Malaysian Journal of Syariah and Law
مجلة الشريعة والقانون بماليزيا

Vol. 13, No. 2, pp. 456-475 | AUGUST 2025
DOI: https://doi.org/10.33102/mjsl.vol13no2.1036

التحديات القانونية للخطر السيبراني على المعاملات التجارية

LEGAL CHALLENGES OF CYBER RISK ON COMMERCIAL TRANSACTIONS

[i]Alaa Hussein Ali, [i]Wurood Khalid Mohameed & [ii,]*Mahmood Shaker Alaloosh,

[i]Faculty of Law, University of Anbar, Ramadi 31001, Anbar Governorate, Iraq
[ii]Faculty of Management and Economics, University of Kirkuk, Kirkuk 36001, Kirkuk Governorate, Iraq

*(Corresponding author) e-mail: mahmoodshaker@uokirkuk.edu.iq

Article history:
Submission date: 24 October 2024
Received in revised form: 9 April 2025
Acceptance date: 16 May 2025
Available online: 31 August 2025

Keywords:
Cyber risk, cybersecurity, electronic commercial transactions, cyber risk insurance, al-khaṭar as-sībirānī, al-amn as-sībirānī, al-muʿāmalāt at-tijārīyah al-iliktrūnīyah, at-taʿmīn ʿalā al-makhāṭir as-sībirānīyah

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Ali, A. H., Mohameed, W. K., & Alaloosh, M. S. (2025). Al-taḥaddiyāt al-qānūniyyah lil-khaṭar al-saybirānī ʻalā al-muʻāmalāt al-tijārīyah: Legal challenges of cyber risk on commercial transactions. *Malaysian Journal of Syariah and Law*, *13*(2), 456-475. https://doi.org/10.33102/mjsl.vol13no2.1036

ABSTRACT

Cyber risk has become one of the most prominent threats facing modern societies, as attackers rely on cyberspace to carry out illegal cyber-attacks targeting sensitive data and information. These attacks, which are increasing with the digital transformation and the spread of electronic commercial transactions, pose significant challenges in both cybersecurity and legal domains. While cyber risk differs from traditional risks by being intangible and invisible, its impact can be widespread on individuals, companies, and institutions. This research aims to shed light on the legal challenges associated with cyber risk and its impact on electronic commercial transactions. The study addresses how to confront these challenges by analyzing the available legal mechanisms and exploring solutions that may mitigate the effects of cyber-attacks. It also focuses on the importance of enhancing cybersecurity, which is a fundamental means to protect information and commercial transactions in the digital age, emphasizing the need to provide both technical and human resources to achieve it. The research employed a descriptive and analytical approach to study the phenomenon of "cyber risk", define its dimensions, and explore ways to address it. Additionally, the concept of "cybersecurity" was analyzed from multiple perspectives, including the technical and legal challenges that hinder its effective realization. The study arrived at several important findings, including that cyber risk constitutes an invisible threat that is often discovered after a certain period, making it more difficult to counteract. Achieving cybersecurity requires significant human and technical resources to minimize these attacks. Moreover, the study pointed out the difficulties faced by insurance companies in dealing with cyber risk insurance, as they have cautiously begun insuring it due to its complexities. The study recommended several proposals to combat cyber risk, including the development of national cybersecurity strategies, strengthening the infrastructure of information and communication systems, and raising awareness among individuals and companies about the importance of cybersecurity and the necessity of using technology safely and effectively.

ملخص البحث

أصبح الخطر السيبراني من أبرز التهديدات التي تواجه المجتمعات الحديثة، حيث يعتمد المهاجمون على الفضاء السيبراني لتنفيذ هجمات إلكترونية غير قانونية تستهدف البيانات والمعلومات الحساسة. هذه الهجمات، التي تتزايد مع التحول الرقمي وانتشار المعاملات التجارية الإلكترونية، تشكل تحديا كبيرا في مجالات الأمن السيبراني والقانوني على حد سواء. ومع أن الخطر السيبراني يختلف عن المخاطر التقليدية بكونه غير ملموس وغير مرئي، فإن تأثيره يمكن أن يكون واسع النطاق على الأفراد والشركات والمؤسسات. يهدف هذا البحث إلى تسليط الضوء على التحديات القانونية المرتبطة بالخطر السيبراني وتأثيره على المعاملات التجارية الإلكترونية. يتناول البحث كيفية مواجهة هذه التحديات من خلال تحليل الآليات القانونية المتاحة والبحث عن حلول يمكن أن تقلل من تأثير الهجمات السيبرانية. كما يركز على أهمية تعزيز الأمن السيبراني، الذي يشكل وسيلة أساسية لحماية المعلومات والمعاملات التجارية في العصر الرقمي، مع التأكيد على ضرورة توفير الموارد التقنية والبشرية لتحقيقه. اعتمد البحث على المنهج الوصفي والتحليلي في دراسة ظاهرة "الخطر السيبراني" وتحديد أبعاده وسبل التصدي له. كما تم تحليل مفهوم "الأمن السيبراني" من جوانب متعددة، بما في ذلك التحديات التقنية والقانونية التي تعيق تحقيقه بفعالية. توصلت الدراسة إلى عدة نتائج مهمة، منها أن الخطر السيبراني يشكل تهديدا غير مرئي يكتشف بعد مرور وقت معين على حدوثه، مما يزيد من صعوبة التصدي له. كما أن تحقيق الأمن السيبراني يحتاج إلى موارد بشرية وتقنية كبيرة للحد من تلك الهجمات. بالإضافة إلى ذلك، أشارت الدراسة إلى الصعوبات التي تواجه شركات التأمين في التعامل مع التأمين على المخاطر السيبرانية، حيث بدأت هذه الشركات تدريجيا في التأمين عليه بحذر، نظرا لتعقيداته. أوصت الدراسة بعدة مقترحات للتصدي للخطر السيبراني، منها وضع استراتيجيات وطنية للأمن السيبراني، وتعزيز البنى التحتية لنظم المعلومات والاتصالات، ونشر الوعي بين الأفراد والشركات حول أهمية الأمن السيبراني وضرورة استخدام التكنولوجيا بشكل آمن وفعال.

مقدمة

في عصرنا الرقمي المتسارع، أصبح التهديد السيبراني واحدا من أبرز التحديات التي تواجه المجتمعات الحديثة على الأصعدة الاقتصادية والاجتماعية والأمنية. فقد أدى الاعتماد المتزايد على التكنولوجيا في مختلف جوانب الحياة إلى ظهور الفضاء السيبراني كبيئة جديدة تتجاوز قيود الزمان والمكان. هذا الفضاء يوفر فرصا كبيرة للنمو والتطور، لكنه في الوقت نفسه أصبح ساحة واسعة للنشاطات غير القانونية. حيث تستغل جماعات وأفراد هذا الفضاء الرقمي لتنفيذ هجمات سيبرانية تهدف إلى تحقيق مصالح خاصة، متجاوزين الحدود الجغرافية والسياسية.

لم تعد الجرائم الإلكترونية مجرد تهديدات محتملة، بل أصبحت ظاهرة متزايدة ومتعددة الأبعاد تتوسع باستمرار. لم تقتصر هذه الجرائم على سرقة المعلومات أو اختراق الأنظمة فحسب، بل تطورت لتشمل هجمات واسعة النطاق تؤثر على البنى التحتية الحيوية للدول والشركات الكبرى، مما يعرض الأمن القومي والاقتصاد العالمي للخطر. ومع تقدم تقنيات الذكاء الاصطناعي وإنترنت الأشياء، أصبح تعقيد هذه الجرائم أكبر، مما يجعل من الصعب اكتشاف الجناة والتصدي لهم بالأساليب التقليدية.

الانتقال من المجتمع التقليدي إلى المجتمع الرقمي، ومن الفضاء المادي إلى الفضاء الافتراضي، أوجد واقعا جديدا يستدعي استجابات قانونية وأمنية متطورة. هذا الفضاء الافتراضي يتجاوز الحدود القومية، مما يزيد من التحديات المرتبطة بملاحقة مرتكبي الجرائم السيبرانية وتقديمهم للعدالة. ومع تزايد معدلات الجرائم السيبرانية وارتفاع أعداد مرتكبيها، أصبحت هذه الجرائم من أخطر التهديدات التي تواجه المجتمعات في القرن المقبل.

في ظل هذا الواقع الجديد، أصبح من الضروري تعزيز القدرات التقنية لمكافحة هذه الجرائم، بالإضافة إلى تطوير إطار قانوني وتنظيمي دولي يتماشى مع التحديات التي يفرضها الفضاء الرقمي. تهدف هذه الدراسة إلى استكشاف التداعيات القانونية للعصر الرقمي وفهم كيفية التصدي للتحديات السيبرانية التي تؤثر بشكل مباشر على المعاملات التجارية والاقتصادية على المستويين الوطني والدولي.

تكمن أهمية هذا البحث في تزايد المخاطر السيبرانية على الشركات والمؤسسات نتيجة الانتشار الواسع لاستخدام التكنولوجيا. هذا الخطر بلا شك له تأثير كبير على المعاملات التجارية الإلكترونية بشكل عام، ومن هنا تبرز الحاجة إلى البحث عن حلول وآليات تحد من هذه المخاطر. سنتناول في هذا البحث التحديات التي تواجه هذا المجال على الرغم من صعوبتها.

تتمثل مشكلة البحث في صعوبة مواجهة ومعالجة الخطر السيبراني وإيجاد حلول وآليات قانونية وتقنية تحد منه بسبب طبيعته الرقمية والافتراضية (Rosley *et al.*, 2023). وعلى الرغم من التحديات الكبيرة التي تفرضها هذه الظاهرة، من الضروري الوقوف على مدى فعالية الآليات المستخدمة حاليا لمواجهتها، خاصة وأن الجناة في هذه الهجمات السيبرانية غالبا ما يكونون مجهولين، مما يصعب من تحقيق الأمن السيبراني والحفاظ على الاقتصاد، لا سيما في إطار المعاملات التجارية الإلكترونية.

نهدف من خلال هذا البحث إلى تسليط الضوء على الخطر السيبراني والأمن السيبراني، وفهم التحديات القانونية التي تواجه المجتمعات في سبيل تحقيقه، بالإضافة إلى استكشاف الآليات القانونية التي يمكن أن تحد من المخاطر السيبرانية في المعاملات التجارية.

منهجية البحث

سيعتمد هذا البحث على المنهج الوصفي والتحليلي للوصول إلى فهم شامل لظاهرة "الخطر السيبراني" و"الأمن السيبراني"، وتحليل التحديات المرتبطة بهما. سنقوم في الجزء الوصفي بتحديد المفاهيم الأساسية المرتبطة بالموضوع، من خلال مراجعة الأدبيات والتشريعات المعنية بالجرائم السيبرانية والأمن السيبراني، مع توضيح نشأة وتطور هذه الظواهر في السياق الرقمي المعاصر. كما سنستعرض أنواع الهجمات السيبرانية وتحديد الفئات الأكثر استهدافا وتأثير هذه الهجمات على المستويات الاقتصادية والاجتماعية والأمنية. أما في الجانب التحليلي، سنقوم بدراسة التحديات القانونية والتقنية التي تعيق تحقيق الأمن السيبراني، مع التركيز على العوائق التي تواجه الدول في مواجهة هذه التهديدات بسبب الطبيعة العابرة للحدود للفضاء السيبراني. ختاما، سيساعد هذا المنهج في تحقيق هدف البحث، وهو فهم العلاقة بين الخطر السيبراني والأمن السيبراني، وتحديد الأدوات والآليات القانونية التي يمكن من خلالها تعزيز الأمن في الفضاء الرقمي.

المفهوم القانوني للخطر والأمن السيبراني

يتطلب البحث بمفهوم الخطر السيبراني التعريف به، وإذا ماتم ذلك يجدر بنا التطرق الى التعريف بالأمن السيبراني.

التعريف بالخطر السيبراني

يعد الخطر السيبراني من الأخطار التي أنتجها العالم الافتراضي نتيجة تزايد استخدام شبكات الإنترنت في مختلف دول العالم، إلا أن استخدامها قد لا يكون بالشكل القانوني الصحيح، وهذا الخطر يعد من الأخطار الحديثة نسبيا فلا بد من تعريفه، كما أن هذا الخطر يتميز بخصائص معينة وهو ما سنتناوله.

تعريف الخطر السيبراني

يعرف الخطر السيبراني بأنه "آثار انتهاك البيانات بدون الهجوم على نظام المعلومات، أو آثار الهجوم على نظام المعلومات أي الدخول غير المشروع لنظام المعلومات (Samia Tibah, 2018)، وهناك من عرفه بأنه "تصرف يدور في العالم الافتراضي القائم على استخدام البيانات الرقمية ووسائل اتصال تعمل إلكترونيا، فهو هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، يهدف تعطيل أو إتلاف أو الاستحواذ على البيانات المتوفرة فيها (Al-Fatlawi, 2016).

ويعرف أيضا بأنه "تعبير جامع يشمل جميع الأفعال المرتكبة ضد بيانات أو نظم حاسوبية او باستخدامها، فهو بذلك يشمل الجرائم المرتكبة بحق المعلومات الحاسوبية أو استخدام موارد المعلومات لأغراض غير مشروعة (Addan, 2012).

كما عرف بأنه المخاطر التي تواجه المستخدمين مهما كان نوعهم سواء أفراد أو جماعات أو غيرها على الإنترنت (Walia, 2023; Ghaql & Zakrir, 2023). بينما عرفه البعض الآخر بأنه هجمات يتم تنفيذها بواسطة أجهزة الحاسوب عبر شبكات الإنترنت والاتصالات الرقمية بهدف تغيير أو تعطيل برامج أو تدمير معطيات أو سرقة معلومات أو اختراق أنظمة التحكم والأوامر، والعمل على إحداث أضرار في أنظمة وبرامج وأجهزة الطرف الآخر وتعطيلها عن العمل ، وغالبا ما تستهدف هذه الهجمات البنية التحتية للدول، ومحاولة إحداث أكبر الأضرار بها، ومحاولة إصابتها بالشلل التام؛ كي تعجز عن تقديم الخدمات للسكان (Ben Zrarah & A'rab, 2023).

وقد عرف الخطر السيبراني بوصفه جريمة سيبرانية بأنه ذلك النوع من النشاط الإجرامي الذي تستخدم فيه تقنيات الحاسوب الآلي، بطريقة مباشرة أو غير مباشرة، والهدف من ذلك النشاط الإجرامي تنفيذ الفعل الإجرامي المقصود (Ben Brughouth, 2023).

ويمكن أن يعرف الباحث الخطر السيبراني أنه "انتهاك للبيانات والخصوصية من خلال الهجوم على أنظمة المعلومات بدخول غير مصرح به، بهدف سرقة معلومات أو تعطيل برامج أو إتلافها وتدميرها".

خصائص الخطر السيبراني

يتميز الخطر السيبراني بخصائص وأسس فنية تختلف عن المخاطر التقليدية (Baghdadi, 2023)، ويمكن أن نجمل تلك الخصائص بما يأتي:

الأخطار السيبرانية أخطار مترابطة

إذ إن ترابط أنظمة وأجهزة الإعلام الآلي مع ترابط المستخدمين من شأنه أن يزيد من غموض هذا النوع من الأخطار، كما أن ترابط تلك الأنظمة والأجهزة يزيد من ترابط الأخطار السيبرانية ومن ثم هناك صعوبة بفصلها.

الأضرار الناشئة عنه يمكن أن تزيد مستقبلا

فيلاحظ بأن الأضرار والكوارث التي يخلفها الخطر السيبراني أضرار غير ثابتة ومحددة بداية، كما في الأضرار التي تخلفها الأخطار التقليدية التي يمكن حصرها.

يعد من الأخطار الديناميكية

تنتج الكوارث والمخاطر السيبرانية بنسبة ٩٠٪ لسببين: الأول: خطأ الإنسان، والثاني: سلوك الإنسان، فمن غير الممكن التنبؤ بسلوك الإنسان العمدي "الجريمة" وغير العمدي "الخطأ" في هذا النوع من الأخطار التي تكون سببا لوقوع وخطورة الكثير من الأضرار والكوارث السيبرانية، فقد يكون خطأ معالجة بيانات أو احتمالية سرقة، كل ذلك يجعل من الأخطار السيبرانية أكثر تشعبا وتنوعا قياسا على الأخطار الأخرى.

صعوبة تقييم الخسائر الناتجة عنه

تلحق الأخطار السيبرانية بالضحية سواء أكانوا أفرادا أم شركات أم دولا خسائر مالية كبيرة، وأضرارا فعالة، إلا أن تلك الخسائر يصعب تقييمها، ونرى أن ذلك يكون بسبب طبيعة الأخطار السيبرانية غير الملموسة وغير المرئية، بخلاف الخسائر الناتجة عن الأخطار التقليدية المعروفة التي يمكن تقييمها وتحديدها بدقة ويسهل اكتشافها (كالحريق، والسرقة، والصواعق)، أما الخطر السيبراني فلا يتم اكتشافه عادة إلا بعد مدة زمنية معينة، وأحيانا لا يكتشف الضحية أنه قد تعرض لهجمة أو خطر سيبراني أصلا.

عدم وجود قاعدة بيانات إحصائية تتعلق بالخسائر الناتجة عنه

يلاحظ صعوبة إيجاد قاعدة بيانات تتعلق بالمخاطر السيبرانية والأضرار والكوارث الناتجة عنها؛ وذلك بسبب أن الأخطار السيبرانية تنصب على البيانات والمعلومات الخاصة بالأفراد والشركات والمؤسسات وهذه قد تمنع التصريح بكل المعلومات والتفاصيل التي تتعلق بالأضرار التي تخلفها الهجمات السيبرانية، كون تلك المعلومات قد ترتبط بأمور اقتصادية فعالة لتلك الجهات، وهذا ينعكس في النهاية على صعوبة توفر قاعدة بيانات بشأن ذلك.

يتميز بكونه خطرا صعب التأمين عليه من حيث الأصل

وذاك بسبب عدم توفر الشفافية في العلاقة بين المؤمن له والمؤمن، إذ إن التأمين من الخطر السيبراني تكون المعلومات هي محل الأشياء المؤمنة وتتميز بالحساسية، لذا فإن المؤمن له عادة لا يريد التصريح بتلك المعلومات لشركة التأمين كونها ذات قيمة اقتصادية.

صعوبة تحديد مصدر الخطر

يعد صعوبة تحديد مصدر الهجوم السيبراني وتعقبه من أبرز خصائص الخطر السيبراني، حيث تكمن الخطورة في تعذر معرفة هوية الفاعل أو الجهة المنفذة، مما يصعب من إجراءات الضبط والملاحقة أو تحميل المسؤولية، لا سيما إذا كان الفاعل دولة. كما أنه في كثير من الحالات، قد ينفذ الهجوم دون أن يكشف أو يعرف مدى الضرر وحجم المعلومات التي تم اختراقها، وقد تنحصر نتائج التحقيقات في تحليلات وتكهنات دون وجود دليل مادي أو تقني قاطع على هوية المعتدي (Abdul Hamid, 2023).

التعريف بالأمن السيبراني

يعد الأمن السيبراني ركيزة من ركائز السياسة الجنائية الأمنية نتيجة لأهمية الدور الذي يلعبه في تحقيق استقرار المعاملات والأمن بصورة عامة، لذا كان لزاما أن نعرف الأمن السيبراني، ومن ثم نعرج على أهميته.

تعريف الأمن السيبراني

يشهد العالم تطورا كبيرا في وسائل الاتصال، وبالمقابل هناك استخدام غير مشروع من قبل بعض مستخدمي الشبكة العنكبوتية، الأمر الذي أدى إلى ظهور جرائم من نوع خاص وهي جرائم عابرة للحدود والقارات تختلف عن الجرائم التقليدية وتسمى ب"الجرائم الإلكترونية" أو "جرائم المعلوماتية" أو "الجرائم المستحدثة" أو "الجرائم السيبرانية" (Kotaf, 2022) وتشكل تحديا لما يسمى بالأمن السيبراني، وتعرف كلمة سيبرانية بأنها "علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل (Attia, 2019).

ويعرف الأمن السيبراني بأنه "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة التي تستهدف البيانات (Shammari, 2020).

ويعرف أيضا بأنه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توفر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني (Siwan & Al-Fatlawi, 2015).

كما عرف الأمن السيبراني بأنه "ممارسة الدفاع عن أجهزة الحاسوب والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة أو هو أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنيت" (Jboor al-Ashqar, 2017).

ويعرف بأنه "كافة الإجراءات التنظيمية التي تؤمن الحماية الكافية للمعلومات بجميع أنواعها وأشكالها سواء كانت إلكترونية أو مادية من مختلف المخاطر والهجمات والجرائم وأفعال التخريب والتجسس والحوادث (Berghouth, 2023). وهناك من عرفه بأنه "الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، ومنها الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات (Amoroso, 2007)، ويرى البعض الآخر بأن الأمن السيبراني هو عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة (Kemmerer, 2003).

ونلاحظ من التعريفات أعلاه بأن أجهزة الأمن السيبراني لها القدرة على ردع الجرائم السيبرانية أو الحد منها أو التقليل من وقوعها، ويمكن أن يعرف الباحث الأمن السيبراني بأنه مجموعة الوسائل والإجراءات التقنية المتخذة للحد أو التقليل من الهجمات السيبرانية التي يقوم بها القراصنة على أجهزة الحاسوب وجميع الأجهزة المتصلة بالإنترنت، وحماية المعلومات وخصوصية البيانات للأفراد والشركات والمؤسسات والدول بصورة عامة.

أهمية الأمن السيبراني

أصبحت التوعية بأهمية الأمن السيبراني ضرورة ملحة لمكافحة الجريمة السيبرانية، من أجل تحقيق الأمن السيبراني بشكل فعال للحد من الخطر السيبراني وتوفير الحماية من اختراق البيانات التابعة للدول أو للشركات أو المؤسسات عموما (Ben Khadra & Bouzidaf, 2024; Wan Ismail *et al.,* 2024).

يلعب الأمن السيبراني دورا مهما في تنمية تكنولوجيا المعلومات، فحماية البنى التحتية وتعزيز توفير الأمن السيبراني يعدان عنصرين مهمين لكل دولة وتحقيق رفاهها الاقتصادي، وبذلك باتت حماية المستهلكين وأمن المعلومات الإلكترونية عبر شبكات الإنترنت جزءا لا يتجزأ من سياسات الدول عموما؛ لما لها من أثر اقتصادي جلي (Gerke, 2012).

ويعد ردع الجرائم السيبرانية الواقعة على المنتج والمستهلك عند إجراء المعاملات التجارية الإلكترونية من العناصر المهمة للأمن السيبراني، إذ من خلاله يمكن اتخاذ الإجراءات القانونية اللازمة وتوفير الوسائل المناسبة لحماية بيانات العملاء المستهلكين والمنتجين من أي اختراق أو هجوم سيبراني يقوم به القراصنة من خلال تعطيل نظام المعلومات أو سرقة البيانات أو المعلومات الشخصية أو تشفيرها بحيث لا يمكن لأطراف المعاملة التجارية فكها (Lkhweider & Mashtoub 2018).

ونرى بأن اهتمام الدولة بتعزيز الأمن السيبراني بصورة عامة وفي إطار المعاملات التجارية على وجه الخصوص له أهمية كبيرة كونه يحقق الحماية للأفراد والشركات وللمعلومات التي تتعلق بنشاطهم التجاري، فيوفر الأمان لهم وهذا يؤدي إلى سهولة وكثرة إجراء المعاملات التجارية الإلكترونية، ومن شأن ذلك تطور اقتصاد البلد.

وعليه لا بد من التركيز على توفير الأمن السيبراني في شتى المجالات من خلال البحث عن آليات فعالة تحدد أو تقلل على الأقل من الهجوم السيبراني الذي يشنه المخترقون على الأشخاص أو المؤسسات أو الشركات مما يعرضهم إلى أضرار بالغة وخسائر مالية كبيرة لربما تصل في بعض الأحيان إلى مستوى الخسائر التي تخلفها الكوارث الطبيعية.

إن غاية وهدف الأمن السيبراني هو توفير الحماية للأفراد والمؤسسات والشركات من خلال المحافظة على مواردها المالية، والبشرية، والتقنية، والتنظيمية، والمعلوماتية، بحيث تتمكن من أداء وإنجاز مهامها، وضمان عدم تعرضها للضرر من خلال الحد أو التقليل من التهديدات السيبرانية (Abdullah, 2023).

لذا كان توفير التدابير القانونية والآليات التقنية والإجرائية أمرا لا بد منه يقع على عاتق المجتمع الدولي عموما، فلا بد من أن تتعاون الدول فيما بينها من أجل التوصل إلى أفضل الحلول وأنجع المعالجات لمواجهة هذا الخطر العابر للقارات والحدود.

التحديات القانونية لتحقيق الأمن السيبراني وآليات الحد من الخطر السيبراني في المعاملات التجارية

هناك تحديات تعترض تحقيق الأمن السيبراني وهو ما سنبحثه، وللوصول إلى هذا الهدف أوجدت آليات للحد من الخطر السيبراني في المعاملات التجارية وهذه الآليات سنبينها فيما يأتي:

التحديات القانونية لتحقيق الأمن السيبراني

يواجه الأمن السيبراني تحديات قانونية قد تكون من داخل الشركة التي تكون محل بحثنا. وقد تكون من خارج الشركة وهذه سنبينها.

تحديات من داخل الشركة

كان للتطور السريع للتكنولوجيا الرقمية الأثر البالغ في تعرض الشركات للعديد من المخاطر والمتمثلة بالجرائم السيبرانية، التي تتنبأ بعواقب اقتصادية كبيرة على الرغم مما حصل من تقدم في المجالات القانونية والتعاون الدولي، إلا أنه لا تزال هناك عدد من التحديات ؛وذلك بسبب طبيعة تلك الجرائم التي لا تقف عند الحدود الوطنية وبسبب مجهوليتها (Addan, 2012).

تعد التهديدات المتمثلة بوقوع هجمات إلكترونية ناجحة واحدة من أهم المخاطر التجارية التي تواجهها جميع الشركات والمؤسسات بجميع الصناعات وجميع الأحجام، وتعد تلك التهديدات أخطارا عالية المستوى بسبب قلة الوعي بأهمية الأمن السيبراني (Ghaql & Zakrir, 2023).

ويلاحظ بأن الهجمات السيبرانية قد نمت بشكل ملحوظ من حيث حجمها وتعقيدها منذ ظهور فيروسات الحاسوب الأولى في السبعينيات، وباتت دودة موريس أول هجوم كبير على الإنترنت في عام ١٩٨٨،كما أن عدد الأجهزة المتصلة بالإنترنت وشبكات الشركات قد ارتفع بشكل كبير في السنوات ما بعد الحرب العالمية الثانية، وهناك أيضا ارتفاع في نسبة الاعتماد على أنظمة تكنولوجيا المعلومات من قبل الشركات وبشكل كبير في السنوات الأخيرة، وبالمقابل يتم وضع ميزانيات منخفضة للأمن السيبراني من قبلها (Ghaql & Zakrir, 2023).

ومن المعلوم بأن الخطر المتعلق بأمن تكنولوجيا المعلومات له تأثير على إتاحة وسلامة وسرية المعلومات ونظام المعلومات والبنى التحتية للشركة، وتصل الهجمات المتأتية من داخل الشركة إلى ٦٠٪ سواء من الزبائن أو العاملين أو الزوار، أو المجهزين ، والمتدربين أو مزودي الخدمة، فكل هؤلاء بإمكانهم الاطلاع على المعاملات التجارية، وعلى أسرار تكنولوجية أو مالية أو تجارية، كما بإمكانهم تسريب تلك المعلومات والأسرار ويمكنهم كذلك الحصول على المعلومات من سلة المحذوفات، كون أن هذه الأسرار والمعلومات لم يتم حذفها بشكل نهائي، إذ يمكن استرجاع تلك المعلومات بسهولة، فيمكن أن يحصلوا على أنواع من العقود التجارية التي تم إبرامها عبر شبكات الإنترنت وبيانات البورصة وعناصر محاسبية وعناصر مالية (Baghdadi, 2023).

مثال ذلك في عام ٢٠١٦، تعرضت شركة "*Uber*" لاختراق أمني كبير أدى إلى تسريب بيانات حوالي (٥٧) مليون مستخدم و(٦٠٠) ألف رخصة قيادة. كما أظهرت التحقيقات أن المهاجمين تمكنوا من الوصول إلى نظام تخزين البيانات من خلال حساب مطور على منصة "*GitHub*"، حيث لم تكن هناك سياسات أمنية كافية لحماية كلمات المرور والبيانات المهمة الحساسة. وقد عد هذا الاختراق من أبرز حالات الإهمال في تطبيق إجراءات الأمن السيبراني في الشركات التقنية الكبرى (Federal Trade Commission, 2018).

من خلال الحادثة واجهت شركة "*Uber*" تحديات قانونية كبيرة نتيجة لهذا الاختراق، من أبرزها انتهاك قوانين حماية البيانات مثل قانون الخصوصية في ولاية كاليفورنيا. كما أخذ على الشركة عدم الإبلاغ الفوري للسلطات المختصة عن هذا الاختراق، في مخالفة واضحة للوائح الإفصاح الإلزامي التي تفرض على الشركات إعلام المستهلكين والسلطات المختصة فور حدوث خروقات أمنية.

وكذلك واجهت شركة "*Tesla*" في عام ٢٠١٨ حادثة داخلية خطيرة جدا تمثلت بقيام أحد موظفيها،يدعى "مارتن تريب"، بتخريب أنظمة الإنتاج عن طريق تغيير إعداداتها، بالإضافة إلى إفشاء وتسريب معلومات سرية إلى أطراف خارجية بدون تخويل رسمي. ووصفت الشركة هذا الفعل بأنه يرتقي إلى مستوى "التجسس الصناعي"، مما أدى إلى تبعات قانونية وتقنية كبيرة.

من أبرز التحديات القانونية التي كشفتها هذه الحادثة ضعف الضوابط الرقابية المتعلقة بصلاحيات الوصول إلى البيانات المهمة الحساسة. كما أظهرت الحادثة وجود تقصير في سياسات الأمان الداخلي التي من المفترض أن تحكم وصول الموظفين إلى المعلومات ذات الطابع الحساس، مما سهل للموظف تنفيذ أفعاله دون اكتشافها في الوقت المناسب.

وقد أدى هذا الفعل من الموظف إلى تعطيل في عمليات الإنتاج، ما تسبب بخسائر مادية ومعنوية للشركة. كما سارعت شركة "Tesla" إلى اتخاذ إجراءات قانونية ورفعت دعوى قضائية ضد الموظف المتورط "*Martin Tripp*"، في محاولة لمحاسبته على الضرر الذي ألحقه بالشركة واستعادة ثقة المستثمرين والمستهلكين، وفي سنة ٢٠٢٠، توصل الموظف المتورط إلى تسوية مع شركة "*Tesla*" حيث وافق "*Martin Tripp*"، بموجبها على دفع مبلغ (٤٠٠,٠٠٠) دولار كتعويضات، بالإضافة الى دفع (٢٥,٠٠٠) دولار كغرامة لانتهاكه أمر الحماية الصادر عن المحكمة، والذي كان مضمونه منع الكشف عن المعلومات المهمة السرية. كما ألزمته التسوية بتدمير أي معلومات سرية حصل عليها أثناء فترة عمله في الشركة (Alexis, 2020).

في هذا الصدد، تبنت دول مثل الإمارات العربية المتحدة قانون مكافحة الجرائم الإلكترونية (٢٠٢١)، الذي يجرم الوصول غير المصرح به إلى الأنظمة، ويفرض عقوبات على تسريب المعلومات السرية (UAE Government, 2021). وفي سلطنة عمان، صدر قانون حماية البيانات الشخصية (٢٠٢٢) بموجب مرسوم سلطاني رقم ٦ / ٢٠٢٢، يهدف إلى حماية البيانات الشخصية للأفراد

حيث نصت المادة (١٩): "يلتزم المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة". أما على المستوى الدولي، ساعدت اتفاقية بودابست لمكافحة الجرائم الإلكترونية (٢٠٠١) في تعزيز التعاون بين الدول لملاحقة الجرائم العابرة للحدود (Council of Europe, 2001).

تحديات من خارج الشركة

وقد تكون التحديات من خارج الشركة وأهمها هجوم "أنظمة الإعلام الآلي"، ومنها البرمجيات الخبيثة "وهي برمجية يتم تضمينها وبرمجتها وإدراجها عمدا في نظام الحاسوب لأغراض ضارة، بدون رضا المالك، فقد تستخدم لعرقلة تشغيل الحاسوب، جمع معلومات حساسة، أو الوصول إلى أنظمة الكمبيوتر الخاصة"، ومن الأمثلة على البرمجيات الخبيثة القنابل الموقوتة *bomb logic*، الفيروسات *viruses*، باب المصيدة *backdoor*، أحصنة طروادة *Trojans*، الديدان *computer worms*، وبرامج التجسس *key logger*، الذي يقوم بتسجيل كل المعلومات وكل ما يقوم الشخص بكتابته يقوم بتسجيله وإرسالها إلى المخترق، وهناك برامج نزعة الفدية وهي "نوع من البرمجيات الخبيثة يقوم عن طريقها الهاكر

بتشفير ملفات الشركة أو الشخص الضحية الذي يقوم بفتح البرنامج في حاسوبه ومن ثم يطلب منه مبلغا معتبرا من المال لكي يقوم الهاكر بفك تشفير ملفاته (Ghaql & Zakrir, 2023).

أما حصان طروادة فهو "عبارة عن برنامج خبيث يقوم بالتحكم عن بعد بجهاز أو حاسوب شخص قام بفتح هذا البرنامج في حاسوبه".

وهناك "اختراق خطوط الاتصال" وهي "قيام جماعة من المخترقين باختراق سيرفر يقدم خدمات اتصال ومن بعد تملكه لرقم الهاتف (الهاتف الخادم او السيرفر) يقوم بالاتصال إلى خطوط اتصالاته التي تأخذ أموالا مقابل مكالمة (أرقام الهاكر التي تأخذ أرصدة عند الاتصال بها) ومن ثم يضخم فاتورة الشركة أو المؤسسة التي تمتلك سيرفر الاتصال الذي تم اختراقه".

وأيضا هناك الصفحات المزورة للمواقع لسرقة بيانات تسجيل الدخول للضحايا بعد أن يقوم المخترق باستنساخ الموقع الذي يريد استنساخه؛ حيث يقوم بإرسال رابط مزور للضحايا فتقوم الأخيرة بإدخال معلوماتها، ومن ثم يتم التقاطها من قبل المخترق (Baghdadi, 2023).

ومن أمثلتها الهجوم السيبراني الذي يعرف بـ"*WannaCry*" استهدف نظام الصحة الوطني البريطاني (*NHS*)، حيث أدى إلى تعطيل واسع للخدمات الصحية نتيجة استغلال ثغرات في أنظمة التشغيل غير المحدثة، مما كشف عن ضعف البنية التحتية الرقمية. وقد أبرز الهجوم تحديات قانونية عدة، منها عدم الامتثال لتحديثات الأمان وصعوبة ملاحقة المهاجمين عابري الحدود، فضلا عن خسائر اقتصادية عالمية قدرت بنحو (٤) مليارات دولار (National Audit Office, 2017).

وكذلك تعرضت شركة "*Colonial Pipeline*" في عام ٢٠٢١ لهجوم إلكتروني بواسطة برمجية الفدية "*DarkSide*"، ما أدى إلى تعطيل أكبر خط أنابيب لنقل الوقود في الولايات المتحدة، ودفع فدية بلغت (٤,٤) مليون دولار لاستعادة الأنظمة. كشف الهجوم عن تحديات قانونية، أبرزها ضعف التعاون الدولي في تعقب المجموعات الإجرامية الإلكترونية، إضافة إلى قصور التشريعات القائمة في التصدي لهجمات تستهدف البنية التحتية الحيوية (U.S. Department of Justice, 2021).

آليات الحد من الخطر السيبراني

نتيجة التطور التكنولوجي أصبح العالم وكأنه يعيش في قرية صغيرة ،وعلى الرغم من إيجابيات التكنولوجيا الرقمية إلا أنها تحتوي على مخاطر تهدد الحياة الإنسانية في شتى المجالات، وباتت هذه المخاطر تؤرق الدول والشركات والمؤسسات بل حتى حياة الأفراد الخاصة، الأمر الذي يحتم توفير الأمن السيبراني والبحث عن معالجات ووضع آليات لمواجهة التهديدات السيبرانية على الرغم من التحديات التي قد تعترض ذلك، لذا أوجد المجتمع الدولي في سبيل الحد من

الهجمات السيبرانية وبغية المحافظة على الاقتصاد عددا من الآليات لعلها تفيد في تحقيق الأمن السيبراني للشركات والمؤسسات، ومن بين تلك الآليات التأمين وهذا ما سوف نتناوله في (الفرع الأول)، كما أن للذكاء الاصطناعي دورا في الحد من الخطر السيبراني وسوف نوضحه في (الفرع الثاني):

التأمين

يعد التأمين من الأخطار السيبرانية آلية قانونية حديثة وتقنية تعالج وتحد من تلك الظاهرة، أو بما يعرف بالجرائم الإلكترونية التي باتت تمثل تهديدا حقيقيا لأمن الشركات والدول والأشخاص على حد سواء، وطبيعة هذا الخطر تتمثل بكون هذا الخطر يصيب شيئا غير مادي وغير ملموس وهي المعلومات، وكقاعدة عامة أن المعلومات صعبة التأمين نتيجة طبيعتها غير الملموسة؛ ونظرا لكون الخطر السيبراني خطرا غير تقليدي وغير مرئي فهو خطر تقني، وبذات الوقت يشكل من الأخطار الكبرى التي من شأنها أن تؤثر على الاقتصاد (Baghdadi, 2023).

يمكن تعريف العقد السيبراني للتأمين بأنه "عقد تأمين أضرار يكتتب به المؤمن له والمؤمن، يدفع الأول قسط تأمين (مبلغ من المال)، ويدفع الثاني شركه التأمين في حال تحقق الخطر المبين في وثيقه التأمين مبلغ تأمين للمؤمن له (مكتتب العقد) أو المستفيد المبين في العقد؛ وذلك في ضمان الأضرار والمسؤولية المدنية عند رجوع الغير على الشركة أو المؤسسة أو الشخص الطبيعي المؤمن له(تعويض مالي)، ومساعدة عينية لحل الأزمة السيبرانية (تعويض عيني)؛ وذلك بإرسال فريق خبراء في الإعلام الآلي عند حدوث الكارثة السيبرانية" (Baghdadi, 2023).

ويمكن تعريف التأمين السيبراني بأنه "عملية تأمينية يقوم بها المؤمن لتعويض أضرار الكارثة السيبرانية"، عندما يتم اكتشاف الكارثة السيبرانية من قبل المؤمن له، فإنه لا يجد الأشخاص ذات الكفاءة التي يمكنها التحكم في الكارثة، ولا يعرف الالتزامات التي تقع على عاتقه عند حدوثها؛ لهذا يجب اكتتاب عقد تأمين سيبراني؛ لأن من بين الضمانات التي يتم اقتراحها ضمانات المساعدة، إذ تمتلك شركات التأمين خبراء ومختصين في تسيير الكارثة معترفا بهم، فتغطي له شركه التأمين مختلف تكاليف هذه الخبرة وترسل له الخبراء للتحكم في الكارثة السيبرانية (Baghdadi, 2023).

ومثال ذلك تعرضت شركة "*Mondelez*" التي تمتلك علامات تجارية مثل أوريو وكادبوري، لهجوم سيبراني مدمر باستخدام برنامج الفدية "*NotPety*"، مما تسبب في تعطيل (١,٧٠٠) سيرفر و (٢٤,٠٠٠) جهاز كمبيوتر. حيث اعتمدت الشركة على وثيقة تأمين سيبراني من "*Zurich Insurance*" لتغطية تكاليف استجابة الحادث، مثل استعادة البيانات وإصلاح البنية التحتية. ومع ذلك، رفضت "*Zurich*" دفع التعويض البالغ (١٠٠) مليون دولار، بحجة أن الهجوم يصنف ك "عمل عدائي" مستثنى من الوثيقة (Adriano, 2022). تم تسوية النزاع خارج المحكمة لاحقا، مما أظهر أهمية التأمين السيبراني في تعويض الشركات عن الأضرار الناجمة عن الهجمات الإلكترونية، لكنه كشف تحديات تتعلق بتحديد نطاق التغطية في الهجمات المعقدة.

كما أن الدول الرائدة في مجال تشريعات التأمين السيبراني تهدف إلى تحويل المخاطر التقنية إلى شركات التأمين ومن أبرز التشريعات:

الولايات المتحدة

قانون *2015* Cybersecurity Information Sharing Act (CISA) المادة (١٠٤): تلزم الشركات بمشاركة بيانات التهديدات السيبرانية مع الحكومة مقابل حماية قانونية. يؤثر هذا القانون على سياسات التأمين من خلال تشجيع الشفافية في إدارة المخاطر. إرشادات ولاية نيويورك للتأمين السيبراني (٢٠١٧): القسم ١٧.٥٠٠: تلزم شركات التأمين بتقديم تغطية شاملة للاختراقات، بما في ذلك تكاليف الاستجابة القانونية واستعادة البيانات.

الاتحاد الأوروبي

توجيه (2022) NIS2 Directive المادة (٢١): تلزم الشركات في القطاعات الحيوية (مثل الطاقة والصحة) بتبني تدابير أمنية صارمة، وربطها بسياسات التأمين كشرط للامتثال. التوجيه العام لحماية البيانات(GDPR): المادة (٣٣): تلزم الشركات بالإبلاغ عن الاختراقات خلال ٧٢ ساعة، مما يؤثر على شروط التأمين وضرورة تغطية الغرامات المالية.

وعليه نرى بأن التأمين من الخطر السيبراني يمثل تقنية قانونية حديثة للتقليل أو الحد من إضراره وبموجبه يتم تحويل ونقل الخطر التقني هذا إلى شركات التأمين للحصول على التعويض في حال وقوع أخطار سيبرانية، إلا أن التأمين من هذا الخطر ليس بالأمر السهل، فالتأمين على هذا النوع من الأخطار غالبا ما يرفضه المؤمن؛ وذلك لصعوبة التأمين عليه لأسباب معينة، ومن أهمها أنه في حالة وقوع الخطر السيبراني فإن المؤمن له لا يستطيع الكشف عنه دون أن يراه، إذ إن القراصنة بإمكانهم خرق أنظمة المعلومات دون أدنى شعور من جانب المؤمن له بالخطر الذي حاق به.

الذكاء الاصطناعي

يعرف الذكاء الاصطناعي بأنه "علم وهندسة صناعة الآلات الذكية، وخاصة برامج الحاسوب الذكية" (Top 10 Characteristics of Artificial Intelligence. 2023)، ويعرف أيضا بأنه هو فرع علم الحاسب الذي يتعامل مع محاكاة السلوك الذكي في أجهزة الكمبيوتر وقدرة الماكينة على تقليد السلوك البشري (Sadia, 2021). وهناك من عرفه بأنه ذكاء الآلة أو الحاسوب الذي يمكنه من تقليد القدرات البشرية (Kanade, 2022)، فالذكاء الاصطناعي هو مصطلح يعبر عن سلسلة من التطورات للتقنيات التي يشهدها العالم خلال السنوات القليلة الماضية.

يعمل الذكاء الاصطناعي على نقل الذكاء إلى الآلات كي تتمكن من العمل والتشغيل والتفاعل كالبشر ويهدف أيضا إلى المساعدة في اتخاذ القرارات وفق سيناريوهات الوقت الفعلي، ويتميز الذكاء الاصطناعي بخصائص من بينها أنه يحتوي على روبوتات المحادثة "وهي عبارة عن برنامج يوفر نافذة لحل مشكلات العملاء من خلال الإدخال الصوتي أو النصي (Ben Ali, 2023) ونجد كثيرا من الشركات قد انتقلت من مديري العمليات الصوتية إلى هذه الروبوتات كي تساعد في حل مشكلات العملاء، وتقترح المنتجات للمستخدمين.

ويهدف الذكاء الاصطناعي إلى إجراء التنبؤات المستقبلية وتوقع نتائج الأفعال، إذ يستخدم التخطيط عبر الروبوتات في إدارة المخاطر والأمن السيبراني، ويمكن استخدام الذكاء الاصطناعي في المعاملات الرقمية عبر المؤسسات المالية، فعلى سبيل المثال نجد أن البنوك قللت من اعتمادها على البشر كلما أمكن ذلك والاعتماد على روبوتات الدردشة، سواء تعلق الأمر بمعالجة المعاملات أو تقديم الاستشارة أو خدمة العملاء (Helena Franco, 2023).

ففيما يتعلق بروبوتات الدردشة الخاصة بالخدمات المصرفية، فهي روبوتات محادثه يتم نشرها من قبل البنوك لتعزيز تجارب العملاء في جميع منصات الخدمات المصرفية الرقمية، إذ تساعد على تحسين مشاركه العملاء، وتسهل العمليات، الأمر الذي يجعل الخدمات المصرفية أكثر سهولة، كما تضمن روبوتات المحادثة المصرفية توفير القدرة على التحدث إلى ملايين العملاء من قبل المؤسسات المالية في وقت واحد وتنبه العملاء بشكل استباقي إلى المشاكل التي من المحتمل وقوعها، وتمكن روبوتات الدردشة المستخدمين من دفع الفواتير وتتبع المعاملات المالية وسداد الفواتير عن طريق بطاقات الائتمان وتعيين المدفوعات أو الغائها (Emily Cummins, 2023).

يتم إجراء أعداد كبيرة من المعاملات الرقمية يوميا، إذ يقوم المستخدمون بسحب الأموال ودفع الفواتير وإيداع الشيكات والقيام بالعديد من التطبيقات أو الحسابات عبر الإنترنت، وعليه فإن القطاع المصرفي على سبيل المثال بحاجه متزايدة لتكثيف جهود الأمن السيبراني واكتشاف الاحتيال (Aschi *et al.*, 2023).

تتجلى فوائد الذكاء الاصطناعي في القطاعات المصرفية بشكل خاص، إذ إن الذكاء الاصطناعي يمكنه كشف الاحتيال ، ومع تزايد يقظة المؤسسات المالية يغير المحتالون سلوكهم، ولكن في ظل وجود نظام يكشف عن الاحتيال بالذكاء الاصطناعي يمكن أن يتم اكتشاف الخطر السيبراني على الفور؛ ذلك أن الذكاء الاصطناعي يستطيع أن يحلل كميات كبيرة من البيانات من أجل انتقاء المعاملات المشبوهة (Ben Ali, 2023).

كما يفيد الذكاء الاصطناعي بتخفيض التكاليف والمخاطر، فبقدر ما يكون للتفاعل البشري من فائدة إلا أنه لا يخلو من العيوب، وهي الأخطاء الشائعة، وذلك يمكن أن يكون له تداعيات خطيرة، فإن الضغط الخاطئ على مفتاح من قبل الموظفين، يعرض المؤسسة للمسؤولية حتى لو كان الموظفون متمرسين على القيادة، وهذا يلحق ضررا لا يمكن إصلاحه بالنسبة لسمعة المؤسسة (Ben Ali, 2023).

ومن ثم نجد أن أنظمة الذكاء الاصطناعي تقلل من هذه المخاطر من خلال جمع بين التقنيات التنبؤية، والتعليمية لحل مشاكل المعاملات، وعلى الرغم من أهميه الذكاء الاصطناعي وخاصه عند إجراء المعاملات المصرفية، إلا أن الذكاء الاصطناعي يعد تقنيه ناشئة لا تخلو من المخاطر التجارية.

وبناء على ذلك يجب على المؤسسات المالية أن تجري توازنا بين فوائد الذكاء الاصطناعي من ناحية وبين المخاطر والتحديات من ناحية أخرى، فعلى سبيل المثال نجد أن من بين التحديات القانونية في هذا المجال هي كيفية تحديد المسؤولية القانونية الناشئة عن خطأ قرارات الذكاء الاصطناعي، وإشكاليات انتهاكات الخصوصية، واتخاذ القرارات التي لا يمكن الطعن فيها، أو الرجوع عنها.

فقد أطلقت دولة الإمارات العربية المتحدة في عام ٢٠١٩ الاستراتيجية الوطنية للأمن السيبراني، بهدف تعزيز بيئة سيبرانية آمنة ومرنة تدعم تطلعات الأفراد والشركات. تتضمن الاستراتيجية ٦٠ مبادرة ضمن خمسة محاور رئيسية، منها تصميم إطار قانوني شامل للأمن السيبراني، وتمكين منظومة حيوية للأمن السيبراني، وبناء قدرات وطنية متخصصة، وحماية الأصول الحيوية في قطاعات مختلفة، وتعزيز التعاون المحلي والدولي في المجال. ألزمت القطاعات الحيوية بتبني معايير أمنية عالية، مثل استخدام الذكاء الاصطناعي لاكتشاف الهجمات (UAE National Cybersecurity Strategy, 2021).

الجدير بالذكر أن تطبيق الأمن السيبراني يعد أحد تطبيقات الذكاء الاصطناعي ويمكن تعريفه بأنه "ممارسه الحماية لأجهزة الحاسوب والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة (Ben Ali, 2023). تأخذ المؤسسات والشركات على عاتقها مسؤوليه تأمين البيانات بالمحافظة على العملاء وثقتهم والامتثال للمتطلبات التنظيمية، فالشركات والمؤسسات تعتمد أدوات وتدابير الأمن السيبراني من أجل توفير الحماية للبيانات الحساسة من الوصول غير المصرح به، وكذلك منع أي انقطاعات للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه (Ben Ali, 2023).

يمكن للشركات والمؤسسات تطبيق الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين العمليات والتقنيات والأفراد، فتنفذ استراتيجيات الأمن السيبراني عن طريق العمل مع متخصصين في الأمن السيبراني ، إذ يقوم هؤلاء المتخصصون بتقييم المخاطر الأمنية لأنظمة الحوسبة الحالية ومخازن البيانات والشبكات والتطبيقات والأجهزة المتصلة الأخرى، ومن ثم ينشئ هؤلاء المتخصصون في الأمن السيبراني إطار عمل شاملا له، ويقومون بتنفيذ تدابير وقائية في المؤسسة (Ben Ali, 2023).

إذ تعمل العناصر جميعا لخلق طبقات متعددة من الحماية ضد التهديدات والمخاطر المحتملة على جميع نقاط الوصول إلى البيانات، فهي تقوم بتحديد المخاطر وتحمي البنية الأساسية والبيانات وتحمي الهويات وتستجيب وتحلل السبب الجذري وترصد أوجه الخلل والأحداث، فيمكن للذكاء الاصطناعي أن يعالج الكثير من القيود ويسهم في المساعدة على تحديد المعاملات الخطرة بصورة أكثر فعالية من الإنسان، فكلما تم تدريب الآلة على المزيد من العينات للعمليات

الاحتيالية زاد هذا الأمر من إمكانيه تعرف الآلة على الاحتيال، ومن ثم يمكن القول بتحقيق الأمن السيبراني في مجال المعاملات التجارية ، وبذلك يقوم الذكاء الاصطناعي بتقليل المخاطر السيبرانية أو الحد منها.

المقترحات

أ. يجب اعتماد سياسة واستراتيجيات معينة للأمن السيبراني عند إجراء المعاملات التجارية الإلكترونية وفق دراسات تتولاها هيئات ذات خبرة واختصاص في هذا المجال، تتلاءم مع البيئة الداخلية للدولة ومع خصوصياتها.

ب. وضع خطط متكاملة لتكريس الأمن السيبراني كمشروع وطني يلقى دعما من قبل الدولة ويحظى بمتابعة من قبل المسؤولين الحكوميين وتوفير الموارد التقنية مادية وبشرية، مع توفير بنية تشريعية متكاملة تضمن تحقيق الحماية للأفراد والشركات والمؤسسات عند إجراء المعاملات التجارية الإلكترونية وتسهيلها في ظل العصر الرقمي ، وعلى الأمن السيبراني فهم آليات مواجهة الخطر السيبراني الواقع على المعاملات التجارية الإلكترونية ومعرفة خصائصه وتطوره.

ج. ضرورة مواكبة تطور العصر الرقمي، إذ لا بد من التعامل مع المشكلة بطرق منظمة ومنهجية واحترافية ومهنية، فلا بد من أن تنصب الجهود في نشر الوعي لدى الأفراد والشركات بالمخاطر السيبرانية ، وضرورة الوعي بأهمية تحقيق الأمن السيبراني ، والحث على الاستخدام السليم لتكنولوجيا المعلومات والاتصالات ، وإدراك قيمة ذلك لتجنب مضار الهجمات السيبرانية من خلال عقد المؤتمرات والندوات العلمية في الجامعات والمراكز البحثية تضم الخبراء والمختصين لدراسة الظاهرة ووضع الحلول المناسبة.

د. إيجاد بنى تحتية لأنظمة المعلومات والاتصالات بحيث يكون هناك ترابط بأنظمة تكنولوجيا المعلومات بين الجهات الحكومية المركزية والمحلية ، وتسمح بانسيابية المعلومات بينها وبين الأفراد والشركات وهذا من شأنه أن يحافظ على الاقتصاد عند إجراء المعاملات التجارية الإلكترونية.

الخاتمة

في خاتمة بحثنا توصلنا إلى جملة من الاستنتاجات والمقترحات نبينها كالآتي:

أ. يتمثل الخطر السيبراني بالهجمات الإلكترونية على أجهزة الحاسوب والأجهزة المتصلة بالإنترنت فتصيب المعلومات، ويتميز عن المخاطر التقليدية بأنه خطر غير ملموس وغير مادي، وغير مرئي لا يتم اكتشافه إلا بعد مرور فترة معينة من حدوثه.

ب. يعد الأمن السيبراني وسيلة من خلالها يمكن المحافظة على المعلومات والبيانات بصورة عامة والمعاملات التجارية الإلكترونية التي ترتبط بالاقتصاد، ويحتاج الى بذل الجهود وتوفير موارد تقنية وبشرية لتحقيقه للحد أو التقليل من الهجمات الإلكترونية السيبرانية.

ج. نظرا للخصائص التي يتميز بها الخطر السيبراني عن الأخطار التقليدية نجد أنه من الصعوبة التأمين عليه كآلية من آليات الحد من الهجمات الإلكترونية السيبرانية، ومن ثم نلاحظ بأن شركات التأمين بدأت التأمين عليه بصورة تدريجية إلا أنها تتعامل معه بحذر وأن محل التأمين هي المعلومات محل المعاملات التجارية الإلكترونية التي تعد ذات قيمة اقتصادية.

د. يمكن للذكاء الاصطناعي من تقليل المخاطر السيبرانية أو الحد منها من خلال معالجة الكثير من القيود، ويسهم في المساعدة على تحديد المعاملات الخطرة بصورة أكثر فعالية من الإنسان، فكلما تم تدريب الآلة على المزيد من العينات للعمليات الاحتيالية زاد هذا الأمر من إمكانيه تعرف الآلة على الاحتيال.

References

Abdul Hamid, E. E. D. M. K. (2023). Cyber-attacks on smart city: Infrastructure, legal challenges and confrontation strategy. *Dirasat: Shari'a and Law Sciences*, *50*(3), 54–70. https://doi.org/10.35516/law.v50i3.2864

Abdullah, M. B. G. (2023). Tatbiqat qaidat "al-darar yuzal" fi majal al-amn al-siberani: Applications of the principle "harm must be removed" in cybersecurity. *Mujallat al-Ibrahimi lil-Adab wa al-Ulum al-Insaniyah*, *5*(2), 130-154.

Addan, N. (2012). Al-aliyat al-qanuniyah li-muwajahat tahadiyat al-fada' al-siberani – Al-Jaza'ir namuthajan: Legal mechanisms to combat cyber space challenges: Algeria as a model. *Mujallat al-Jazā'iriyah lil-ʿUlūm al-Siyāsiyyah wa al-ʿIlāqāt al-Duwaliyah*, *5*(1), 8-24.

Adriano, L. (2022, November 8). *"Zurich, Mondelez settle longstanding lawsuit over $100 million claim: Suit alleged that the insurer had failed to honor its promises".* Cyber. https://www.csoonline.com/article/3661898/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim.html

Akoush, S. (2022). Al-aliyat al-qanuniyah wa al-taqniyah li-muwajahat al-makhatir al-tiknolojiyah: Bitaqat al-aitiman namuthajan: Legal and technical mechanisms to combat technological risks: Credit cards as a model. *Majallat al-Ulum al-Qanuniyah wa al-Ijtima'iyah*, *7*(1), 400-411.

Alexis, K. (2020, December 22). *"Tesla whistleblower ordered to pay $400,000 and destroy leaked information"*. Yahoo Finance. https://finance.yahoo.com/news/martin-tripp-settlement-with-tesla-160512420.html

Al-Fatlawi, A. O. (2016). Al-hajamat al-siberaniya: Mafhumha wa al-mas'uliyah al-duwaliyah al-nashia anha fi dhaw' al-tanzim al-duwali al-muasir: Cyberattacks: Their concept and emerging international responsibility under contemporary international regulations. *Majallat al-Muhakkik al-Hilli lil-Ulum al-Qanuniyah wa al-Siyasiyah*, *4*, 211-224.

Amazon Web Services. (n.d.). "*Amazon web services"*. Amazon. https://aws.amazon.com/

Amoroso, E. G. (2007). *Cybersecurity*. S. Press.

Aschi, M., Bonura, S., Masi, N., Messina, D., & Profeta, D. (2023, March 4). Cybersecurity and fraud detection in financial transactions. In *Big data and artificial intelligence in digital finance* (pp. 269–280). Springer.

Attia, I. (2019). Makanat al-amn al-siberani fi manzumet al-amn al-watani al-jaza'iri: The role of cybersecurity in Algeria's national security system. *Majallat Misdaqiyah*, *1*(1), 65-84.

Baghdadi, C. (2023). Tamin al-khatar al-siberani*:* Cyber risk insurance. *Majallat Herodot lil-Ulum al-Insaniyah wa al-Ijtima'iyah, 7*(25), 237-257.

Ben Ali, S. (2023). Musahamat al-dhaka' al-istina'i fi al-kashf an al-ihtial fi al-qita' al-masrifi bi-istikhdam tatbiq al-amn al-siberani Bank Danske al-dinmarki namuthajan: AI's role in detecting fraud in the banking sector: The Danish Bank Danske as a model. *Majallat Ab'ad Iqtisadiyah, 13*(2), 39-63.

Ben Brughouth, L. (2023). Al-amn al-siberani wa himayat khususiya al-bayanat al-raqamiyah fi al-jaza'ir fi 'asr al-tahawul al-raqami wa al-dhaka' al-istina'i: Cybersecurity and data privacy protection in Algeria in the age of digital transformation and AI. *Al-Majalla al-Duwaliyah lil-Itisalat al-Ijtima'i*, *10*(1), 443-457.

Ben Khadra, H., & Bouzidaf, S. (2024). *Dawr al-dhaka' al-istina'i fi al-kashf wa al-hadd min al-ihtial ala al-bataqat al-aitiman al-bankiyah 'ala al-mustawa al-dawli* (The role of AI in detecting and preventing credit card fraud internationally. *Mujallat al-Ibda', 14*(2), 274-292.

Ben Zrarah, A., & A'rab, F. (2023). Al-hulul al-raqamiyah al-ibtikariah fi majal himayat al-hawiya wa al-khususiya wa al-amn al-siberani khilal jaihah COVID-19: Innovative digital solutions in protecting identity, privacy, and cybersecurity during COVID-19. *Mujallat al-Dirasat al-I'lamiyah wa al-Ittisaliyah*, *3*(1), 58-66.

Berghouth, L. (2023). Al-amn al-siberani wa himayat khususiya al-bayanat al-raqamiyah: Cybersecurity and protection of digital data privacy in Algeria. *International Journal of Social Communication*, *10*(1), 56-69.

Council of Europe. (2001). "*Convention on cybercrime"*. Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Cummins, E. (2023). *"The 10 best banking chatbots (and how your financial institution can use them, too)"*. Netomi. https://www.netomi.com/banking-chatbots

Cybersecurity and Infrastructure Security Agency. (2021). "*Cybersecurity infrastructure security agency act"*. CISA. https://www.cisa.gov

Cybersecurity Information Sharing Act (CISA). (2015). "*S.754 — 114th Congress: Cybersecurity Information Sharing Act of 2015"*. U.S. Congress. https://www.congress.gov/bill/114th-congress/senate-bill/754

Franco, H. (2023). *"Chatbots in banking: The new must-have in customer care"*. Inbenta. https://www.inbenta.com/

General Data Protection Regulation (GDPR). (2018). *"EU Regulation 2016/679 on data protection and privacy"*. https://gdpr-info.eu

Gerke, M. (2012). *"Fahm al-jarimah al-siberaniyah: al-zahair wa al-tahadiyat wa al-istijabah al-qanuniyah: Understanding cybercrime: Phenomena, challenges, and legal response"*. International Telecommunications Union. https://www.itu.int/en/Pages/default.aspx

Ghaql, J., & Zakrir, A. (2023). Al-amn al-siberani wa al-shumul al-mali fi dhil al-tahawul al-raqami lil-qita' al-mali: Cybersecurity and financial inclusion in the digital financial sector. *Mujallat al-Tanmiya al-Iqtisadiya*, *8*(1), 37-56.

InterviewBit. (2023, February 26). *"Top 10 characteristics of artificial intelligence"*. https://www.interviewbit.com/blog/characteristics-of-artificial-intelligence/

Jboor al-Ashqar, M. (2017). *Al-siberaniyah hajis al-'asr*. Al-Markaz al-Arabi lil-Buhuth al-Qanuniyah wa al-Qada'iyah: Beirut.

Kanade, V. (2022). *"What is artificial intelligence (AI)? Definition, types, goals, challenges, and trends in 2022"*. Spiceworks. https://www.spiceworks.com

Kemmerer, R. A. (2003). *Cyber security*. University of California, Santa Barbara.

Kotaf, S. (2022). Al-amn al-siberani wa al-madhamin al-mafhumiyah al-murtabita bihi: Cybersecurity and its conceptual implications. *Majallat Tibna lil-Dirasat al-'Ilmiyah al-Akademiyah*, *5*(2), 273-295.

Lkhweider, N., & Mashtoub, R. (2018). Dawr al-amn al-siberani fi 'ilaj al-irhab al-tijari: The role of cybersecurity in addressing commercial terrorism. *Majallat Ru'a lil-Dirasat al-Ma'rifiyah wa al-Hadariyah, 4*(1), 88–105.

National Audit Office. (2017). *"Investigation: WannaCry cyber attack and the NHS"*. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

New York State Department of Financial Services (NYDFS). (2017). *"Cybersecurity regulations (23 NYCRR 500)"*. https://www.dfs.ny.gov/industry_guidance/cybersecurity

NIS2 Directive. (2022). *"Directive (EU) 2022/2555 on a high common level of cybersecurity across the Union"*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Rosley, N. A., Hashim, H., & Chow Jen-T'Chiang , N. Z. (2023). Combating the macau scam in Malaysia: Strategies for mitigation and resolution from civil law and Sharī'ah Perspectives. *Law, Policy, and Social Science*, *2*(2), 30–44.

Sadia, S. (2021). *Tabani al-dhaka' al-istina'i fi sharikat al-tamin ka-al-iya li-ta'aziz al-shumul al-mali: Dirasat halat sharikat AXA* (Adoption of AI in insurance companies as a mechanism to enhance financial inclusion: A case study of AXA). *Majallat al-Jaza'iriyah li-Iqtisad al-Idarah*, *15*(1), 45–62.

Shammari, S. (2020). Al-amn al-siberani ka-murtakaz jadid fi al-istratigiyah al-'iraqiyah: Cybersecurity as a new pillar in Iraq's strategy. *Qadhaya Siyasiyah*, *12*(62), 273-295.

Siwan, H., & Al-Fatlawi, A. (2015). Al-amn al-siberani wa al-hurub al-siberaniyah: Cybersecurity and cyber wars. *Khiyamat al-Iraq Newspaper*, Issue 4.

Tibah, S. (2018). *"Présentation cyber risques"*. Compagnie centrale de réassurance (CCR). https://www.ccr.dz/images/pdf/cyber-risks-ccr.pdf

U.S. Department of Justice. (2021, June 7). *"Department of Justice seizes $2.3 million in cryptocurrency paid to ransomware extortionists Darkside"*. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

UAE Government. (2019). *"UAE national cybersecurity strategy"*. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/national-cybersecurity-strategy

UAE Government. (2021). *"Federal Decree-Law No. 34 of 2021 on combatting rumours and cybercrimes".* Official Gazette of the United Arab Emirates. https://uaelegislation.gov.ae/en/legislations/1526

Walia, I. K. (2023). Cyber surveillance and privacy issues vis-à-vis international law. *Brawijaya Law Journal*, *10*(2), 219–241. https://doi.org/10.21776/ub.blj.2023.010.02.05

Wan Ismail, W. A. F., Abdul Mutalib, L., Mamat, Z., Hashim, H., Baharuddin, A. S., Mohammed Hassan, B. M., & Alias, M. A. A. (2024). Analysis of the concept of acceptance and verification of e-kitabah as a method of proof according to Islamic legislation in Malaysia. (2024*). LexForensica: Journal of Forensic Justice and Socio-Legal Research, 1*(1), 1-12.