

[الحماية القانونية لمهددات الأمن السيبراني على المعاملات المالية]

إعداد الباحثان:

[د. هبة أبوبكر عوض - أستاذ مساعد/قسم القانون الخاص - كلية الحقوق - جامعة البريمي]

[الطالبة: عطية جابر خميس السعدية - كلية الحقوق - جامعة البريمي - المستوى الرابع]

الملخص:

في العصر الرقمي الذي نعيش فيه اليوم، أصبحت التكنولوجيا جزءاً لا يتجزأ من حياتنا اليومية، مع تزايد الاعتماد على الإنترنت والشبكات الرقمية في مختلف الأنشطة الاقتصادية والاجتماعية، حيث برز مفهوم الأمن السيبراني كعنصر أساسي لحماية المعلومات والبنية التحتية الرقمية. يُعد الأمن السيبراني مفهوماً حديثاً نسبياً، لكنه أصبح حيوياً في مواجهة التهديدات المتزايدة من الهجمات الإلكترونية والاختراقات، ويواجه العالم اليوم أهم التحديات القانونية التي ألقى بها الفضاء السيبراني، حيث برزت إشكالات قانونية تتطلب اهتماماً لحل النزاعات التي يمكن أن تنشأ عنها، وأضيف إلى قائمة الحقوق الأساسية والحريات المعترف بها في الدساتير والتشريعات الدولية حقوقاً أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم، التي تشمل أساليب ممارسة واس خدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الإنترنت، و الحق في حماية ملكية البرامج المعلوماتية.

وفي المقابل ظهرت التزامات جديدة ذات طابع اقتصادي، كالإلتزام بحفظ بيانات الاتصالات للأشخاص الطبيعيين والمعنويين على السواء، مع ضرورة الإلتزام بحماية البيانات بالإضافة إلى حماية الحق في الخصوصية، فضلاً عن التحولات المتوقعة على مستوى سياسات القطاعات المالية والتجارية، والتي تشهد تزايداً في الأعمال الإجرامية والتهديدات السيبرانية.

مصطلحات البحث: الأمن السيبراني- مهددات- التكنولوجيا - الشبكات الرقمية- البرامج المعلوماتية - الانترنت- المعاملات المالية-المؤسسات المالية- الحماية القانونية.

DOI: <https://doi.org/10.62690/ijssp2536>

[Legal Protection of Cybersecurity Threats to Financial Transactions]

Reserchers:

[Dr. Hiba Abubakr Awad]

[Student: Atiya Jaber Khamis Al-Saadi]

Summary:

In the digital age in which we live today, technology has become an integral part of our daily lives, with increasing reliance on the Internet and digital networks in various economic and social activities, where the concept of cybersecurity has emerged as an essential element for protecting information and digital infrastructure. Cybersecurity is a relatively new concept, but it has become vital in the face of increasing threats from cyber-attacks and hacking, and the world today faces the most important legal challenges posed by cyberspace, as legal problems have emerged that require attention to resolve disputes that may arise from them, and other rights have been added to the list of fundamental rights and freedoms recognized in international constitutions and legislation, such as the right to access the World Wide Web, and some concepts have expanded, which include methods of practicing and using information and communication technologies, such as the right to create electronic blogs, the right to create online gatherings, and the right to protect the ownership of information programs.

In contrast, new obligations of an economic nature have emerged, such as the obligation to preserve communications data for both natural and legal persons, with the necessity of adhering to data protection in addition to protecting the right to privacy, as well as the expected changes in the policies of the financial and commercial sectors, which are witnessing an increase in criminal acts and cyber threats.

Search terms: Cybersecurity - Threats - Technology - Digital Networks - Information Programs - Internet - Financial Transactions - Financial Institutions - Legal Protection.

يهدف البحث من خلال فقراته للآتي:

- 1- بيان مفهوم الأمن السيبراني، باعتباره عنصر أساسي لحماية المعلومات والبنية التحتية الرقمية، والوقوف على مدى الإشكالات القانونية المتمثلة في التهديدات المتزايدة الناجمة عن الهجمات الإلكترونية والاختراقات.
- 2- كما يسعى البحث الى تقديم شواهد تطبيقية لمهددات الأمن السيبراني على المعاملات المالية، وبيان أثرها في تعطيل الخدمات المالية وانتهاك البيانات الشخصية، وممارسة الاحتيال الالكتروني.
3. الوصول إلى حلول ناجعة أهمها خلق أنظمة تشريعية تواكب التطور الرقمي والتقني، مما يضمن مبادئ الثقة والسلامة والاستقرار التي تلازم العمليات المالية، من خلال القواعد التشريعية والاجتهادات القضائية.

إشكالية البحث: تكمن إشكالية البحث في التساؤلات الآتية: -

- 1- مدى تأثير مهددات الأمن السيبراني على سير المعاملات المالية، وضمان أداء المؤسسات المالية لدورها في تفعيل العلاقات المالية في بيئة آمنة ونزيهة.
- 2- الوقوف على قصور التشريعات المالية، والتشريعات ذات الصلة، وضرورة تعزيز دورها في توفير الحماية القانونية في المعاملات المالية؟

ومن ثم السؤال كيف للاجتهادات التشريعية والقضائية الحد من مهددات الأمن السيبراني.

منهج البحث: تقتضي طبيعة البحث أن نعتمد على المنهج الاستقرائي في دراسة مفهوم الأمن السيبراني ونشأته، وتطوره، وبيان صوره، وذلك باستعراض الشواهد التطبيقية لمهددات الأمن السيبراني، عن طريق المنهج التحليلي بدراسة جزئيات البحث الرئيسة وتناول الجوانب الموضوعية، مع مراعاة قواعد الكتابة البحثية المستقرة واتباع قوالب التوثيق والكتابة.

خطة تقسيم البحث: يجري تناول الموضوع على ضوء هدف واسئلة البحث في ثلاثة مطالب وخاتمة:

استهلال: مفهوم الأمن السيبراني ونشأته وتطوره

المطلب الأول: صور الهجمات السيبرانية على نظم المعلومات والشبكات الالكترونية

المطلب الثاني: مهددات الأمن السيبراني على المعاملات المالية.

المطلب الثالث: الحماية القانونية لمهددات الأمن السيبراني على المعاملات المالية

الخاتمة: تضم نتائج وتوصيات

المطلب الاول: تعريف الأمن السيبراني ونشأته وتطوره

أولاً: مفهوم الأمن السيبراني:

الأمن السيبراني هو مصطلح يتكون من كلمتين: "الأمن" و "السيبراني".

يُعرف الأمن بأنه نقيض الخوف، ويعبر عن حالة من السلام والطمأنينة. كلمة "أمن" تأتي من الجذر اللغوي الذي يعبر عن الاطمئنان وزوال القلق، حيث يُقال إن الشخص "أمنٌ من الشر" أي أنه سَلِمَ منه. وفي تعريف قاموس بنغوين للعلاقات الدولية، يُشير الأمن إلى غياب التهديدات للقيم النادرة. على الرغم من أن مصطلح الأمن القومي قد أصبح شائعاً بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وخاصةً بعد معاهدة وستفاليا عام 1648م، التي وضعت الأساس لقيام الدولة القومية. وتشكلت خلال حقبة الحرب الباردة الإطارات النظرية والمؤسسية التي أدت إلى ظهور تعبير "استراتيجية الأمن القومي"، بالإضافة إلى تركيز المصطلحات المرتبطة بتلك الحقبة مثل الاحتواء، الردع، التوازن، والتعايش السلمي، بهدف تعزيز الأمن والسلم وتجنب الحروب المدمرة التي شهدتها النصف الأول من القرن العشرين. وبالنسبة لمصطلح الحرب السيبرانية، فقد اعتمد بعض الأفراد على أيديولوجية أمنية أو عسكرية تهدف إلى تحقيق الأهداف على الصعيد الأمني أو العسكري تجاه "العدو المفترض". بينما فضّل آخرون استخدام مصطلح "الهجمات السيبرانية" كوصف واقعي يعبر عن أفعال

تحدث في عالم افتراضي يعتمد على البيانات الرقمية ووسائل الاتصال الإلكترونية. لقد تطور هذا المفهوم ليتوسع ليشمل تحقيق أهداف أمنية أو عسكرية ملموسة من خلال اختراق مواقع إلكترونية حساسة، خاصة تلك التي تُعتبر ذات أولوية مثل أنظمة حماية محطات الطاقة النووية أو المطارات ووسائل النقل الأخرى. نظرًا لأن مصطلح "الحرب" يعتبر غير مرغوب فيه حاليًا في سياق التنظيم القانوني الدولي، فإن "الهجمات السيبرانية" تُعتبر أكثر ملاءمة للموضوع الذي تتناوله هذه الدراسة، خاصةً أن العديد من الدول قد أشارت إلى هذا المصطلح واعتبرته سلوكًا يُؤخذ في الاعتبار أثناء النزاعات المسلحة، وفقًا للقانون الدولي الإنساني.¹

مصطلح "السيبراني" أصبح واحدًا من أكثر المفاهيم استخدامًا في معجم الأمن الدولي. يشير الأصل الإيثيمولوجي² للكلمة "cyber" إلى أصول يونانية، حيث تُشتق من كلمة "Kubernetes" التي تعني الشخص الذي يدير دفة السفينة. تستخدم هذه الكلمة بشكل مجازي للإشارة إلى "المتحكم". ومن المثير للاهتمام أن العديد من المؤرخين ينسبون أصل هذا المصطلح إلى عالم الرياضيات الأمريكي "نوربرت وينر"، الذي يعد المؤسس الروحي للسبرنتيكية من خلال مؤلفه الشهير "Cybernetics: or Control and Communication In the Animal and the Machine". في هذا الكتاب، أشار وينر إلى أن السبرنتيكية تتعلق بالتحكم والتواصل لدى الحيوان والآلة والإنسان، ومع مرور الوقت، تم استبدال مصطلح "الآلة" بالحاسوب بعد الحرب العالمية الثانية.³

أما في الاصطلاح فهناك تعريفات متعددة لمفهوم الأمن السيبراني، حيث يتم تعريفه عادةً بأنه مجموعة من الإجراءات الدفاعية ضد الهجمات السيبرانية وتبعاتها، بما في ذلك تنفيذ التدابير الوقائية الضرورية. على سبيل المثال، يعتبر Pekka and Martti في كتابهم "Cyber Security : Analytics, Technology, and Automation" الأمن السيبراني يشمل جميع الإجراءات الدفاعية والتدابير الوقائية لحماية البيانات والمعلومات الإلكترونية من الاختراق والاعتداءات القرصنة، بما في ذلك استخدام الأدوات المتخصصة في مكافحة القرصنة وكشف ووقف الفيروسات وتأمين الاتصالات المشفرة. وفقًا لتعريف وزارة الدفاع الأمريكية "البنتاغون"، يعتبر الأمن السيبراني جميع الإجراءات التنظيمية اللازمة لحماية جميع أشكال المعلومات الإلكترونية والمادية من الأنشطة الإجرامية مثل الهجمات والتخريب والتجسس والحوادث. ويمكن تعريف الأمن السيبراني أيضًا بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات المتصلة بالإنترنت، فهو المجال الذي يعني بحماية الأنظمة والبيانات من الاعتداءات والهجمات الإلكترونية. يشمل ذلك وضع معايير الحماية وتنفيذها والامتثال لها لضمان سلامة البيانات والمعلومات ومنع وقوعها في أيدي الأشخاص غير المخولين. ويرتبط هذا الأمن ارتباطًا وثيقًا بأمن

¹ الأمن السيبراني: المفهوم وتحديات العصر. د. فارس عمارات، إبراهيم الحمامصه ٢٠٢٢- الطبعة الأولى. دار الخليج للنشر والتوزيع-عمّان. ص ١٣-١٤.

² مصطلح الإيثيمولوجيا: علم التأثيل، علم يبحث عن العلاقات التي تربط كلمة بوحدة قديمة جدًا تعد هي الأصل (الأثلة). بالمعنى القديم، هي البحث عن المعنى الأصلي والأولي للكلمة. <https://ar.m.wikipedia.org/wiki/>

³ الأمن السيبراني: المفهوم وتحديات العصر. د. فارس عمارات، إبراهيم الحمامصه ٢٠٢٢- الطبعة الأولى. دار الخليج للنشر والتوزيع-عمّان. ص ١٤-١٥.

المعلومات، حيث أن الوصول إليها أو بثها أو الاطلاع عليها والتلاعب بها أو استغلالها هو ما يقف غالباً وراء عمليات الاعتداء على الشبكات والإنترنت.⁴

عرف الاتحاد الدولي للاتصالات الأمن السيبراني كمنظومة متكاملة تشمل المهام، والوسائل، والسياسات، والإجراءات الأمنية، والمبادئ التوجيهية، واستراتيجيات إدارة المخاطر، والتدريبات، وأفضل الممارسات، والتقنيات المستخدمة لحماية الفضاء السيبراني والممتلكات الرقمية للمؤسسات والمستخدمين. كما أشار إلى أنه يتضمن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي تهدف إلى منع الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات والنظم الإلكترونية والاتصالات. الهدف من ذلك هو ضمان استدامة عمل نظم المعلومات، وتعزيز حماية وسرية الخصوصية للبيانات الشخصية، بالإضافة إلى اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر المحتملة في الفضاء السيبراني.⁵

ويمكن تعريف الأمن السيبراني استناداً إلى أهدافه كنشاط يهدف إلى حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات. كما يعمل على تقليل الخسائر والأضرار التي قد تحدث نتيجة المخاطر والتهديدات، ويسعى لإعادة الوضع إلى طبيعته بسرعة، مما يضمن عدم توقف عجلة الإنتاج وعدم تحول الأضرار إلى خسائر دائمة.⁶

نستنتج مما سبق إن الأمن السيبراني هو مفهوم شامل يهدف إلى حماية الأنظمة المعلوماتية، البرمجيات، والشبكات من التهديدات والهجمات الإلكترونية. يشمل هذا المفهوم الإجراءات التقنية والقانونية التي تضمن الحفاظ على سرية المعلومات، سلامتها، وتوفرها في مواجهة الهجمات التي قد تنطوي على اختراق البيانات، السرقة الرقمية، أو التلاعب بالأنظمة الإلكترونية.

ثانياً: نشأة وأهمية الأمن السيبراني

1. الأهمية:

أصبحت دراسة الأمن السيبراني واحده من تبعات التطور التكنولوجي والرقمي، الذي يشهده العالم ، حيث التطور التكنولوجي في كافة المجالات ، لذا أصبحت دراسة المخاطر التكنولوجية في مجال الحاسب الرقمي معترفاً لجدل الفقهاء في ظل المهددات السيبرانية التي اجتاحت قطاع الشركات والمؤسسات التجارية والاقتصادية ، ولعل هذا من أسباب أهميه دراسة مهددات الأمن السيبراني على المعاملات المالية، لتأثيرها على تلك القطاعات الحيوية ، مما يستلزم التصدي لحماية البيانات والشبكات والأنظمة الإلكترونية من الجهات والاختراقات التي قد تعطل أنشطتها وتزعزع استقرارها.

⁴ الامن السيبراني: المفهوم وتحديات العصر . د. فارس عمارات، ابراهيم الحمامصه ٢٠٢٢-الطبعة الاولى. دار الخليج للنشر

والتوزيع-عمّان. ص ١٥-١٦.

⁵ مجلة كلية الشريعة والقانون، جامعة الازهر، فرع أسيوط العدد الرابع والثلاثون الاصدار الاول، يناير ٢٠٢٢م الجزء الثالث، وسائل

حماية الامن السيبراني "دراسة فقهية تأصيلية مقارنه بالنظم المعاصرة"، أ. د عادل موسى عوض جاب الله، ص ٢٢٤٣

⁶ المركز العربي للبحوث القانونية و القضائية، السيبرانية هاجس العصر، د. منى الاشقر جبور، ص ٢٦.

2. مراحل تطور الأمن السيبراني⁷

الأمن السيبراني هو مجموعة من التدابير والآليات التي تهدف إلى حماية الأنظمة والشبكات والأجهزة والمعلومات من الهجمات الرقمية. على مر السنين، تطورت هذه التقنيات والأساليب بشكل ملحوظ استجابة للتهديدات المتزايدة والمتطورة.

- البدايات المبكرة (الأربعينيات - السبعينيات)

قبل ظهور أجهزة الكمبيوتر، كانت الحماية تقتصر بشكل كبير على حماية المعلومات الورقية والمادية. على الرغم من وجود محاولات لتأمين المعلومات العسكرية والدبلوماسية خلال الحروب، فإن فكرة الأمن السيبراني لم تكن موجودة بعد. حيث بدأ الأمن السيبراني مع أولى محاولات التشفير، خصوصًا خلال الحرب العالمية الثانية مع استخدام آلة إنجما التي ساعد على فك تشفيرها خبراء مثل آلان تورينج، مما وضع أساسيات علم التشفير الحديث.

- التشفير بالمفتاح العام (السبعينيات)

في السبعينيات، تم تقديم التشفير بالمفتاح العام بواسطة وايتفيلد ديفي ومارتن هيلمان، مما أحدث ثورة في تبادل البيانات بشكل آمن عبر الإنترنت دون الحاجة لتبادل المفتاح السري.

- ظهور الفيروسات (الثمانينات)

خلال الثمانينيات، ظهر أول فيروس كمبيوتر يُعرف بـ فيروس الدماغ، وقد شكل بداية لعصر التهديدات السيبرانية حيث بدأت الفيروسات تتطور وتصبح أكثر تعقيدًا وخطورة.

ومع تطور الشبكات، ظهرت الحاجة إلى تأمين البيانات المنقولة عبر الشبكات، وتم تطوير بروتوكولات أمان الشبكات، مثل بروتوكول TCP/IP، مما مهد الطريق للأمن السيبراني الحديث.

- شبكة الإنترنت وSSL (التسعينيات)

في عام 1991، تم اختراع الشبكة العالمية (WWW)، مما أدى إلى نمو هائل في عدد المستخدمين والبيانات المتداولة على الإنترنت، وزيادة الهجمات السيبرانية، مثل البرمجيات الخبيثة والهجمات الموزعة.

ومع ظهور شبكة الويب العالمية في التسعينيات، ظهرت الحاجة لتأمين الاتصالات عبر الإنترنت. حيث بدأت الشركات والمؤسسات الحكومية في الاستثمار بشكل أكبر في حلول الأمن السيبراني لحماية شبكاتها وأنظمتها، حيث تم تطوير بروتوكول SSL لتأمين تبادل البيانات، مما أسهم في حماية المعاملات المالية والتجارية. كما تطورت

⁷ مقال بعنوان "من اللغز إلى التشفير: معالم تاريخ الأمن السيبراني". ٢٩/أكتوبر/٢٠٢٣.

<https://fastdigitaltechnology.com/a>

كذلك تقنيات التشفير، وأصبحت جزءاً أساسياً من حماية البيانات المنقولة عبر الإنترنت، كما تم تأسيس أولى أنظمة كشف التطفل (IDS).

- توسع الشركات والسياسات (2000-الحاضر)

شهد العقد الأول من القرن الحادي والعشرين توسعاً كبيراً في قطاع الأمن السيبراني مع ظهور شركات متخصصة لحماية المنظمات والأفراد من التهديدات، بالإضافة إلى تطور تقنيات مثل جدران الحماية وأنظمة كشف التسلل. زادت أهمية هذه التقنيات مع ارتفاع وتيرة الاختراقات السيبرانية.

وشهدت هذه الفترة تطوراً كبيراً في التهديدات السيبرانية مع ظهور تقنيات جديدة مثل الذكاء الاصطناعي وإنترنت الأشياء (IoT)، ما أدى إلى توسع نطاق الهجمات. من أبرز السمات لهذه المرحلة:

الهجمات الموجهة المتقدمة (APT): بدأت الهجمات السيبرانية تصبح أكثر تنظيماً وتعقيداً، حيث تستهدف مؤسسات بعينها بهدف سرقة البيانات الحساسة.

التشريعات الجديدة: ظهرت قوانين ولوائح جديدة تنظم الأمن السيبراني، مثل النظام العام لحماية البيانات (GDPR) في الاتحاد الأوروبي، الذي يهدف إلى حماية بيانات المستخدمين الشخصية.

المطلب الثاني: صور الهجمات السيبرانية على نظم المعلومات والشبكات الالكترونية

طبيعة مخاطر الأمن السيبراني:

مما لا شك فيه، أن تكنولوجيا المعلومات والاتصالات، تتيح إمكانات هائلة، وغير مسبقة، لإنتاجية أفضل في جميع القطاعات، وللتواصل عبر القارات. إلا أن البنية التحتية لهذه التقنيات، ت مثل ارتباطاً بين مصالح متعددة، وخدمات مختلفة، ودول عديدة، الأمر الذي يجعل من الاخطار في المجال السيبراني، أخطاراً عالمية. فلا يمكن لأي جهة، أن تضمن بقاءها في منأى عن الاخطار، ما دامت سلامة الآخرين

الأمن السيبراني هو مجال يتعامل مع حماية نظم المعلومات والشبكات من الهجمات الإلكترونية، ويعتبر محورياً أساسياً في ظل التقدم التكنولوجي المتسارع. ومع ذلك، يواجه هذا المجال العديد من الإشكالات القانونية، التي يمكن تلخيصها في النقاط التالية:

أولاً: التعدي الإلكتروني (الجرائم الإلكترونية)

القوانين المتعلقة بالجرائم الإلكترونية تختلف من دولة لأخرى. الشركات تحتاج إلى فهم كيفية حماية نفسها قانونياً من الهجمات الإلكترونية مثل القرصنة أو التهديدات المستندة إلى البرمجيات الخبيثة. عدم وجود إطار قانوني واضح في بعض المناطق يمكن أن يزيد من التحديات.

تعددت التعريفات المتعلقة بالجريمة الإلكترونية، ويعود هذا الاختلاف إلى الأسس أو المنطق الذي تم اعتماده في كل تعريف، حيث ارتبطت معظم التعريفات بشكل مباشر بين الفعل الإجرامي والحاسب الآلي كأداة رئيسية لتنفيذ الجريمة، مما يُظهر دور الحاسوب على نحو إيجابي أكثر من كونه سلبياً، من ناحية أخرى، تناولت تعريفات أخرى الجريمة المعلوماتية على أنها تلك التي تتعلق بالنظام المعلوماتي أو تحدث ضمن ونطاقه.

يرى مؤيدو التعريفات المحدودة للجريمة الإلكترونية أنها تتجلى فقط عندما يكون الفعل الجرمي موجهاً بالأساس إلى النظم المعلوماتية ذاتها. وهذا الرأي يستبعد الحالات التي تُستخدم فيها التكنولوجيا الحديثة لارتكاب جرائم تقليدية. ومن أبرز مؤيدي هذا الاتجاه الأستاذ Sieber، الذي يعرف الجريمة الإلكترونية بأنها أي سلوك غير قانوني أو غير مصرح به يتعلق بمعالجة البيانات آلياً أو نقلها. يتناول الفقيه MERWE الجريمة المعلوماتية من خلال تعريفها كفعل غير مشروع يرتكبه الحاسب الآلي. بينما عرفها آخرون على أنها تتعلق بالأفعال الإجرامية التي يستخدم فيها الحاسوب كأداة رئيسية. وفي تعريف آخر، رأى الفقيه rosblat أن الجريمة المعلوماتية تمثل نشاطاً غير مشروع يهدف إلى نسخ أو تغيير أو حذف المعلومات المخزنة على الحاسب الآلي. ومن جهته، اعتبر الفقيه Friedman الجريمة المعلوماتية جريمة ضد المال ترتبط باستخدام معالجة المعلومات الآلية. واعتبرت الأستاذ Mass هذه الجرائم اعتداءات قانونية تتم من خلال المعلوماتية بهدف تحقيق الربح. بينما عرف الأستاذ Parker الجريمة المعلوماتية كفعل إجرامي عمدي يؤدي إلى خسارة للمجني عليه أو ربح للتفاعل. أما الأستاذة قورة نائلة، فقد عرفت الجريمة الإلكترونية بأنها أي فعل غير مشروع يتطلب معرفة تكنولوجيا الحاسبات الآلية بشكل كبير. في حين وافقها الأستاذ فالي علال، موضحاً أن الجريمة المعلوماتية تشمل الجرائم التي تتعلق بالمعلومات والبيانات المخزنة في الحاسب أو الأنظمة المعلوماتية، سواء كانت هذه المعلومات متاحة للجمهور أو سرية.⁸

بالرغم من جهود العديد من الدول العربية، مثل دولة الإمارات العربية المتحدة وسلطنة عمان، لإصدار تشريعات لمكافحة الجرائم الإلكترونية، إلا أن هذه التشريعات لا تغطي جميع أشكال الإجمام المعلوماتية المتجددة مع تطور التكنولوجيا، والظهور المتتالي والمتسارع لأنماط تكنولوجيا متقدمة، ويظهر هذا الفراغ في الاتفاق القانوني حول تصنيفات الإجمام المعلوماتي فرصة للمجرمين لتنظيم أنفسهم عالمياً، مما يجعل كل الدول تحت خطر دائم يتجاوز الحدود الجغرافية، لذا، يُعتبر التعاون الدولي ضرورة ملحة لمواجهة هذه السلوكيات الإجرامية، التي تتميز بخصائص فريدة مقارنة بالجرائم التقليدية. وما تنجم عنه من أضرار تهدد استقرار وسلامة المعاملات

أشكال التعدي الإلكتروني

استهداف البنية التحتية للمصرف الإلكتروني أو تعطيل عملها:

تشمل البنية التحتية في أي قطاع مالي: أنظمة الدفع والتسوية، ومنصات التداول، ودائع الأوراق المالية المركزية، والأطراف المقابلة المركزية. وتعتبر البنى التحتية للقطاعات المالية في الدولة -خاصة الدول النامية - نقطة الضعف الرئيسية في فشل الأمن السيبراني لهذه القطاعات والذي قد يتحقق نتيجة لتهاك أو تعطل عمل البنية التحتية للقطاع ذاته أو لمجموعة من المؤسسات المالية الرئيسية في القطاع نتيجة لتركز المخاطر، أو عدم وجود بدائل في حالة البنية التحتية.⁹

⁸ الجريمة الإلكترونية: مدخل إلى الإطار المفاهيمي، عبد الحميد المليحي، مجلة المنارة.

32: Emanuel Kopp، Lincoln Kaffenberger، and Christopher Wilson

“Cyber Risk ,Market Failures, and Financial Stability”, Working Paper No.17/185,IMF, 2017.

وهو الامر الذي يمكن أن يؤدي إلى اضطرابات كبيرة في سير العمل بالقطاع المالي.¹⁰ أو تقويض ثقل العماء في المصارف. فعلى سبل المثال، في ٢٧ يونيو ٢٠١٤ شهد أكبر بنك محلي في بلغاريا FIB عملية تشغيل من جانب المودعين وسط حالة من عدم اليقين بسبب قرار بنك آخر - بعد رسائل البريد الإلكتروني المخادعة التي تشير إلى أن FIB كان يعاني من نقص في السيولة. بلغت ودائع التمدقات الخارجة في ذلك اليوم ١٠% من إجمالي الودائع لدى البنوك، وكان على البنك استخدام خطة لمساعدة السيولة مقدمة من السلطات.¹¹

استهداف الهواتف الذكية:

والتي أصحت وسيلة الإتصال السيرياني ودخول الكثير من العماء على حساباتهم المصرفية من خلالها، أو إجراء عمليات البى والشراء من خلال تلك الهواتف، ويحاول المهاجمون تركيز اهتمامهم على اختراق هذه الأجهزة. والتي ينشأ تهديدها نتيجة للأسباب التالية:

- أن غالبية مستخدمى الهواتف الذكية ليس لديهم المعرفة الكافية بالثغرات الأمنية لهذه الهواتف.
- أن المراهجين دائماً يلجأون إلى التحايل على مالكي الهواتف الذكية لتوجيههم على تحميل تطبيقات تحت سيطرتهم.
- يكمن خطر الهواتف الذكية في تطبيقاتها الخاصة بدخول العملاء من خلالها لحساباتهم المصرفية، الأمر الذي يتيح للمراهجين فرصة الحصول على المعلومات المصرفية أو إصابة النظام الإلكتروني للمصرف بالفيروسات التي تعطل عمل النظام أو بعض أجزاءه، وذلك عبر العديد من الوسائل الاحتيالية وفق الآتي:

أ- الاختراقات:

الاختراقات تعد من أبرز التحديات التي تواجه الأمن السيرياني في العصر الحديث، حيث تشكل تهديداً كبيراً على الأفراد والمؤسسات والحكومات على حد سواء. تنتشر الاختراقات الإلكترونية عبر عدة أساليب تستهدف سرقة البيانات أو تعطيل الخدمات.

¹⁰ د. مروة فتحي السيد البغدادي ، اقتصاديات الأمن السيرياني في القطاع المصرفي ، مجلة البحوث القانونية والاقتصادية، الاسكندرية،

العدد 26، 2021

¹¹ Friedman :“Taking cyber risk management to the next level – Lessons learned From the front

lines at financial institutions”, Deloitte Insight, June 2016.

<https://www.alchourouk.com/index.php/article%D8%B9%D8%B5%D8%B1->

صور الاختراقات:

1. التصيد الاحتيالي (Phishing): يعتمد على إرسال رسائل بريد إلكتروني أو روابط زائفة لخداع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات مالية. هذا النوع من الهجمات يعد شائعًا ويستهدف الأفراد والمؤسسات بشكل متزايد.¹²
2. هجمات الفدية (Ransomware): يقوم المخترقون بتشفير البيانات الهامة وطلب فدية مالية مقابل فك التشفير. يعتبر هذا النوع من الهجمات خطرًا كبيرًا، حيث قد يترتب عليه فقدان بيانات هامة أو تسريبها إلى الخارج.¹³
3. الهجمات باستخدام الهندسة الاجتماعية: المخترقون يعتمدون على خداع الأفراد لجعلهم يقدمون معلومات سرية عبر استخدام تقنيات مثل التصيد أو الاتصالات الزائفة، وهذه الهجمات قد تكون مدمرة بسبب قدرتها على الوصول إلى بيانات حساسة من خلال الاحتيال.¹⁴
4. استغلال الثغرات الأمنية: تستهدف هذه الهجمات الثغرات الموجودة في الأنظمة أو البرامج غير المحدثة، مما يمكن المخترقين من الوصول غير المصرح به إلى البيانات الحساسة.¹⁵

ينقسم المخترقون إلى طائفتين:

- ١- الهاكر، أو المتسلل، هو شخص يمتلك مهارات متقدمة في استخدام الحاسوب وبرامجه ولديه فضول لاستكشاف حسابات الآخرين بطرق غير قانونية. وكما يتضح من اسمهم، فإن الهاكرز يعتبرون متطفلين يتجاوزون أنظمة الشبكات، لكن عادةً ما تفتقر دوافعهم إلى الكراهية أو التخريب، بل غالبًا ما تأتي من رغبة في التحدي وإثبات الذات. تتكون هذه المجموعة أساسًا من المراهقين والشباب (طلاب) والشباب العاطلين عن العمل.
- ٢- الكراكر أو المقتحم هو فرد يتسلل إلى نظم الحاسوب بهدف الاطلاع على المعلومات المخزنة فيها، أو إلحاق الضرر بها، أو العبث بها، أو حتى سرقتها. وقد شاع استخدام هذا المصطلح الجديد في عام 1985 من قبل أول مجموعة تُعرف باسم "الهكرز" للرد على الاستخدام المسيء لمصطلح "هكرز" من قبل الصحفيين.¹⁷ لقد استفادت هذه المجموعة بشكل كبير من التقنيات التي طورتها فئة الهكرز، وبدأت تستخدمها بشكل سلبي في اعتداءات تشير إلى ميولات إجرامية. ومن الخصائص المميزة لهذه المجموعة هو تبادل المعلومات بينها. في الآونة

¹² الأمن السيبراني: استراتيجيات حماية البيانات وتجنب الاختراق، ١٩ يوليو ٢٠٢٣م. <https://www.alqiyady.com/>

¹³ أنواع الهجمات الإلكترونية، ٣٠ أغسطس ٢٠٢٤م. <https://www.secprint.sa/cyber-attacks-types>

¹⁴ المرجع السابق، الأمن السيبراني: استراتيجيات حماية البيانات وتجنب الاختراق، ١٩ يوليو ٢٠٢٣م.

¹⁵ المرجع السابق، أنواع الهجمات الإلكترونية، ٣٠ أغسطس ٢٠٢٤م.

¹⁶ كيف يعمل الهاكرز على اختراق الأنظمة وكيف يمكن الحماية منهم؟ موقع النجاح ١٥ ديسمبر ٢٠٢٣م.

<https://www.annajah.net/>

¹⁷ المؤتمر الدولي الرابع للعلوم الاجتماعية "الكويت" ٢٠١٠م، الجرائم المعلوماتية أنواعها وصفات مرتكبيها، منصور الجهني، ص ٤.

الأخيرة، بدأت هذه الطائفة بتنظيم مؤتمرات لمخترقي الكمبيوتر، يدعى إليها خبراء لمناقشة وسائل الاختراق وكيفية تنظيم أنشطتهم.

ب- الاحتيال الإلكتروني:

أدت الثورة التكنولوجية، وما صاحبها من ظهور البنوك الإلكترونية والتحويلات المالية إلكترونياً، إلى زيادة احتمال وقوع الجرائم الإلكترونية، ولا سيما الاحتيال الإلكتروني. حيث تعتمد المصارف والمؤسسات المالية حالياً بشكل أساسي على الأنظمة الإلكترونية لإجراء التحويلات المالية التي تتم يومياً، وبمبالغ ضخمة. مع توافر تقنية نقل الأموال إلكترونياً عبر البنوك العالمية في غضون دقائق، أصبح بإمكان العملاء الذين يمتلكون أرصدة في تلك البنوك إجراء هذه العمليات من أي مكان في العالم دون الحاجة للذهاب إلى المصرف مباشرة. يعتبر الاحتيال الإلكتروني من أكثر الجرائم الإلكترونية شيوعاً حول العالم، مما يؤدي إلى خسائر اقتصادية فادحة ويشكل مصدر قلق متزايد للمعنيين بالأمر، حيث تهدد هذه الجرائم ثقة الأفراد في الوسائل التقنية الحديثة لنقل الأموال. وتزداد خطورة الاحتيال الإلكتروني عندما نتعرف على أن المعلومات المتعلقة بالجهات الاقتصادية المختلفة أصبحت مخزنة في الحواسيب،¹⁸ مما يسهل الوصول إليها من أي مكان في العالم، خصوصاً مع تقدم وسائل الاتصال الحديثة. ومع أن الإجراءات الأمنية التقنية تسعى لحماية هذه المعلومات، إلا أنها لا تزال غير كافية، إذ توجد العديد من الثغرات الأمنية التي يستغلها المهاجمون لتحقيق أهدافهم في الكسب غير المشروع. تشكل الأموال الإلكترونية والودائع هدفاً لمجرمي المعلوماتية، من خلال التلاعب بمدخلات الأنظمة الإلكترونية، مثل تغذية الحاسوب ببيانات غير صحيحة أو التلاعب بالبرامج. يُعرّف الاحتيال الإلكتروني، أو الغش الإلكتروني، بأنه أي سلوك احتيالي يتعلق بمعالجة البيانات الإلكترونية بهدف تحقيق منفعة أو مصلحة مالية. كما عرفت هيئة الأمم المتحدة الاحتيال الإلكتروني بأنه إدخال أو حذف أو تعديل البيانات أو البرامج أو التدخل في معالجة البيانات والتي تؤدي إلى خسارة اقتصادية أو فقدان ملكية شخص آخر، بقصد تحقيق مكسب اقتصادي غير مشروع. يمكن أن يتخذ الربح غير المشروع نتيجة الاحتيال الإلكتروني شكلين: الأول مباشر، حيث يُحوّل الفاعل المال إلى حسابه، والثاني غير مباشر، حينما يتجنب الفاعل تسديد التزام مالي. معظم حالات الاحتيال بواسطة الحاسوب تهدف لجني المال تأتي من داخل الجهات المستهدفة، لا من خارجها؛ فمرتكبو الاحتيال الإلكتروني عادةً ما يكونون أفراداً لديهم سلطة في التعامل مع المعلومات التي يحتويها النظام الإلكتروني، مما يجعل هذه النوعية من الجرائم تُصنّف أحياناً كجرائم داخلية، نظراً لحدوثها داخل المؤسسة الضحية وبواسطة أحد منتمي إليها.

¹⁸ د/ عبد الله خبابية: الاقتصاد المصرفي، مؤسسة شباب الجامعة، الإسكندرية، ٢٠٠٨، ص ٩١

ت- البرمجيات الخبيثة¹⁹

تشير البرمجيات الخبيثة إلى أي برنامج يمنح بعض التحكم أو السيطرة الكاملة على جهاز الكمبيوتر الخاص بالضحية لمن قام بإنشائه لهذا الغرض. تتفاوت الأضرار التي قد تلحقها هذه البرامج، فقد تكون خفيفة مثل تغيير اسم المؤلف في مستند معين، أو جسيمة مثل الوصول الكامل إلى الجهاز مع عدم القدرة على تعقبها.

يمكن تصنيف أنواع البرمجيات الخبيثة كما يلي:

1. الفيروسات (Viruses)

2. الديدان (Worms)

3. برامج التجسس (Spywares)

4. أحصنة طروادة (Horses Troja)

تُعرف فيروسات الكمبيوتر بأنها برامج تهاجم وتلف برامج معينة، وتنتقل إلى برامج أخرى عند تشغيل الملفات المصابة.

أما ديدان الحاسوب، فهي نوع من الفيروسات التي تقوم بإنشاء نسخ من نفسها تلقائياً، مما يجعلها قادرة على إحداث أضرار على نطاق واسع. على عكس الفيروسات التي تحتاج إلى ملفات مضيفة للإنتشار، تتصرف الديدان كبرامج مستقلة ولا تتطلب مساعدات لنشر نفسها.

برامج التجسس تتماثل مع إعلانات البرامج لكنها تحمل نوايا ضارة، حيث يبقى المستخدم غير مدرك لهذه الغزوات. يمكن لهذه البرامج جمع ونقل المعلومات الشخصية، وتصنف كبرمجيات تخترق الخصوصية بسبب نقلها للمعلومات دون علم المستخدم.

أما أحصنة طروادة، فهي من البرمجيات الخبيثة التي تبدو كبرمجيات آمنة، حيث تخدع المستخدمين لتحميلها وتطبيقها على أنظمتهم. عند تنشيطها، تبدأ بالحاق الأذى بالنظام مما يؤدي إلى مشكلات مزعجة أو أضرار.

المطلب الثالث: الحماية القانونية لمهددات الأمن السيبراني على المعاملات المالية

أولاً: نطاق الأمن السيبراني

يشمل الأمن السيبراني مجموعة واسعة من العمليات والتدابير التي تهدف إلى حماية الأنظمة الرقمية، الشبكات، والمعلومات من التهديدات الإلكترونية. يتنوع هذا النطاق بناءً على أنواع الحماية والأهداف المختلفة داخل المجال:

1. أمن الشبكات: يتعلق بحماية البنية التحتية للشبكات التي تربط الأنظمة والمستخدمين. يشمل تقنيات مثل الجدران النارية (firewalls)، وأنظمة كشف التسلل (IDS)، وأنظمة منع التسلل (IPS). هذا النوع

¹⁹ مقدمة في الامن السيبراني، ايمن الحربي، واحة أم القرى للاستشارات.

من الأمن يركز على منع الوصول غير المصرح به إلى الشبكات ويشمل مراقبة حركة المرور داخل الشبكة لتحديد أي نشاط مريب.²⁰

2. أمن المعلومات: يهدف إلى حماية البيانات المخزنة أو المتداولة عبر الشبكات من الوصول غير المصرح به أو التعديل أو السرقة. تتضمن تقنيات هذا المجال التشفير لضمان سرية البيانات، والمصادقة لضمان صحة المستخدمين المصرح لهم بالوصول.²¹

3. أمن التطبيقات: يتعامل مع حماية البرمجيات والتطبيقات من الثغرات التي يمكن أن يتم استغلالها من قبل المهاجمين. يتضمن هذا النوع عمليات مراجعة الكود (code review) واختبار الاختراق (penetration testing) لضمان عدم وجود ثغرات يمكن أن تعرض النظام للخطر.²²

4. إدارة المخاطر السيبرانية: تتعلق بتحديد وتحليل المخاطر المحتملة التي تواجه الأنظمة الرقمية والشبكات، واتخاذ التدابير اللازمة للحد من تأثير تلك المخاطر. يشمل ذلك تحليل التهديدات المحتملة وتصميم استراتيجيات وقائية مبنية على أسس علمية وتقنية.²³

5. الاستجابة للحوادث السيبرانية: يهدف هذا المجال إلى تقديم خطط طوارئ لمواجهة الهجمات الإلكترونية. يتضمن إجراءات لتحديد التهديدات والاستجابة السريعة للتخفيف من الأضرار الناجمة عن هذه الهجمات. يُعتبر هذا الجانب ضروريًا لاحتواء الاختراقات وتقليل الآثار السلبية.

ثانياً: انتهاك سرية البيانات الشخصية

تزايدت المخاوف بشأن كيفية جمع وتخزين واستخدام البيانات الشخصية من قبل الشركات والمؤسسات. تحتاج القوانين إلى إحكام قبضتها على حماية البيانات وتحديد المسؤوليات القانونية في حال حدوث خروقات.

تعتبر حماية البيانات الشخصية من أكبر التحديات التي يواجهها الأمن السيبراني في العصر الحديث، خصوصاً مع تزايد الاعتماد على التكنولوجيا والذكاء الاصطناعي. إن البيانات الشخصية، بما في ذلك المعلومات المالية والطبية والمعلومات الحساسة الأخرى، تُعد هدفاً مهماً للهجمات الإلكترونية. هذه الهجمات تهدد الشركات والأفراد، وقد تؤدي إلى خروقات كبيرة في الأمن تؤثر سلباً على الثقة بين العملاء والشركات.²⁴

²⁰ الامن السيبراني: تعريفه وأهميته وكيف يعمل ومجالاته وأنواع التهديدات والتقنيات الحديثة، خالد سامر، ١٩ يناير ٢٠٢٤م،

<https://blog.zamn.ap>

²¹ ما هو الامن السيبراني، هيئة الاتصالات والفضاء والتقنية.

<https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx>

²² الدليل الشامل لفهم الامن السيبراني الرقمي، ٢٥ ديسمبر ٢٠٢٣م. <https://bluemediasa.com/cyber-security>

²³ الامن السيبراني: تعريفه وأهميته وكيف يعمل ومجالاته وأنواع التهديدات والتقنيات الحديثة، خالد سامر، ١٩ يناير ٢٠٢٤م.

<https://blog.zamn.6->

²⁴ دليل شامل للأمن السيبراني و حماية البيانات الشخصية، حسام عرموش. <https://www.rmg-s>

تتنوع أساليب حماية البيانات الشخصية بين تشفير البيانات، إدارة الوصول، واستخدام جدران الحماية وأنظمة كشف التسلل. ومن الضروري أيضًا وضع خطط أمنية متكاملة تشمل توعية الموظفين حول كيفية التعامل مع التهديدات السيبرانية مثل البرمجيات الخبيثة وهجمات الحرمان من الخدمة (DDoS).²⁵

ومن أبرز التحديات التي تواجه حماية البيانات الشخصية هي التوازن بين الحفاظ على خصوصية الأفراد وتأمين الأنظمة من الهجمات. تتطلب هذه العملية تطوير أنظمة سياسات صارمة تشمل تنظيم تدفق البيانات، تطبيق تشريعات خصوصية البيانات، وضمان توافق المنظمات مع المعايير الدولية مثل ISO 27001.²⁶

كما أن المنتدى العربي للأمن السيبراني يُعد منصة مهمة للنقاش حول حماية البيانات في ظل الذكاء الاصطناعي، حيث يبحث في الحلول والاستراتيجيات اللازمة لتأمين البيانات الشخصية.²⁷

ثالثاً: حماية مهددات الأمن السيبراني على المعاملات المالية²⁸

في مسح لصندوق النقد الدولي على البنوك المركزية والسلطات الرقابية، أشار إلى أن أطر سياسات الأمن السيبراني لا تزال غير كافية في الغالب، ولا سيما في اقتصادات الأسواق الصاعدة والاقتصادات النامية. فعلى سبيل المثال، يطبق حوالي نصف البلدان فقط التي شملها المسح استراتيجيات وطنية أو أطر تنظيمية مخصصة للأمن السيبراني في القطاع المالي.

وبهدف **تعزيز صلابة** القطاع المالي، على السلطات تم وضع استراتيجيات وطنية كافية لحماية الأمن السيبراني، مصحوبة بأطر تنظيمية وقدرات رقابية فعالية، بما في ذلك:

- التقييم الدوري لبيئة الأمن السيبراني، وتحديد المخاطر النظامية المحتملة الناجمة عن الروابط والتركزات، بما في ذلك المرتبطة بمقدمي الخدمات الخارجيين.
- تشجيع "النضج" السيبراني بين شركات القطاع المالي، بما في ذلك الاستعانة بخبراء الأمن السيبراني في مجالس الإدارات، وهو ما تؤيده التحليلات الواردة في الفصل، والتي تشير إلى أن تعزيز الحوكمة السيبرانية قد يساهم في الحد من المخاطر السيبرانية.
- تحسين "النظافة السيبرانية" للشركات - أي سلامة أمنها ونظمها على شبكة الإنترنت (بما في ذلك استخدام مضادات البرمجيات الخبيثة والمصادقة متعددة العوامل) - والتدريب والتوعية.
- إيلاء الأولوية لجمع وإبلاغ البيانات عن حوادث الأمن السيبراني، وتبادل المعلومات بين المشاركين في القطاع المالي لتعزيز التأهب الجماعي.

²⁵ الامن السيبراني: دليلك لحماية البيانات والمعلومات، ٩ مايو ٢٠٢٤م،

²⁶ المرجع السابق، دليل شامل للأمن السيبراني وحماية البيانات الشخصية، حسام عرموش.

²⁷ المنتدى العربي للأمن السيبراني "حماية البيانات الشخصية عصر الذكاء الاصطناعي"، ٣ ديسمبر ٢٠٢٣م.

<https://www.alchourouk.com>

²⁸ د. مروة فتحي السيد البغدادي، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، الاسكندرية،

العدد 26، 2021

ونظرا لأن الهجمات غالبا ما تنشأ من خارج البلد الأصلي للشركة المالية ويمكن تحويل مكاسبها المالية عبر الحدود، يتعين التصدي بنجاح للمخاطر السيبرانية.

وفي حين أن حوادث الأمن السيبراني واقعة لا محالة، يحتاج القطاع المالي إلى القدرات اللازمة لتقديم الخدمات الأساسية أثناء هذه الاضطرابات. ولذلك ينبغي للشركات المالية وضع إجراءات للاستجابة والتعافي واختبارها. وعلى السلطات الوطنية أيضا تنفيذ بروتوكولات للاستجابة وأطر لإدارة الأزمات، مع ضمان فعاليتها.

ويضطلع صندوق النقد الدولي بدور فعال في مساعدة البلدان الأعضاء على تعزيز أطر الأمن السيبراني عبر تقديم المشورة بشأن السياسات، كجزء من [برنامج تقييم القطاع المالي](#) ومن خلال [أنشطة بناء القدرات](#).²⁹

المطلب الرابع: وسائل حماية مهددات الأمن السيبراني في مجال المعاملات المالية

أولاً: إحداث ثورة تشريعية حامية للتصدي لمهددات الأمن السيبراني

في ظل شيوع الهجمات السيبرانية بشكل متزايد، يجب أن يكون التشريعات المالية قادرة لصد الهجمات السيبرانية، واستئناف أعمالها بسرعة حتى في مواجهة هجمة ناجحة، حماية للمعاملات وحفاظاً على الحقوق. ولا يزال ما يسمى باستراتيجيات الاستجابة ومعاودة النشاط في طور النشأة، ولا سيما في البلدان منخفضة الدخل، ومن ثم تحتاج إلى دعم في تطويرها، ومن الضروري وضع التدابير والاحترازمات التشريعية والتنظيمية على المستوى الوطني لدعم الاستجابة والمحافظة على سلامة واستقرار المعاملات خاصة أنشطة المؤسسات والخدمات العابرة للحدود.

العديد من الدول لا تمتلك تشريعات واضحة وشاملة تتعلق بالأمن السيبراني، مما يعيق القدرة على التصدي للتهديدات الإلكترونية بفعالية. في بعض الحالات، قد تكون القوانين الموجودة غير كافية أو غير محدثة لتجاري الحادثة.

وتعد قضايا نقص التشريعات المتعلقة بالأمن السيبراني من أبرز التحديات التي تواجه العديد من الدول العربية. فرغم التقدم الكبير في استخدام الإنترنت والتكنولوجيا، تظل القوانين المتعلقة بحماية الفضاء السيبراني غير كافية في مواجهة التهديدات المتزايدة.

في المنطقة العربية، لوحظ وجود فجوة في التشريعات السيبرانية المناسبة التي تحمي الأفراد والمؤسسات من الجرائم الإلكترونية. العديد من الدول تعتمد على قوانين جزئية أو قديمة لا تغطي التحديات السيبرانية

²⁹ تستند هذه التدوينة إلى الفصل الثالث من عدد إبريل 2024 من تقرير الاستقرار المالي العالمي بعنوان "مخاطر الأمن السيبراني: مخاوف متزايدة إزاء الاستقرار المالي الكلي، التهديدات السيبرانية المتزايدة تثير شواغل ملحّة حول الاستقرار المالي، ازداد خطر الهجمات السيبرانية النظامية في ظل نمو التحول الرقمي وتساعد الاضطرابات الجغرافية-السياسية.

[فابيو ناتالوتشي](#)، [ماهفاش سعيد قرشي](#)، [فيلكس سونثايم](#)

الحديثة، مثل الجرائم الإلكترونية، حماية البيانات الشخصية، والتعامل مع الهجمات السيبرانية المنظمة. بالإضافة إلى ذلك، بعض التشريعات لا تتماشى مع المعايير الدولية أو لا توفر آليات تطبيق فعالة.³⁰ من بين أبرز المشاكل هو غياب قانون شامل ومتكامل ينظم الفضاء السيبراني في الدول العربية. على سبيل المثال، توصي العديد من الجهات بضرورة تحديث التشريعات المتعلقة بحماية البيانات، وتطوير قوانين أكثر وضوحاً وشمولاً لمكافحة الجرائم الإلكترونية، إضافة إلى تعزيز التعاون بين الدول العربية في هذا المجال. وتسعى بعض المؤسسات الدولية والإقليمية، مثل لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا)، إلى تقديم إطار توجيهي لتحسين التنسيق بين الدول العربية وتطوير تشريعات سيبرانية موحدة. هذه الجهود تهدف إلى بناء بيئة سيبرانية آمنة تتماشى مع المعايير الدولية وتعزز الحكومة الإلكترونية.³¹

ثانياً: تمكين أساليب الرقابة والردع³²

زيادة تبادل المعلومات المالية، بوصفه السمة الغالبة للمعاملات المالية، يجعلها عرضة للتهديدات والهجمات على مستوى القطاعين العام والخاص، لذا لزم تعزيز أساليب الردع بشكل فعال، والقضاء على العوائق التي تكون غالباً ناشئة عن شواغل الأمن الوطني وقوانين حماية البيانات، وعلى الأجهزة الرقابية والبنوك المركزية، والشركات أن تضع بروتوكولات، وممارسات لتبادل المعلومات من شأنها العمل بفعالية في ظل هذه القيود، وومن الممكن تخفيض الحواجز القائمة من خلال نموذج متفق عليه عالمياً لتبادل المعلومات، وزيادة استخدام منصات المعلومات المشتركة، وتوسيع الشبكات التي تحظى بالثقة.

ثالثاً: تقوية الشبكات الالكترونية

يعد تقوية الشبكات الالكترونية أمراً ملحاً للتصدي لمخاطر تعطيل وتوقف المعاملات المالية، حيث يمكن أن يؤدي حادث سيبراني جسيم في إحدى المؤسسات المالية إلى تقويض الثقة، وربما تنشأ عنه موجة بيع عارمة في الأسواق أو سحب جماعي للودائع المصرفية في الحالات القصوى. ورغم أننا لم نشهد حتى الآن سحباً جماعياً للودائع إثر هجمات سيبرانية، يشير تحليلنا إلى خروج تدفقات محدودة من الودائع بوتيرة ثابتة إلى حد ما من البنوك الأمريكية الأصغر حجماً عقب الهجمات السيبرانية.

كما يمكن أن تنشأ تداعيات حادة على النشاط الاقتصادي نتيجة الحوادث السيبرانية التي تؤدي إلى تعطيل الخدمات الأساسية، مثل شبكات المدفوعات، فعلى سبيل المثال، تعرض بنك "ليسوتو" المركزي إلى هجمة في ديسمبر أدت إلى تعطيل نظام المدفوعات الوطني، وبالتالي توقف المعاملات في البنوك المحلية.

³⁰ أهم توصيات المؤتمر الدولي حول "الأمن السيبراني في التشريعات العربية"، يوسف العيصامي، ١٩ يوليو ٢٠٢١م، المستقلة بريس.

<https://www.almostaquilla-press.com/articles/34265>

³¹ الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا، التشريعات السيبرانية. <https://archive.unescwa.org/ar/>

³² راجع حول هذا الموضوع، د. علم الدين بانقا، مخاطر الهجمات الالكترونية السيبرانية وآثارها الاقتصادية، دراسة حالة، دور مجلس التعاون الخليجي، سلسلة دراسات تنمية، المعهد العربي للتخطيط، الكويت، العدد 63، أبريل 2019.

رابعاً: الرقابة على مقدمي خدمات التكنولوجيا

نمو اعتماد الشركات المالية على مقدمي خدمات تكنولوجيا المعلومات الخارجيين، والذي قد يزداد بمرور الوقت مع صعود أهمية الذكاء الاصطناعي، ويمكن لمقدمي الخدمات الخارجيين تعزيز صلابة العمليات، ولكنهم يجعلون أيضاً القطاع المالي عرضة لصدمات نظامية، فعلى سبيل المثال، تعرض أحد مقدمي خدمات تكنولوجيا المعلومات السحابية لهجوم باستخدام فيروسات الفدية عام 2023 نتج عنه انقطاع الخدمات عبر 60 اتحاد ائتماني في الولايات المتحدة في آن واحد، لذا يجب على السياسات وأطر الحوكمة أن تواكب المخاطر السيبرانية الهائلة والمتنامية التي تواجه النظام المالي العالمي بسبب زيادة التحول الرقمي والاضطرابات الجغرافية-السياسية

ونظراً لأن الحوافز الخاصة ربما لا تكون كافية للتصدي للمخاطر السيبرانية – فالشركات على سبيل المثال قد تمتنع عن نشر معلومات كاملة حول تداعيات تلك الحوادث على النظام المالي – مما يتطلب التصدي التشريعي لها.

خامساً: تفعيل وسائل الحماية القانونية

1. إدارة مخاطر العمليات المصرفية الإلكترونية

أشارت لجنة بازل للرقابة المصرفية إلى أهمية قيام البنوك بوضع السياسات، والإجراءات التي تتيح إدارة مخاطر العمل المصرفي الإلكتروني من خلال تقييم المؤسسات والرقابة عليها ومتابعتها، والتي تندرج تحت إدارة مخاطر العمليات المصرفية الإلكترونية.، ويصحب ذلك جملة من المخاطر الأخرى: كمخاطر السمعة، ومخاطر التشغيل، والتنظيم.

2. زيادة الوسائل الحمائية للأمن السيبراني³³

زيادة الوسائل الحمائية للأمن السيبراني تتطلب أساساً لحماية المعاملات المالية، بحيث تصبح الهجمات السيبرانية أكثر تكلفة وخطراً من خلال إجراءات فعالة لمصادرة عائدات الجريمة ومقاضاة المجرمين، وتعزيز الجهود الدولية لمنع المهاجمين وتعطيلهم وردعهم، الأمر الذي يخفف من حدة المخاطر، ويتطلب التعاون الوثيق بين أجهزة إنفاذ القانون وجهات القضاء والجهات المسؤولة عن إدارة المعاملات المالية والاقتصادية، أو عن الأمن، عبر البلدان والهيئات المعنية، ولأنّ القراصنة لا يعترفون بالحدود يجب تبني الإنفاذ العالمي للقوانين والاتفاقيات التي تجابه مهددات الأمن السيبراني على المستوى الإقليمي والدولي.

وحيث أصبحت أدوات القرصنة الآن أقل تكلفة وأكثر سهولة وأشهد قوة، مما يتيح للقراصنة ذوي المهارات المحدودة إلحاق ضرر أكبر مقابل نسبة ضئيلة من التكلفة السابقة. ويؤدي التوسع في الخدمات القائمة على الأجهزة المحمولة (وهي المنصة التكنولوجية الوحيدة المتاحة للكثيرين) إلى زيادة فرص القرصنة. ويستهدف المهاجمون المؤسسات كبرىها وصغيرها والبلدان غنيها وفقيرها، ويعملون عبر الحدود. ولذلك يجب أن تكون محاربة الجريمة السيبرانية والحد من مخاطرها مسؤولية مشتركة عبر البلدان وفي داخلها،

³³ انظر حول هذا الموضوع، د. خالد ممدوح العزي، الجرائم المالية الإلكترونية، الجرائم المصرفية أنموذجاً، بحث مقدم في المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس، لبنان، 2024-2025، مارس 2017، ص 6-7.

وبينما لا تزال المؤسسات المالية هي من يضطلع بالعمل اليومي الأساسي في مجال إدارة المخاطر - صيانة الشبكات وتحديث البرمجيات وإنفاذ عملية "نظافة سيبرانية" قوية - فإن هناك حاجة أيضاً لمعالجة التحديات المشتركة وإدراك التداعيات والروابط المتبادلة عبر مختلف أجزاء النظام المالي. فحوافز الاستثمار في الحماية غير كافية بالنسبة لفرادى الشركات؛ والتنظيم والتدخل من جانب السياسة العامة ضروريين للوقاية من نقص الاستثمار وحماية النظام المالي الأوسع نطاقاً من عواقب الهجمات المحتملة.³⁴

وعلى ذلك فإنّ ازدياد حجم وعدد الهجمات السيبرانية، أضحت أكثر قوة، حيث أنّ ما سجلته الشركات في السابق من خسائر طفيفة نسبياً نتيجة الهجمات السيبرانية، شهد بعضها لاحقاً خسائر أكثر حدة، فعلى سبيل المثال، تحملت هيئة الاستعلام الائتماني الأمريكية Equifax غرامات بقيمة تجاوزت مليار دولار أمريكي عقب تعرضها لحادث ضخم عام 2017 نتج عنه اختراق بيانات حوالي 150 مليون عميل، الأمر الذي يستلزم الاستفادة من تلك المخاطر ومواكبة الأجهزة الإدارية والتنظيمية للمؤسسات المالية، وجهات إنفاذ القوانين بتكاتف جهود الأجهزة التشريعية والعدلية لوضع المزيد من المعايير المحاسبية والرقابية.³⁵

الخاتمة:

تظل التعاملات المالية وبشكل خاص المصرفية، هي أكثر القطاعات الاقتصادية تعرضاً لمهددات الأمن السيبراني، لاسيما المخاطر المستقبلية ويرجع هذا إلى طبيعتها الفنية، التي تتداخل بها العديد من التركيبات والحزم والشبكات الرقمية والتكنولوجية، مما يفاقم الإشكالات القانونية التي تؤدي إلى زعزعة العلاقات المالية.

وفي ضوء ما سبق انتهى البحث إلى النتائج والتوصيات التالية:

النتائج:

- 1- تطور المهددات السيبرانية وتجدها، يعد غاية في التعقيد مما يخرجها عن الأطر التنظيمية التقليدية المحددة، الأمر الذي يستلزم وقوف جهات التشريع والقضاء في ترقب دائم ومستمر للاجتهادات التشريعية والفقهية التي تحد من المخاطر التشغيلية والتقنيات المتجددة.
- 2- تطور مهددات الأمن السيبراني، يحفز قطاعات المال والشركات لخلق أنظمة قوية تتبنى تدابير وإجراءات وقائية من تلك المخاطر تجعل تلك الإجراءات أكثر وضوحاً وانضباطاً، ممّا يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر، وتطوير وتحسين الأمن السيبراني، ويخفف وطأة الهجمات السيبرانية ويقلل الخسائر والأضرار الناجمة عنها.
- 3- أنّ السبيل الوحيد لمكافحة الجرائم السيبرانية هو الأمن السيبراني.

³⁴ المخاطر السيبرانية ... التهديد الجديد للاستقرار المالي ، بقلم: جنيفر إليوت ونابجل جنكينسون ، [Jennifer Elliott, Nigel Jenkinson](#) ، 7 ديسمبر 2020.

³⁵ التهديدات السيبرانية المتزايدة تثير شواغل ملحّة حول الاستقرار المالي ، ازداد خطر الهجمات السيبرانية النظامية في ظل نمو التحول الرقمي وتساعد الاضطرابات الجغرافية-السياسية، فابيو ناتالوتشي ، ماهافاش سعيد قرشي ، فيليكس سونثايم ، 11 أبريل 2024

التوصيات:

1. زيادة المعايير الرقابية على المؤسسات والقطاعات المالية، والتي تتطلب أهمية تضمين الإستراتيجيات والسياسات الخاصة بتلك المؤسسات نظم إدارة المخاطر السيبرانية.
2. التحديث الدوري لقوانين حماية الأمن السيبراني وإستراتيجياتها، وتضمين التشريعات المالية قواعد خاصة، تواكب التطور السبراني، للتقليل من المخاطر السيبرانية على المعاملات المالية.
3. التعاون بين المؤسسات المالية الوطنية والإقليمية والدولية لاعتماد معايير وأدلة موحدة لمكافحة الأخطار السيبرانية على المعاملات المالية.
3. إنشاء مراكز وأجهزة دولية حديثة لحماية الأمن السيبراني لتوظيف خبراء من المتخصصين ذوي معرفة تقنية عالية ومواكبة أحدث التقنيات في هذا المجال، وتتضمن مختبرات حديثة لجمع الأدلة الرقمية وتدريب المحققين..
4. نشر الوعي العام بحماية الأمن السيبراني من خلال التعريف بـ التكنولوجيا الملائمة والتطوير المستمر للبحرث والقدرات للحد من المخاطر التكنولوجية المستجدة.

قائمة المصادر والمراجع:

- د. خالد ممدوح العزي، الجرائم المالية الالكترونية، الجرائم المصرفية أنموذجاً، بحث مقدم في المؤتمر الدولي الرابع عشر مركز جيل البحث العلمي: الجرائم الالكترونية، طرابلس، لبنان، مارس 2017.
- د. عبد الله خبابة: الاقتصاد المصرفي، مؤسسة شباب الجامعة، الإسكندرية، ٢٠٠٨.
- د. علم الدين بانقا، مخاطر الهجمات الالكترونية السيبرانية وآثارها الاقتصادية، دراسة حالة، دور مجلس التعاون الخليجي، سلسلة دراسات تنمية، المعهد العربي للتخطيط، الكويت، العدد 63، أبريل 2019.
- د. فارس عمارات، ابراهيم الحمامصه الأمن السيبراني: المفهوم وتحديات العصر، ٢٠٢٢-الطبعة الاولى. دار الخليج للنشر والتوزيع-عمّان؟
- د. مروة فتحي السيد البغدادي، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، الاسكندرية، العدد 26، 2021.
- أ. د عادل موسى عوض جاب الله، وسائل حماية الامن السيبراني "دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة"، مجلة كلية الشريعة والقانون، جامعة الازهر، فرع أسيوط العدد الرابع والثلاثون الاصدار الاول، يناير ٢٠٢٢م الجزء الثالث.
- د. منى الاشقر جبور، إصدارات المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، المركز العربي للبحوث القانونية والقضائية، السيبرانية هاجس العصر. 2016-07-26.

[فابيو ناتالوتشي](#)، [ماهفاش سعيد قرشي](#)، [فيلكس سونثايم](#)، إصدارات صندوق النقد الدولي - الفصل الثالث من عدد إبريل 2024 من تقرير الاستقرار المالي العالمي بعنوان "مخاطر الأمن السيبراني: مخاوف متزايدة إزاء الاستقرار المالي الكلي في ظل نمو التحول الرقمي وتصاعد الاضطرابات الجغرافية-السياسية، أبريل 2024.

جنيفر إليوت ونايجل جنكينسون، مقال منشور على الموقع الإلكتروني لصندوق النقد الدولي، [Jennifer Elliott, Nigel Jenkinson](#) المخاطر السيبرانية ... التهديد الجديد للاستقرار المالي، 7 ديسمبر 2020.

الأمن السيبراني: استراتيجيات حماية البيانات وتجنب الاختراق، ١٩ يوليو ٢٠٢٣م.

قرارات الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا، التشريعات السيبرانية.
<https://archive.unescwa.org/ar/>

كيف يعمل الهاكرز على اختراق الانظمة وكيف يمكن الحماية منهم؟ موقع النجاح ١٥ ديسمبر ٢٠٢٣م.
<https://www.annajah.net/>

منصور الجهني، المؤتمر الدولي الرابع للعلوم الإجتماعية "الكويت" ٢٠١٠م، الجرائم المعلوماتية انواعها وصفات مرتكبيها.

خالد سامر، الأمن السيبراني: تعريفه وأهميته وكيف يعمل ومجالاته وانواع التهديدات والتقنيات الحديثة، ١٩ يناير ٢٠٢٤م، <https://blog.zamn.ap>

ما هو الأمن السيبراني، هيئة الاتصالات والفضاء والتقنية.
<https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx>

الدليل الشامل لفهم الأمن السيبراني الرقمي، ٢٥ ديسمبر ٢٠٢٣م. <https://bluemediasa.com/cyber-security>

حسام عرموش، دليل شامل للأمن السيبراني وحماية البيانات الشخصية <https://www.rmg-s>

الأمن السيبراني: دليلك لحماية البيانات والمعلومات، ٩ مايو ٢٠٢٤م،
المنتدى العربي للأمن السيبراني "حماية البيانات الشخصية عصر الذكاء الاصطناعي، ٣ ديسمبر ٢٠٢٣م.
<https://www.alchourouk.com>

يوسف العيصامي، توصيات المؤتمر الدولي حول "الأمن السيبراني في التشريعات العربية"، ١٩ يوليو ٢٠٢١م، المستقلة بريس. <https://www.almostaquilla-press.com/articles/34265>

مقال بعنوان "من اللغز إلى التشفير: معالم تاريخ الأمن السيبراني" ٢٩/أكتوبر/٢٠٢٣م.
<https://fastdigitaltechnology.com/ar>

الأمن السيبراني: استراتيجيات حماية البيانات وتجنب الاختراق، ١٩ يوليو ٢٠٢٣م.
<https://www.alqiyady.com>

Emanuel Kopp ، Lincoln Kaffenberger, and Christopher Wilson.

“Cyber Risk, Market Failures, and Financial Stability”, Working Paper No.17/185, IMF, 2017.

S. Friedman: “Taking cyber risk management to the next level - Lessons learned from the front lines at financial institutions”, Deloitte Insight, June 2016.