MESR
منار الشرق للدراسات والأبحاث
Manar Elsharq for Studies & Research
مجلة الشرق الأوسط
للدراسات القانونية والفقهية

الأبعاد القانونيّة والاجتماعيّة للأمن السيبراني

ا. م. د. احمد حاتم جبار عطيه

كلية القانون / الجامعة المستنصرية

ahmedhatem@uomustansiriyah.edu.iq

استلام البحث: 15/06/2025	مراجعة البحث: 14/07/2025	قبول البحث:10/08/2025

الملخص:

يتناول هذا البحث دراسة مفهوم الأمن السيبراني، وأبعاده القانونية والاجتماعية، في ظل التوسع المتسارع في استخدام التكنولوجيا الرقمية، واعتماد الأفراد والمؤسسات على الفضاء الإلكتروني في مختلف الأنشطة. في المبحث الأول تم توضيح تعريف الأمن السيبراني لُغويًّا باعتباره حماية وأمان الفضاء المعلوماتي من أي تهديد أو اعتداء، بينما عرف اصطلاحيًّا على أنه مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية البيانات والشبكات والأنظمة الرقمية من الوصول غير المصرح به أو التدمير أو التعديل.

أما المبحث الثاني فقد ركز على الأبعاد الأساسية للأمن السيبراني، حيث أوضح المطلب الأول أن البعد القانوني يشمل التشريعات والسياسات التي تضعها الدول لمكافحة الجرائم الإلكترونية، وحماية الخصوصية، وتحديد المسؤوليات وفرض العقوبات المناسبة. كما بين أن الإطار القانوني يجب أن يكون مرنًا وقابلًا للتطوير لمواكبة التطورات التقنية والتهديدات المستجدة. أما المطلب الثاني فقد تناول البعد الاجتماعي موضحا أن الوعي المجتمعي والتثقيف الرقمي يشكلان خط الدفاع الأول في حماية الأمن السيبراني، إذ يسهمان في تعزيز السلوكيات الآمنة لدى الأفراد وتقليل مخاطر الاختراق والابتزاز الرقمي.

خلص البحث إلى أن تحقيق الأمن السيبراني يتطلب تكاملا بين التشريعات القانونية والممارسات الاجتماعية، إضافة إلى التعاون الدولي وتبادل الخبرات من أجل بناء بيئة رقمية آمنة تدعم التنمية المستدامة وتحافظ على الأمن الوطني في مواجهة التهديدات العابرة للحدود.

الكلمات المفتاحية: الأمن السيبراني، الجرائم الإلكترونية، الفضاء الإلكتروني، البيانات، الشبكات، الأنظمة الرقمية، الخصوصية، التشريعات.

Abstract

This research examines the concept of cybersecurity and its legal and social dimensions considering the rapid expansion in the use of digital technology and the reliance of individuals and institutions on cyberspace for various activities. The first section defines cybersecurity linguistically as the protection and security of information space from any threat or attack. It is technically defined as a set of procedures, technologies, and policies aimed at protecting data, networks, and digital systems from unauthorized access, destruction, or modification.

The second section focuses on the basic dimensions of cybersecurity. The first section explains that the legal dimension includes the legislation and policies enacted by countries to combat cybercrimes, protect privacy, define responsibilities, and impose appropriate penalties. It also demonstrates that the legal framework must be flexible and scalable to keep pace with technological developments and emerging threats. The second section addresses the social dimension, explaining that community awareness and digital education constitute the first line of defense in protecting cybersecurity, as they contribute to promoting safe behavior among individuals and reducing the risks of hacking and digital extortion.

The study concluded that achieving cybersecurity requires an integration of legal legislation and social practices, as well as international cooperation and the exchange of expertise to build a secure digital environment that supports sustainable development and maintains national security in the face of transnational threats.

Keywords: cybersecurity, cybercrime, cyberspace, data, networks, digital systems, privacy, legislation.

المقدمة

أحدثت الثورة الرقمية تغير في أسلوب إدارة المعلومات والتواصل مما أوجد بيئة جديدة تحمل فرصًا واسعة للنمو والتطوير، لكنها في الوقت نفسه فرضت تحديات تتعلق بحماية الفضاء الإلكتروني من المخاطر والتهديدات المتزايدة التي تستهدف البيانات والأنظمة الحيوية ومع تزايد الاعتماد على التقنيات الحديثة في المعاملات والخدمات برزت أهمية الأمن السيبراني كعامل رئيسي لضمان استقرار البنية التحتية الرقمية واستمرارية العمل المؤسسي.

من الاتجاه القانوني ظهرت الحاجة إلى تشريعات متخصصة تعالج خصوصية الجرائم الإلكترونية وتحدد آليات المساءلة والعقوبات بما يتناسب مع طبيعتها العابرة للحدود، أمّا من الجانب الاجتماعي فإن رفع الوعي بمخاطر الفضاء الرقمي وتبني الممارسات الآمنة في استخدام التكنولوجيا يمثلان خط الدفاع الأول في مواجهة التهديدات مما يجعل التكامل للإطار القانوني والوعي ضروري لبناء بيئة رقمية آمنة.

أهمية البحث

تنبع أهميته من كونه يتناول قضية معاصرة تمسُّ أمن الدول واستقرار المجتمعات في ظل الاعتماد المتزايد على التكنولوجيا الرقمية فهو يسهم في توضيح الإطار القانوني المنظم لمواجهة الجرائم الإلكترونية وحماية البيانات إضافة إلى إبراز الدور المجتمعي في تعزيز الاستخدام الآمن للتقنيات الحديثة كما يتيح هذا البحث فهما أعمق للتحديات التي يفرضها الفضاء الإلكتروني وسبل مواجهتها من خلال تكامل الجهود القانونية والتوعوية بما يضمن بيئة رقمية آمنة تدعم التنمية وتحافظ على المصالح الوطنية

أهداف البحث

1. توضيح الإطار القانوني المنظم للأمن السيبراني ودوره في مواجهة الجرائم الإلكترونية وحماية البيانات.
2. تحليل البعد الاجتماعي للأمن السيبراني وأثر الوعي المجتمعي في الحد من المخاطر الرقمية.
3. بيان أهمية التكامل بين الجوانب القانونية والاجتماعية لبناء بيئة رقمية آمنة ومستقرة.

المشكلة البحثية

تتمثل المشكلة في أن تطور الفضاء الإلكتروني وتزايد الاعتماد على التكنولوجيا الحديثة صاحبه تقدم في التهديدات والجرائم السيبرانية التي تتجاوز الحدود الجغرافية؛ مما كشف عن قصور في الأطر القانونية وضعف في الوعي المجتمعي بأساليب الوقاية والحماية الرقمية، وهذا ما يهدد أمن المعلومات واستقرار المؤسسات ويثير الحاجة إلى معالجة متكاملة تجمع بين الجوانب القانونية والاجتماعية، ومن هنا يطرح البحث سؤاله الرئيسي: **"كيف يمكن توظيف الأبعاد القانونية والاجتماعية للأمن السيبراني في مواجهة التهديدات الرقمية وبناء بيئة رقمية آمنة ومستدامة"؟.**

منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي من خلال دراسة الأدبيات القانونية والاجتماعية المتعلقة بالأمن السيبراني.

الخطة البحثية

المبحث الأول: مفهوم الأمن السيبراني

- المطلب الأول: تعريف الأمن السيبراني لغويًا
- المطلب الثاني: تعريف الأمن السيبراني اصطلاحيًا

المبحث الثاني: أبعاد الأمن السيبراني

- المطلب الأول: الأبعاد القانونية
- المطلب الثاني: الأبعاد الاجتماعية

المبحث الأول: مفهوم الأمن السيبراني

الأمن السيبراني هو مصطلح يتكون من كلمتين هما "Cyber security"، والأصل كلمة "سيبر" تعود إلى الأصل اللاتيني، حيث تعني الحماية المعلوماتية، وبالتالي، يشير الأمن السيبراني إلى حماية المعلومات بشكل عام، وهو مجال أوسع من مجرد أمن المعلومات، يمكن تعريف الأمن السيبراني على أنه مجموعة من الأدوات التكنولوجية والإدارية المستخدمة لمنع الوصول غير المصرح به وسوء الاستخدام، وكذلك لاستعادة البيانات الإلكترونية وأنظمة المعلومات والاتصالات التي تحتوي عليها، والهدف من ذلك هو ضمان توفر واستمرارية أنظمة المعلومات، وكذلك حماية سرية وأمان البيانات الشخصية لحماية المواطنين.[1]

المطلب الأول: تعريف الأمن السيبراني لغويًّا

الأمن السيبراني يتكون من كلمتين: "الأمن" و"السيبراني"،

الأمن يعني العكس من الخوف، وهو يدل على السلامة. كلمة أمن تأتي من الفعل أمن، وتعني الراحة النفسية وهدوء القلب وابتعاد الخوف. يمكن القول إن الشخص "أمن من الشر" عندما يكون بعيدًا عن الخطر. عرّف قاموس بنغوين للعلاقات الدولية الأمن بأنه مصطلح يدل على عدم وجود تهديدات للقيم الهامة. [2]

أما السيبراني، فهو مصطلح شائع في مجال الأمن الدولي. إذا نظرنا إلى أصل كلمة "cyber"، نجد أنها مأخوذة من كلمة يونانية "kybernetes" التي تعني الشخص الذي يتحكم في توجيه السفينة. وتستخدم للدلالة على "الحاكم". العديد من المؤرخين يشيرون إلى أن أصل هذا المصطلح يعود إلى عالم الرياضيات الأمريكي نوربرت وينر، الذي عاش بين 1894م و1964م، وكان يرغب في وصف التحكم الآلي.

هو يعتبر مؤسس علم السبرنيتيكية من خلال كتابه المعروف " Cybernetics or control and communication in the Animal and the machine"، في هذا الكتاب، يقترح وينر أن السبرنيتيكية تعني التحكم والتواصل بين الحيوان والآلة، وبعد الحرب العالمية الثانية تم استبدال مصطلح "الآلة" بكلمة "الحاسوب".[3]

---

[1] خاطر، نوري حمد، "حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف"، بحث منشور في مجلة المنارة العدد (2) كانون ثاني جامعة آل البيت، المفرق، 2012، ص 35

[2] إيفانز غراهام نوينهام جيفري، "قاموس بنغوين للعلاقات الدولية: الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004"، ص200.

المطلب الثاني: تعريف الأمن السيبراني اصطلاحيًّا

يمكن وصف الأمن السيبراني بأنه حماية الشبكات والأنظمة المعلوماتية، بالإضافة إلى البيانات والمعلومات والأجهزة المرتبطة بالإنترنت. وبالتالي، فهو المجال الذي يتضمن الإجراءات والمعايير والقياسات اللازمة للتعامل مع التهديدات، ومنع التعديات، أو تقليل تأثيراتها في أسوأ الظروف.

يرتبط هذا النوع من الأمن بشكل وثيق بأمن المعلومات. فإن الوصول إلى المعلومات أو نقلها أو الاطلاع عليها أو حتى التلاعب بها واستخدامها بشكل غير صحيح يكون غالبًا وراء الاعتداءات على الشبكات والإنترنت.[1]

إن الاعتماد على المعلومات هو واقع لا يمكن تجاهله، مما يعني أنه يجب الاعتماد أكثر على الأنظمة الإلكترونية التي تعالج هذه البيانات. عند مناقشة الأمن، من الضروري تعريف الخطر، وهو التهديد الذي تواجهه الأنظمة. يتضمن ذلك تحديد نقاط الضعف أو الثغرات الموجودة فيها، والإجراءات الضرورية التي يجب اتخاذها لتقليل الخطر.[2]

التهديد هو نوع من الأعمال المعادية التي يمكن أن تُمارس ضد النظام، بينما نقاط الضعف تشير إلى مدى تعرض النظام لهذا التهديد في وضع معين. أما التدابير المطلوبة لمواجهة ذلك، فهي لا تقتصر فقط على الجانب التكنولوجي، بل تشمل أيضاً تعزيز المهارات، وزيادة الوعي، والتدريب، وتبادل المعرفة، بالإضافة إلى مجموعة من القواعد المحددة التي ينبغي اتباعها.[3]

إن الخطر متعلق بأمان الشبكات وأمان الإنترنت من جانبين: الأول هو البنية التحتية التي تتعلق بنقاط الدخول والخروج وتخزين المعلومات والتجسس عليها، والثاني هو الأعمال التخريبية والتدميرية التي تؤثر على ذلك، وتضر بالأموال والأشخاص.

نظرًا لأن الشبكة العالمية تتطلب معايير فنية وتقنية خاصة، فإن ربط الشبكات بها يعرضها لمخاطر مماثلة. لذا، يمكن أن يحدث هجوم على النظام مما يؤدي إلى توقفه عن تقديم خدماته، أو يكشف عن أسرار الأفراد والشركات، سواء كانت شخصية أو متعلقة بالصناعة والمهنة، أو يمكن أن يتسبب في فقدان بيانات حساسة، أو نشر معلومات غير صحيحة.[4]

يجب علينا التمييز بين المعلومات والتكنولوجيا وأدواتها. المعلومات هي نتاج معالجة البيانات بطرق معينة باستخدام التكنولوجيا، سواء لجمعها أو الوصول إليها أو تخزينها ومعالجتها. لذلك، الخطوة الأولى نحو تحقيق الأمن هي مراقبة هذه التكنولوجيا، خاصة في جانب الاتصالات، ومتابعة حركة المعلومات لضمان سهولة الوصول إليها وانسيابها، ومنع التنصت من جهة المنافسين أو من أي جهة تريد الهجوم.[5]

---

[3] منى الأشقر جبور، "السيبرانية هاجس العصر، بيروت: جامعة الدول العربية – المركز العربي للبحوث القانونية والقضائية"، 2016 150 ص

[1] جبور، منى الاشقر، "السيبرانية، هاجس العصر، جامعة الدول العربية"، القاهرة، مصر، 2018، ص 241.

[2] رستم هشام محمد خليل، "الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون عدد 2 شرطة دبي"، دبي، الامارات العربية المتحدة، 2012،

[3] "دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام 2010"، ص 314

[4] الرومي، محمد أمين، "جرائم الكمبيوتر والأنترنت دار المطبوعات الجامعية، الإسكندرية"، مصر، 2013، ص 7.

[5] الشهري، حسن بن أحمد، "قانون دولي موحد لمكافحة الجرائم الإلكترونية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب"، تصدر عن جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، العدد 27، العدد 53 رجب 1432هـ.

من هنا، يتوجب على المؤسسات والأفراد العمل على تأمين الاتصالات من خلال الحفاظ على سريتها، مع ما قد ينشأ عن ذلك من تحديات تتعلق بمكافحة الجرائم والأمن. وفي هذا السياق، يعني الأمن ألا يتم استخدام النظام إلا للأغراض التي صُنع من أجلها وضمن الحدود المسموح بها. [1]

الأمن السيبراني، وفقًا لتعريف الاتحاد الدولي للاتصالات في تقريره عن "توجهات الإصلاح في الاتصالات للعام 2010–2011"[2]، يشمل مجموعة من المهام مثل تجميع الوسائل والسياسات والإجراءات الأمنية، والمبادئ التوجيهية، واستراتيجيات إدارة المخاطر، والتدريبات والممارسات الأفضل، والتقنيات لحماية البيئة السيبرانية وممتلكات المؤسسات والمستخدمين. [3]

هدف الحماية هو ردع المعتدين أو منعهم من تحقيق أهدافهم، وتحقيق مستوى مقبول من المخاطر من خلال وضع خطة أمن تتناسب مع البيئة التقنية، والبشرية، والتنظيمية، والقانونية. ومع ذلك، فإن الأمن العام الشامل الذي ينطوي على ضمان كامل أمر يصعب تحقيقه. فلكل نظام نقاط ضعف خاصة به تجعل بعض الأشخاص يرون أن قوة النظام تقاس بأضعف نقاط ضعفه.

من المؤكد أيضًا أن اهتمامات الأمن تختلف حسب الموارد والمواد المهددة. فالمواقع التجارية تختلف عن الحكومية، والتي تختلف بدورها عن المواقع المالية والعقارية، والتي أيضًا تختلف عن مواقع الترفيه والمقامرة.

بناء على ذلك، يمكن تعريف الأمن السيبراني، استنادًا إلى أهدافه، بأنه الجهد المبذول لحماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، وذلك لضمان تقليص الخسائر والأضرار المحتملة في حال حدوث المخاطر والتهديدات، وفتح المجال لإعادة الأمور إلى وضعها الطبيعي بأسرع ما يمكن، حتى لا يتوقف الإنتاج ولا تتحول الأضرار إلى خسائر دائمة.[4]

في سياقه العام، يمتلك الأمن تعريفات متعددة تتراوح بين القدرات العسكرية، واستقرار النظام، إلى حماية القيم الأساسية في مجتمع ما. ومع ذلك، بغض النظر عن وجهات النظر الفلسفية والسياسية المتنوعة حول هذا الموضوع، اللافت هو القلق الذي تشعر به معظم الدول في الوقت الحالي حيال تعرض أمنها القومي[5]، بسبب الهجمات السيبرانية. تكنولوجيا المعلومات والاتصالات قد زادت من مستوى الخطر، حيث وفرت مصادر جديدة ومتعددة وموارد ضخمة لتحقيق أهدافها، مع انخفاض فرص تعرض الجهة المعتدية للمخاطر. مؤشرات ذلك يمكن ملاحظتها في التعاون المتزايد بين الأجهزة الأمنية والاقتصادية، بجانب الربط الذي يحدثه قادة العالم بين الأمن السيبراني، والاقتصاد، والأمن القومي.

يتداخل الأمن السيبراني مع الأمن القومي بشكل وثيق جدًا. التكنولوجيا التي فتحت آفاقًا جديدة، أثرت على الثقافة وساعدت في انتشار الثقافة المحلية عالميًا، قد بدأت تهدد الهوية الوطنية والقومية. الأجيال الصاعدة تتأثر بما تصل

---

[1] معاشي، سميرة، "ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني"، العدد السابع جامعة محمد خيضر بسكرة، الجزائر، 2011.

[2] فورة نائلة عادل، "جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية دار النهضة العربية"، القاهرة، مصر، 2014.

[3] "دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات لعام"2010، ص 421.

[4] حسن سعيد عبد اللطيف،" إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت دار النهضة العربية"، القاهرة، ط.4، 2017، ص2014.

[5]) Wayne M. Alder. 2018 "Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim". P. 114.

إليه عبر الإنترنت، مما يجعل الهوية تبدو وكأنها تخضع لعملية إعادة تشكيل بفعل تكنولوجيا المعلومات، حيث يسعى العديد من الأفراد لاستخدامها في بناء مجتمعهم الخاص وأماكنهم الفريدة.

كأي مجال آخر، يعتبر الأمن السيبراني مساحة تضم الأفراد الذين يتمسكون بقيمهم ومصالحهم المختلفة، والتي قد تتأثر أو تؤثر. هناك مؤشرات تشير إلى أن بعض المجموعات ذات المصالح الخاصة قد تهدد بالظهور كبديل لهوية تجمع تحت مظلتها مجتمعات أكبر من الأفراد.

في وقت سابق، اعتبر المسؤول السابق عن الأمن الوطني في الولايات المتحدة، أن الإنترنت قد زادت من مخاطر تعرض النظام لمستويات غير مسبوقة. كان هذا إشارة إلى التهديدات الجديدة التي تستهدف الأمن القومي، والتي يمكن أن تظهر بأشكال غير متوقعة وتمس مجالات حيوية. كما أشار الرئيس الأمريكي الحالي، باراك أوباما، إلى أن الأمن السيبراني يأتي على رأس أولوياته، واعتبر التهديدات من هذا المجال من أخطر القضايا على الصعيد الاقتصادي وأمن الدولة، وقد تمت ترجمة ذلك عمليًا بتعيين مسؤول عن الأمن السيبراني للتواصل والتنسيق المستمر معه، ليكون جزءاً من الأمن القومي والمجلس الاقتصادي الوطني.

في هذا السياق، عرفت التوصية الأوروبية في عام 2002 الأمن القومي بأنه: "أمن الدولة والدفاع والسلامة العامة". وبالتالي، فإن الأمن القومي يشمل جميع الإجراءات القانونية والإدارية والعسكرية والأمنية التي تهدف إلى حماية دولة معينة من أي تهديدات قد تضر بسلامة مواطنيها، وأراضيها، وسيادتها، بما في ذلك حماية بنيتها التحتية الأساسية، وأنظمة الاتصالات والمعلومات.[1]

وعلى المستوى العربي، رغم عدم وجود تعريف شافٍ للأمن القومي، حاولت الأمانة العامة لجامعة الدول العربية تقديم دراسة في عام 1992، حيث تم تعريف الأمن القومي بأنه قدرة الأمة على الدفاع عن أمنها وحقوقها، والحفاظ على استقلالها وسلطتها على أراضيها، وتعزيز القدرات العربية في مجالات السياسة والاقتصاد والثقافة والمجتمع، مستندة إلى القوة العسكرية والدبلوماسية، مع الأخذ في الحسبان الاحتياجات الوطنية لكل دولة، والقدرات المتاحة، والتغيرات الداخلية والإقليمية والدولية التي تؤثر على الأمن القومي العربي.[2]

يظهر بوضوح أنه مع تحول الأنظمة، وتغير أنماط الحروب، وتوازن القوى، تطور مفهوم دور الدولة، وتوسع مفهوم الأمن القومي ليشمل سلامة المواطنين والبلاد، وكذلك الأمن الاقتصادي والاجتماعي والإنساني.[3]

تعتبر الباحثة أن الأمن السيبراني يعد من أهم القضايا التي تعتمد عليها القيادات العليا في أي دولة لتطبيق أساليب التخطيط الاستراتيجي في إدارتها ورسم سياساتها الداخلية والخارجية، بما يتناسب مع تداخل المصالح المرتبطة بالبيئة الداخلية والإقليمية والدولية، مع الانتباه إلى أي تحديات أو تهديدات يمكن أن تؤثر على المصالح الحيوية للأمن الوطني، مما يتطلب وضع سياسات وخطط استراتيجية منسقة لمواجهة تلك التحديات، لضمان تحقيق المكاسب وتفادي أكبر قدر ممكن من الخسائر.

---

(1) EVELYNE, JACQUES (2020). "REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p. 231.

(2) الشهري، علي زايد محمد الجبيري، "الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية"، رسالة (دكتوراه) – جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية، 2019.

(3) حجازي، عبد الفتاح بيومي، "النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي"، الإسكندرية الطبعة الأولى، 2003.

المبحث الثاني: أبعاد الأمن السيبراني

إن الأمن السيبراني يخص جميع المسائل الاقتصادية والاجتماعية والسياسية، والإنسانية وذلك انطلاقًا من التعريف المعطى له، على أنه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم بأمان من جهة أولى، ومن كونه يرتبط ارتباطاً وثيقاً بسلامة مصادر الثروة في العصر الحالي، ونعني بها البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، والإبداع، والقدرة على المنافسة من جهة ثانية[1] لذا، لا بد من التوقف عند أبعاد الأمن السيبراني، على أن نستعرضها كما يلي:

المطلب الأول: الأبعاد القانونية

يعتبر تنظيم الأمن السيبراني من قبل الأفراد والمؤسسات والحكومة أمرًا مهمًا، حيث إن له نتائج قانونية ومتطلبات تستدعي الانتباه نحو ضرورة وضع قواعد خاصة لحل النزاعات التي قد تنجم عنه.

ولذلك، من المهم أخذ بعض التغيرات التي رافقت ظهور مجتمع المعلومات في الاعتبار. بالإضافة إلى الحقوق الأساسية والحريات الإنسانية المنصوص عليها في الدساتير والقوانين الدولية، تم إضافة حقوق جديدة مثل الحق في الوصول إلى الإنترنت العالمي. كما تم توسيع بعض المفاهيم لتشمل طرق جديدة للتفاعل باستخدام تقنيات المعلومات والاتصالات، مثل الحق في إنشاء المدونات الإلكترونية، الحق في تكوين تجمعات عبر الإنترنت، وكذلك الحق في حماية ملكية البرمجيات المعلوماتية.[2]

كذلك، برزت موجبات جديدة، ذات انعكاسات اقتصادية، ومنها على سبيل المثال: موجب الاحتفاظ ببيانات الاتصالات وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى، لما يعنيه هذا الأمر، من كلفة خاصة بحفظ المحتوى وإدارته. ويبقى أن المحور الأساس، في حماية الأشخاص الطبيعيين والمعنويين على السواء، تبقى ضرورة حماية البيانات، لا سيما الشخصية والحساسة منها، إضافة إلى حماية الحق في الخصوصية.

وذلك يضاف إلى ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية، والتجارية، على ضوء الحاجة إلى إعادة صياغتها، بما ينسجم مع توسع استخدام الشبكات الاجتماعية، والمسائل القانونية التي لا بد وأن تثار، على مستوى حماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال والمستخدمين، والملكية الفكرية. فالسنوات القادمة، لا بد وأن تشهد تصاعدًا في أعداد الأعمال الجرمية، والممارسات غير القانونية، في الأمن السيبراني، ما يعني عمليًا، ازدياد عدد القضايا التي سترفع أمام المحاكم، ما يستدعي، إعداد البيئة التنظيمية والتشريعية، وبناء قدرات هيئات المكافحة والحكم. [3]

ومما لا شك فيه، أن النزاعات القانونية ستطاول: الإعلان الذي يرتكز إلى أطياف مستخدمي الإنترنت، انطلاقًا من اهتماماتهم البحثية، أو المواقع التي يزورونها، والاختراقات، والتسريبات للبيانات الشخصية والمالية، سواء منها

---

[1] شمدين عفاف، "الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات"، بدون دار نشر، دمشق، 2013، ص 311.

[2] الشهري، "فايز بن عبد الله، استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت مجلة البحوث الأمنية"، الرياض: كلية الملك فهد الأمنية، مركز الدراسات، 2011.

[3] القهوجي، علي عبد القادر، "الحماية الجنائية للبيانات المعالجة إلكترونياً"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عقد خلال الفترة من 1-3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية، 2013.

المقصودة أو غير المقصودة، ومسؤوليات الجهة التي تملكها، أو تديرها، والحق في تصحيح البيانات الشخصية، ومحوها، وتعديلها.[1]

وترى الباحثة أن على المشرع وضع الاسس التي تحد من مخاطر الخدمات في القطاعات المالية والقطاعات المصرفية أكثر عرضة للهجمات الأمنية، ويتطلب العمل على الخدمات المصرفية عبر الإنترنت مستوى معينًا من المعرفة بتكنولوجيا المعلومات لأن الكثير من تهديدات أمن الإنترنت لا تزال مستمرة، مما يجبر البنوك على اعتماد تدابير جديدة لحماية عملائها من خلال نشر سياسات أمن المعلومات لضمان تجربة مصرفية عبر الإنترنت أكثر أمانًا.

1. الأطر القانونية والتنظيمية

تتركز المخاطر القانونية بشكل رئيسي في عدم وجود الأطر القانونية والتنظيمية المناسبة للتعامل مع النتائج الناتجة عن الأنشطة القانونية وغير القانونية التي تتم في الفضاء السيبراني، يتطلب النشاط الاقتصادي والتجاري تحديدًا دقيقًا للحقوق والواجبات، حيث إن مستخدمي التقنيات عبر هذا الفضاء يحتاجون إلى إطار يحمي استخدامهم. عندما تكون هذه الأطر القانونية غائبة، فإن الجرائم السيبرانية تؤثر سلبًا على العمليات المتعلقة بحقوق الإنسان، وقد تؤدي إلى العنف وتسبب أضرارًا اقتصادية كبيرة. لذا، فإن حماية أصول المعلومات والتكنولوجيا تتطلب إدارة مخاطر الأمن السيبراني بشكل منهجي، وفقًا للسياسات والإجراءات التنظيمية والمتطلبات القانونية.

2. الأمن القانوني وعدم التناقض في القوانين

بناءً على ذلك، تتمثل المخاطر القانونية في غياب الأمن القانوني، أو في وجود تناقضات في القوانين، مما يزيد من مستوى المخاطر بسبب غياب ملاحقة فعالة تتناسب مع طبيعة الأعمال والجرائم السيبرانية التي تتجاوز الحدود. وهذا يؤثر على أي مواطن في أي مكان بالعالم، بالإضافة إلى الدول وأمنها واستقرارها. إن المخاطر التي تواجه الأفراد والدول هائلة وغير محصورة بالأطر القانونية الحالية التي لا تتناسب مع التطورات في الفضاء السيبراني. لذلك، هناك حاجة ملحة للإسراع في تكوين قيادات سيبرانية وزيادة القدرات العسكرية لتشمل النزاعات السيبرانية، مع ضرورة عدم تعارض هذه الجهود مع التشريعات.[2]

3. التعاون الدولي

نظرًا للطبيعة العابرة للحدود لمجتمع الفضاء السيبراني، يعترف قطاع تطوير الاتصالات بأهمية التعاون الدولي لتعزيز الثقة في استخدام تكنولوجيا المعلومات والاتصالات وضمان توفرها وأمان استخدامها. ولذلك، يُعتبر من الضروري دعم الدول لوضع تدابير ملموسة لنظمها الوطنية بالأمن السيبراني، وذلك لمعالجة مخاوف الأطراف المعنية وتشجيع تبادل أفضل الممارسات على المستوى العالمي. بما أن الهجمات السيبرانية يمكن أن تأتي من أي مكان، فإنها تتطلب تعاونًا دوليًا لتحقيق التحقيقات المناسبة والنظم القضائية. من المعروف أن التعاون الدولي يعد أحد المتطلبات الأساسية لضمان الأمن السيبراني عالميًا.

---

[1] عوض محمد محي الدين، "مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات"، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 2009.

[2] منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية"، المركز العربي للبحوث القانونية والقضائية اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٨-٢٧ أغسطس (آب)، ٢٠١٢، ص ٤.

وفي عامي 2003 و2005، اتفقت دول العالم في القمة العالمية لمجتمع المعلومات على ضرورة توفير أدوات فعالة لتعزيز التعاون الدولي بشأن الأمن السيبراني. لذا، ينبغي أن يكون هذا التعاون مدفوعًا بالرغبة المشتركة في السلام والمصالح الملائمة لكل دولة. كما دعا المؤتمر الإقليمي الخامس للأمن السيبراني، المعقد من قبل المركز العربي الإقليمي للاتحاد الدولي للاتصالات، لتنسيق التعاون في المنطقة العربية وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمان في تكنولوجيا المعلومات والاتصالات.[1]

4. تطوير اتفاقيات لمكافحة الجرائم

أدرجت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية ما تعتبره أفعالاً غير قانونية، حيث تناولت الجرائم المتعلقة بسرية الأنظمة والبيانات وسلامتها، وكذلك الجرائم المرتبطة بالأجهزة والمحتوى وحقوق الملكية الفكرية.

5. تقنين سياسات وقائية

تشمل الإجراءات لبناء الثقة والشعور بالأمان في استخدام تكنولوجيا المعلومات والاتصالات، فضلًاعن ضرورة حماية البيانات الشخصية، وهي من الأولويات التي تستدعي التعاون والتنسيق بين الحكومات والمنظمات المعنية والقطاع الخاص. لقد اتخذت معظم الدول المتقدمة خطوات فعالة تتعلق بالسياسات الدفاعية والوقائية ضد الهجمات السيبرانية، حيث خصصت دول مثل الولايات المتحدة الأمريكية وأستراليا والمملكة المتحدة مبالغ كبيرة لتعزيز مسائل الأمن السيبراني. [2]

هذا يدل على مدى اهتمام هذه الدول بترسيخ الثقة والاستقرار، لأن العلاقات الدولية باتت مهددة بسبب الاختراقات والانتهاكات على الشبكات العالمية. ولم يتأخر الجانب الأمريكي في تأسيس قيادة عسكرية جديدة متخصصة في الأمن السيبراني. كما اقترح الاتحاد الدولي للاتصالات وضع خطة وطنية للأمن السيبراني، لكن هذا يتطلب استراتيجية شاملة تشمل مراجعة دقيقة لممارسات الوطنية.[3]

6. إنشاء وحدات خاصة لمكافحة الجرائم

تزايدت الأنشطة العسكرية في هذا المجال، والتي تشمل الحماية وإجراء تدريبات على مستوى الضعف وآليات الرد. وقد صاغت وزارة الدفاع البريطانية استراتيجية خاصة بها حول العمل في الفضاء السيبراني منذ عام 2011م. وقد أعلن رئيس الوزراء، جوردن براون، عن تشكيل وحدة متخصصة لمكافحة الجرائم السيبرانية. على نفس المسار، أنشأت مصر وحدة طوارئ الإنترنت والحاسوب في عام 2012م.

---

[1] منى الأشقر جبور، مرجع سابق، ص6.

[2] حمدون إ. "تورية البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات"، فريق الرصد الدائم لأمن المعلومات الاتحاد العالمي للعلماء، إيرتشه، صقلية، يناير ٢٠١١، ص5.

[3] "تقرير ITU الوثيقة: 14/10RPM–ARB–، قطاع تنمية الاتصالات الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات ٢٠١٠ لمنطقة الدول العربية دمشق الجمهورية العربية السورية"، ١٩–١٧ يناير ٢٠١٠، ص54.

7. تنفيذ القوانين ونجاح التشريعات

في هذا الإطار، يُلاحظ تقاعس بعض الإدارات عن تنفيذ القوانين، كما يتضح في قوانين حماية الملكية الفكرية حيث تنتشر سرقة البرامج بشكل كبير في الدول العربية. يعود ذلك إلى عدم وجود إدارة متخصصة أو ضعف قدرة الإدارة المعنية على المراقبة بسبب نقص الموارد.[1]

ورغم إنشاء بعض مراكز الاستجابة لطوارئ الإنترنت في البلدان العربية، لا يزال بعضها غير فعال بما فيه الكفاية، كما أن القوانين المنسقة حول الجرائم السيبرانية تعزز من التحقيقات وتقديم المجرمين للعدالة. من الضروري القيام بمزيد من الجهود في كل هذه المجالات.

المطلب الثاني: الأبعاد الاجتماعية

تتيح طبيعة الإنترنت المفتوحة، وخاصة من خلال المدونات ووسائل التواصل الاجتماعي، لأي فرد أن يعبر عن آرائه السياسية وطموحاته الاجتماعية بطرق متنوعة. بالإضافة إلى ذلك، إن مشاركة كافة فئات المجتمع ومكوناته تعتبر وسيلة لتعزيز المجتمع وتحسينه، حيث تخلق فرصًا للاطلاع على أفكار ومعلومات جديدة. كما أن هناك حاجة جماعية لضمان استقرار الأمن السيبراني والمجتمع الذي يعتمد عليه. ومن المعروف أن تواصل مجتمع ما مع آخر يسهم في تبادل المعرفة والأفكار، مما يؤدي إلى تشكيل احتياجات جديدة وآفاق للتعاون والتكامل.[2]

علاوة على ذلك، توفر الإنترنت إمكانيات كبيرة للمجالات العلمية والثقافية والخدمية، مما يسهل الوصول إلى مناطق نائية وفئات معينة، مثل كبار السن والمرضى وذوي الاحتياجات الخاصة. بالإضافة إلى ذلك، تلعب الإنترنت دورًا هامًا في تبادل المعلومات أثناء الأزمات الإنسانية والكوارث، حيث تساعد في تأمين المساعدات وتوزيعها swiftly.

ولا تقتصر الأبعاد الاجتماعية على توفير الأمان للمواطن في حياته اليومية واستخدام تكنولوجيا المعلومات والاتصالات في تعزيز نشاطاته، بل تتجاوز ذلك إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، إضافة إلى العادات والتقاليد، عبر إنشاء المجموعات، التي تهتم بنشر الوعي حول هذه المسائل.

في هذا الصدد، تؤكد المنظمات والجهات الدولية على أهمية نشر ثقافة الأمان في مجال الأمن السيبراني، وأهمية تعاون جميع مكونات المجتمع لتحقيق هذه الثقافة وضمانها. لا شك أن التهديدات السيبرانية تؤثر على المجتمع بأسره، سواء كان ذلك نتيجة الاعتماد على الخدمات الأساسية مثل الطاقة والنقل والصحة والاتصالات، أو من خلال المحتوى الذي يتدفق في مجال الأمن السيبراني.

إن المحتويات غير القانونية وغير الملائمة تؤثر بشكل سلبي على قيم المجتمع وتساهم في زيادة الجرائم. وهناك العديد من الأمثلة على ذلك، مثل الإباحية، وترويج المخدرات والدعارة، والإرهاب، وتجنيد الأفراد لأغراض تهدد الأمن والسلام الدوليين. لذلك، يجب علينا بناء مجتمع واعٍ ومدرك لمخاطر العالم السيبراني، يمكنه التعامل مع الحد الأدنى من معايير السلامة، مع وعي بالعواقب القانونية المحتملة لبعض السلوكيات في مجال الأمن السيبراني.[3]

---

[1] خالد كاظم أبو دوح "الأمن السيبراني للدول والأفراد الأمر الذي لا بد منه، المجلة العربية الأمن السيبراني حروب الأرقام الصماء"، ع ٤٩٨، الرياض، السعودية، ٢٠١٨، ص ٣٠.

[2] العنزي، سليمان، "وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير"، الرياض: جامعة نايف العربية للعلوم الأمنية، 2013.

[3] النفروز، علي، "جرائم نظم المعلومات، دار السناء للنشر"، الأردن، عمان، 2017، ص 114.

ويري الباحث أن على مزودي الأمن السيبراني وضع حماية وقوانين تعمل على حماية المجتمعات من جميع مظاهر الاحتيال ومظاهر الاختراق.

لقد جاء في تقرير الاتحاد الدولي للاتصالات (ITU)٢٠١٠ بشأن الأبعاد الاجتماعية للأمن السيبراني أن الثورة الرقمية غيرت كيفية التعامل التجاري وكيفية عمل الحكومات. وأدت العولمة والتقدم التكنولوجي إلى إضعاف البنية التحتية وبالتالي جعلتها هدفاً محتملاً لهجمات إرهابية، حيث تواجه البلدان مخاطر حقيقية للأعداء أن يستغلوا مواطن الضعف التي تعاني منها أنظمة المعلومات الدقيقة. فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومي، وهنا تكمن المخاطر الاجتماعية التي يمكن تفسيرها في ضوء الآتي:[1]

1. تطور الجرائم الإلكترونية وزيادة معدلاتها

مع تزايد استخدام الأنظمة المعلوماتية والأجهزة المتصلة بالإنترنت في الروتين اليومي، يرتفع عدد المستخدمين للفضاء الإلكتروني، مما يؤدي إلى زيادة فرص وقوع الجرائم والانتهاكات. تشمل هذه التهديدات مسائل مثل الفيروسات وهجمات الحرمان من الخدمة، وسرقة البيانات، والبريد الوارد غير المرغوب فيه، والخداع، وكلها تؤثر سلباً على مصداقية تكنولوجيا المعلومات والاتصالات وتعيق عمل المجتمعات.

وقد ذكر تقرير من مؤسسة ماكينزي توقعات بزيادة المعلومات الرقمية بمعدل 44 في المئة بين عامي 2009م و2020م.

ومن المخاطر السيبرانية التي يُتوقع ازديادها في المستقبل، هجوم الفدية، الذي وصفته وزارة العدل الأمريكية بأنه استراتيجية جديدة في عالم الجرائم الإلكترونية. يُعتقد أن المبلغ المدفوع كفدية يقترب من مليار دولار سنويًا، مع توقع أن تتعرض الشركات التجارية لهجمات فدية كل 14 ثانية بحلول عام 2019. ووفقًا للتقارير العالمية، تسبب فيروس الفدية بخسائر مالية تزيد عن خمسة مليارات دولار في عام 2017، وهو رقم مرتفع للغاية لذلك العام. ومن الأمثلة على الهجمات الإلكترونية تلك التي حدثت ضد شبكة الكهرباء في أوكرانيا، مما جعل البلاد تعاني من انقطاع الكهرباء لساعات. [2]

وبهكذا، فإن الحروب الإلكترونية تتجاوز حدود البيانات والمعلومات إلى استهداف البنى التحتية والأنظمة الحيوية مثل المفاعلات النووية وأنظمة الطاقة والمجالات الطبية والنقل، مما يرفع مستوى التهديدات التي تواجه الدول.

من المتوقع أيضًا أن تزداد التحديات والمخاطر في الفترة القادمة، وخاصةً في عام 2016، حيث أظهر تقرير أن الهجوم السيبراني على شركة أرامكو السعودية أدى إلى استبدال خمسين ألف قرص صلب على الحواسيب الخاصة بهم، ولم تتمكن الشركة من استخدام الإنترنت لأكثر من خمسة أشهر تقريبًا. وقد أفاد تقرير لشركة نورتون الأمريكية خلال أغسطس 2016 أن 262،538،686 شخصًا في المملكة كانوا ضحايا لهجمات سيبرانية أو تأثروا بجرائمها، حيث أشار التقرير إلى أن 85% من السكان تعرضوا لهجمات سيبرانية، وهو ما يعكس نسبة أعلى من المتوسط العالمي بعشر مرات.[3]

---

[1] الشواء سامي، "الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي"، القاهرة، 2009، ص28/25.

[2] International Telecommunication Union72Understanding Cybercrime: A Guide for Developing Countries, at ", April 2009.

[3] سندالي، عبد الرزاق (2017) "التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر" 19–20 نيسان المملكة المغربية.

من بين أكبر الاختراقات المعروفة سرقة بيانات حسابات شركة ياهو (Yahoo)، التي شملت ثلاثة مليارات حساب، بالإضافة إلى اختراق إكيفاكس (Equifax) في عام 2017م، الذي أثرّ على 5. 145 مليون عميل. وهذا يُظهر الحاجة الملحة لتعزيز الأمن السيبراني من الناحيتين التقنية والتشريعية، بالإضافة إلى نشر ثقافة المواطنة الرقمية لرفع مستوى الأمان في الفضاء الإلكتروني.

لذا، فقد حذر المسؤولون في مؤتمر أمن المعلومات السنوي في منطقة الشرق الأوسط وشمال أفريقيا لعام 2017 من أن المنطقة تواجه تحديات حرجة تتعلق بحماية المعلومات والبنى التحتية من الهجمات الإلكترونية، مثل التخريب والابتزاز والاحتيال. وتشير التقارير إلى تكرار حوادث اختراق الأنظمة وسرقة البيانات، مثل الاختراق الذي تعرضت له أنظمة سوني، والذي أدى إلى تسرب بيانات مليون مستخدم.

إن ظهور ما يعرف بالويب العميق (Deep Web) وكذلك الويب المظلم (Dark Web) يعقد الأمور، حيث يتم استخدام هذه الشبكات لتعزيز الأنشطة الإجرامية. ومع زيادة أعداد المستخدمين للتكنولوجيا في المنطقة العربية، تتصاعد مستويات الجرائم الإلكترونية، وتظهر مجموعة من السلوكيات السلبية مثل التنمر والاحتيال والابتزاز الإلكتروني، وهي مشاكل اجتماعية متعددة. لقد تطورت الصراعات في الفضاء الإلكتروني، وأصبحت تمثل تهديداً أكبر للأمن القومي من النزاعات المباشرة. كما كشفت دراسة حديثة أن أكثر من 65% من محترفي تكنولوجيا المعلومات في دول مجلس التعاون الخليجي يعتقدون أن المنطقة هدف رئيسي للجرائم الإلكترونية.

في النهاية، يظهر الوضع الحالي أن الفضاء الإلكتروني أصبح يشكل تهديدًا حقيقيًا في ظل غياب الرقابة الفعالة. لمكافحة جميع أشكال الجرائم الإلكترونية مثل الابتزاز والفدية والتجسس والاعتداءات، يجب تنفيذ سياسات أمن سيبراني قوية وأنظمة حماية فعالة.[1]

2. استهداف الأمن القومي

يلاحظ أن التهديدات الأمنية قد ازدادت بطرق متسارعة لم يشهدها العالم من قبل حتى شملت السياحة والتجارة والاقتصاد، وطالت أمن الدول والمجتمعات.[2]

وفي هذا الخصوص، أشار تقرير صادر عن وكالة الأمن القومي الأمريكي إلى أن هناك ٢٣٢ جهاز حاسب آلي تتعرض لاختراقات وهجمات سيبرانية في كل دقيقة على امتداد العالم مما أضاف صعوبة عالية في المقدرة على اللحاق بمجرمي السيبر تقنيًا وفنيًا. كما أكدت الدراسات التي أصدرها الاتحاد الدولي للاتصالات (ITU) في يوليو ٢٠١٧ أن هناك ضرورة ملحة في مجالات التعليم والتدريب والدراسات لرفع مستوى المهارات والمعرفة في الأمن، هذا إلى جانب إن هناك أربع فئات رئيسة للتهديدات السيبرانية للأمن القومي هي:

الحرب السيبرانية والتجسس الاقتصادي، وهما يرتبطان الى حد كبير بالدول وفئة الجريمة السيبرانية، والإرهاب السيبراني، اللذين يرتبطان في الأغلب بجهات فاعلة غير تابعة لدولة معينة.

---

[1] السراج، عبود، "مفهوم جرائم المعلوماتية، واقع وآفاق بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية الذي نظمته الجامعة الأردنية واتحاد المحامين العرب خلال الفترة 18-19 كانون الثاني عام "2013.

[2] البشري محمد أمين، "التحقيق في الجرائم المستحدثة، الرياض جامعة نايف العربية للعلوم الأمنية"، مركز الدراسات والبحوث، 2014.

3. تهديد القيم والأخلاق

ومن الأبعاد الاجتماعية الحماية من تدنى المستويين القيمي والأخلاقي فالمحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبي على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين.[1]

وعليه، لا بد من بناء مجتمع مسئول، ومدرك لمخاطر الفضاء السيبراني، قادر على التعامل مع قواعد السلامة ومدرك للعواقب القانونية، التي يمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات ورؤوس الأموال.

الخاتمة

يتضح من خلال تناول مفهوم الأمن السيبراني من الناحيتين اللغوية والاصطلاحية أنه يمثل منظومة متكاملة تهدف إلى حماية الفضاء الرقمي من كافة المخاطر والتهديدات التي قد تطال البيانات والأنظمة والشبكات كما يتضح أن تطور التكنولوجيا والاعتماد الكبير على الوسائط الرقمية في مختلف مجالات الحياة جعل الأمن السيبراني ضرورة ملحة للحفاظ على استقرار المجتمعات وضمان استمرارية الخدمات الحيوية.

ومن خلال استعراض الأبعاد القانونية للأمن السيبراني تبين أن الإطار التشريعي يلعب دورًا محوريًا في مواجهة الجرائم الإلكترونية وتحديد المسؤوليات ووضع العقوبات اللازمة بما يتوافق مع طبيعة الفضاء الرقمي بينما أبرزت الأبعاد الاجتماعية أن وعي الأفراد والمؤسسات يمثل خط الدفاع الأول في تعزيز أمن المعلومات وتقليل فرص الاختراق أو الاستغلال غير المشروع. ومن ثم فإن الأمن السيبراني ليس مجرد مسألة تقنية، بل هو قضية قانونية ومجتمعية تتطلب تكاملًا في الجهود بين التشريعات والممارسات الاجتماعية. وفي ظل التهديدات المتزايدة فإن بناء بيئة رقمية آمنة يستلزم مزيجًا من التشريعات الفعالة والتوعية المستمرة لضمان تحقيق الأمن والاستقرار في الفضاء الإلكتروني وحماية المصالح الوطنية والتنموية.

النتائج

1. الأمن السيبراني مفهوم متعدد الأبعاد يجمع بين الجوانب التقنية والقانونية والاجتماعية.
2. التشريعات والسياسات القانونية تشكل أساسًا لمواجهة الجرائم الإلكترونية وحماية البيانات.
3. الوعي المجتمعي والممارسات الآمنة عنصر أساسي في تعزيز الحماية الرقمية.

التوصيات

1. تطوير الأطر التشريعية بما يواكب التغيرات السريعة في الجرائم السيبرانية.
2. تعزيز برامج التثقيف الرقمي لرفع الوعي لدى الأفراد والمؤسسات.

[1] رستم هشام، "جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين"، مجلة الدراسات القانونية، جامعة أسيوط، عدد 17 القاهرة، 2009.

3. تشجيع التعاون الدولي لتبادل الخبرات وأفضل الممارسات في مواجهة التهديدات الإلكترونية.

قائمة المصادر

أولا: المراجع العربية

1. خاطر، نوري حمد، حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، بحث منشور في مجلة المنارة العدد (2) كانون ثاني جامعة آل البيت، المفرق، 2012، ص 35
2. إيفانز غراهام نوينهام جيفري، قاموس بنغوين للعلاقات الدولية: الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004، ص200.
3. منى الأشقر جبور، السيبرانية هاجس العصر، بيروت: جامعة الدول العربية – المركز العربي للبحوث القانونية والقضائية، 2016 150 ص
4. جبور، منى الاشقر، السيبرانية، هاجس العصر، جامعة الدول العربية، القاهرة، مصر، 2018، ص 241.
5. رستم هشام محمد خليل، الجوانب الإجرامية للجوانب المعلوماتية، مجلة الأمن والقانون عدد 2 شرطة دبي، دبي، الامارات العربية المتحدة، 2012،
6. دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات، لعام 2010، ص 314
7. الرومي، محمد أمين، جرائم الكمبيوتر والأنترنت دار المطبوعات الجامعية، الإسكندرية، مصر، 2013، ص 7.
8. الشهري، حسن بن أحمد، قانون دولي موحد لمكافحة الجرائم الإلكترونية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف للعلوم الأمنية، المملكة العربية السعودية، العدد 27، العدد 53 رجب 1432هـ.
9. معاشي، سميرة، ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، العدد السابع جامعة محمد خيضر بسكرة، الجزائر، 2011.
10. فورة نائلة عادل، جرائم الحاسب الاقتصادية دراسة نظرية وتطبيقية دار النهضة العربية، القاهرة، مصر، 2014، ص 9.
11. دليل الأمن السيبراني للبلدان النامية الاتحاد الدولي للاتصالات لعام 2010، ص 421.
12. حسن سعيد عبد اللطيف، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت دار النهضة العربية، القاهرة، ط.4، 2017، ص2014.
13. الشهري، علي زايد محمد الجبيري، الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة (دكتوراه) – جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية، 2019.
14. حجازي، عبد الفتاح بيومي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية الطبعة الأولى، 2003.

15. شمدين عفاف، الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات، بدون دار نشر، دمشق، 2013، ص 311.
16. الشهري، فايز بن عبد الله، استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الإنترنت مجلة البحوث الأمنية، الرياض: كلية الملك فهد الأمنية، مركز الدراسات، 2011.
17. القهوجي، علي عبد القادر، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت والذي عقد خلال الفترة من 1–3 مايو، كلية الشريعة والقانون، جامعة الإمارات العربية، 2013.
18. عوض محمد محي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 2009.
19. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٨–٢٧ أغسطس (آب)، ٢٠١٢، ص ٤.
20. حمدون إ. تورية البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، فريق الرصد الدائم لأمن المعلومات الاتحاد العالمي للعلماء، إيرتشه، صقلية، يناير ٢٠١١، ص5.
21. تقرير ITU الوثيقة: 14/10RPM–ARB–، قطاع تنمية الاتصالات الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات ٢٠١٠ لمنطقة الدول العربية دمشق الجمهورية العربية السورية، ١٩–١٧ يناير ٢٠١٠، ص54.
22. خالد كاظم أبو دوح الأمن السيبراني للدول والأفراد الأمر الذي لا بد منه، المجلة العربية الأمن السيبراني حروب الأرقام الصماء، ع ٤٩٨، الرياض، السعودية، ٢٠١٨، ص ٣٠.
23. العنزي، سليمان، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية، 2013.
24. النقروز، علي، جرائم نظم المعلومات، دار السناء للنشر، الأردن، عمان، 2017، ص 114.
25. الشواء سامي، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث في مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 2009، ص28/25.
26. سندالي، عبد الرزاق (2017) التشريع المغربي في مجال الجرائم المعلوماتية، ضمن أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر 19–20 نيسان المملكة المغربية.
27. السراج، عبود، مفهوم جرائم المعلوماتية، واقع وآفاق بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية الذي نظمته الجامعة الأردنية واتحاد المحامين العرب خلال الفترة 18–19 كانون الثاني عام 2013.
28. البشري محمد أمين، التحقيق في الجرائم المستحدثة، الرياض جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، 2014.

29. رستم هشام، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، ورقة عمل مقدمة إلى اللجنة العلمية لإعداد التقرير الوطني المصري لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجرمين، مجلة الدراسات القانونية، جامعة أسيوط، عدد 17 القاهرة، 2009.

ثانيا: المراجع الأجنبية

1. Wayne M. Alder (2018). Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim. P. 114.
2. EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p. 231.
3. EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p. 231.
4. Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009.
5. EVELYNE, JACQUES (2020) REGULATING CYBERSECURITY What civil liability in case of cyber-attacks p. 231.
6. Understanding Cybercrime: A Guide for Developing Countries, at 72, International Telecommunication Union, April 2009.