان الأخرى التي تحدث في الخوادم والأجهزة وخدمات الشبكة.
- تخطيط استمرارية الأعمال: يتعلق تخطيط استمرارية الأعمال حول مدى الاستعداد للتدخل أو التهديد السيبراني من خلال تحديد التهديدات التي تتعرض لها المنظمة في الوقت المحدد وتحليل كيفية تأثر العمليات وكيفية التغلب عليها.
- أمن العمليات: يستخدم أمن العمليات لحماية وظائف المنظمة.
- تعليم وتدريب الموظفين: لكي يتم الحفاظ على الأمن السيبراني للمؤسسة من الضروري أن تقوم المنظمة بتدريب موظفيها على الأمن السيبراني؛ بحيث يجب أن يكون كل موظف على دراية بالهجمات المتعلقة بالتصيد الإلكتروني، كذلك أن يكون لديه القدرة على التعامل مع التهديدات الإلكترونية التي قد يواجهونها.

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

المبحث الثاني: النظم القانونية للأمن السيبراني والمحافظة على الصحة العامة

تشكل حماية خصوصية المرضى وتأمين معلوماتهم الصحية إحدى المتطلبات الأساسية في مجال الرعاية الصحية وخاصة بعد تزايد حملات القرصنة الإلكترونية، والتي طالت شتى القطاعات في عدد من دول عالم، لذلك كان من الضروري أن تقوم مؤسسات الرعاية الصحية بتوفيرُ أعلى مستويات الأمن لحفظ سجلات بيانات المرضى، وتأمين الأجهزة المتصلة بالإنترنت.

المطلب الأول: التنظيم القانوني للأمن السيبراني في حماية الصحة في دولة قطر

مع التقدم التكنولوجي واعتماد الأنظمة الصحية على الحلول الرقمية، أصبح الأمن السيبراني ضرورة لضمان حماية البيانات الصحية وسلامة العمليات المرتبطة بالصحة العامة، إذ تتعلق بتحسين وحماية صحة المجتمع من خلال الوقاية من الأمراض، وتعزيز الرعاية الصحية؛ حيث بات تعتمد الصحة العامة الحديثة على الأنظمة الرقمية لتحليل البيانات، التواصل، وإدارة الطوارئ، وللبحث في التنظيم القانون للأمن السيبراني في دولة قطر نتناول الإطار القانوني المنظم للأمن السيبراني في دولة قطر في (الفرع الأول)، ومن ثم البحث في تحقيق الأمن السيبراني في ظل إنشاء وكالة الأمن السيبراني في (الفرع الثاني).

الفرع الأول: الإطار القانوني المنظم للأمن السيبراني في دولة قطر

تناول المشرع القطري في القانون رقم (14) لسنة 2014م المتعلق بمكافحة الجرائم الإلكترونية في الباب الثاني تحت عنوان الجرائم؛ حيث تضمن الفصل الأول منه جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية، وعاقب المشرع بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها، وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة (المادة، 2). وهذا ما ينطبق على الدخول غير المشروع إلى بيئة المؤسسات الصحية التي تتضمن بيانات ومعلومات عن صحية تتعلق بالكوادر الطبية والإدارية، أو سجلات المرضى.

وفي إطار تحقيق الأمن السيبراني تضمن القانون سالف الذكر الدخول غير المشروع عمدًا، دون وجه حق، بأي وسيلة، موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ... وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية مالكه أو القائم على إدارته (المادة، 3)، وهذا تأكيد من المشرع القطري على تحقيق الأمن السيبراني في القطاعات العامة ومنها القطاع الصحي، وذلك لحماية الأصول الرقمية والإلكترونية في المؤسسات الصحية في دولة قطر.

وفي سبيل المحافظة على النظام العام بعناصره (الأمن العام، والصحة العامة، والسكينة العامة، والآداب العامة)، فقد جاء في الفصل الثاني تحت عنوان جرائم المحتوى؛ حيث يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار موقعاً إلكترونياً عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، لنشر أخبار غير صحيحة، بقصد تعريض سلامة الدولة أو نظامها العام أو أمنها الداخلي أو الخارجي للخطر ... ويعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على (250,000) مائتين وخمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل من روج أو بث أو نشر، بأي وسيلة، تلك الأخبار غير الصحيحة بذات القصد(المادة، 6). ويؤكد المشرع القطري في القانون سالف الذكر إذا كان الهدف من الدخول إلى المحتوى بقصد تعريض عناصر النظام للخطر من خلال نشر معلومات غير صحيحة عن دولة قطر على وجه العموم، أو القطاع الصحي على وجه الخصوص بقصد إساءة سمعة الدولة وتعريض أمنها الصحي للخطر بالعقوبات سالفة الذكر، وبهذا نلاحظ أن المشرع القطري في هذا القانون نظم حماية الصحة العامة من خلال تحقيق الأمن السيبراني في المؤسسات الصحية بدولة قطر.

كما حقق المشرع القطري الحماية للصحة العامة وتحقيق الأمن السيبراني من خلال القانون رقم (13) لسنة 2016م بشأن حماية خصوصية البيانات الشخصية؛ حيث نصت المادة الثالثة من هذا القانون على أنه: "لكل فرد الحق في حماية خصوصية بياناته الشخصية، ولا يجوز معالجة تلك البيانات إلا في إطار الشفافية والأمانة واحترام كرامة الإنسان والممارسات المقبولة، وفقاً لأحكام هذا القانون"، كما نصت المادة الرابعة على أنه لا يجوز للمراقب معالجة البيانات

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

الشخصية، إلا بعد الحصول على موافقة الفرد، ما لم تكن المعالجة ضرورية لتحقيق غرض مشروع للمراقب أو الغير الذي تُرسل إليه البيانات. وبهذا نجد أنَّ المشرع القطري نظم حماية البيانات الشخصية في هذا القانون وعلى درجة من الأهمية لما لها علاقة بخصوصية الأفراد، وبما أنَّ البيانات الشخصية في المؤسسات الصحية من الضروري أن تكون متوافرة في سجلات المرضى، فقط حرص المشرع القطري على حمايتها وعدم الإفصاح عنها لما يتعلق بالحقوق الشخصية للأفراد.

تأكيدًا على ذلك، فقد نصت المادة السادسة عشر من القانون ذاته على أنه تعد بيانات شخصية ذات طبيعة خاصة، البيانات المتعلقة بالأصل العرقي، والأطفال، والصحة أو الحالة الجسدية أو النفسية، والمعتقدات الدينية، والعلاقة الزوجية، والجرائم الجنائية، وللوزير أن يضيف أصنافاً أخرى من البيانات الشخصية ذات الطبيعة الخاصة، إذا كان من شأن سوء استخدامها أو إفشائها إلحاق ضرر جسيم بالفرد، كما لا يجوز معالجة البيانات الشخصية ذات الطبيعة الخاصة، إلا بعد الحصول على تصريح بذلك من الإدارة المختصة، وفقاً للإجراءات والضوابط التي يصدر بتحديدها قرار من الوزير، كما للوزير، بقرار منه، فرض احتياطات إضافية لغرض حماية البيانات الشخصية ذات الطبيعة الخاصة، وهذا يعني أن المشرع القطري أولى اهتمامًا خاصًا بالبيانات الشخصية للأفراد في الدول وجعلها على درجة من السرية لما فيها من مصلحة حماية الأمن الصحي وتحقيق الأمن السيبراني في المؤسسات الصحية بدولة قطر.

الفرع الثاني: حماية الأمن السيبر اني في دولة قطر

في إطار تعزيز الأمن السبراني في دولة قطرتم استحداث الوكالة الوطنية للأمن السيبراني بموجب القرار الأميري رقم (1) لسنة 2021، الصادر بتاريخ 25 مارس 2021، وتتبع الوكالة بموجبه، مجلس الوزراء وقد أتى قرار الإنشاء لتوحيد رؤى وجهود تأمين الفضاء السيبراني للدولة والمحافظة على الأمن الوطني السيبراني.

إذ أنَّ هدف الوكالة المحافظة على الأمن السيبراني وتنظيمه، وتعزيز المصالح الحيوية للدولة وحمايتها في مواجهة تهديدات الفضاء السيبراني، ويكون لها في سبيل تحقيق ذلك ممارسة كافة الاختصاصات والصلاحيات وبوجه خاص إعداد الاستراتيجية الوطنية للأمن السيبراني وتحديثها بالتنسيق مع الجهات المعنية.

وتعمل الوكالة إلى تعزيز الأمن السيبراني من خلال متابعة العمل الجاد والدؤوب من خلال المشاريع والبرامج التي تهدف إلى تعزيز الأمن السيبراني وتوفير بيئة سيبرانية آمنة وفقًا لأحدث النظم وأفضل الممارسات العالمية في هذا المجال، بما يحقق بناء وتطوير تكنولوجيا المعلومات

والاتصالات والتحول الرقمي، وتقديم حلول قيمة لمواجهة التحديات السيبرانية، ودعم بناء القدرات والابتكار من أجل تحقيق فضاء سيبراني آمن يعود بالنفع على جميع الأفراد والمؤسسات في دولة قطر، ويلبي متطلبات التنمية الوطنية المستدامة، ويعزز من مكانة دولة قطر إقليمًيا وعالميًا في هذا المجال الحيوي.

لقد سعت دولة قطر إلى تعزيز الأمن السيبراني؛ حيث وضعت الاستراتيجية الوطنية للأمن السيبراني (2024 – 2030م) في 17 سبتمبر 2024م، وقد هدفت الاستراتيجية إلى الإسهام الفاعل في تحقيق رؤية قطر الوطنية 2030م، وتعزيز مكانة دولة قطر لتكون في طليعة الدول الساعية إلى ضمان الاستخدام الآمن للتقنيات الحالية والناشئة.

وأن الأمن السيبراني لا يمكن تحقيقه إلا عبر تضافر جهود الجهات والمؤسسات الحكومية والخاصة والجهات المعنية، ومن هنا جاء شعار الاستراتيجية الوطنية الثانية للأمن السيبراني ورؤيتها اللذين يرتكزان على الجهود الموحدة لتعزيز الثقة في الفضاء السيبراني لضمان تقدم وازدهار دولة قطر، والارتقاء بمنظومة الأمن السيبراني في الدولة.

تضمنت المبادئ التوجيهية للاستراتيجية على القيم المتمثلة في: المسؤولية المشتركة، والنهج القائم على إدارة المخاطر، والتركيز على النتائج، وحقوق الأفراد الشخصية، والازدهار الاقتصادي والتنسيق والتعاون، مشيراً إلى أن هذه المبادئ تعد بمثابة القواعد الرئيسية لتحقيق الأمن السيبراني الوطني وتسهم في عملية التوجيه والإرشاد اللازمتين للتنفيذ.

وقد ركزت هذه الاستراتيجية على خمس ركائز أساسية أولها الأمن والمرونة في منظومة الأمن السيبراني في دولة قطر، وتتمثل الركيزة الثانية في التشريعات والتنظيمات وإنفاذ القانون من أجل فضاء سيبراني آمن، فيما تهدف الركيزة الثالثة إلى تحقيق اقتصاد مزدهر ومبتكر وقائم على البيانات، وتتمثل الركيزة الرابعة في تنمية الثقافة السيبرانية والارتقاء بالقدرات والكوادر الوطنية، فيما تهدف الركيزة الخامسة إلى تعزيز التعاون والشراكات في الأمن السيبراني إقليميًا ودوليًا.

المطلب الثاني: الأمن السيبراني في حماية الصحة في سلطنة عُمان ودولة الإمارات

شهدت سلطنة عُمان ودولة الإمارات العربية المتحدة في السنوات الأخيرة تحولاً رقميًا واسع النطاق بمختلف القطاعات، في إطار رؤية شاملة تهدف إلى تحقيق التنمية المستدامة وتعزيز الاقتصاد الرقمي؛ حيث بدأت بالفعل اتخاذ خطوات مهمة نحو مواجهة هذا التحدي، للحفاظ على استقرارها الأمني ومواجهة تهديدات سيبرانية متزايدة التعقيد بشكل يومياً نتيجة التطور التقني المتسارع عالمياً.

ISNN : 2253-0592 EISSN : 2588-199X / Prefix: 10.46315

الفرع الأول: الأمن السيبراني في سلطنة عُمان وحماية الصحة العامة

أطلقت سلطنة عُمان في أكتوبر/2022 "الهيئة الوطنية للأمن السيبراني"، التي تعمل على وضع سياسات وتنسيق جهود الدفاع السيبراني بين مختلف القطاعات، لحماية البنية التحتية الحيوية مثل قطاعات الطاقة والمواصلات من الهجمات السيبرانية، كما أصدرت في فبراير 2023 قانونًا للأمن السيبراني، يهدف إلى حماية البيانات الشخصية للمواطنين والمقيمين، ويفرض على الشركات والمؤسسات العامة والخاصة الالتزام بمعايير صارمة لحماية الشبكات والبنية التحتية الإلكترونية، ومنها حماية الصحة العامة والبيانات المرتبطة في القطاع الصحي.

في مايو 2023 تم إطلاق "أكاديمية الأمن السيبراني العمانية"، التي تقدم برامج تدريبية متقدمة بالتعاون مع مؤسسات تعليمية دولية مثل جامعة "كارنيجي ميلون" الأمريكية، لتطوير مهارات الشباب العماني في مجال الأمن السيبراني، كما وقعت في يوليو 2023 اتفاقية تعاون مع الاتحاد الأوروبي لتعزيز التعاون في مجال الأمن السيبراني، وتبادل الخبرات الفنية وتنظيم تدريبات مشتركة، بالإضافة إلى تقديم الدعم الفني لتعزيز البنية التحتية السيبرانية في السلطنة.

الفرع الثاني: الأمن السيبراني في دولة الإمارات العربية وحماية الصحة العامة

أعلنت دولة الإمارات العربية المتحدة في يناير 2023 إنشاء مركز متقدم للأمن السيبراني يعنى بمراقبة وحماية البنية التحتية الرقمية للدولة، ويعتمد على تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة للكشف عن الهجمات السيبرانية بشكل استباقي.

وفي فبراير 2023 أطلقت مبادرة "المبرمجين السيبرانيين"، وهي برنامج تدريبي يهدف إلى تطوير مهارات الشباب الإماراتي في مجال الأمن السيبراني، بالشراكة مع كبرى الشركات التقنية العالمية.

***-خاتمة**

يُعد الأمن السيبراني عنصرًا حاسمًا في حماية الصحة العامة في العصر الرقمي؛ حيث حققت دولة قطر تقدمًا ملحوظًا من خلال قوانينها واستراتيجياتها، لكن الحاجة إلى تحسين الوعي وتعزيز القدرات التقنية لا تزال قائمة. ومقارنة بالتجارب الخليجية الأخرى، تمتلك دولة قطر الأساس اللازم لتطوير إطار قانوني شامل يحمي الصحة العامة من التهديدات السيبرانية.

أولاً: النتائج

1. إنَّ مصطلح الأمن السيبراني مصطلح حديث الظهور في العقود الأخيرة نتيجة لثورة تكنولوجيا المعلومات لذلك تعددت التعريفات على ضوء الاجتهادات الفقهية والممارسات العملية الدولية.

2. إنَّ من أهم المفاهيم المرتبطة بالأمن السيبراني الجرائم السيبرانية؛ حيث يهدف الأمن السيبراني في حفظ وحماية المعلومات الموجودة على الشبكات، ويحرص على تقديم المعلومات الصحيحة ومن مصادر موثوقة للمستخدمين.

3. يعتبر الأمن السيبراني أحد الأبعاد المحورية في سياق مفهوم الأمن الوطني الشامل، لذا فإن إيلاء هذا الموضوع الاهتمام الكافي من قبل الجهات الرسمية وغير الرسمية من شأنه أن يسهم في الحفاظ على الأمن الوطني.

4. ترتبط قدرة الدولة في مواجهة الجرائم السيبرانية بوجود استراتيجيات ورؤية واضحة في هذا الصدد، ومراجعة مستمرة لما يواكب الفضاء السيبراني من تطور في الأساليب والأدوات المستخدمة، حيث أن تلك الجرائم في تطور مستمر بالتزامن مع التطور التكنولوجي الهائل الذي يشهده العالم.

5. تتطلب القدرة على مواجهة الجرائم السيبرانية وتعزيز الأمن السيبراني التطوير المستمر للاستراتيجيات ذات العلاقة، وتوظيف الإعلام توظيفًا إيجابيًا في إطار نشر الوعي المجتمعي حول الجرائم السيبرانية وتداعياتها في الأمن الوطني.

6. قطعت دولة قطر شوطًا مميزًا في مجال الحفاظ على الأمن السيبراني سواءٌ في تطوير التشريعات أو إعداد الاستراتيجيات والوكالات المتعلقة بالأمن السيبراني، إدراكًا منها لحجم تأثير الجرائم السيبرانية في منظومة الأمن الوطني، مما جعلها قادرة على مواجهة تحديات ومخاطر الجرائم السيبرانية.

ثانيًا: التوصيات

1. تعزيز التشريعات، وذلك من خلال تحديث القوانين لتواكب التهديدات السيبرانية المستجدة.

2. تدريب العاملين في القطاع الصحي على ممارسات الأمن السيبراني لحماية خصوصية الأفراد.

3. ضرورة المراجعة المستمرة لاستخدامات المواقع الإلكترونية، ووضع القيود اللازمة في إطار ضبطها والحيلولة دون استخداماتها السلبية التي تؤثر في الأمن السيبراني.

4. تطوير نموذج للأمن السيبراني العربي يتم من خلاله تطوير الإطار الاستراتيجي لضمان تبادل الخبرات والمعلومات.

**

***- قائمة المراجع**

أولاً: المراجع العربية

أ- الكتب

الحيدري، زينب (2019). الأمن السيبراني – المخاطر – التحديات – المواجهة، دار الشرق للطباعة والنشر والتوزيع، ط1، الدوحة، قطر.

الردايدة، عبد الكريم (2010). الجرائم المستحدثة واستراتيجية مواجهتها، ط1، دار ومكتبة الحامد للنشر والتوزيع، عمان، الأردن.

الشريف، محمد عبد العزيز (2013). المواجهة التشريعية والأمنية للسلوك الإجرامي الإلكتروني، مطابع الشرطة، معهد تدريب الشرطة – قسم العلوم الشرطية، دولة قطر.

شرابشة، ليندة (2012). السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية، المركز الجامعي، الرباط، المغرب.

عبد الله، عبد الكريم عبد الله (2007). جرائم المعلوماتية والإنترنت - دراسة مقارنة، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان.

عبابنة، محمود، والرازقي محمد (2005). جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن.

ب-الرسائل الجامعية

أبو حسين، حنين جميل (2021) الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن.

الأوجلي، سالم محمد سليمان (1997). أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، أطروحة دكتوراه، جامعة عين شمس، مصر.

الحمادي، خالد سليمان (2019). جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري – دراسة مقارنة، رسالة ماجستير، جامعة قطر، دولة قطر.

ج- الأبحاث

بانقا، علم الدين (2019). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية – دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للتخطيط، العدد (63)، دولة الكويت.

الخياط، أحمد مصبح (2019). تصور مقترح لتطوير إدارة الأعمال في ضوء مدخل إدارة المخاطر بمؤسسات الأعمال الكويتية، المجلة العلمية الاقتصاد والتجارة، الكويت، ص327-351.

الدوسري، خليفة (2019). الجريمة السيبرانية - المحددات النظرية والسياسات الجنائية وآليات المكافحة والوقاية، الدوحة، دولة قطر.

زروقة، إسماعيل (2018). الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بو ضياف المسيلة، المجلد (10) العدد (1)، الجزائر.

السمحان، مني عبد الله (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (111)، مصر.

العبدالات، طلال، والزعارير أحمد (2016). أثر مواقع التواصل الاجتماعي في ارتكاب الجريمة الإلكترونية في الأردن: التفكك الأسري كعامل مُعدل – دراسة تحليلية، مجلة الدراسات الأمنية، الأردن.

عبد الرحمن، فهد أحمد (2023). الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، مجلة دراسات الخليج والجزيرة العربية، العدد (190)، 257-298.

القحطاني، مداوي (2015). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها "نحو استراتيجية شاملة لمكافحة الجريمة الإلكترونية في دول مجلس التعاون الخليجي، جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية، الرياض، السعودية.

محمد، إبراهيم زيد (2012). الأمن الشامل والنظام العالمي الجديد: دراسة في آفاق الاستراتيجية الأمنية للدول العربية، المركز العربي للدراسات الأمنية والتدريب، الرياض. السعودية.

المطيري، خالد ظاهر عبد الله جابر السهيل (2002). دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد (38)، 969-1066.

الهزاني، نورة ناصر (2023). ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات، مجلة مكتبة الملك فهد الوطنية، العدد (28)، 61-121.

**

ثانياً: المراجع الأجنبية

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, *Methodologies, Tools and Applications*: 60-80. Hershey, PA: IGI Global.

Donalds, Charlotte, & Kweku-Miata. (2019). toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior* 92 (2019), pp 403-418.

Kure, Halima Ibrahim, Shameful Islam & Mohammad Abdu Razzaque (2018). *An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System*, Sic, p 898.

Naira, Anil, Elzotbek Rustambekovb, Michael McShane & Stave Fainshmidt (2014). Enterprise Risk Management as a Dynamic Capability: A test of its effectiveness during a crisis, *Article in Managerial and Decision Economics*, pp 554-565.

James, Paul (2014). "Human Security as a Left-Over of Military Security, or as Integral to the Human Condition". In Paul Bacon and Christopher Hobson. Human Security and Japan's Triple Disaster. *London: Routledge*. p 73.

Saunders, F. C., Gale, A. W., & Sherry, A. H. (2015). Conceptualizing uncertainty in safety-critical projects: a practitioner perspective. *International Journal of Project Management*, 33(2), 467–478.

Shad, Muhammad Kashif & Fong-Woon Lai (2019). Enterprise Risk Management Implementation and Firm Performance: Evidence from the Malaysian Oil & Gas Industry, I*nternational Journal of Business & Management*; Vol. (14), No. (9); p47-53.

Sinha, Tanmoy (2019). Risk Assessment and Management, *Memorial University of Newfoundland*, Canada, 1-6.

Stitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016. Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues,* 6(2): 197–210.

Taveras, Pedro (2019). Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack, All content following this page was uploaded by Pedro Taveras on 15 April 2019.

Tasoulla, H, & Jain K (2014). The Social Dimension of Security: Exploring How Surveillance Systems Relate to Interior Design, Interior Design Educators Council, *and Journal of Interior Design* 34 (3), p12.