

جامعة محمد البشير الإبراهيمي برج بوعريرج
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم الاقتصادية

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي

الميدان: علوم اقتصادية، تجارية، وعلوم التسيير
الشعبة: علوم اقتصادية
التخصص: اقتصاد نقدي ومالي

من إعداد الطالبتين:

- بن خلف الله منال

- بوجليدة شيماء

بعنوان:

مخاطر التكنولوجيا المالية في القطاع المصرفي وآليات الحد منها

تحت إشراف:

أ.د. موسى بن منصور

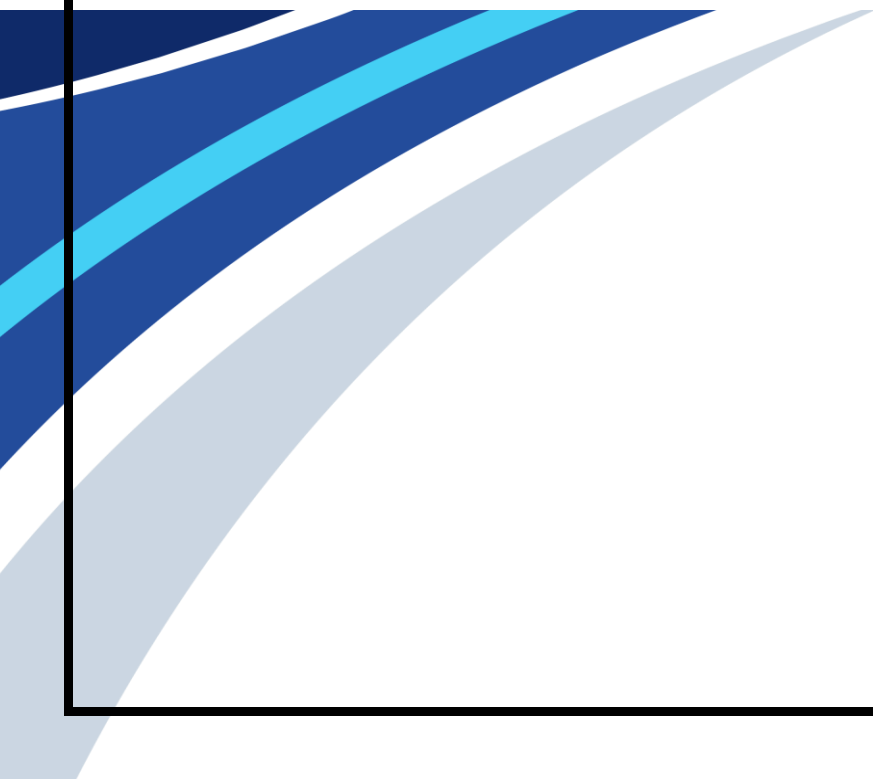
أعضاء لجنة المناقشة

رئيساً	أستاذ التعليم العالي	توفيق براهيم شاوش
مشرفاً	أستاذ التعليم العالي	موسى بن منصور
مناقشاً	أستاذ التعليم العالي	خميسي قايدوي

السنة الجامعية 2024-2025

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

١٤٣٨



الإهداء

لم تكن الرحلة قصيرة ولا طريق محفوفًا بالتسهيلات لكنني فعلتها،

فالحمد لله الذي يسر البدايات وبلغنا النهايات بفضلته وكرمه

اهدي هذا النجاح لنفسي الطموحة أولاً ابثدت بطموح وانتهت بنجاح ثم إلى كل من سعى معي

لإتمام مسيرتي الجامعية دمت لي سنداً لا عمر له

وبكل حب اهدي ثمرة نجاحي وتخرجي :

إلى النور الذي أضاء دربي، إلى العزيز الذي حملة اسمه فخراً، إلى معلمي الأول الرجل الذي

سعى طوال حياته لنكون الأفضل حفظك الله وجزاك عني خير الجزاء ، دمت فخر حياتي

.....والدي العزيز.....

إلى مصدر الأمان الذي استمد منه قوتي إلى نور عيني وحضي الجيد وفوزي وفخري، إلى اليد

الخفية والقلب الحنون وصاحبة الدعاء الصادق أُمي الغالية، إلى ما كانت الداعم الأول لتحقيق

طموحي إلى من كانت ملجأً ويدي اليمنى في حياتي.

.....أُمي الغالية....

إلى ضلعي الثابت وأمان أيامي، إلى ملهمي نجاحي ...إلى خيرة أيامي وصفوتها، إلى قرة عيني

...أخواتي الغاليتين...

إلى صديقتي التي كانت النور في عتمتي، والسند في ضعفي والفرح في أيامي، فأنتي الجزء من

كل خطوة في حياتي شكراً لأنك كنتي دائماً داعمتي

....صديقتي الجميلة...

وآخر دعوانا أن الحمد لله رب العالمين

"منال"

إلى منبع الحنان ومعقد الأمل والرجاء.....رمز التفاني والدي العزيز إجلالا وإكبارا.
إلى من تدمع عينها لفرحي وحزني.....ينبوع الحنان والدتي الحبيبة برا وإحسانا.
إلى مصدر الأمل والعطاء..... أخواتي وإخواني إكراما حبا وفخرا.
إلى من كانت بجانبني في كل لحظة في التعب والضحك في اليأس والأمل.....منال أهديك
هذا العمل الذي كنا نحلم بإنجازه معا وهانحن نصل.
إلى كل من علمني حرفا وإلى من شاركني هذا المشوار الأكاديمي الأستاذ بن منصور
موسى كنت مشرفا ومعينا بعد الله تعالى.
هانحن نطوي آخر صفحة من عمر قضيناه بين جدران الجامعة سنفترق عن مقاعد كانت لنا
وطنا وعن أيام شكلت فينا ما نحن عليه اليوم رحلة لم تكن سهلة.
أهدي هذا العمل لنفسي التي قاومت وثابرت رغم كل الشغرات لأصل لشعور الاعتزاز والفخر.
"شيماء"

شكر وعرفان

الحمد لله رب العالمين والصلوة والسلام على نبيه الصادق الأمين وبعد يسعدنا أن نتقدم بجزيل الشكر

وعظيم الامتنان إلى الأستاذ

"بن منصور موسى"

الذي تفضل بالإشراف على هذه المذكرة وإحاطتنا بالدعم وكرم الأخلاق ومنحنا الكثير من وقته لإخراج هذا العمل في

شكله النهائي

فله كل الشكر والتقدير والاحترام وجعله الله في موازين حسناته كما يسرنا التوجه بجزيل شكرنا إلى أعضاء لجنة المناقشة

الذين تفضلوا بالموافقة على مناقشة المذكرة وإبداء ملاحظاتكم القيمة لإثراء البحث وإجاءته أكثر

ختاماً نتقدم بالشكر لكل من ساهم من قريب أو من بعيد في انجاز هذا العمل والله ولي التوفيق

المخلص:

هدفت هذه الدراسة إلى إبراز المخاطر المختلفة الناشئة عن استخدام التكنولوجيا المالية بتقنياتها المعتمدة في القطاع المصرفي، سواء كانت سيبرانية، تنظيمية وتشريعية، أو متعلقة بالسوق والبيئة والسمعة، من أجل فهم أثارها المحتملة على سلامة واستقرار البيئة المالية في المؤسسات المالية، كما سعت إلى استعراض أبرز الآليات الوقائية والضوابط التي يمكن اعتمادها للتقليل من حدة هذه المخاطر، كتفعيل حوكمة تكنولوجيا المعلومات وتطوير الأطر القانونية وتعزيز التعاون بين مختلف الجهات الرقابية والتنظيمية لضمان بيئة مصرفية آمنة ومستدامة في ظل التحول الرقمي المتسارع.

وقد توصلت الدراسة إلى جملة من النتائج تمحورت حول أن التكنولوجيا المالية على الرغم من مزاياها العديدة في تطوير القطاع المصرفي إلا أنها تحمل معها مخاطر متعددة بإمكانها أن تكون لها آثار عكسية لذا وجب العمل بشكل مستمر على تقديم آليات تسمح بتقليل أو تفادي تلك المخاطر مع الحفاظ على المزايا والآثار الإيجابية التي تتميز بها.

الكلمات المفتاحية: التكنولوجيا المالية، الأمن السيبراني، آليات الحد من المخاطر، حوكمة تكنولوجيا المعلومات.

Abstract:

This study aimed to highlight the various risks arising from the use of financial technology and its adopted techniques in the banking sector, whether they are cyber, regulatory and legislative, or related to the market, environment, and reputation, in order to understand its potential impact on the safety and stability of the financial environment within financial institutions , It also sought to review the key preventive mechanisms and controls that can be adopted to mitigate the severity of these risks, such as implementing information Technology governance, developing legal frameworks, and enhancing cooperation among various regulatory and supervisory authorities, in order to ensure a secure and sustainable banking environment amid the accelerating digital transformation The study reached a set of conclusions, centered around the fact that, despite the numerous advantages of financial technology in advancing the banking sector, it also carries multiple risks that could have adverse effects Therefore, it is essential to continuously provide mechanisms that help reduce or avoid these risks while preserving the benefits and positive impacts that financial technology offers .

Key words: financial technology, Cyber security, information technology Governance, Risk Mitigation Mechanisms.

قائمة المحتويات

العنوان	الصفحة
الإهداء	-
شكر وعرفان	-
ملخص الدراسة	I
قائمة المحتويات	II
قائمة الجداول	III
قائمة الأشكال	IV
مقدمة	أ-ج
الفصل الأول: الإطار المفاهيمي للتكنولوجيا المالية	05
المبحث الأول: مفاهيم أساسية حول التكنولوجيا المالية	09-05
المبحث الثاني: تقنيات التكنولوجيا المالية	18-11
الفصل الثاني: مخاطر التكنولوجيا المالية	21
المبحث الأول: مفاهيم أساسية حول مخاطر التكنولوجيا المالية	25-21
المبحث الثاني: مخاطر أمن المعلومات	41-26
المبحث الثالث: مخاطر أخرى	58-42
الفصل الثالث: آليات الحد من مخاطر التكنولوجيا المالية	61
المبحث الأول: المتطلبات الأمنية للحد من مخاطر التكنولوجيا المالية	66-61
المبحث الثاني: سبل مواجهة المخاطر التنظيمية والتشريعية	69-66
المبحث الثالث: حوكمة التكنولوجيا المعلومات	76-70
الخاتمة	78-76
قائمة المراجع	85-80
فهرس المحتويات	88-87

قائمة الجداول

الصفحة	عنوان الجدول	رقم الجدول
09	مراحل تطور الثورة الصناعية	01
52	أمثلة رئيسية للمخاطر القانونية وكيفية تأثيرها	02

قائمة الأشكال

رقم الشكل	عنوان الشكل	الصفحة
01	طريقة عمل الحوسبة السحابية	16
02	نمو سوق برمجيات الذكاء الاصطناعي العالمي	19
03	طبقات الفضاء السيبراني	35
04	مرتكزات الأمن السيبراني	37
05	أبعاد الأمن السيبراني	38
06	أنواع المخاطر السيبرانية	39
07	أنواع الهجمات الإلكترونية (السيبرانية)	43
08	وضع إجمالي المدفوعات السنوية لبرامج الفدية	48
09	أنواع المخاطر التنظيمية	50
10	أنواع مخاطر الامتثال	50
11	أنواع مخاطر السمعة	18
12	أهم أنواع مخاطر السوق	23

مقدمة

يقصد بالتكنولوجيا المالية على أنها الاختراعات أو الابتكارات التكنولوجية الحديثة في مجال القطاع المالي التي تشمل مجموعة من البرامج الرقمية التي تستخدم في العمليات المالية للبنوك مثل المعاملات مع الزبائن وتحويل الأموال، والتي زاد انتشار استخدامها خاصة مع توسع التحرير المالي والثورة التكنولوجية، ولعل ما أثبت حاجة القطاعات المالية لهذه الاستخدامات هي موجة كوفيد 19 الذي يعتبر أكبر وأعرق أزمة في العالم حيث أحدث تغيرات جذرية شاملة وقوية مست جميع القطاعات، أين أثبتت مختلف منتجات التكنولوجيا المالية فعاليتها في ربط الزبائن بمؤسساتهم المصرفية، ويعد قطاع المصارف من أكثر القطاعات تأثراً وارتباطاً بالتكنولوجيا المالية، حيث قامت بتقديم العديد من الحلول والخدمات المالية الرقمية المبتكرة بطرق سريعة وسهلة، وأقل تكلفة، إضافة إلى دورها الكبير في توسيع نطاق الوصول إلى الخدمات المالية لكافة شرائح المجتمع والمساهمة في الرفع من مستويات الشمول المالي وتعزيزه، ورغم التطور الهائل في الخدمات المالية نتيجة لاستخدام تكنولوجيا الاتصال والرقمنة، إلا أنها لا تخلو من المخاطر والتحديات المعقدة، التي تتجاوز في طبيعتها الإطار التقني لتشمل الجوانب القانونية والتنظيمية وحتى الأخلاقية، ما قد يؤدي إلى زعزعة استقرار الأسواق المالية وأمن البيانات وتراجع ثقة المستخدمين في الأنظمة الرقمية، وفي ضوء هذه التحديات أصبح من الضروري تطوير آليات فعالة للحد من هذه المخاطر، من خلال التحديث المستمر للأطر التشريعية والتنظيمية، وتعزيز الأمن السيبراني.

إشكالية الدراسة: على ضوء ما سبق تمحورت إشكالية الدراسة في السؤال الرئيسي التالي:

ما هي أهم مخاطر التكنولوجيا المالية على النظام المصرفي وما هي السبل الكفيلة للحد منها؟

من أجل معالجة وتحليل هذه الإشكالية وبغية الوصول إلى فهم واضح لها، تم طرح الأسئلة الفرعية التالية:

- ما هي مخاطر التكنولوجيا المالية وما هي أهم خصائصها؟
- ماهي الأنواع المختلفة للمخاطر الناتجة عن استخدام التكنولوجيا المالية في القطاع المصرفي؟
- فيما تكمن الإجراءات المتخذة من قبل الأنظمة المصرفية ومؤسسات التكنولوجيا المالية لمجابهة وإدارة تلك المخاطر عبر العالم؟

فرضيات الدراسة:

للإجابة عن الأسئلة المطروحة السابقة ومن ثم معالجة إشكالية الدراسة تمت صياغة الفرضيات التالية:

- لمخاطر التكنولوجيا المالية خصائص تختلف عن بقية المخاطر بسبب ارتباطها بالتقنيات الحديثة.
- تتعد مخاطر التكنولوجيا المالية حيث تشمل ما هو تقني كالهجمات السيبرانية، وما هو قانوني وتنظيمي مثل غياب الأطر القانونية الملائمة.
- هناك العديد من المحاولات الدولية التي ساهمت من تقليل أضرار هذه المخاطر.

أهمية الدراسة:

تستمد هذه الدراسة أهميتها من أهمية الموضوع بحد ذاته، حيث تناولت موضوع التكنولوجيا المالية الذي أصبح مثيرا للاهتمام في القطاع المالي، وكذلك يعتبر مسلكا لتطوير وعصرنة المنظومة المالية والمصرفية، كما ركزت على نظرة أخرى للتكنولوجيا المالية وهي أهم المخاطر المرتبطة باستخدام تقنيات التكنولوجيا المالية وكيفية التعامل معها ليس فقط التركيز على مزاياها.

أهداف الدراسة:

تسعى هذه الدراسة إلى الوقوف على ماهية التكنولوجيا المالية، أو ماهية المخاطر التي تعيق تطورها وانتشارها، مع الإشارة إلى أهم الأساليب التي انتهجتها العديد من الدول في سبيل تقادي تلك المخاطر وأثارها العكسية.

منهج الدراسة:

في إطار هذا البحث ومن أجل معالجة إشكالية موضوع الدراسة تم الاعتماد على المنهج الوصفي التحليلي، وهو المنهج الأكثر استخداما وشيوعا في العلوم الاقتصادية والتجارية وعلوم التسيير، وقد اعتمدت الدراسة في جمع المعلومات من مصادر كالكتب والمقالات العلمية، مما ساعد في بناء تصور عن الإطار النظري لمخاطر التكنولوجيا المالية وإبراز أسبابها وأثارها المختلفة على النظام المصرفي، كما تطرقت لإبراز الآليات المتبعة للحد من هذه المخاطر على المستويين المحلي والدولي.

حدود الدراسة:

- الحدود الموضوعية: تناولت هذه الدراسة مخاطر التكنولوجيا المالية في النظام المصرفي والية الحد منها.

أسباب اختيار الموضوع: هناك عدة أسباب لاختيار هذا الموضوع منها ما هو ذاتي وما هو موضوعي نوجزها فيما يلي:

- ارتباط الموضوع بمجال تخصصنا وهو الاقتصاد النقدي والمالي؛
- الميول الشخصي لكل المواضيع التي تخص التكنولوجيا المالية؛
- حداثة الموضوع والانتشار الواسع للتكنولوجيا المالية.

الدراسات السابقة

تناولت موضوع مخاطر التكنولوجيا المالية في النظام المصرفي وآلية الحد منها العديد من الدراسات إما بشكل مباشر أو غير مباشر، لعل أهم هذه الدراسات ما يلي:

■ دراسة جريوة إلهام، "دور التكنولوجيا المالية في تطوير الأداء المصرفي"، أطروحة دكتوراه، تخصص اقتصاد نقدي وبنكي، جامعة غرداية، 2024/2023. هدفت هذه الدراسة إلى إبراز أهمية التكنولوجيا المالية في تحقيق جودة الأداء المصرفي، من خلال وصول الخدمات المصرفية لكافة العملاء وكذلك تخفيض التكاليف والوقت وبالمقابل تقديم خدمات سريعة وجودة أكثر، واكتشاف التحديات التي تواجه المصارف الجزائرية في تبني التكنولوجيا المالية، خاصة في ظل التأخر في التحديث الرقمي. وقد خلصت هذه الدراسة إلى عدة نتائج أهمها وجود أثر إيجابي للتكنولوجيا المالية على الأداء المصرفي من حيث الكفاءة، السرعة، وتوسيع قاعدة العملاء. ووجود تحديات الكبيرة تواجه المصارف الجزائرية في هذا المجال، خاصة ما يتعلق بالبنية التحتية الرقمية، والكوادر المؤهلة، والتشريعات القانونية.

■ دراسة ساعد بوقرص، "الأمن السيبراني وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة"، مجلة الأبحاث في الحماية الاجتماعية، المجلد 03، العدد 01، السنة 2022. هدفت هذه الدراسة إلى تسليط الضوء على واحدة من أهم مخاطر التكنولوجيا المالية وهي الأمن السيبراني والتهديدات والتحديات الأمنية المتزايدة في البيئة الرقمية، وتحديد أبرز المخاطر التي تواجه الأفراد والمؤسسات في هذا الإطار، مع الإشارة إلى السبل الوقائية من هذه التهديدات وتقوية الأمن المعلوماتي لمؤسسة أو البلد كالجزائر. وقد خلصت هذه الدراسة إلى عدة نتائج أهمها ضرورة رفع الوعي بأهمية الأمن السيبراني وأثره على المؤسسات والأفراد ومحاولة تطوير استراتيجيات مرنة وشاملة يمكن تطبيقها على المؤسسات المختلفة لتحسين إدارة المخاطر السيبرانية.

■ دراسة محمد قوجيل، عبد العزيز طيبة، "مخاطر التكنولوجيا المالية في القطاع المصرفي _دراسة تنظيمية واحترافية_، مجلة الاقتصاد والمالية، المجلد 08، العدد 02، 2022. هدفت هذه الدراسة إلى تسليط الضوء على المخاطر المختلفة المرتبطة باستخدام التكنولوجيا المالية في القطاع المصرفي، حيث قامت بمراجعة مجموعة من التدابير التنظيمية والاحترافية التي وضعتها جهات مختلفة. وقد خلصت هذه الدراسة إلى عدة نتائج أهمها الحاجة إلى فهم المتكامل لأنواع المخاطر المالية المرتبطة بالتكنولوجيا المالية (مخاطر السوق، مخاطر السمعة...) وضرورة وضع خطط لتجنب هذه المخاطر وكذلك ضمان سيرورة عمل العمليات المصرفية.

■ Fitri Amalia "The Fintech Book: the financial technology handbook for investors; entrepreneurs and visionaries"، journal of Indonesian Economy and business, volume 31, number 03, 2016.

هدفت هذه الدراسة إلى تسليط الضوء على الأسواق الناشئة وحلول التكنولوجيا المالية لهذه الأسواق، وكيفية تأثير التكنولوجيا على أنماط الدفع والتمويل والاستثمار وتحليل، المساهمات المختلفة من شركات والتي 20 دولة. وقد خلصت هذه الدراسة إلى عدة نتائج أهمها أن ظهور التكنولوجيا المالية أدى إلى زيادة الشمول المالي من خلال تسهيل الوصول إلى القروض والاستثمار والتمويل الجماعي. وأن التكنولوجيا المالية توفر

حلول حيوية للشركات الصغيرة والمتوسطة التي تعاني من محدودية الوصول إلى الخدمات المالية التقليدية في الدول النامية.

✚ هيكل الدراسة:

لمعالجة الإشكالية المطروحة والإجابة على الأسئلة المتفرعة عنها قسمنا هذه الدراسة إلى ثلاثة فصول، **الفصل الأول** يتضمن الإطار المفاهيمي للتكنولوجيا المالية، حيث قسم إلى مبحثين، المبحث الأول يتناول المفاهيم الأساسية للتكنولوجيا المالية، أما المبحث الثاني يتناول تقنيات التكنولوجيا المالية، بينما خصصنا **الفصل الثاني** لتغطية أهم مخاطر التكنولوجيا المالية، حيث تم تقسيمه إلى ثلاثة مباحث، المبحث الأول تم فيه تقديم المفاهيم الأساسية حول مخاطر التكنولوجيا المالية، وقمنا بتسليط الضوء في المبحث الثاني على مخاطر امن المعلومات، أما المبحث الثالث تم التركيز على المخاطر الأخرى للتكنولوجيا المالية، وفي **الفصل الثالث** والأخير تطرقنا إلى آليات الحد من مخاطر التكنولوجيا المالية، حيث تم تقسيم هذا الفصل إلى ثلاثة مباحث، المبحث الأول يتناول المتطلبات الأمنية للحد من مخاطر التكنولوجيا المالية، أما المبحث الثاني يتناول الحماية التشريعية والتنظيمية من مخاطر التكنولوجيا المالية، والمبحث الثالث يركز على حوكمة التكنولوجيا المالية، كما تم في النهاية إعداد خاتمة الدراسة التي تضمنت نتائج الفصول مع توضيح اختبار صحة الفرضيات، متبوعة بجملة من الاقتراحات المستنتجة، وأخيرا تم صياغة آفاق الدراسة.

✚ صعوبات الدراسة:

واجهتنا في سبيل إتمام مختلف جوانب هذه الدراسة العديد من الصعوبات أهمها قلة الكتب حول موضوع التكنولوجيا المالية، وعدم توفر البيانات والإحصائيات حول حجم بعض أنواع المخاطر وحجم أثارها الجزئية والكلية.

الفصل الأول:

الإطار المفاهيمي للتكنولوجيا المالية

تمهيد:

ساهمت التكنولوجيا المالية في تغيير البيئة الرقمية حيث طورت خدمات الدفع الإلكتروني والخدمات المصرفية وساهمت في تحقيق الكفاءة والفعالية إلى أن أصبحت تلعب دور رئيسي في تطوير النظام المالي. وفي هذا الفصل سنتطرق إلى ماهية التكنولوجيا المالية ومراحل تطور وأهم تقنياتها في المبحثين التاليين:

المبحث الأول: مفاهيم أساسية للتكنولوجيا المالية.

المبحث الثاني: تقنيات التكنولوجيا المالية.

المبحث الأول: مفاهيم أساسية للتكنولوجيا المالية

عُرفت التكنولوجيا المالية كظاهرة تجمع بين الابتكار التكنولوجي والخدمات المالية، بهدف تحسين الكفاءة وتبسيط المعاملات المالية، كما يشير مفهوم استخدام التكنولوجيا المالية إلى تقديم الخدمات المالية بطرق أسرع باستخدام تقنيات متطورة، وفي هذا المبحث تطرقنا لأهم العناصر التي تبرز المفهوم الدقيق للتكنولوجيا المالية مع التركيز على خصائصها ومجالات استخدامها المتعددة مع إبراز أهميتها المتزايدة.

المطلب الأول: تعريف التكنولوجيا المالية وخصائصها

التكنولوجيا المالية هي أحد أبرز ملامح التغيير في النظام المالي حيث اندمجت الابتكارات التكنولوجية مع الخدمات المالية، لإنتاج حلول أكثر فاعلية وسرعة وأماناً ومرونة في تلبية احتياجات المستخدمين، وفي هذا المطلب سنقدم أهم تعريفات لتكنولوجيا المالية مع ذكر أهم خصائصها.

أولاً: تعريف للتكنولوجيا المالية:

قبل التطرق لتعريف التكنولوجيا المالية لابد أولاً من تعريف مصطلح التكنولوجيا بشكل عام، الذي يحتوي على كلمتي هما:¹

- تكنو: هو لفظ يوناني قديم يعني الصناعة أو التشغيل؛
- لوجيا: هو لفظ مشتق من اللغة اليونانية القديمة أيضاً، ويعني علم أو منهج.

¹ ابن قيده مروان وآخرون، التكنولوجيا المالية الابتكارات والحلول الرقمية، كتاب جماعي، مخبر التنمية المحلية المستدامة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة يحي فارس، المدينة، الجزائر، 2022، ص 62.

- **التعريف الأول:** هي أي ابتكار يتم توظيفه في الخدمات المالية، أو أي أفكار مبتكرة تهدف إلى تحسين عمليات إدارة الخدمات المالية من خلال اقتراح حلول تقنية وفقا لمواقف العمل المختلفة، وقد تؤدي الأفكار المبتكرة أيضا إلى نماذج أعمال جديدة.²
- **التعريف الثاني:** هي مشتقة من اقتران منطقتين متكاملتين، الخدمات المالية والحلول القائمة على التكنولوجيا المتقدمة، وقد ترجمت كلمة بكاموس أكسفورد على النحو التالي برامج الكمبيوتر وغيرها من التقنيات المستخدمة لدعم أو تمكين الخدمات المصرفية والمالية.³
- **التعريف الثالث:** عرفها معهد البحوث الرقمية في العاصمة البولندية "دبلن" بأنها: عبارة عن الاختراعات والابتكارات التكنولوجية الحديثة في مجال قطاع المالية، وتشمل هذه الاختراعات مجموعة من البرامج الرقمية التي تستخدم في العمليات المالية للبنوك والتي ضمنها (المعاملات مع الزبائن والخدمات المالية مثل تحويل الأموال وتبديل العملات وحسابات نسب الفائدة) وغير ذلك من العمليات المصرفية.⁴
- **التعريف الرابع:** عرف مجلس الاستقرار المالي التكنولوجيا المالية بأنها ابتكارات مالية باستخدام التكنولوجيا يمكنها استحداث نماذج أو تطبيقات أو عمليات أو منتجات جديدة، لها أثر مادي وملاموس على الأسواق والمؤسسات المالية، وعلى تقديم الخدمات المالية بحيث يحدد التعريف العناصر الأساسية للتكنولوجيا المالية، والمتمثلة فيما يلي:
 - **ابتكارات مالية:** هي وليدة استخدام التكنولوجيا المالية، وبالتالي يحدد التعريف الوصول لمنتجات مالية مبتكرة باستخدام وسائل تكنولوجية متطورة في مجال المعاملات المالية، مما يؤدي إلى اختفاء النقود الورقية بشكل كامل من التداول.
 - **استخدام التكنولوجيا:** الشق الضروري لابتكار وتسويق المنتجات المالية التي تزيد من النشاط المالي للمؤسسات المالية.
 - **الأثر المادي:** إن انتشار المنتجات المالية المعتمدة على التكنولوجيا، من شأنه ترك الأثر الحقيقي على النشاط الاقتصادي والمالي، من حيث زيادة التوظيف المالي وتوفير التمويل اللازم للنشاط الاقتصادي، بما يترك أثرا

² هشام حمزة، التكنولوجيا المالية (مفهوم، تطور، مخاطر)، مجلة الكترونية تصدر عن المعهد المصرفي المصري لمتابعة مستجدات القطاع المصرفي ورصد آراء القائمين على الصناعة المصرفية المصرية، Ebi. masrafeyou. http://www. Eg Gov. (13،1130/02/2025).

³ عمارية بخته، غنية مجاني، دور تكنولوجيا المالية في دعم القطاع المصرفي، مجلة (المدير) المجلد 07، العدد 02، 2020، ص98.

⁴ نور الدين كروش، مستقبل الصناعة المصرفية الإسلامية في ظل تطورات التكنولوجيا المالية، مجلة الدراسات المحاسبية والمالية المتقدمة، المجلد 04، العدد 02، أكتوبر 2020، ص118.

ملموسا على اقتصاديات الدول المعتمد للتكنولوجيا المالية من خلال زيادة مساهمة القطاع المالي في الناتج المحلي الإجمالي.⁵

- **تعريف لجنة بازل للرقابة المصرفية:** التكنولوجيا المالية هي أي تكنولوجيا أو ابتكار مالي ينتج عنه أعمال أو عملية أو منتج جديد له تأثير على الأسواق والمؤسسات المالية. ومن التعاريف السابقة، نستنتج أن التكنولوجيا المالية توصف على أنها تعتبر صناعة مالية جديدة تتضمن تلك المنتجات والخدمات، التي تعتمد على التكنولوجيا لتحسين نوعية الخدمات المالية، وتتميز هذه التكنولوجيا بأنها أسرع، أرخص وأسهل.

ثانياً: خصائص التكنولوجيا المالية

تعد التكنولوجيا المالية من أبرز التطورات التي غيرت شكل الخدمات المالية في العالم، فهي تجمع بين التكنولوجيا والتمويل لتقديم خدمات مالية بطرق جديدة وأكثر سهولة، ولفهم هذه السهولة من المهم التعرف على الخصائص الأساسية للتكنولوجيا المالية، التي يمكن حصرها فيما يلي:⁶

- **تكلفة أقل:** يسمح لعدد أكبر من المستخدمين للوصول إلى الخدمات المالية وخاصة الشركات والأفراد غير المخدمين مصرفياً؛
- **خصوصية أكثر:** خدمات ومنتجات التكنولوجيا المالية مصممة وفقاً لرغبات العملاء الشخصية فكل بنك له حاجات مختلفة عن حاجات المصارف الأخرى ويمكن الوصول إلى ذلك من خلال عدد من القنوات؛
- **سرعة أكبر:** منتجات وخدمات التكنولوجيا المالية تعتمد غالباً على التكنولوجيا التقنية لإنجاز الإجراءات والعمليات وهذا يعني توفير وتيرة أسرع للخدمات؛
- **انتشار أوسع:** منتجات وخدمات التكنولوجيا المالية ممكن أن تكون عابرة للحدود حيث يمكنها خدمة عملاء لا ينتمون لبقعة جغرافية واحدة؛
- **قابلية للمقارنة:** إذ أن خدمات ومنتجات التكنولوجيا المالية تمكن عملاء من المقارنة بين العديد من الشركات والمصارف من حيث الخدمة المالية والأسعار.

بالإضافة إلى الخصائص الأساسية السابقة يمكن الإشارة إلى بعض الخصائص الأخرى التالية:⁷

⁵علاش أحمد، دور التكنولوجيا المالية في دعم النشاط المالي والابتكار تجربة البحرين، مجلة الإبداع، المجلد 9، العدد 1، 2019، ص332.

⁶كوثر طلحي، نهاد زواوي، دور ابتكارات التكنولوجيا المالية في تطوير الخدمات المالية الإسلامية، مجلة دراسات في المالية الإسلامية والتنمية، المجلد 04، العدد 7، 2023، ص35.

⁷بن قيدة مروان وآخرون، مرجع سابق، ص 62.

- التكنولوجيا المالية هي مجموعة من المعارف والمهارات والطرق والأساليب المالية والمصرفية؛
- التكنولوجيا بمفاهيمها المختلفة ليست هدفا في حد ذاته بل وسيلة تستخدمها المؤسسات المالية والمصرفية لتحقيق أهدافها؛
- إن الخدمة المالية المصرفية في المجال الرئيسي لتطبيق التكنولوجيا لا يقتصر على أداء الخدمة المالية والمصرفية بل يمتد إلى الأساليب الإدارية.
- وأيضا: ⁸ هي منتجات وخدمات تعتمد على التكنولوجيا لتحسين نوعية الخدمات المالية التقليدية؛
- تتميز التكنولوجيا المالية بأنها سهلة وسريعة ومنخفضة التكلفة؛
- يمكن لعدد كبير من الأفراد الوصول لخدمات التكنولوجيا المالية؛
- التكنولوجيا المالية ليست هدفا بقدر ما هي وسيلة.

المطلب الثاني: التطور التاريخي للتكنولوجيا المالية

لمعرفة التطور التاريخي للتكنولوجيا المالية يجب أولا المرور على مراحل الثورة الصناعية حيث مرت كما يوضحها الجدول بأربعة مراحل رئيسية، استخدمت في المرحلة الأولى الطاقة البخارية والماء لميكنة وزيادة الإنتاج، واستخدمت في المرحلة الثانية الطاقة الكهربائية للإنتاج الضخم، في حين استعملت الثورة الصناعية الثالثة الالكترونيات المتقدمة وتكنولوجيا المعلومات لجعل الإنتاج مستقلا، أما الثورة الصناعية الرابعة فقد انطلقت منذ منتصف القرن الماضي والتي تتميز بثورة رقمية تتجسد في اندماج التقنيات والأنظمة المادية السيبرانية التي تلمس الخطوط الفاصلة بين المجالات الاقتصادية والمادية والبيولوجية والرقمية.

الجدول رقم (01): مراحل تطور الثورة الصناعية

المرحلة الأولى	المرحلة الثانية	المرحلة الثالثة	المرحلة الرابعة
من 1780 إلى نهاية القرن 18	من 1870 إلى بداية ق 19	1960_1970	من 1970 إلى الآن
إدخال أول مرافق التصنيع الميكانيكية التي تعمل بالماء والبخار	إدخال الإنتاج الضخم الذي يعمل بالطاقة الكهربائية	استخدام الالكترونيات وتكنولوجيا المعلومات لتحقيق مزيد من أتمتة التصنيع	إدخال الأنظمة المادية السيبرانية Cyber physical Systems

⁸براهيمي فائزة، مساهمة تقنية سلسلة الكتل في تعزيز التكنولوجيا المالية، مجلة التنمية والاستشراف للبحوث والدراسات، المجلد 06، العدد 02، ديسمبر 2021، ص 97.

المصدر: بوخاري لحلو، مدخل إلى التكنولوجيا المالية، محاضرات مقدمة لطلبة السنة الثانية ماستر، من موقع https://elearning.univ_bba.dz

أولاً: مراحل تطور التكنولوجيا المالية

مرت عبر ثلاث مراحل أساسية نذكرها:

- **المرحلة الأولى (1866_1967):** ظهرت هذه المرحلة مع تمرير أول كابل اتصالات عبر المحيط الأطلسي، فيما ظهر في عام 1918 ما يطلق عليه بنظام Fed wire والذي يعتبر أول نظام تحويل أموال إلكتروني، وفي عام 1950 تم تقديم بطاقات الائتمان الحديثة، وفي عام 1966 تم إنشاء شبكة التلكس العالمية التي تلعب دورا هاما في توفير الاتصالات اللازمة للمرحلة التالية في تطوير التكنولوجيا المالية.
- **المرحلة الثانية (1967_2008):** في هذه المرحلة بقيت التكنولوجيا المالية مهيم علىها داخل قطاع صناعة الخدمات المالية التقليدية حيث تمثل هذه الفترة التحول من التناظرية إلى الرقمية ولقد تم فيها إطلاق أول آلة حاسبة محمولة و أول صراف آلي تم تبييته من قبل بنك Barclays عام 1967، كما تميزت هذه المرحلة بإنشاء بورصة ناسداك NASDAQ أول بورصة رقمية في العالم والتي تعتبر بداية لكيفية عمل الأسواق المالية و في عام 1973 ثم تأسيس SWIFT جمعية الاتصالات المالية بين البنوك في جميع أنحاء العالم، ولازلت تعتبر من الاتصالات الأكثر استخداما مابين المؤسسات المالية مما يسهل حجم المدفوعات عبر الحدود، في حين شهدت ثمانينات القرن العشرين ظهور أجهزة الكمبيوتر في العالم، حيث تم تقديم الخدمات المصرفية عبر الانترنت إلى العالم والتي ازدهرت في التسعينات من خلال نماذج أعمال الانترنت و التجارة الالكترونية ولقد أحدثت المصرفية عبر الانترنت تحولات كبيرة في كيفية فهم الناس للمال و علاقتهم بالمؤسسات المالية وانتهى هذا العصر بالأزمة المالية العالمية 2008.
- **المرحلة الثالثة (2008_حتى الآن):** يمكن القول إن الأزمة المالية العالمية لعام 2008 كانت نقطة تحول كبرى في تاريخ التكنولوجيا المالية حيث أثرت على فئتين من الناس، الأولى الناس الذين فقدوا الثقة في النظام المصرفي والفئة الثانية تتمثل في المتخصصين الماليين الذين فقدوا وظائفهم وأصبحوا الآن اقل تعويضا. كان غضب الناس وتآكل ثقتهم في النظام المصرفي، بمثابة ارض خصبة مثالية للابتكار المالي مما فسح المجال لصعود التكنولوجيا المالية يعتبر هذا توقيتا جيدا لان المواطنين الرقميين (جيل الألفين) أصبحوا كبارا بما يكفي ليكونوا عملاء محتملين، وكانت تفضيلا تهم تشير إلى خدمات الهاتف المحمول التي فهموها وأتقنوها بدلا من

المصرفيين الذين لا يملكونهم الاتصال بهم سمحت هذه الظروف لمقدمي التكنولوجيا المالية عرض خدمات جديدة وحديثة بتكلفة أقل من خلال المنصات مصممة جيدا، أو تطبيقات الهاتف المحمول.⁹

المطلب الثالث: أهمية ودوافع تبني التكنولوجيا المالية

في ظل التحول الرقمي الذي يشهده العالم فقد أصبح تبني التكنولوجيا المالية أمرا ضروريا حيث يساهم في تحسين الخدمات المالية وجعلها أسرع وأكثر كفاءة وأسهل في الوصول لجميع فئات المجتمع، كما تبني هذه التكنولوجيا كان بعدة دوافع مثل انتشار الانترنت ورغبة العملاء في خدمات سريعة وآمنة وفي هذا المطلب سنوضح أهمية التكنولوجيا المالية ودوافع تبنيها.

أولا: أهمية التكنولوجيا المالية

تساهم التكنولوجيا المالية في رفع كفاءة تقديم الخدمات المالية وتحسين خدمة العملاء كما يمكن أن تساهم في تحفيز التنوع الاقتصادي والنمو المنشئ لفرص الحصول على التمويل، فضلا عن ذلك فإن التكنولوجيا المالية تفرض على المنظمين والمشاركين في السوق تحديات في الموازنة بين العوائد والمخاطر المحتملة للابتكارات المالية الحديثة لضمان استمرارهم وبقائهم في السوق، يمكن تلخيص أهميتها في النقاط التالية:

- تعطي مجموعة كبيرة من الخدمات المالية مثل: عمليات التمويل الجماعي، وحلول الدفع عبر الانترنت، والتحويلات المالية الدولية، وأدوات إدارة المحافظ الاستثمارية بالانترنت والتي عززت المصارف التقليدية عن تقديمها لعدد كبير من المتعاملين؛
- تعمل على تغيير هيكل الخدمات المالية بشكل عام، واليات تقديم الخدمات المصرفية للعملاء بشكل خاص مما يجعلها أسرع وأرخص وأكثر أمانا وشفافية وإتاحة لهذه الخدمات؛
- تساهم في تحقيق ميزة تنافسية للمؤسسات المالية والشركات الناشئة في مجال التكنولوجيا المالية فكلما كانت هذه المؤسسات أكثر تقدما من الناحية التكنولوجية كلما زادت قدرتها على المنافسة بالمستويين الإقليمي والدولي؛
- تحقيق الشمول المالي إذ تساعد تطبيقات التكنولوجيا المالية الملايين من العملاء من الاندماج المالي، وذلك نتيجة سهولة الوصول إلى الخدمات المالية؛

⁹أنظر: بوطريف لويظة، واقع التكنولوجيا المالية الإسلامية في ظل التحديات الراهنة، مجلة الأصيل للبحوث الاقتصادية والإدارية، المجلد 05، العدد 02، ديسمبر 2021، ص 470 وبوخاري لحلو، مدخل إلى التكنولوجيا المالية، محاضرات مقدمة لطلبة السنة الثانية ما ستر، من موقع: https://elearning.univ_bba.dz.

- تعزيز فرص الامتثال بالقوانين الدولية والتعاون بين البنوك من خلال دعم عمليات مكافحة تمويل الإرهاب وغسل الأموال، كذلك زيادة وسهولة التعاون بين البنوك في مجال الامتثال بالقوانين المصرفية العالمية.¹⁰

ثانياً: العوامل التي ساعدت في التحول إلى التكنولوجيا المالية:

- يرجع تحول إلى التكنولوجيا المالية إلى تطور الهائل في الصناعات التكنولوجية مما يؤدي إلى حتمية استخدامها، فيمكن حصر هذه العوامل فيما يلي:
- ثورة الاتصالات والمعلومات: كانت من أهم المحركات الرئيسية، التي أحدثت تحولاً وتغيراً جوهرياً في طبيعة عمل القطاع المالي، حيث وفرت أدوات سمحت بابتكار خدمات مالية جديدة تتسم بالسرعة، السهولة والأمان.
- الوتيرة السريعة: إذ تستخدم فيها الهواتف الذكية والانترنت، حيث أن هذا القطاع ابرز تغيرات متلاحقة ومستمرة بفعل الابتكار التكنولوجي المتواصل، فكل يوم تقريباً تظهر حلول جديدة تعتمد على الذكاء الاصطناعي.
- التجارة الالكترونية: تلعب التجارة الالكترونية دوراً محورياً في دعم وتطوير التكنولوجيا المالية، ولقد أدى إلى تسريع الحاجة إلى حلول مالية رقمية مرنة وسريعة.
- تزايد دخول العديد من المؤسسات المالية غير المصرفية: كشرركات التأمين وشركات التمويل، ومنافستها للبنوك حتى أصبحت العديد من المؤسسات يقدم مجموعة خدمات مالية وثيقة الصلة بعمل البنوك.
- القبول المتزايد من العملاء للخدمات المالية: يرجع القبول لها بسبب التأثير الإيجابي للعمليات والخدمات المالية، وذلك لسهولة الاستخدام، إذ يمكن للعملاء إدارة شؤونهم المالية على مدار الساعة بفضل التطبيقات والمواقع الالكترونية المتاحة.

المبحث الثاني: تقنيات التكنولوجيا المالية

أحدثت التكنولوجيا المالية تغيرات جذرية في قطاع الخدمات المالية، حيث باتت تستخدم في تقديم العديد من الخدمات سواء للأفراد أو الشركات والمؤسسات المالية بطرق سريعة وسهلة وبأقل تكلفة، وتتفاعل الموجة الجديدة من ثورة التكنولوجيا المالية بشكل مكثف مع التقنيات الجديدة، وسنتعرف عليها من خلال مطلبين، الأول يركز على تقنية البلوك تشين، والثاني حول الحوسبة السحابية، والمطلب الثالث حول الذكاء الاصطناعي.

المطلب الأول: تقنية البلوك تشين

¹⁰ كوثر طلحي، مرجع سابق، ص35.

تعتبر تقنية البلوك تشين من أبرز الابتكارات التكنولوجية في القرن الحادي والعشرين، وقد بدأت في الظهور بشكل واضح مع ظهور العملات الرقمية مثل البيتكوين، ورغم أنها لا تزال في مراحلها الأولى إلا أن مستقبلها يبدو واعدا في بناء أنظمة أكثر عدالة وشفافية حول العالم.

أولاً: الخلفية التاريخية لتقنية البلوك تشين.

كان أول ظهور لتقنية البلوك تشين سنة 2008 على يد الياباني "ساتوشي ناكاموتو" كجزء من عملة البيتكوين الرقمية، فقد أرسل "ساتوشي" دراسة تقييمية إلى البريد الإلكتروني الخاص بقائمة من المعروفين باهتمامهم بالعملات المشفرة، تضمنت الدراسة المبادئ الأساسية التي تقوم عليها كل من عملة البيتكوين والطريقة التي تعتمد عليها، وفي السنة الموالية وضع "ساتوشي" أول تقنية بلوك تشين موضع التنفيذ بعدما أقدم على تعدين أول عملة بتكوين وطرحها للتداول، وقد حققت هذه العملة شهرة واسعة ورواجا عالميا.

فقد تمكن "ساتوشي" من تعدين 50 وحدة منها، ليعقبها أول صفقة للعملة بين "ناكاموتو وال فيني"، كما أن سعر البيتكوين وصل إلى 1 دولار سنة 2011. إن ظهور البلوك تشين كان مرافقا لظهور البيتكوين، مما جعل البعض لا يفرق بينهما ويعتبرهما وجهان لعملة واحدة، لكن في الأصل هما مختلفتين، فالبلوك تشين تسمح بتخزين المعاملات في البيتكوين ولها استخدامات أخرى، أما البيتكوين فليست سوى الاستخدام الأول للبلوك تشين.¹¹

ثانياً: تعريف تقنية البلوك تشين

- **التعريف الأول:** البلوك تشين عبارة عن دفتر أستاذ موزع لا مركزي تسجل فيه المعاملات متسلسلة زمنياً، يتم الاعتماد في تسجيلها على التشفير ما يجعلها مضادة للعبث، وتُسجل المعاملات بطريقة مترابطة ككتل حيث تكون كل معاملة شفافة لباقي المشاركين في الشبكة، حيث تعمل سلسلة الكتل هذه على التحقق من هوية المستخدم ومشاركتها بطريقة آمنة ومتسقة وشفافة في الشبكة.¹²

¹¹ طروبيا ندير، تكنولوجيا البلوك تشين وتأثيراتها على المستقبل الرقمي للعملات الاقتصادية: الفرص والتحديات، جامعة أحمد دراية (الجزائر)، مجلة أبحاث اقتصادية معاصرة، العدد 03، 2020.

¹² حبرية الهام، دور التكنولوجيا المالية في تطوير الأداء المصرفي، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث ل م د في الاقتصاد النقدي والبنكي، جامعة غرداية، الجزائر، 2024/2023، ص 28.

- **التعريف الثاني:** البلوك تشين هي عبارة عن شبكة معلومات تحتوي على مجموعة من الأجهزة أو العقد، وكل جهاز فيه قاعدة بيانات ودفتر الأستاذ، حيث يقوم بحفظ كل المعلومات التي تتم داخل الشبكة، وكل معاملة تتم بجهازين للتحقق منها، وتأكيد صحتها من قبل بقية أجهزة الشبكة.¹³
- **التعريف الثالث:** تعرف البلوك تشين بأنها قاعدة بيانات تستخدم شبكة للتشفير لتوفير مصدر واحد للمعلومة، مما يسمح للأطراف المشاركة ذات المصالح المشتركة في إنشاء سجل دائم وغير قابل للتغيير وشفاف للمعاملات التبادلية والمعالجة دون الاعتماد على سلطة مركزية.¹⁴
- ومن التعاريف السابقة نستنتج أن تقنية بلوك تشين هي عبارة آلية برمجية لامركزية تسجل فيه المعاملات، ويكون التسجيل فيه بطريقة مترابطة وتعتمد على الشفافية والأمان.

ثالثا: وظائف تقنية لبلوك تشين

- تعد تقنية البلوك تشين كبرمجية رقمية لتسجيل ونقل أصل المعلومات ثم حفظ وتخزين التعاملات المالية الرقمية، ومن ثم يتم تشفيرها وتوثيقها بأسلوب لا مركزي وآمن ونزيه، والمتمثلة في:¹⁵
- **نقل وإرسال أصل الملفات:** تعمل تقنية لبلوك تشين على تسجيل الملف بما فيه من وثائق وبيانات مختلفة ومنه نقلها إلى الطرف الآخر عبر شبكة الانترنت، ولكن نقل أصل الشيء وليس نسخة منه كما يحدث في العادة عند إرسال أيميل عبر الانترنت حيث ترسل نسخة من الملف الأصلي إلى الطرف الآخر بينما يبقى الأصل لدى الطرف الأول حيث يمكن لهذا الأخير الاحتفاظ بالملف الأصلي، غير أن هذا لا يتصور حدوثه أثناء التعامل بتقنية البلوك تشين.
 - **التخزين وحفظ المعلومات:** تتيح تقنية لبلوك تشين إنشاء البيانات وتخزينها بشكل لا مركزي وموزع على جميع الأجهزة المرتبطة بالشبكة التي تقوم جميعها بالتحقيق من صحة البيانات وتمائلها بناء على قواعد التوافق الجماعي المحدد، ويتم تخزين البيانات في سجل المعاملات موحد كنسخ متطابقة على جميع الأجهزة وليس كنسخة وحيدة في جهاز مركزي معين، ويضم السجل قائمة مستمرة على شكل سلسلة من المعاملات التي تسمى بالكتل ويتم ربطها على قيمة تسمى الهاش وتشفيرها لحماية السرية وتأمين صحة البيانات.

¹³ خليل عبير، علواني نوال، دور تقنية البلوك تشين في التعاملات التجارية، مذكرة مكملة لنيل شهادة الماستر في القانون، تخصص قانون أعمال، جامعة 8 ماي 1945، قالمة، الجزائر، 2023/2022، ص 12.

¹⁴ صفار محمد، شرشم محمد، واقع وتحديات تكنولوجيا البلوك تشين في القطاع المالي والمصرفي (تجربة بعض الدول العربية)، مجلة الاقتصاد والتنمية المستدامة، جامعة وهران، الجزائر، المجلد 05، العدد 02، 2022، ص 151.

¹⁵ بن علي صليحة، تقنية البلوك تشين أساس تفعيل آلية عمل العقود الذكية، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 07، العدد 02، جوان 2022، ص 960/959.

- **توثيق وأتمتة مسار المعاملة:** تعمل تقنية لبلوك تشين بأتمتة كافة مسار المعاملة، فتحل محل الوسطاء التقليديين في تقديم خدمة التوثيق وحفظ الوثائق الموقعة الكترونيا والذي يقتضي إتمامه وقتا طويلا وإجراءات معقدة وأموالا طائلة تستفيد منها مكاتب الوساطة، بينما تحتاج تقنية لبلوك تشين مشاركة العديد من الأفراد قد تصل إلى الملايين في توثيق وأتمتة المعاملة الواحدة.

المطلب الثاني: الحوسبة السحابية

شهد العالم في السنوات الأخيرة تطورا هائلا في مجال تكنولوجيا المعلومات والاتصالات مما أدى إلى ظهور مفاهيم وتقنيات جديدة غيرت طريقة عمل الأفراد والشركات، ومن أبرز هذه التقنيات الحديثة الحوسبة السحابية.

أولاً: نشأة الحوسبة السحابية بدأ استخدام مصطلح الحوسبة السحابية لأول مرة في أواخر الستينات، ولقد استلهم مصطلح الحوسبة السحابية من رمز السحابة الذي كان يستخدم في كثير من الأحيان لتمثيل الانترنت في خرائط ورسوم بيانية، وكما هو الحال مع كثير من تقنيات الجديدة الأخرى.¹⁶

وكانت على اليد عالم الحاسوب **Jhon Mc Carthy** عندما عبر عن الفكرة بقوله "قد تنظم الحوسبة لكي تصبح منفعة عامة في يوم من الأيام، وانه سوف يكون شراء طاقة الحوسبة بنفس طريقة شراء الكهرباء من هيئة الكهرباء، أما المصطلح أستخدم لأول مرة في محاضرة عام 1997 من قبل **Ramnath Cellpa** حيث وصفها إنها نموذج حوسبة جديد، أما التطور الفعلي للحوسبة السحابية بدأ عام 1999 حيث قدمت شركة **Sals force** موقع لتقديم تطبيقات المؤسسات ثم قامت شركة **Amazon** بتدشين خدمة **Amazon web**

¹⁶ المبارك رعاش، وآخرون، توظيف الحوسبة السحابية في النشر الالكتروني الأكاديمي للبحوث العلمية، جامعة الجزائر 2، الجزائر، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 07، العدد 06، أكتوبر 2022، ص 537.

services عام 2002، ثم أطلقت AC2 في عام 2006 كخدمة تجارية على شبكة الأنترنت في عام 2007، باشرت شركتي Google و IBM مع عدد من الجامعات مشروع بحثي عن الحوسبة السحابية.¹⁷

ثانيا: تعريف تقنية الحوسبة السحابية

لقد تعددت تعريف حول الحوسبة السحابية ويمكن تعريفها على النحو التالي:

- **التعريف الأول:** عرفها المعهد الوطني للمعايير والتكنولوجيا NIST على أنها نموذج لتمكين الوصول الدائم والملائم للشبكة بناءً على الطلب والمشاركة بمجموعة من مواد الحوسبة (الشبكات، الخوادم، وحدات التخزين، التطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بأقل جهد إداري أو تفاعل مزود الخدمة، ويتكون نموذج السحاب هذا من خمسة خصائص أساسية وثلاث نماذج خدمة وأربعة نماذج نشر.¹⁸
- **التعريف الثاني:** تعرفها منظومة الحوسبة السحابية على أنها استخدام إمكانيات حواسيب أخرى أو سيرفرات ذات قدرات كبيرة في القيام بمهام معينة لصالح المستخدم سواء كان هذا المستخدم فردا أو شبكة كمبيوتر محلية وتتم هذه الخدمات من خلال الأنترنت.¹⁹

ومن التعريفين السابقين نستنتج أن الحوسبة السحابية تعرف بأنها خوادم وحواسيب متصلة بالأنترنت يتم فيها تخزين وتوزيع ورفع وتحميل البيانات.

ويمكن توضيح عمل الحوسبة السحابية ببيان في الشكل التالي:

الشكل رقم (01): طريقة عمل الحوسبة السحابية

¹⁷ خولة واصل، أثر تبني الحوسبة السحابية على الأداء الوظيفي دراسة حالة المؤسسة الجزائرية للتأمين، أطروحة دكتوراه لنيل شهادة دكتوراه علوم فرع علوم التسيير، تخصص أنظمة المعلومات ومراقبة التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2020/2019، ص 03.

¹⁸ واصل خولة، رجم خالد، واقع استخدام خدمة الحوسبة السحابية بمؤسسة موبليس، جامعة ورقلة، الجزائر، مجلة العلوم الإنسانية، المجلد 09، العدد 01، 2019، ص 31.

¹⁹ العياشي زرزار، حمزة بن وريدة، الحوسبة السحابية: المفهوم والخصائص (تجارب دول وشركات رائدة)، مجلة أرصاد للدراسات الاقتصادية والإدارية، جامعة 20 أوت 1955 سكيكدة، الجزائر، المجلد 02، العدد 02، ديسمبر 2019، ص 187.



المصدر: <https://ar.wikipedia.org> (23/01/2025، 15:30).

حيث يتم في الحوسبة السحابية استخدام مجموعة متنوعة من الأجهزة، منها الحواسيب المكتبية والحواسيب المحمولة والهواتف الذكية وأجهزة المساعدة الرقمية للوصول إلى البرامج ومساحات التخزين ومنصات تطوير التطبيقات عبر الإنترنت، وكل ذلك عن طريق خدمات مقدمة من قبل مزودي الحوسبة السحابية.

ثالثاً: خصائص الحوسبة السحابية

تمتاز الحوسبة السحابية بعدة خصائص نذكر منها:

- **مركزية المستخدم:** والذي يصبح بمجرد اتصاله بالسحابة مالكا لما يجرئه عليها من مستندات وتطبيقات يستطيع مشاركتها عبر الإنترنت؛
- **مركزية المهام:** فبدلاً من تركيز السحابة على التطبيقات مثل معالجة النصوص وما يمكنها القيام به، ينصب تركيزها على احتياجات المستخدمين؛
- **مركزية البنية التحتية:** مما يساعد على التحرر من أعباء إنشائها وإدارتها والتركيز على المتطلبات الأساسية للمؤسسة؛
- **طاقة الحوسبة:** والتي تنتج من خلال ارتباط مئات أو آلاف من أجهزة الحاسب والخوادم معاً؛
- **الذكاء:** المطلوب استخراج وتحليل البيانات الضخمة المخزنة على مختلف الخوادم السحابية؛
- **البرمجة:** وهما المطلب الأساسي عند التعامل مع العديد من المهام الضرورية بالسحابة مثل: حماية امن المعلومات.²⁰

المطلب الثالث: تقنية الذكاء الاصطناعي

²⁰خولة واصل، مرجع سابق، ص 8/7.

لقد شهد العالم تطورا كبيرا في التكنولوجيا، نجد من بين هذه التطورات آلا وهو الذكاء الاصطناعي الذي يعتبر عصب التطور الرقمي ومسار التحول العميق والجذري في نظام المعلومات، وفي هذا المطلب ستعرف على الذكاء الاصطناعي.

أولا: الخلفية التاريخية للذكاء الاصطناعي

ظهر الذكاء الاصطناعي في سنوات الخمسينات، وأستخدم هذا المصطلح للمرة الأولى خلال مؤتمر جامعة دارت مورث بشأن الذكاء الاصطناعي عام 1956، ومنذ ذلك الحين نشر المبتكرون والباحثون 1,6 مليون منشور يتعلق بالذكاء الاصطناعي وأودعوا طلبات براءات لحوالي 340000 يتعلق بالذكاء الاصطناعي، وفي الستينيات بدأ نشاط البحث يتوجه نحو النظم المبنية على تمثيل المعرفة والذي استمر العمل به خلال السبعينيات، ومع بداية الثمانينات حدثت طفرة كبيرة في بحوث الذكاء الاصطناعي.²¹

ثانيا: تعريف الذكاء الاصطناعي

لقد تعدد تعريف حول الذكاء الاصطناعي سنتم تعريفها فيما يلي:

- **التعريف الأول:** يعرف بأنه أحد العلوم المتفرعة من علم الحاسوب، الذي يمكن بواسطته خلق وتصميم برامج الحاسبات التي تحاكي أسلوب الذكاء الإنساني لكي يتمكن الحاسوب من أداء بعض من المهام بدلا من الإنسان التي تتطلب التفكير، السمع، التكلم، والحركة بأسلوب منطقي ومنظم.²²
- **التعريف الثاني:** هو نظرية وتطوير أنظمة الكمبيوتر القادرة على أداء المهام التي تتطلب ذكاء بشري، ومن الأمثلة على هذه المهام الإدراك البصري، التعرف على الكلام، اتخاذ القرارات والتعلم في الظل عدم التأكد.²³
- **التعريف الثالث:** هو عبارة عن برامج تقدم للباحث إرشادات ومساعدات أثناء عملية البحث إلى أن يصل إلى حد التمكن، وتتميز بقدرتها على الكشف عن قدرات وإمكانات الباحث وتكشف أيضا مواطن الضعف لديه وتقوم بعلاجها مما يؤدي إلى دعم وتطوير البحث العلمي.²⁴

²¹ سعاد بويحة، الذكاء الاصطناعي: تطبيقات وانعكاسات، مجلة اقتصاد المال والأعمال، المجلد 06، العدد 04، ديسمبر 2022، ص 91.

²² ليندة صيمود، سهيلة دهماني، الذكاء الاصطناعي تقنية رقمية تقود إلى ابتكار تجربة تعليمية ناشئة في الجزائر. شركة انكيديا نموذجا، مجلة الدراسات الإعلامية والاتصالية، المجلد 02، العدد 02، أكتوبر 2022، ص 03.

²³ زعموكي سالم، مرزق فتيحة حبال، الذكاء الاصطناعي وانعكاساته الاقتصادية على العالم، جامعة زياني عاشور جلفة، الجزائر، مجلة التراث، المجلد 13، العدد 04، ديسمبر 2023، ص 37.

²⁴ سليمان عبد الواحد يوسف، أمل محمد غنايم، اتجاهات الباحثين نحو توظيف تطبيقات الذكاء الاصطناعي في البحث النفسي والتربوي، جامعة قناة السويس، مصر، مجلة التراث، المجلد 13، العدد 04، ديسمبر 2023، ص 66.

ومن التعاريف السابقة نستنتج إن الذكاء الاصطناعي تستعمل فيه الأنظمة والأجهزة التي تحاكي الذكاء البشري لأداء أي مهام، وتفسير البيانات الخارجية بشكل صحيح.

ثالثاً: مجالات الذكاء الاصطناعي

تتعدد مجالات استخدام الذكاء الاصطناعي في مختلف ميادين الحياة، سنتطرق إليه بالتفصيل فيما يلي:²⁵

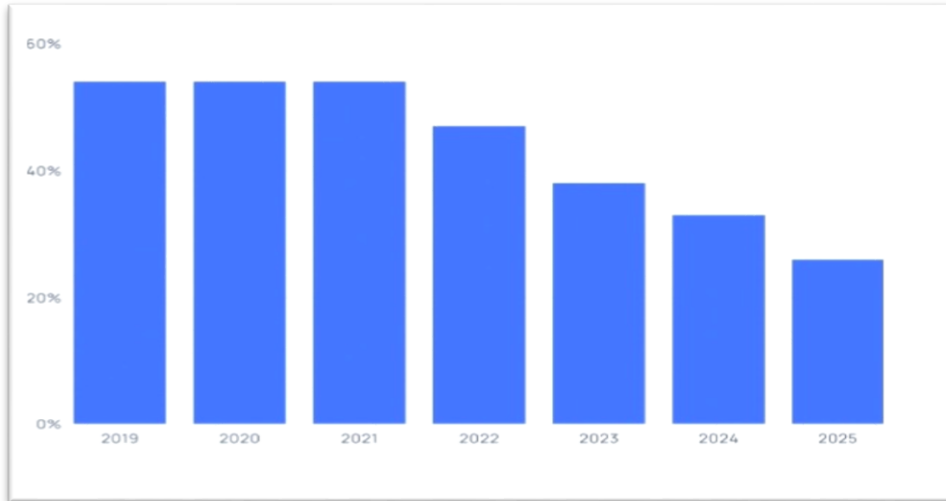
- **معالجة اللغات الطبيعية:** تعد من إحدى مجالات الذكاء الاصطناعي، وهي عبارة عن مجموعة من البرامج والنظم يتم تطويرها من تمكين الكمبيوتر من التعامل مع اللغة البشرية بشكل طبيعي، وتشمل معالجة اللغة الطبيعية جزئين رئيسيين هما الأول فهم اللغات الطبيعية يشير هذا المجال إلى قدرة الكمبيوتر على فهم لغة الإنسان بسهولة أما الثاني: إنتاج اللغات الطبيعية يشير هذا المجال إلى قدرة الكمبيوتر على إنتاج لغة طبيعية بطريقة متشابهة لكيفية إنتاج البشر للغة.
- **الروبوت:** يمثل الروبوت جزءاً مهماً من مجالات الذكاء الاصطناعي، وهو عبارة عن جهاز ميكانيكي مصمم لأداء مهام محددة بشكل آلي وذاتي في مجالات الصناعة والطب والتعليم والزراعة وغيرها.
- **النظم الخبيرة:** هي نوع من أنظمة الذكاء الاصطناعي التي تم تصميمها من أجل محاكاة الخبرة البشرية، تعتمد هذه النظم على المعلومات والمعارف والخبرات التي يتم تخزينها من طرف الخبراء في مجال معين حتى تتمكن الآلة من التعرف على الأسئلة المطروحة عليها أو المواضيع محل النقاش ومن ثم تقديم الحلول أو التوصيات، تستخدم في العديد من المجالات كالطب والهندسة وإدارة الأعمال.
- **التعرف على الكلام:** يعد التعرف على الكلام من مجالات الذكاء الاصطناعي وجزء من معالجة اللغة الطبيعية، يهدف هذا المجال إلى جعل الحاسب قادراً على فهم وتفسير اللغة البشرية عن طريق توجيه الأوامر إلى الحاسب شفها ويقوم هذا الأخير بفهم الأوامر وتنفيذها.
- **التعلم الآلي:** هو جزء أساسي من مجالات الذكاء الاصطناعي، ويقصد به برمجة الحاسوب لتوليد خوارزميات بصفة ذاتية قادرة على تعلم وتحسين أدائها من خلال التفاعل مع البيانات دون الحاجة إلى برمجة يدوية عن طريق تزويد الأنظمة بالبيانات والمعلومات حتى يصبح مستقلاً بذاته.
- **الرؤية بالحاسوب:** هي فرع من مجالات الذكاء الاصطناعي، يقصد به تمكين الأجهزة الحاسوبية من التعرف على الأشخاص أو المشاكل بطريقة تشبه قدرة الإنسان على الرؤية، مثل سيارات القيادة الذاتية، كاميرات المراقبة.

²⁵ هاشمي رشيدة، ملياني عبد الوهاب، الإطار المفاهيمي للذكاء الاصطناعي، جامعة عمار ثلجي الأغواط، الجزائر، مجلة التراث، المجلد 14، العدد 02، جوان 2024، ص 53/54.

- **الدرونز:** تعد الطائرات من دون طيار إحدى مجالات الذكاء الاصطناعي التي أصبحت تستعمل بكثرة في الآونة الأخيرة، تعمل هذه الطائرات بواسطة التحكم عن بعد أو بشكل ذاتي ولها عدة استخدامات كالتصوير الجوي، مراقبة الحدود والمحاصيل الزراعية، توصيل الطرود.

سنلاحظ من خلال الرسم البياني نمو سوق برمجيات الذكاء الاصطناعي العالمي:

الشكل (02): نمو سوق برمجيات الذكاء الاصطناعي العالمي



المصدر: <https://ar.wikipedia.org> (18/01/2025، 19:25).

الرسم البياني يوضح نمو سوق برمجيات الذكاء الاصطناعي العالمي من خلال الفترة من 2019 إلى 2025، المحور الأفقي يبين السنوات أما المحور العمودي يمثل النسبة المئوية.

- في السنوات 2019، 2020، 2021 نسبة النمو كانت مرتفعة تقارب أو تتجاوز 80 بالمئة؛
- في سنة 2022 كان انخفاض ملحوظ حوالي 70 بالمئة؛
- في سنة 2023 تراجع سوق برمجيات الذكاء الاصطناعي العالمي إلى 55 بالمئة؛
- في سنة 2024 و 2025 وصلة النسبة إلى 40 بالمئة.

وهنا نستنتج أن هناك وجود انخفاض تدريجي في نمو سوق برمجيات الذكاء الاصطناعي أو ربما هذه نسبة الاعتماد في السوق العالمي خلال هذه الفترة. قد يعود هذا الانخفاض إلى عوامل مثل تشبع السوق، التحديات التنظيمية، أو ظهور بدائل أخرى.

خلاصة الفصل الأول:

يهدف هذا الفصل إلى تقديم خلفية نظرية شاملة حول مفهوم التكنولوجيا المالية من خلال توضيح تعريفها على أنها دمج بين الابتكار التكنولوجي والخدمات المالية بهدف تقديم حلول مالية أكثر كفاءة ومرونة، وقد مرت بمراحل متعددة حيث بدأت باستخدام التكنولوجيا البسيطة في البنوك ثم تطورت مع ظهور الانترنت والبنوك الرقمية إلى مرحلة ما بعد 2008 التي شهدت توسعا في استخدام الذكاء الاصطناعي والعملات المشفرة، مما أدى إلى جعل التكنولوجيا المالية عنصرا أساسيا في تطوير الأنظمة المالية لما توفره من كفاءة وخفض في التكاليف، كما تركز التكنولوجيا المالية على مجموعة من التقنيات الحديثة أهمها سلاسل الكتل التي تتيح تسجيل المعاملات بشكل موزع وآمن وغير قابل للتلاعب، والذكاء الاصطناعي حيث يستخدم لتحليل كميات ضخمة من البيانات ما يساعد على تقديم خدمات مالية مخصصة في وقت قياسي، والحوسبة السحابية التي

توفر بنية تحتية مرنة وقابلة للتوسع تمكن المؤسسات المالية من تخزين ومعالجة البيانات بكفاءة عالية وأقل تكلفة، وهذه التقنيات تؤدي لتوفير بنية تحتية مرنة وقابلة للتوسع.

الفصل الثاني:

مخاطر التكنولوجيا المالية

تمهيد

يعتمد عصر الثورة الرقمية على التكنولوجيا في مختلف القطاعات، خلق ركيزة أساسية في المنظومة المالية والإدارية وهي (المعلومات)، ومع توسع الاعتماد على النظم الالكترونية برزت الحاجة إلى حماية هذه المعلومات، فقد أصبحت مخاطر أمن المعلومات من أبرز التحديات التي تواجه المؤسسات، تتبعها عدة مخاطر كالمخاطر التشغيلية الناتجة عن فشل الأنظمة ومخاطر السوق التي تنشأ في حالة الفشل في الاستجابة لتغيرات السوق المالية وغيرها من المخاطر الأخرى، وفي هذا السياق تم تقسيم هذا الفصل إلى ثلاث مباحث التالية:

المبحث الأول: مفاهيم أساسية حول مخاطر التكنولوجيا المالية؛

المبحث الثاني: مخاطر أمن المعلومات؛

المبحث الثالث: مخاطر الأخرى

المبحث الأول: مفاهيم أساسية حول مخاطر التكنولوجيا المالية

في ظل التحول الرقمي المتسارع الذي يشهده النظام المالي، برزت التكنولوجيا المالية كقوة دافعة لإعادة تشكيل الخدمات المالية والمصرفية التقليدية، وتتجلى مخاطر التكنولوجيا المالية الناشئة عن استخدام تكنولوجيا المعلومات والانترنت وتظهر هذه المخاطر من خلال الإخفاقات والخروقات فالأنظمة.

المطلب الأول: مفهوم مخاطر التكنولوجيا المالية

تعد المخاطر جزءاً لا يتجزأ من مختلف جوانب الحياة، فهي تمثل إمكانية حدوث أحداث أو تطورات غير مرغوب فيها قد تؤثر سلباً على الأهداف المنشودة وفي هذا المطلب سنتعرف على مفهوم المخاطر بشكل عام والمخاطر المالية بشكل خاص.

أولاً: مفهوم المخاطر

لقد تعددت التعاريف حول المخاطر يمكن تعريفها على النحو التالي:

- **التعريف الأول:** المخاطر كلمة مستوحاة من المصطلح اللاتيني Rescass أو Risque والذي يدل على الارتفاع في التوازن وحدث تغيير ما مقارنة مع ما كان منتظر.²⁶

²⁶ أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص 302.

- **التعريف الثاني:** هي حالة عدم التأكد المرتبطة بتكبد خسارة مادية أو معنوية، تلازم الشخص عند اتخاذ قرار ما مما ينتج عنه حالة معنوية تتصف بالقلق والتردد وعدم التأكد من النتائج القرارات المتخذة.²⁷
- **التعريف الثالث:** عرفت لجنة التنظيم المصرفي وإدارة المخاطر المنبثقة عن هيئة قطاع المصارف في الولايات المتحدة الأمريكية فقط عرفت المخاطر بأنها احتمال حصول الخسارة، إما بشكل مباشر من خلال خسائر في نتائج الأعمال أو خسائر في رأس المال، أو بشكل غير مباشر من خلال وجود قيود تحدد قدرة المنظمة على الاستمرار في تقديم أعمالها وممارسة نشاطاتها من جهة، وتحد من قدراتها على استغلال الفرص المتاحة في بيئة العمل من جهة أخرى.²⁸
- من التعاريف السابقة نستنتج أن المخاطر هيا عبارة عن احتمالية وقوع الحدث وتأثير احتمالية التقلبات في القيمة السوقية للمؤسسة.

ثانيا: أنواع المخاطر

هناك عدة معايير تصنف على أساسها المخاطر التي تواجه المصارف ومن أهمها:

- **تصنيف معهد المحاسبين والمراجعين بانكلترا وويلز ICAEW:** تتكون من مخاطر بيئة الداخلية ومخاطر البيئة الداخلية:
- **مخاطر البيئة الخارجية:** تنتج عن ظروف وأحداث تقع خارج نطاق رقابة إدارة المصرف ويصعب إدارة هذا النوع من المخاطر.
- **مخاطر البيئة الداخلية:** هي المخاطر التي تنتج عن ممارسة المؤسسة لأنشطتها، وتنقسم إلى (مخاطر مالية وغير مالية).
- **تصنيف Cabedo & Tirado:** انه يجب الإفصاح عن كافة المخاطر سواء قابلة للقياس أو غير قابلة للقياس، أو مخاطر ناتجة عن ظروف تخضع لرقابة الإدارة أو ناتجة من ظروف تخضع لرقابة الإدارة، وتم تصنيف الواجب قياسها والإفصاح عنها إلى ثلاثة أنواع (مخاطر الأعمال، المخاطر الاستراتيجية، المخاطر المالية).

²⁷ هشام معيري، مراد زايد، المخاطر الاجتماعية للمؤسسات (المفهوم واستراتيجيات الوقاية)، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، مجلة المعيار، المجلد 28، العدد 5، 2024، ص 625.

²⁸ ياسع ياسمين، المخاطر المالية من خلال العمليات المصرفية الالكترونية، مجلة دراسات اقتصادية، جامعة بومرداس، الجزائر، المجلد 15، العدد 02، 2022، ص 23/22.

- تصنيف حسب المعيار الدولي للتقارير المالية IFRS الأدوات المالية: تم تصنيف هذا المعيار المخاطر إلى ثلاث أنواع:
- مخاطر الائتمانية: هي المخاطر التي سببها طرف في أداء مالية إلى خسارة مالية للطرف الآخر عند الامتناع بالوفاء بالتزامه.
- مخاطر السيولة: المخاطر الناتجة عن صعوبة وفاء المؤسسة بالتزاماتها المالية، يتم تسويتها من خلال تسليم نقد أو موجود مالي آخر.
- مخاطر السوق: هي مخاطر تذبذب القيمة العادلة أو التدفقات النقدية المستقبلية لأداء مالية بسبب التغيرات في أسعار السوق.²⁹

ثالثا: تعريف مخاطر التكنولوجيا المالية

- **التعريف الأول:** يعرف بأنه احتمال وقوع خسائر محتملة الحدوث، وهو فرصة الحدوث عائد مخالف للعائد المتوقع. أي احتمال اختلاف العائد الفعلي على العائد المتوقع.³⁰
 - **التعريف الثاني:** هي عبارة عن مقياس نسبي تتجم عن إمكانية الخسائر الناتجة عن الفشل في تحقيق الهدف المالي الذي يعكس خطر عدم اليقين بشأن أسعار صرف العملات الأجنبية، أسعار الفائدة، أسعار السلع، أسعار الأسهم، جودة الائتمان والسيولة.³¹
 - **التعريف الثالث:** تعرف بأنها كل خطر ناتج عن ابتكار وتقديم أو تسويق منتج أو خدمة جديدة تعتمد على التكنولوجيا المالية، وتخضع للمعالجة الآلية وهي تتميز بسرعة الظهور أو الاكتشاف، وتسمى أيضا بمخاطر الانترنت والتي تصنف ضمن المخاطر التشغيلية التي تستهدف أصول المعلومات وتكنولوجيا مما يؤثر على سرية وعلى توافر وسلامة تلك المعلومات والأنظمة.
- ومن التعاريف السابقة يمكن تعريف مخاطر التكنولوجيا المالية بأنها كل اختراق أو خسارة أو تأثير تتعرض له الأنظمة والتطبيقات التكنولوجية المالية الحديثة.

²⁹ حيدر عبد الحسين حميد المستوفي، أهمية الإفصاح عن المخاطر خلال دورة حياة المؤسسة المالية، المركز الجامعي بركة، الجزائر، مجلة طلبة للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، 2022، ص1664/1640.

³⁰ خليل غربي، محفوظ جبار، إدارة المخاطر المالية ودورها في التنبؤ بالفشل المالي باستخدام نموذج sherro للبنك الوطني الجزائري 2016/2019، مجلة المنهل الاقتصادي، جامعة الشهيد حمه لخضر بالوادي، الجزائر، المجلد 5، العدد 1، ماي 2022، ص41.

³¹ كلاش مريم، بهلول نور الدين، دور إدارة المخاطر المالية في تقييم الأداء المالي للمؤسسة الاقتصادية، دراسة حالة مجمع صيدال، جامعة سوق أهراس، الجزائر، المجلد 11، العدد 03، أفريل 2021، ص439.

المطلب الثاني: أشكال مخاطر التكنولوجيا المالية

تعد التكنولوجيا المالية من ابرر الابتكارات التي غيرت المشهد المالي العالمي، حيث ساهمت في تسريع العمليات المصرفية، غير أن هذا التطور السريع يصاحبه عدد من المخاطر المتنوعة، تتمثل ابر أشكال هذه المخاطر في (مخاطر السوق، مخاطر التشغيلية) في هذا المطلب سنتطرق إلى هذه المخاطر.

أولاً: مخاطر السوق

تعرف مخاطر السوق بأنها هي الخسارة المحتملة الناجمة عن تقلبات سعر الفائدة، وذلك بسبب التطورات غير المواتية لعوامل السوق وقد تكون سلاح ذو حدين قد تحقق المؤسسة بسببها أرباحاً عالية بمستوى النشاط الاقتصادي وخاصة المؤسسات التي تنتج سلعا صناعية أو التي تتصف أعمالها بالموسمية كشرركات الطيران.³² حيث أن مخاطر السوق في مجال التكنولوجيا المالية تشير إلى الخسائر المحتملة التي تقع فيها المؤسسات والشركات المالية مثل: تقلبات أسعار الأصل الرقمية، تغير سلوك المستهلكين، المنافسة الشديدة.³³

ثانياً: مخاطر التشغيلية

أدى التطور السريع إلى تزايد عنصر المخاطر في مختلف المجالات لا سيما قطاع البنك وفيما يلي سنتعرف على مفهوم المخاطر التشغيلية التالية : هي المخاطر الناجمة عن ضعف في الأشخاص أو الأنظمة أو حدوث ظروف خارجية، وهي مخاطر الخسارة الناتجة عن احتمالية عدم كفاية أنظمة المعلومات وعلى مجلس الإدارة والإدارة التنفيذية بالبنك تطوير سياسات عامة وخطط لإدارة هذه المخاطر بالإضافة لتأسيس معايير وموجات لتقليل مخاطر التشغيل.³⁴ حيث أنها ترتبط بالإخفاق في العمليات الداخلية التي تحدث داخل المؤسسة، التي تؤدي قد تؤدي إلى خسائر مالية سمعة سيئة للمؤسسة تتمثل هذه الإخفاقات في الأخطاء البشرية، مشكلات في سلسلة التوريد التقنية المتمثلة في الحسبة السحابية.

ثالثاً: مخاطر السمعة

³²لوييزة أوصغير، مخاطر السوق في البنوك الدولية واستراتيجيات إدارتها حسب المعايير الدولية للجنة بازل مجموعة سوسيتي جنرال نموذجاً، مجلة نور للدراسات الاقتصادية، مجلد 06، عدد10، ص71.

³³ أحلام بوعلي، ثريا سعيد، إدارة المخاطر التشغيلية في البنوك التجارية: دراسة حالة لعينة من البنوك التجارية في الجزائر، المجلة الجزائرية للتنمية الاقتصادية، عدد03، 2015، ص119.

³⁴ المرجع نفسه، ص119.

هي ناتجة عن انخفاض إيرادات المصرف أو قاعدة عملائه نتيجة عدم تقيد البنك بالأنظمة والقوانين والمعايير الصادرة عن السلطات الرقابية، حيث يلحق هذا النوع من المخاطر ضررا كبيرا بالمصرف، باعتبار أن طبيعة عمله تتطلب الحفاظ على ثقة المودعين والمقرضين وبصفة عامة على السوق³⁵ وبالتالي مخاطر السمعة ناتجة أساسا عن مخاطر الناشئة عن الفشل في التشغيل السليم للمصرف بما لا يتماشى مع الأنظمة والقوانين الخاصة بذلك وإن هذه المخاطر غير قابلة للقياس الرياضي، مما يزيد من صعوبة تقديرها³⁶

رابعا: مخاطر امن المعلومات

تعتمد الخدمات المالية التي تقدمها منصات الفينتك بشكل كبير على التكنولوجيا الرقمية، إذ تؤثر سرية وموثوقية وأمن التكنولوجيا المالية بشكل مباشر على جودة الخدمات المالية وأمن المستخدمين، من خلال ظاهرة الاحتيال المالي وتسريب معلومات العملاء سيتم التطرق له بالتفصيل في المبحث المالي³⁷.

خامسا: مخاطر الأمن السيبراني

يعبر عن احتمال حدوث الخسائر التي قد تنتج عن مخاطر الانترنت المتعلقة بالمؤسسة المالية كفقدان البيانات أو الخسارة المالية أو الاضطراب والإضرار بسمعة المنظمة بسبب فشل أنظمة التكنولوجيا، سيتم تفصيلهم في المبحث التالي³⁸.

المبحث الثاني: مخاطر امن المعلومات

³⁵ عبد الحفيظ احمد، صديقي مليكة، دور الحكومة في الحد من مخاطر السمعة في البنوك التجارية، مجلة إدارة الأعمال والدراسات الاقتصادية، مجلد 05، عدد 02، 2019، ص 241/240.

³⁶ عبد الحفيظ احمد، صديقي مليكة، دور الحكومة في الحد من مخاطر السمعة في البنوك التجارية، مجلة إدارة الأعمال والدراسات الاقتصادية، المجلد 05، العدد 02، 2019، ص 241/240.

³⁷ محمد قوجيل، عبد العزيز طيبة، مرجع سابق، ص 189.

³⁸ المرجع نفسه، ص 190.

المخاطر السيبرانية هي أحد أبرز التحديات التي تهدد سرية المعلومات وسلامة الأنظمة الرقمية وقد دفعت هذه التهديدات إلى تعزيز مفهوم الأمن السيبراني، الذي يشمل التقنيات والإجراءات التي تؤدي لحماية الأصول الرقمية من أي اختراق ويندرج تحت هذا الإطار تصنيف متنوع لأنواع المخاطر السيبرانية سنوضح من خلال هذا المبحث المفهوم الدقيق للمخاطر السيبرانية ومفهوم الأمن السيبراني كما نوضح أنواع المخاطر السيبرانية.

المطلب الأول: مفهوم المخاطر السيبرانية والفضاء السيبراني

يعتبر الفضاء السيبراني مكوناً أساسياً في ظل التطور التكنولوجي المتسارع إذ يشمل كل البنيات التحتية الرقمية والأنظمة والشبكات التي تستخدم لتخزين ومعالجة المعلومات، وبموازاة هذا التوسع ظهرت المخاطر السيبرانية وهي مجموعة من التهديدات والهجمات التي تستهدف هذا الفضاء مثل التجسس الإلكتروني وبرمجيات الفدية وفي هذا المطلب سنوضح المفهوم الدقيق لهذه المخاطر والفضاء الذي تستهدفه.

أولاً: تعريف المخاطر السيبرانية

قبل شرح المخاطر السيبرانية لابد من معرفة مفهوم السيبرانية:

- كلمة السيبرانية: مشتقة من الكلمة اللاتينية "سايبير" cyber، ومعناها تخيلي أو افتراضي، وتعني كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي.

يمكن تعريف المخاطر السيبرانية كما يلي:

التعريف الأول: يعتبر مصطلح يشير بصورة أدق لإجمالي أنماط المخاطر، سواء تعلقت بالحاسب أو بشبكات التكنولوجيا، ويتشكل كيان السايبر في الدول كلها بشكل عام من وجود ثلاثة عناصر أساسية تضم: الأجهزة الصلبة hardware، والبرمجيات الرقمية software، والعامل البشري من مبرمجين ومستخدمين.³⁹

³⁹ أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، المجلد 3، العدد 35، 2020، ص 302.

التعريف الثاني: يشير إلى التهديدات المحتملة التي تستهدف الأنظمة الإلكترونية، الشبكات، البيانات الرقمية والتي قد تؤدي خسائر مالية. وتزداد هذه المخاطر مع تنامي الاعتماد على التكنولوجيا الرقمية وخصوصا في القطاعات الحيوية مثل: القطاع المصرفي.⁴⁰

من التعريفين السابقين نجد أن المخاطر السيبرانية هي تهديدات وتحديات تواجه الأنظمة الرقمية في ظل مجتمع رقمي عن طريق معرفة ثغرات ونقاط الضعف للأجهزة واستغلالها. وليبيان كلمة المخاطر السيبرانية لابد أن نعرف البيئة التي تحدث فيها هذه المخاطر وهي الفضاء السيبراني:

ثانيا: الفضاء السيبراني ومكوناته

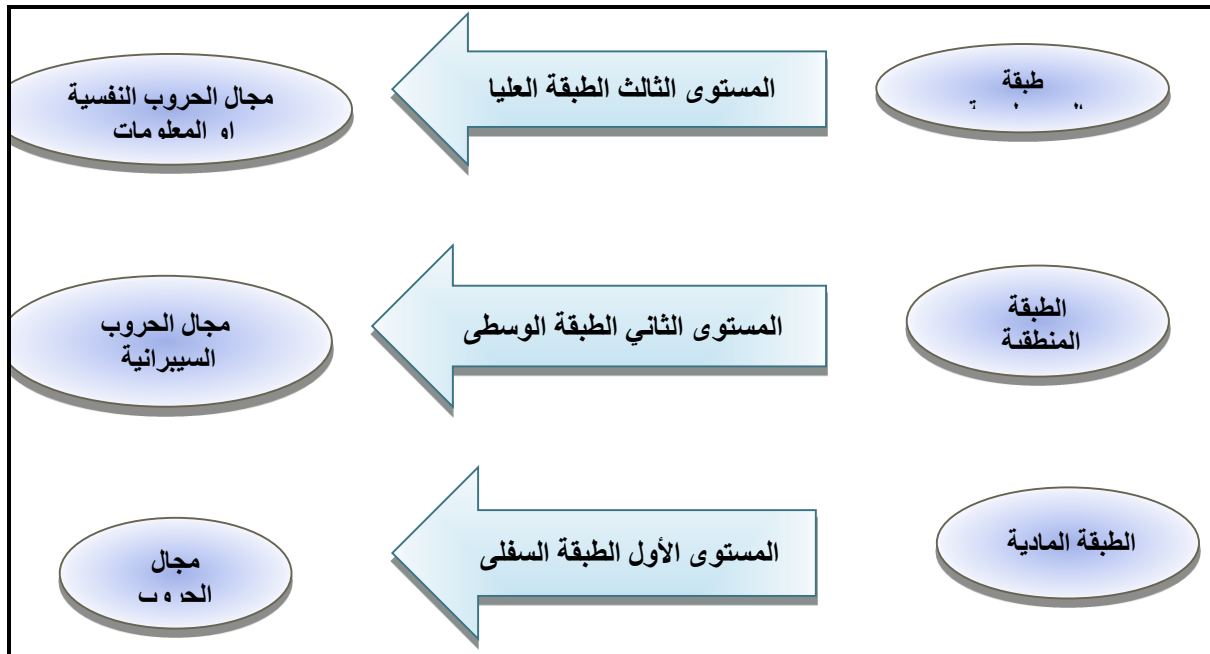
- **تعريف الفضاء السيبراني:** هو فضاء افتراضي، أنشأ عن طريق الترابط الموجود بين جميع أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية والأشياء المتصلة بالإنترنت وكل ما بها من معلومات وبرمجيات في العالم كله، حيث أن هذا الفضاء يعرف بالفضاء الخامس للحروب بعد الفضاءات البري والبحري والجوي، له خصائص كثيرة ومتعددة حيث يعتبر:

- ✓ فضاء معقد وواسع الانتشار وسهل الولوج إليه ومتغير وقابل للتوسيع أنيا؛
 - ✓ فضاء للتبادلات والمواجهات بين الفاعلين؛
 - ✓ فضاء إدارته لامركزية للغاية؛
 - ✓ فضاء تكون فيه التبادلات والتطورات سريعة؛
 - ✓ فضاء به خصوم متعددين ومنقلبين للغاية؛
 - ✓ فضاء مترابط كليا وجميع حلقات سلسلته يمكن أن تصاب بهجمة سيبرانية.⁴¹
- **مكونات الفضاء السيبراني:** يتكون هذا الفضاء الرقمي من ثلاث طبقات أساسية نوضحها في الشكل التالي:

⁴⁰ابتهاج إسماعيل يعقوب، وآخرون، مؤشر مقترح لإفصاح المحاسبي عن مخاطر السيبرانية في سوق العراق للأوراق المالية على وفق متطلبات الدولية: دراسة اختيارية، جامعة المستنصرية، العراق، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 09، العدد 01، 2022، ص 1407.

⁴¹ساعد بوقرص، الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا هوارى بومدين، المجلد 3، العدد 2022، 1، ص 62.

الشكل (03): طبقات الفضاء السيبراني



المصدر: من إعداد الطلبات بالاعتماد على المرجع: ساعد بوقرص، الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا هواري بومدين، المجلد 3، العدد 1، 2022.

من خلال الشكل رقم 03: نلاحظ أن طبقات الفضاء السيبراني تتمثل في:

- **الطبقة السيميولوجية:** هي الطبقة التي تتعامل مع الرموز والمعاني في الفضاء السيبراني تتكون من كل المحتويات بيانات ومعلومات ورسائل؛
- **الطبقة المادية:** الطبقة التي تمثل البنية التحتية المادية للفضاء السيبراني تشمل الشبكات والميكرو كمبيوترات؛
- **الطبقة المنطقية:** الطبقة التي تتعلق باليات تشغيل الفضاء السيبراني مثل أنظمة الاستغلال والتطبيقات والبروتوكولات.⁴²

هناك العديد من المفاهيم المرتبطة بالمخاطر السيبرانية ومن أهمها ما يلي:

⁴² ساعد بوقرص، مرجع سابق، ص 63.

- مفهوم أمن المعلومات: هو المجال الذي يركز على حماية المعلومات من الوصول غير المصرح به، أو التعديل أو الإتلاف أو الكشف من خلال وسائل وأدوات وإجراءات من أجل حمايتها من المخاطر.⁴³
- مفهوم القوة السيبرانية: عرفها (جوزيف س ناي Joseph S, Ny) بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي مجموعة من الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات، والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل.
- ولتنفيذ هذه القوة لابد من أن تتوفر على مجموعة من العناصر أهمها:
- وجود بنية تحتية سيبرانية: تشمل أجهزة الكمبيوتر، وشبكات الإيصالات، والبرمجيات، وقواعد البيانات لمختلفة الأنظمة والقطاعات.
- بنية مؤسسية: تتولى مهمة ممارسة ومحددة لاستعمال القوة السيبرانية.
- استراتيجية بأهداف واضحة: تحدد طرق العمل والأهداف المرجوة.⁴⁴

المطلب الثاني: الإطار المفاهيمي للأمن السيبراني

يعد الأمن السيبراني مجموعة من السياسات والإجراءات المصممة لحماية الأنظمة والشبكات كما يمثل ركيزة أساسية لضمان السيادة الرقمية، مما يتطلب فهما دقيقا لمفهومه والمرتكزات التي يقوم عليها فضلا عن أبعاده الاجتماعية، والقانونية والسياسية والعسكرية ومن هنا تتبع أهمية هذا المطلب.

أولاً: مفهوم الأمن السيبراني

حسب التعريف الموسع للأمن السيبراني المعتمد لمنظمة الدولية للاتحاد الدولي للاتصالات: هو مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية والتقنيات التي يمكن استخدامها لحماية البيئة الالكترونية وتنظيم أصول المستخدم، تشمل توصيل أجهزة الحوسبة والموظفين والبنية التحتية والخدمات ونظم الاتصالات السلكية واللاسلكية ومجمل المعلومات المرسلة أو المخزنة في البيئة الالكترونية.⁴⁵

⁴³ وليد أبو سعد، أمن المعلومات، الموسوعة العربية للكمبيوتر، قسم دورات التعليمية سلسلة كتب الدورات التعليمية الإلكترونية. <http://www.c4arab.com>، 17.00، ص13.

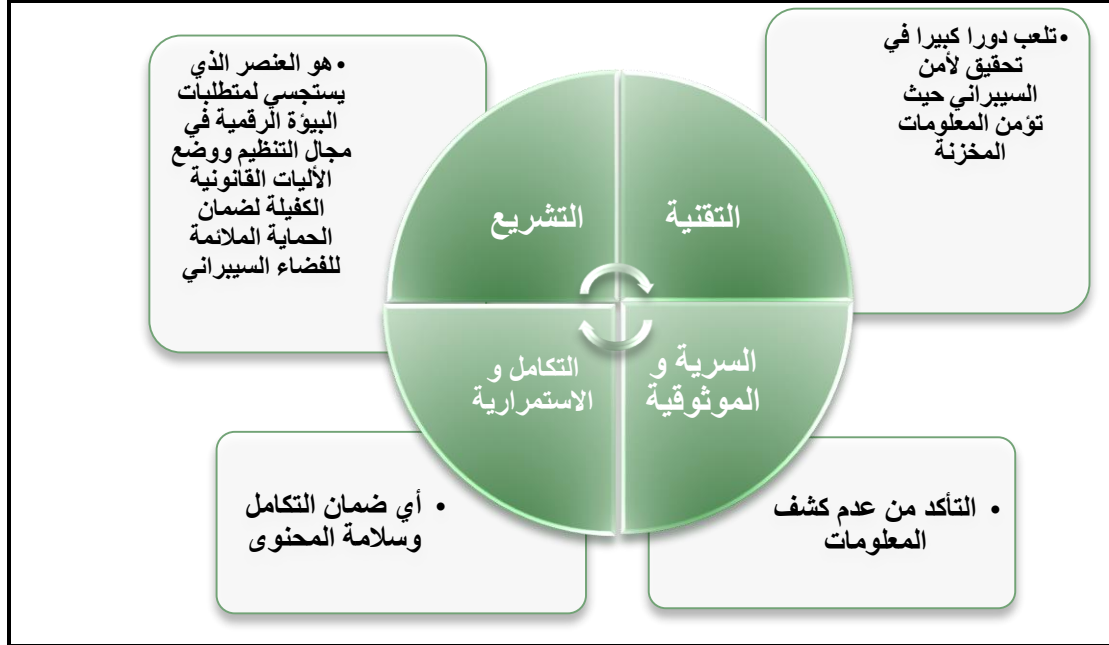
⁴⁴ إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أبريل 2019، ص 1018.

⁴⁵ كريم رقبولي، لخصر نويوة، الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية، مجلة طبنة_المركز الجامعي بركة_الجزائر، المجلد 02، العدد 02، 2019، ص72.

ثانيا: مرتكزات الأمن السيبراني

يرتكز الأمن السيبراني على أربع ركائز أساسية نوضحها في الشكل الموالي:

الشكل(04): مرتكزات الأمن السيبراني

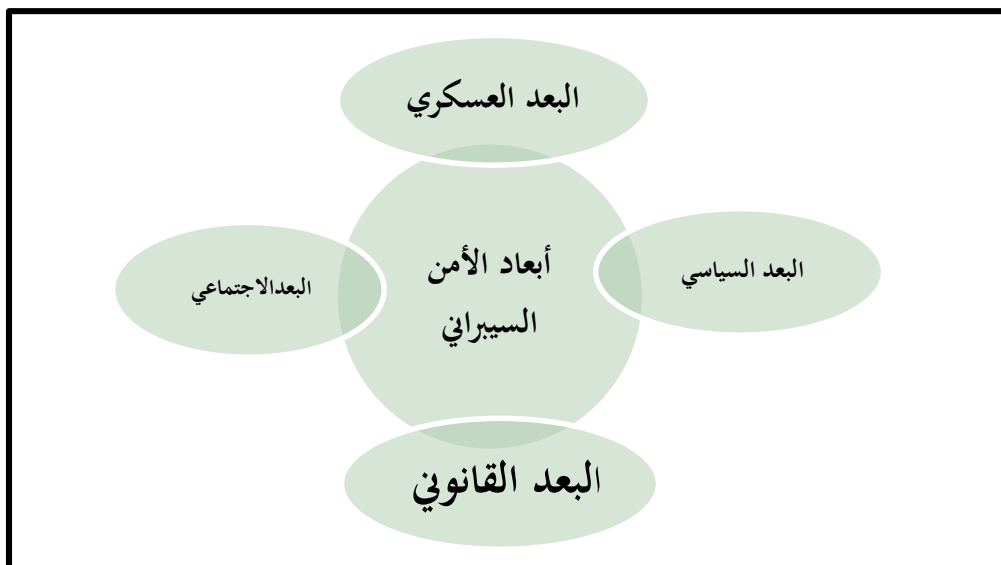


المصدر: من إعداد الطلبات بالاعتماد وسمر محمود، الحروب السيبرانية المخاطر واستراتيجيات تحقيق الأمن السيبراني

الدولي والخارجي، المجلة الاقتصادية للأمن الإنساني، المجلد 07، العدد 02، جويلية 2022، ص 172.

ثالثا: أبعاد الأمن السيبراني يمتد الأمن السيبراني ليشمل مجموعة من الأبعاد المتداخلة التي تعكس طبيعته الشاملة، ولا يقتصر على الجانب التقني فحسب سنوضح أربعة أبعاد أساسية في الشكل الموالي:

الشكل(05): أبعاد الأمن السيبراني



المصدر: من إعداد الطلبات بالاعتماد على بارة سميرة، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح ورقلة، العدد 4، جويلية 2017، ص 273.

خلال الشكل رقم 05: نلاحظ أربعة أبعاد تتمثل في:

- **البعد العسكري:** من المعلوم أن الانترنت قد طورت في بيئة عسكرية بشكل أساسي لتضاف إليها فيما بعد البيئة الأكاديمية بما تمثل من أبحاث تخدم تطوير القدرات العسكرية وتطورها، والانجازات العلمية التي تسهم في تفوق بلد على آخر، تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية.
- **البعد الاجتماعي:** من الضروري تعميم المفهوم الصحيح و السليم للأمن إلى كل المشاركين في الشبكة الدولية للمعلومات إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن، إذا ما صيغت بطريقة واضحة وعرفت ونفذت بذكاء، لذلك من الضروري تثقيف جميع الأفراد من خلال بتنظيم حملات إعلامية لأجل مجتمع معلومات مسؤول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.
- **الأبعاد القانونية:** يترتب على النشاط الفردي والمؤسسي الحكومي، فالفضاء السيبراني نتائج قانونية تستدعي اهتماما خاص لحل النزاعات التي يمكن أن تنشأ عنها، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات. فظهرت حقوق أخرى وتوسعت لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء التجمعات على الأنترنت وكل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تتسجم مع التطورات الحاصلة.
- **البعد السياسي:** يشمل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، التي تعني حقها في السعي إلى تحقيق رفاه شعبها لمنع حدوث تسريبات مختلفة للوثائق الحساسة التي تؤدي لمشكلات عويصة على المستوى الخارجي والدولي.⁴⁶

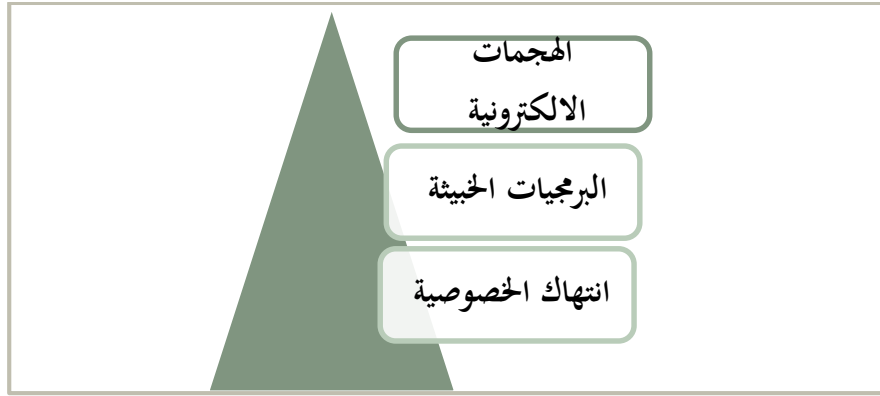
⁴⁶ من إعداد الطلبات بالاعتماد على المراجع التالية:

- بارة سميرة، الأمن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح ورقلة، العدد الرابع، المجلد 02، جويلية 2017، ص 273.
- محمد عبد الله مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، المجلد 01 العدد 6، يناير 2015، ص 65.

المطلب الثالث: أنواع المخاطر السيبرانية.

المخاطر السيبرانية هيا أحد أبرز التهديدات التي تواجه أمن المعلومات واستقرار الأنظمة الإلكترونية وتتتبع هذه المخاطر حسب مصدرها وطبيعتها، فتشمل هجمات تقنية وأخطاء بشرية وثغرات تنظيمية ويهدف هذا المطلب إلى تسليط الضوء على أبرز أنواع المخاطر السيبرانية في الشكل الموالي:

الشكل(06): أنواع المخاطر السيبرانية



المصدر: من إعداد الطالبات.

من خلال الشكل 06: نلاحظ من أهم الصور التي تشكل المخاطر السيبرانية انتهاك الخصوصية، والتي سيتم توضيحها على النحو التالي:

أولاً: الاختراقات السيبرانية (انتهاك الخصوصية) يقصد بها القرصنة السيبرانية تتمثل في عملية نسخ البرمجيات غير المصرح بها أو إعادة إنتاجها أو استخدامها أو تصنيع نسخ بطريقة غير شرعية أو نشر وتوزيع المنتج البرمجي أو استغلاله على نحو مادي أو تقليديها أو محاكاتها والانتفاع بها بدون الحصول على إذن أو تفويض ويمكن للاختراقات أن تتخذ أحد الصور الآتية:

- اختراق المواقع والصفحات السيبرانية على الأنترنت وتدميرها، أو إلغائها أو إتلافها أو العبث بالبيانات والمعلومات المتوفرة عليها؛

- اختراق البريد الإلكتروني للآخرين والاستيلاء عليه واستخدامه في انتحال شخصية الغير؛
اختراق قواعد البيانات وحذف أو تعديل المعلومات الموجودة عليها أو الاستيلاء على المعلومات المتوفرة عليها كأسماء المستخدمين واستخدامهم لإغراض غير مشروعة أو بيعها إلى جهات مستفيدة.⁴⁷

⁴⁷أنظر: أميرة عبد العظيم محمد عبد الجواد، مرجع سابق، ص 310.

ثانياً: البرمجيات الخبيثة Malware Attac: تسمح هذه البرامج الخبيثة للصيادين بمراقبة جميع العمليات المنفذة، من خلال متصفح الشبكة العالمية من قبل المستخدم بالموقع الإلكتروني لمصرف ما، وعند تزويد المستخدم لاسم المستخدم ورمز التعريف الشخصي للدخول على حسابه المصرفي، ففي حالة وجود مثل هذه البرامج في جهاز الضحية، فسيتم التقاط هذه البيانات السرية، وإرسالها إلى الصياد الذي سينتقل بدوره شخصية المستخدم، في التعامل مع الموقع الإلكتروني للمصرف الذي سيتعامل مع الصياد على أنه العميل الحقيقي، من إحدى الطرق المشهورة لهذا الأسلوب هي تركيب مسجل نقرات لوحة المفاتيح في جهاز الضحية والذي من اسمه يقوم بتسجيل النقرات على لوحة المفاتيح، ومن ثم يقوم بإرسالها إلى الصياد، والذي يقوم بدوره بتحليلها واستخلاص البيانات لانتحال شخصية الضحية.⁴⁸

ثالثاً: الهجمات الإلكترونية (الهجمات السيبرانية)

للحجرات الإلكترونية عدة مفاهيم نذكر منها التعريفين التاليين:

التعريف الأول: يقصد بها التهديدات السيبرانية التي تتم باستخدام آليات وشبكات الأنترنت وأجهزة الحاسوب الآلي، بهدف إلحاق الضرر بالأجهزة والشبكات الإلكترونية.

التعريف الثاني: عرفها القيادة الاستراتيجية الأمريكية بأنها تطويع عمليات نظام الكمبيوتر، بهدف منع الخصوم من الاستخدام الفعال لها، فضلاً عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها.⁴⁹

من التعريفين السابقين يمكن تعريف الهجمات السيبرانية بأنها أحد المحاولات الضارة التي تستهدف الأنظمة الرقمية، للوصول للبيانات الحساسة وإلحاق الضرر بها.

- **أصناف الهجمات السيبرانية:** من أجل تنفيذ هذه الهجمات، لابد من وجود أصناف لها نميز بين صنفين أساسيين:

الصنف الأول: الحرب السيبرانية هي كل فعل فردي أو جماعي مخطط له يهدف إلى المساس بوحدة وسلامة النظام المعلوماتي لمؤسسة أو منظمة أو دولة معينة، باستخدام كلي أو بجزء من شبكة الاتصالات سواء الأنترنت أو أنواع من الشبكات الاتصالية الرقمية، بحيث تؤدي إلى حدوث أضرار توازي ما قد

⁴⁸ خالد، بن سليمان الغنبر، الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مركز التميز لأمن المعلومات، http://; COEIA, EDU, S A، 17 فيفري 2025، 10.00.

⁴⁹ عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد إدرا، الجزائر، المجلد 06، العدد 02، 2022، ص 247.

ينجم عن استخدام القوة العسكرية المسلحة وقد صنفها وزارة الدفاع الأمريكية إلى ثلاث أصناف (حرب سيبرانية هجومية، وأخرى دفاعية، واستخبارية).⁵⁰

من خلال التعريف نجد أنها: عبارة على حروب رقمية، تشمل عمليات اختراق الشبكات وزرع البرمجيات الخبيثة لتعطيل أنظمة الدول أو الشركات، كما يشير لأي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي.

وقد تستهدف البنية التحتية للدولة: يشمل هذا الاستهداف سلسلة من الهجمات المعلوماتية على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية الوطنية، وينشأ عن هذا تعطيل العديد من مرافق الحياة في البلاد، وسيادة الفوضى، ولا يتوقف الأمر عن هذا الحد فهناك مثلا شبكات المعلومات الطبية، والتي يمكن التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى، وكذا اختراق نظم التحكم بخطوط الملاحة الجوية والبحرية، قد يؤدي للتصادم فيما بينهما بسبب خلل في برامج هبوط الطائرات وإقلاعها.⁵¹

الصنف الثاني: الإرهاب السيبراني هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب، وتعتمد هذه الهجمات على الترويع وبث الخوف ومجهولية المصدر، وفي هذا الصدد يحذر الخبراء من خطر أكيد يكمن في شن هجمات سيبرانية، على البنية التحتية والأنظمة وسرقة الخطط والخرائط والاستراتيجيات العسكرية.⁵²

تستهدف الهجمات الاستراتيجية العسكرية التي تعد من أخطر الهجمات نقل كميات هائلة من المعلومات عبر شبكات المعلومات بصورة يومية، وقد أصبحت تشكل خطرا كبيرا، فهذه الهجمات تستهدف الأهداف

⁵⁰ ربيعي حسين، وسمر محمود، الحروب السيبراني المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والخارجي، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 02، جويلية 2022، ص 177.

⁵¹ أميرة عبد العظيم، محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، المجلد 03، 2020، ص 322.

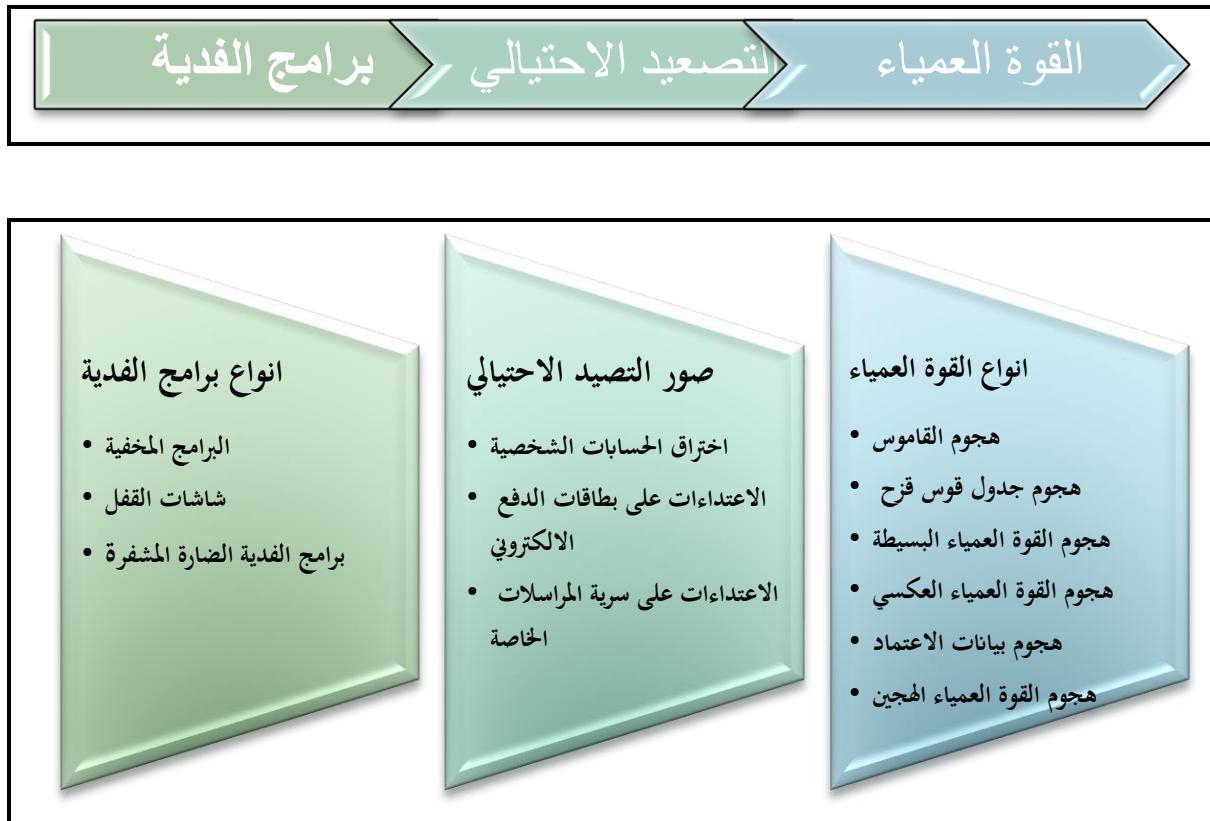
⁵² بن صابر بالقاسم، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، العدد 04، جوان 2017، ص 194.

العسكرية دون المدنية، ورغم محاولات حكومات الدول عزل المعلومات العسكرية عن العالم، عن طريق التدقيق في اختيار الأشخاص المتعاملين معها إلا أنها قد تتعرض لهجمات إلكترونية.⁵³

- أنواع الهجمات الإلكترونية (السيبرانية):

توجد أنواع عديدة للهجمات الإلكترونية (السيبرانية) نوضحها في الشكل التالي:

الشكل (07): أنواع الهجمات الإلكترونية (السيبرانية)



المصدر: من إعداد الطالبات

1. هجمات القوة العمياء: يسمى هجوم القوة الغاشمة وهو محاولة لكسر كلمة المرور أو اسم المستخدم أو العثور على المفتاح المستخدم لتشفير الرسالة، باستخدام نهج التجربة والخطأ والأمل في النهاية عن طريق التخمين، بشكل صحيح هذه طريقة هجوم قديمة لكنها لا تزال فعالة وشائعة لدى المتسللين. قد يستغرق كسر كلمة المرور من بضع ثوان، إلى سنوات عديدة لذا قام المتسللون بتطوير أدوات للقيام بالمهمة بشكل أسرع من بين الأدوات نجد القواميس، وهيا الأداة الأساسية، حيث يستعمل المتسللين قواميس عديدة وبلغات مختلفة وبأحرف وأرقام خاصة وهذا ما يعرف بهجمات القاموس.⁵⁴

⁵³ أميرة عبد العظيم، محمد عبد الجواد، مرجع سابق، ص322.

⁵⁴ القوة العمياء والحماية الرقمية (2019، apr. 28، http:// digital , protection, Tech, apr. 28، 2025، 17:00).

- أنواع هجوم القوة العمياء لها ستة أنواع أساسية:
 - هجوم القاموس: يخمن أسماء المستخدمين أو كلمات المرور باستخدام قاموس من السلال أو العبارات المحتملة؛
 - هجوم جدول قوس قزح: جدول محسوب مسبقا للالتفاف حول قدرات تجزئة التشفير؛
 - حشو بيانات الاعتماد: هجوم يستخدم بيانات اعتماد الحساب المسروقة للحصول على وصول غير مصرح به إلى حسابات المستخدمين؛
 - هجوم القوة العمياء البسيطة: يستخدم طريقة التخمين يدويا دون استخدام أي برامج؛
 - هجوم القوة العمياء العكسي: تستخدم كلمة مرور نموذجية أو مجموعة متنوعة من كلمات المرور ضد العديد من أسماء المستخدمين التي يمكن تصورها؛
 - هجوم القوة العمياء الهجين: تبدأ من الأساس المنطقي الخارجي لمعرفة نوع كلمة المرور التي قد تتجح وبعد ذلك تتقدم بالطريقة البسيطة للتعامل مع محاولة العديد من الأصناف المحتملة.⁵⁵
2. هجمات التصيد الاحتيالي: هي أحد أنواع الجرائم الإلكترونية التي تقوم على انتحال المخترق أو المحتال لحساب شخصية أو جهة رسمية موثوقة مثل خدمة العملاء لدى شركة ما، من أجل سرقة البيانات الشخصية للمستخدم، يستهدف المحتالون في غالب الأحيان بيانات مثل رقم بطاقة الائتمان، أو كلمة المرور لحساب شخصي، أو أرقام الحسابات البنكية، ومن أشهر الرسائل المستخدمة في التصيد الاحتيالي البريد الإلكتروني، والروابط الجاهزة لمواقع إنترنت معينة، لكن يمكن أن يتم أيضا بواسطة الرسائل النصية وحتى المكالمات الهاتفية
- صور التصيد الاحتيالي: توجد ثلاثة صور مستهدفة هي:
 - اختراق الحسابات الشخصية: يتعرض النظام المعلوماتي للأفراد والدولة إلى الدخول إليه من قبل أشخاص مجهولين غير مصرح لهم بالدخول، مما يقود إلى نتائج سلبية وأضرار مادية، بسبب الاختراق وإتلاف البيانات أو نسخها أو تزويرها، والاختراق يكون إما منصبا على نظام التشغيل والتحكم في الحاسوب أو عن طريق اختراق الحسابات والمواقع الخاصة بالبريد الإلكتروني والصفحات التي يتم إنشاؤها في مواقع التواصل الاجتماعي والطرق المعتمدة في اختراق الحسابات الشخصية والحاسب الآلي كثيرة وشائعة منها:

⁵⁵ هجوم القوة العمياء، منصة مجرة، <https://mhbarabic.com>, business , revie , (25 مارس 2025)، (17.00).

- **الأحصنة طروادة:** حيث يتم إرسال برنامج التجسس من قبل المستفيد إلى جهاز الضحية ليكون حلقة وصل بينهم، ويتم إرسالها بأكثر من طريقة ومنها بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، أو عن طريق الدردشة في مواقع التواصل، أو رابط معين من بين هذه الهجمات نذكر⁵⁶: هجمات برمجيات حسان طروادة المصرفية التي تستهدف هواتف أندرويد الذكية والتي عرفت ارتفاعاً ملحوظاً، حيث زاد عددها من 420 ألف هجمة في عام 2023 إلى مليون و242 ألف هجمة في عام 2024. وُصّمت برمجيات حسان طروادة المصرفية الخبيثة بهدف سرقة بيانات اعتماد المستخدمين الخاصة بالخدمات المصرفية الإلكترونية، وأنظمة الدفع الإلكتروني، وأنظمة بطاقات الائتمان. كما شاهد عام 2024 قيام المجرمين السيبرانيين بشن 2.8 مليون هجمة شهرياً في المتوسط على الأجهزة المحمولة، متضمنة البرمجيات الخبيثة والبرمجيات الإعلانية والبرامج غير المرغوب فيها. ونجحت منتجات كاسبرسكي في صد 33.3 مليون هجمة في الإجمالي خلال العام.
- **برامج الفيروسات:** هي برامج تصمم لتغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر، إما بالإزالة أو التعديل أو التخريب، ومن طرق الاختراق ما يعرف بتدمير المواقع، وذلك من خلال ضخ الآلاف الرسائل الالكترونية من جهاز الحاسب الخاص بالمتصيد إلى المواقع، واختراق الصفحات الخاصة بالأفراد، والصفحات الرسمية الدولية وتغييرها بصفة أخرى وما يرغب المتصيد بإيصاله للعالم.⁵⁷
- **الاعتداء على السرية المراسلات الخاصة:** يقصد بها التجسس للاطلاع على المعلومات الخاصة، والتي لا يسمح لغير المخولين الاطلاع عليها، فالتجسس هو التعدي على السرية التي تعتبر جوهر الحق في الخصوصية، وذلك لأن المراسلات أياً كان نوعها لا يجوز لغير مصدرها ومن توجه إليه الاطلاع عليها، وغير ذلك يعد انتهاكاً لحرمة المراسلات.
- **الاعتداء على بطاقات الدفع الإلكتروني:** هي سرقة وابتزاز الأموال باستخدام شبكة الانترنت، ويكون عبر الدخول إلى شبكات البنوك، والتحويل الغير المشروع للأموال من حساباتها أو التلاعب في الحسابات المالية المودوعة لدى البنوك، وتحويلها من حساب لآخر أو سرقة الأرقام السرية التي تمكن المتصيد من الدخول إلى الحسابات، وسكون ذلك باستخدام البطاقات البنكية المسروقة.

⁵⁶ تقرير كاسبرسكس يكشف عن تضاعف هجمات سرقة البيانات المصرفية التي تستهدف الهواتف الذكية، 4 مارس 2025، <http://me.kaspersky.com>.

⁵⁷ علياء زامل مشنت، أثر التصيد الاحتيالي في الاعتداء على الخصوصية في المجال الرقمي، مجلة كلية الإمام الكاظم، المجلد 8، العدد 1، ص 17، 2022.

3. **برامج الفدية:** هي نوع من البرامج الضارة من علم الفيروسات المشفرة، والتي تهدد بنشر البيانات الشخصية للضحية أو تمنع الوصول إليها بشكل دائم ما لم يتم دفع فدية حيث تستعمل تقنية، تسمى الابتزاز الفيروسي المشفر، والذي يقوم بتشفير ملفات الضحية مما يجعل الوصول إليها غير ممكناً، وهذا هو الهدف الأساسي لمجرمي برامج الفدية، من أجل الحصول على الأموال من الضحية، ويمكن أن تتراوح التكاليف من بضع مئات من الدولارات إلى آلاف الدولارات، وتكون عملية الدفع غالباً بعملة البيتكوين، وهذا لا يضمن بأن المهاجم سيمنح الضحية، مفتاح فك التشفير الذي يساعده على استعادة ملفاته بعد قيامه بالدفع.

وفقاً لتقرير (Sophos state of Ransomware 2021) ارتفع عدد المنظمات التي قررت دفع فدية إلى 32 % في عام 2021 مقارنة بـ 26 % في 2020 وقد كشف الاستطلاع العالمي أن 8 % فقط من تلك المنظمات استعادت جميع بياناتها على الرغم من دفع الفدية، في حين أن ما يقارب من الثلث 29 % من المنظمات، لم تتمكن من استعادة أكثر من نصف البيانات المشفرة بين الإزعاج المتوسط وأزمة الصواريخ الكوبية الخطير.

كما يمكن تعريف هجوم برامج الفدية: بأنها نوع من البرمجيات الضارة التي يستخدمها المجرمون، ويعمل هذا الفيروس على حجب الوصول إلى النظام، ويقوم بتشفير على البيانات المهمة من أجل أن يطلب فدية من الضحية مقابل فك التشفير.

■ أنواع فيروس الفدية:

- **البرامج المخيفة:** هو برنامج مزيف يظهر لك رسائل منبثقة متكررة، بأنه اكتشف فيروساً أو مشكلة أخرى على جهاز الكمبيوتر الخاص بك، ويوجهك لضرورة الدفع لحل هذه المشكلة، وتعمل بعض الأنواع منها على إغلاق الكمبيوتر بينما، يظهر البعض الآخر تنبيهات منبثقة، على شاشتك دون إتلاف الملفات الفعلية.

- **شاشات القفل:** حيث حين تعرض جهاز الكمبيوتر الخاص بك لفيروس الفدية الضار باستخدام شاشة القفل، فهذا يعني أنك لن تتمكن من استخدام جهاز الكمبيوتر، فبمجرد تشغيله ستظهر شاشة بالحجم الكامل وكثيراً ما تكون مصحوبة بختم يبدو رسمياً، من مكتب التحقيقات الفيدرالي، أو وزارة العدل، حيث

تظهر تلك الشاشة أن نشاطا غير مشروع، قد تم اكتشافه على جهاز الكمبيوتر الخاص بك مثل (أنك تقوم بأعمال القرصنة أو الجرائم الالكترونية).⁵⁸

- **برامج الفدية الضارة المشفرة:** يعد هذا النوع مخيفا للغاية وهؤلاء هم المهاجمون الذين يقومون بسرقة ملفاتك وتشفيرها، ويطالبون بدفع أموال لفك تشفيرها، ويكمن سبب الخطورة الشديدة لهذا النوع من فيروسات الفدية الضارة في أن مجرمو الفضاء الالكتروني يسرقون ملفاتك ولا توجد برامج أمان او برامج استعادة النظام إذا لم تدفع الفدية.

■ **هجمات الفدية وتأثيرها على العالم:**

تدخل برامج الفدية إلى أجهزتك مثل الأنواع الأخرى من البرمجيات الخبيثة الفيروسات، على سبيل المثال يمكن أن تدخل عبر: ⁵⁹

- رسائل البريد الالكتروني أو الرسائل العشوائية غير المرغوب فيها؛
- موقع الانترنت الضارة التي تزورها والتي تحاول تثبيت برامج الفدية؛
- بعض التطبيقات التي قمت بتثبيتها والتي كنت تعتقد أنها جديرة بالثقة.
توجد العديد من الهجمات العالمية ومن أمثلتها:

- حيث تعرضت شركة توزيع مواد كيميائية ألمانية لهجوم من برامج الفدية الضارة، في ابريل 2021 أدى هذا الهجوم الالكتروني، إلى سرقة تواريخ ميلاد أكثر من 6000 شخص وأرقام الضمان الاجتماعي، وأرقام رخصة القيادة بالإضافة إلى بعض البيانات الطبية.

- كما أصبح أكبر موردي اللحوم في العالم هدفا لهجوم برامج الفدية الضارة، في مايو 2021 وبعد إيقاف تشغيل موقع الويب مؤقتا، وإيقاف الإنتاج، ومن أجل استرجاعها أدى بدفع فدية قدرها 11 مليون دولار في Bit coin.

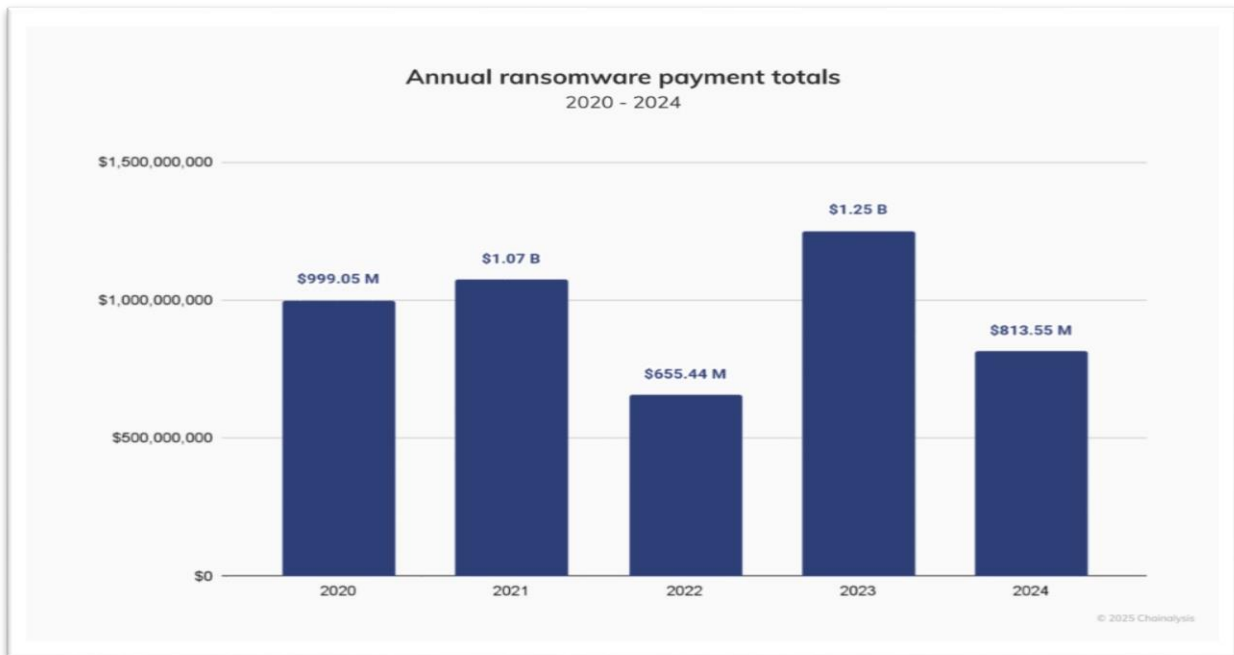
- كما تعرضت إحدى شركات الطيران، في الهند لهجوم برامج الفدية الضارة في مايو 2022، وأدى هذا الحدث إلى تأخير وإلغاء الرحلات فضلا عن تقطع السبل بمئات الركاب⁶⁰.
فيما يلي نوضح مدى تأثير هجمات الفدية على الاقتصاد العالمي:

⁵⁸مؤسسة دعائم التقنية للحاسب الآلي، ما هو فيروس الفدية و أنواعه، وكيف يمكن حماية نفسك ومؤسستك من الاختراق. <http://www.it-pillae.com>. (25فيفري2025، 11.00).

⁵⁹برامج الفدية، موقع إلكتروني، <http://www.Vic.Gov.Au>، (20أفريل2025، 19:00).

⁶⁰ ما هي برامج الفدية، موقع إلكتروني، <http://www.microsoft.com>، (20أفريل2025، 19.30).

الشكل رقم 08: إجمالي المدفوعات السنوية لبرامج الفدية.



[المصدر: https://www.axio:](https://www.axio:المصدر)

Chainalysis (2024). Ransomware trends and Financial Crime Analysis.com 12:30، 13/02/2025
يظهر البيان من شركة إجمالي المدفوعات السنوية لبرامج الفدية بيم عامي 2020 و2024 ويكشف
تذبذب واضح في المبالغ المدفوعة خلال هذه الفترة نلاحظ أنه في عام 2020 بلغت المدفوعات 999,05
مليون دولار

وفي عام 2021، ارتفعت إلى 1,07 مليا دولار مما يشير إلى زيادة نشاط هجمات الفدية أو زيادة معدل
الامتثال للدفع. وانخفاض كبير في 2022 بحيث تراجعت المدفوعات بشكل ملحوظ إلى 655,44 مليون
دولار أي انخفاض حوالي 38,7 عن عام 2021 قد يكون ذلك نتيجة لتحسين استراتيجيات الدفاع
الالكتروني أو زيادة رفض الضحايا دفع الفدية. وإرتفاع حاد في 2023 حيث قفزت المدفوعات إلى
1.25 مليار دولار وهو أعلى مستوى خلال الفترة المدروسة قد يفسر ذلك بتطور أساليب الهجوم وزيادة
الضغط على الضحايا، أو انتشار هجمات أكثر تعقيدا وضررا ثم شهدت انخفاض سنة 2024 حيث
بلغت المدفوعات 813.55 مليون دولار أي بانخفاض حوالي 35 مقارنة بالعام 2023 من خلال هذا
التفسير نستنتج أن اتجاه التذبذب في دفع الفدية تتأثر بتطور الهجمات ومدى استجابة الضحايا وفعالية
الحلول.

المبحث الثالث: مخاطر أخرى

ظهرت العديد من المخاطر التي تؤثر على استقرار المؤسسة المالية ومصادقيتها، تشمل هذه المخاطر مخاطر السوق مثل: تقلبات الأسعار وأسعار الفائدة، والمخاطر التشغيلية كالأعطال التقنية والهجمات الإلكترونية، كما تواجه المؤسسات مخاطر السمعة بسبب انتهاكات البيانات أو الفشل في الامتثال والمخاطر التنظيمية والتشريعية التي تفرضها البيئة القانونية المتغيرة باستمرار وفي هذا المبحث سنسقط الضوء على مفهوم هذه المخاطر.

المطلب الأول: المخاطر التنظيمية والتشريعية.

تظهر هذه المخاطر نتيجة التغيرات التي تطرأ في القوانين، واللوائح وعدم امتثال لها يؤدي إلى عقوبات مالية وكذلك السمعة السيئة للمؤسسة وفي هذا المطلب سوف نتحدث عن المخاطر التنظيمية والمخاطر التشريعية.

أولاً: المخاطر التنظيمية والتشريعية

- مفهوم المخاطر التنظيمية: تعترض عملية أداء المهمات التنظيمية من مواكبة أي صعوبات في ميدان العمل ويمكن تعريف المخاطر التنظيمية ما يلي:
 - التعريف الأول: وهي مخاطر التي قد تؤدي على مواجهة مشاكل في سحب التراخيص أو التعرض للغرامات أو المطالبات القضائية.⁶¹
 - التعريف الثاني: تعرف بأنها تحمل وجهات نظر متباينة تهدف دراستها على تتبع وتعدد وتنوع العوامل المعبرة عنها التي غطت مجموعة من الأعباء الكمية والنوعية في العمل داخل المؤسسة.⁶²ومن التعريفين السابقين يمكن تعريف المخاطر التنظيمية بأنها مجموعة من القوانين تضعها المؤسسة من العمل بها وأي إخفاق في عمل بها يؤدي إلى ظهور مخاطر عدة.
- أنواع المخاطر التنظيمية: تتضمن المخاطر التنظيمية مجموعة من المخاطر نوضحها في الشكل الموالي:

الشكل (09): أنواع المخاطر التنظيمية

⁶¹ مفهوم المخاطر التنظيمية، موقع الكتروني <https://albarakatilaw.com>، (الساعة 11:24، 13ماي2025).

⁶² سلطان احمد خليف، المخاطر التنظيمية والسلوك القيادي دراسة لأراء عينة من القيادات الإدارية في جامعة الموصل، مجلة جامعة الانبار للعلوم الاقتصادية والإدارية، المجلد 5، العدد 10، 2013، ص225.



المصدر: من إعداد الطالبتين بالاعتماد على سلطان احمد خليف، المخاطر التنظيمية والسلوك القيادي دراسة لآراء عينة من القيادات الإدارية في جامعة الموصل، مجلة جامعة الانبار للعلوم الاقتصادية والإدارية، المجلد 5، العدد 10، 2013، ص225.

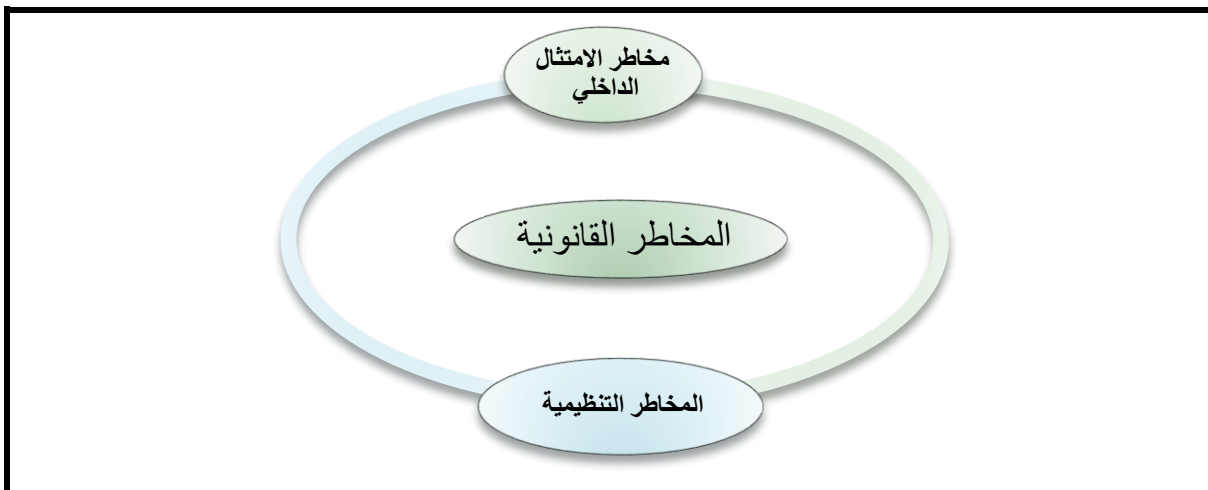
نلاحظ من الشكل أنواع المخاطر التنظيمية يمكن تفصيلها بما يلي:

أولاً: مخاطر الامتثال ودورها في التكنولوجيا المالية

إن مخاطر الامتثال تشير إلى احتمالية تعرض المؤسسات لعواقب سلبية نتيجة في عدم التزام بالقوانين واللوائح والمعايير التنظيمية ذات صلة بنشاطها.

- مفهوم مخاطر الامتثال Compliance risk: وقد يطلق عليها مخاطر عدم الامتثال وهي مخاطر يتعرض لها المصرف نتيجة لعدم التزام بالقواعد والقوانين أو التنظيمات المرتبطة بقواعد القانونية وإن هذه المخاطر قد تؤدي إلى فرض غرامات مالية أو قيود تشغيلية تؤثر على استمرارية الأعمال.⁶³
- أنواع مخاطر الامتثال: تتكون مخاطر الامتثال بعدة أنواع نذكر منها ما يلي:

الشكل (10): أنواع مخاطر الامتثال



المصدر: مفهوم مخاطر الامتثال، موقع الالكتروني، <https://ar.lpcentre.com>، (14/03/205، 13:00).

⁶³ مفهوم مخاطر الامتثال، موقع الالكتروني، <https://ar.lpcentre.com>، (14/03/2025، 13:45).

■ **المخاطر تنظيمية:** يوجد هذا نوع من المخاطر بسبب وجود شكوك داخلية مستمرة في كل شيء له صلة بالعملية التنظيمية والمخاطر التنظيمية لها تأثير على جوانب المؤسسة ومن أمثلة المخاطر التنظيمية هي:

- عدم وضع خطة جيدة لتسيير أعمالها؛

- المبادئ الأساسية التي تما وضعها لم تكن واضحة للعملاء؛

- سوء التقدير الزمني في إعداد العمليات.

■ **النوع الثاني:** المخاطر القانونية تعتبر المخاطر القانونية من الجوانب الهامة في إدارة المخاطر وتشمل التعرض للعقوبات القانونية أو الدعاوى القضائية نتيجة لعدم الالتزام بالقوانين واللوائح المعمول بها وكذلك عدم الفهم الصحيح لشروط العقود أو عدم القدرة على الوفاء بها. وفيما يلي بعض الأمثلة الرئيسية للمخاطر القانونية وكيفية تأثيرها.⁶⁴

الجدول رقم (02): أمثلة رئيسية للمخاطر القانونية وكيفية تأثيرها

نوع المخاطر القانونية	التفاصيل
عقود	تنشأ المخاطر من عدم الفهم الصحيح لشروط العقود أو عدم القدرة على الوفاء بها، مما قد يؤدي إلى دعاوى قضائية أو خسائر مالية
تنظيمات الصناعة	يجب على الشركات الالتزام بالقوانين والتنظيمات الخاصة بصناعاتها، وعدم الامتثال يمكن أن يؤدي إلى غرامات أو تقييدات تشغيلية.
حقوق الملكية الفكرية	المخاطر المتعلقة بانتهاك حقوق الملكية الفكرية، سواء كانت براءة اختراع، علامات تجارية قد يؤدي إلى معارك قانونية مكلفة.
قوانين العمل	العدم الامتثال لقوانين العمل مثل تلك المتعلقة بالصحة والسلامة أو التعويضات وقد يؤدي إلى دعاوى قضائية من الموظفين

المصدر: من إعداد الطالبات بالاعتماد على الموقع الإلكتروني، communication .com..my، (25/03/2025)،

(12:30).

⁶⁴الموقع الإلكتروني، communication .com.. my، (3 مارس، 2025، 13:26).

النوع الثالث: مخاطر عدم الامتثال الداخلي تنشأ مخاطر عدم الامتثال الداخلي من خلال فشل المؤسسات في الالتزام بالسياسات والإجراءات الداخلية المعمول من قبل المؤسسة. وكذلك فقدان سمعتها وعد ثقة الموظفين لها.

■ دور التكنولوجيا في إدارة مخاطر الامتثال

مع التعقيد المتزايد للامتثال تحتاج المؤسسات إلى اعتماد أساليب مبتكرة لإدارة مخاطر الامتثال، تعد التكنولوجيا واحدة من أكثر الأدوات الفعالة وسوف نكتشف دور التكنولوجيا المالية في إدارة مخاطر الامتثال نذكر منها ما يلي:

- **أتمتة عمليات الامتثال:** هيا إحدى مزايا التكنولوجيا المالية في إدارة مخاطر الامتثال هي القدرة على أتمتة عمليات الامتثال، وتتضمن عمليات الامتثال الكثير من المهام اليدوية والتي تستغرق وقتاً طويلاً، وتساعد في تقليل الوقت المستغرق في أنشطة الامتثال والقضاء على الأخطاء.
- **المراقبة في الوقت الحقيقي:** يجب أن توفر التكنولوجيا المالية مراقبة في الوقت لأنشطة الامتثال، وهو أمر ضروري في إدارة وعلى سبيل المثال يمكن للمؤسسات استخدام أدوات مراقبة لتنبيه مدري الامتثال.
- **تحليل البيانات:** تعد تحليل البيانات مجالا آخر حيث يمكن للتكنولوجيا أن تساعد المؤسسات على إدارة مخاطر الامتثال من خلال تحليل بيانات المؤسسة ومن أجل توفير رؤى حول أنشطة الامتثال مثل سجلات تدريب الموظفين ونتائج التدقيق.
- **التدريب على الامتثال:** إن التدريب على الامتثال يساعد المؤسسات على تثقيف الموظفين بشأن متطلبات الامتثال ويقلل من مخاطر عدم الامتثال بفضل التكنولوجيا يمكن للمؤسسات توفير تدريب على امتثال الموظفين بطريقة جاذبية وفعالية.
- **الإبلاغ عن الامتثال:** تعد تقارير الامتثال جانبا مهما لإدارة مخاطر الامتثال. توفر تقارير الامتثال رؤى حول الأنشطة وتساعد على تحديد مجالات عدم الامتثال، ويمكن أن تساعد التكنولوجيا في تحسين تقارير الامتثال من خلال توفير أدوات إعداد التقارير الآلية.⁶⁵

ثانياً: المخاطر المالية تعرف المخاطر المالية في عدم قدرة المنظمات على الوفاء بالتزاماتها المالية وإدارة ديونها. نتيجة عدم الاستقرار أو الخسائر في السوق المالية أو تحركات أسعار الأسهم والعملات وأسعار الفائدة، وتشير إلى الأحداث السلبية المحتملة التي قد تؤثر على الأداء المالي.⁶⁶

⁶⁵ دور التكنولوجيا في إدارة مخاطر الامتثال، <https://Fastercapital.Com>، (2025/04/05، 15:34).

⁶⁶ مفهوم المخاطر المالية، موقع الالكتروني، [HTTPS://BAKKAH.COM](https://BAKKAH.COM)، (2025/04/05، 15:34).

- أنواع المخاطر المالية: هناك عدة أنواع نذكر منها ما يلي:
- مخاطر الائتمان: هي الخسارة المحتملة يتضرر من جرائها القرض ولا يواجهها المقرض لذلك فهي تصيب كل شخص يمنح قرضا سواء كان بنكاً، أو مؤسسة مالية أو منشأة أعمال تباع لأجل.⁶⁷
- مخاطر السيولة: هي المخاطر التي تواجه منشآت الأعمال عندما لا يتوافر لديها الأموال الكافية لمقابلة الالتزامات المالية في الأوقات المحددة لها وتشمل مخاطر السيولة، مخاطر قصيرة الأجل ومخاطر طويلة الأجل علماً بأن كل مؤسسات الأعمال بحاجة لإدارة السيولة التي تبقى في مأمن من الإفلاس.⁶⁸
- مخاطر العملة: هي مخاطر تنتج من خلال تحقيق مكاسب أو خسائر ناتجة عن التقلبات بين العملات المختلفة ويمكن أن تؤثر مخاطر العملة على الجميع الشركات والمؤسسات المالية وهنا يظل الدولار الأمريكي العملة الاحتياطية الأولى في العالم، مما يعني انه الخيار للبلدان الأخرى عندما يرغبون في الاحتفاظ باحتياطيات من النقود الورقية في ميزانياتهم العمومية.⁶⁹

ثالثاً: المخاطر الاستراتيجية

تحدث المخاطر الاستراتيجية عند إتباع الشركة استراتيجية عمل خاطئة، أو عندما لا تعمل طبقاً لنموذج أعمالها أو خطتها أو عندما يفشل مديروها التنفيذيون في إتباع استراتيجية عمل وهو ما يعيق الشركة عن الوصول إلى أهدافها.

تأثير المخاطر التنظيمية على المؤسسات المالية ويمكن أن تشمل هذه المخاطر غرامات مالية، تكاليف قانونية، أضرار سمعة على سبيل المثال في عام 2018 تم تغريم ويلز فارغو بمليار دولار والبنك أيضاً واجهه 500 مليون دولار إضافية في عقوبات وهذا يمكن أن يؤثر على الوضع المالي للمؤسسة وسمعتها في السوق.

الجدول (03): أنواع المخاطر التنظيمية وكيفية إجراء إدارة المخاطر

نوع المخاطر التنظيمية	الوصف	إجراءات إدارة المخاطر
-----------------------	-------	-----------------------

⁶⁷ حفيان جهاد، إدارة المخاطر الائتمانية في البنوك التجارية دراسة استبائية مجموعة من البنوك التجارية العاملة بولاية ورقلة خلال سنة 2012، مذكرة مقدمة لنيل شهادة الماستر في العلوم المالية، جامعة قاصدي مرباح، 2012/2011، ص 08.

⁶⁸ the importance of using information technology in ، abderrazak habbar، Karbnache houri، 2022، ص 16.

⁶⁹ مفهوم مخاطر العملة، موقع الالكتروني <https://www.argaam.com>، (12/04/2025، 14:30).

مخاطر الامتثال	مخاطر ناشئة عن عدم الامتثال للقوانين واللوائح	تطوير سياسات وإجراءات للالتزام
المخاطر المالية	المخاطر المؤثرة على الوضع المالي للمؤسسة	إجراءات التنبؤات المالية واختبارات الضغط
المخاطر الاستراتيجية	مخاطر ناتجة عن التأثيرات التنظيمية على الأهداف الاستراتيجية	تقييم التأثير وتطوير خطط للتخفيف

المصدر: المؤسسة العربية للعلوم ونشر الأبحاث، موقع الكتروني، <http://blog.ajsrp.com>، (11:23، 15/2/2025.)

■ **أسباب المخاطر التنظيمية والمخاطر التشريعية:** عند التحدث عن المخاطر التشريعية والتنظيمية يعني

- التركيز على بيئة الأعمال والبنية التحتية الرقمية ومن أسباب هذه المخاطر نجد
- الافتقار إلى الأطر الرقابية والتنظيمية: يفتقر الكثير من تقنيات التكنولوجيا لمالية إلى تطبيق ممارسات قوية فيما يتعلق بالجوانب التشغيلية وبالحوكمة والمخاطر ومن ذلك العملات المشفرة حيث تعرضت العديد من المبادلات لتوقف متكرر أثناء اضطرابات الأسواق.
- وجود ثغرات في أنظمة البيانات التي تحصل عليها الأجهزة التنظيمية بسبب عدم وضوح هوية مستخدمي هذه الأصول المشفرة، مما يرفع من حالات تبيض الأموال، إضافة إلى اختلاف الأطر التنظيمية التي تطبق على المنظومة البيئية المشفرة باختلاف البلدان مما يجعل من عملية التنسيق جد صعبة
- غياب الأطر التنظيمية يجعل تقنية سلسلة الكتل قادرة على تجاوز حدود السلطات القومية بشكل نسبي أو مباشر.
- المخاطر الناتجة عن التمويل اللامركزي، حيث تبرز مخاطر مرتبطة بعدم قابلية تعديل البنية التحتية اللامركزية مما يجعل حماية المستثمرين أكثر صعوبة.
- المخاطر المتعلقة بأخطاء برمجة العقود الذكية فالمعاملات المركبة ونظم الرموز المغلفة التي تشبه عملية رهن الضمان تساهم في انتشار تداعيات الصدمات عبر النظام وقد تؤثر على الاقتصاد الحقيقي⁷⁰.

المطلب الثاني: مخاطر السمعة والمخاطر البيئية.

في هذا المطلب تم الربط بين المخاطر البيئية ومخاطر السمعة حيث يؤدي مثالا عدم الامتثال للمعايير البيئية إلى فقدان ثقة العملاء والمستثمرين، مما يؤدي لمخاطر سمعة المؤسسة.

⁷⁰ لطرش ذهبية، دراسة تحليلية لفرص ومخاطر التكنولوجيا المالية على الاستقرار المالي، مجلة اقتصاد المال والأعمال، المجلد 8، العدد 01، مارس 2023، جامعة الشهيد حمه لخضر الوادي، الجزائر، 2023، ص 829.

أولاً: مخاطر السمعة

- أنواع مخاطر السمعة: تعرف السمعة على أنها واحدة من أهم أصول الشركة ويمكن أن يكون لها تأثير مباشر على قدرتها على جذب العملاء والبقاء رابحة، كما تشير لتصور العام لها من قبل العملاء والمنافسين، ويمكن أن يستغرق تطوير سمعة الشركة سنوات، ومن المهم للشركات أن تدير سمعتها بعناية لأن التصور العام يمكن أن يتغير بسرعة كبيرة بناءً على الأحداث الصغيرة التي تكتسب قوة الجذب.⁷¹ هناك أربعة أنواع أساسية لمخاطر السمعة نوضحها في الشكل التالي:

الشكل (11): أنواع مخاطر السمعة



المصدر: من إعداد الطلبات بالاعتماد على [http:// www. Question. Pro. com](http://www.Question.Pro.com)، مخاطر السمعة، ماهي أنواعه، (29 أبريل 2025، 13:00).

من الشكل نلاحظ أنه تحدث حالات مخاطر السمعة أحيانا بشكل مباشر بسبب تصرفات الشركة وطرق ممارسة الأعمال، أما مخاطر السمعة بسبب الأحداث الخارجية يمكن أن تؤثر بشكل سلبي، خاصة عندما يكون عن العاملين السابقين تجربة سلبية في الشركة وفي معظم الأحيان تحدث مخاطر من أشخاص ليس لهم صلة مباشرة بالعمل في الشركة، كما يمكن لشريك أو مورد أن يضر بسمعة العلامة التجارية.

- **تأثيرات مخاطر السمعة على المؤسسات المالية:** تعتبر مخاطر السمعة تهديداً استراتيجياً يمكن أن يقوض جهود الشركة وأهدافها، وغالباً ما يكون له عواقب فورية وطويلة الأجل، حيث تنتشر المعلومات

⁷¹ إدارة السمعة ومخاطر المنافسة في الأعمال التجارية، مقال 100 من سلسلة إدارة وتطوير الأعمال، من موقع، business insight، 13 يونيو 2024.

بسرعة، أصبح تأثير مخاطر السمعة على المؤسسات المالية أكثر وضوحًا يمكن أن تتشوه بسبب حادث واحد، مما يؤدي إلى فقدان ثقة العملاء، وانخفاض أسعار الأسهم، وربما ضرر لا يمكن إصلاحه، سنوضح أهم هذه التأثيرات:⁷²

- **التأثير المالي:** يمكن أن تؤدي السمعة المتضررة إلى خسائر مالية مباشرة، على سبيل المثال، بعد فضيحة الانبعاثات لشركة فولكس فاجن، واجهت الشركة غرامات بالمليارات وانخفاضًا كبيرًا في المبيعات، مما يعكس التكلفة المباشرة التي لحقت بسمعتها.
- **الاضطرابات التشغيلية:** يمكن أن تتأثر الأنشطة التشغيلية عندما تتحقق المخاطر المتعلقة بالسمعة فقد يؤدي ذلك إلى تعطيل العمليات التجارية، على سبيل المثال قد يسعى الموردون إلى إبعاد أنفسهم عن مؤسسات ذات سمعة سيئة مما يؤدي إلى مشكلات في سلسلة التوريد.
- **التدقيق التنظيمي:** غالبًا ما تواجه المؤسسات المالية التي تواجه مشكلات تتعلق بالسمعة اهتمامًا متزايدًا من الجهات التنظيمية، لأنها تجذب اهتمام قانوني وتنظيمي غير مرغوب فيه مما يؤدي لزيادة تكاليف الامتثال.
- **وضع السوق :** يمكن أن يتآكل وضع السوق على المدى الطويل بسبب الإضرار بالسمعة، مما يسمح للمنافسين بالاستيلاء على حصته في السوق وهذا يؤدي إلى فقدان ثقة العملاء.
- **الموظفين:** قد يشعرون بالإحباط أو القلق بشأن الأمن الوظيفي مما قيد يؤدي لانخفاض الإنتاجية أو حتى الاستقالات كذلك يؤثر على فرص العمل المستقبلية وخطط التوسع.
- **تحديد مصادر مخاطر السمعة:** تعتبر مخاطر السمعة مصدر قلق استراتيجي لأي مؤسسة، لأنها يمكن أن تؤدي إلى تآكل الثقة وولاء العملاء، مما يؤثر في النهاية على النتيجة النهائية، فهو ينشأ من مجموعة متنوعة من المصادر، ولكل منها الفروق الدقيقة والتأثيرات المحتملة، سنذكر أهمها:
- **تجربة العملاء:** تجارب العملاء السلبية، سواء كانت بسبب سوء الخدمة أو فشل المنتج أو التوقعات غير المبالاة، يمكن أن تتصاعد بسرعة إلى مخاطر كبيرة على السمعة.

⁷² من إعداد الطلبات بالاعتماد على:

- مخاطر السمعة التأثير المضاعف، [http:// www. Fastercapital.com](http://www.Fastercapital.com)، (27 أبريل 2025، 12:00).
- سمعة الشركة كيف تتجنب المخاطر، [http:// www. Rowadalaamal. com](http://www.Rowadalaamal.com)، (27 أبريل 2025، 12:00).

- **سلوك الموظف:** يمكن لتصرفات الموظفين، وخاصة أولئك الذين يشغلون مناصب رفيعة المستوى، أن تنعكس على المؤسسة، تعد حادثة شركة "يوناييتد إيرلاينز" عام 2017، حيث تم إخراج أحد الركاب قسراً من رحلة محجوزة
- **انتهاكات الامتثال:** يمكن أن تؤدي المخالفات التنظيمية إلى فرض غرامات ومعارك قانونية، ولكن الضرر المرتبط بالسمعة قد يكون أكثر تكلفة، لم تسفر فضيحة انبعاثات فولكس فاجن، المعروفة باسم "ديزلجيت"، عن غرامات بالمليارات فحسب، بل ألحقت أضراراً بالغة بسمعة الشركة لسنوات.
- **وسائل التواصل الاجتماعي:** في العصر الرقمي تنتشر المعلومات بسرعة، وكذلك المعلومات الخاطئة، يمكن أن تتسبب تغريده واحدة في انخفاض سعر السهم أو حدوث مقاطعة، كما في حالة حادثة "ستاربكس" عام 2018 التي تضمنت اعتقال رجلين أسودين في أحد متاجر فيلادلفيا.
- **مشكلات سلسلة التوريد:** يمكن أن تؤدي المشكلات مع الموردين، مثل النزاعات العمالية أو الانتهاكات البيئية، إلى تشويه سمعة المنظمة بسبب الارتباط بها، على سبيل المثال، واجهت صناعة الأزياء ردود فعل عنيفة بسبب ظروف المصانع الاستغلالية في البلدان النامية.
- **خروقات الأمن السيبراني:** يمكن أن تؤدي خروقات البيانات إلى فقدان ثقة العملاء، خاصة إذا تم اختراق المعلومات الحساسة، كشف اختراق Equifax في عام 2017 عن البيانات الشخصية لـ 147 مليون شخص، مما أدى إلى ضرر كبير لسمعة مكتب الائتمان.
- **سوء سلوك القيادة:** يمكن للفضائح التي يتورط فيها كبار المسؤولين التنفيذيين أن تلقي بظلالها على المؤسسة بأكملها، تعد استقالة الرئيس التنفيذي لشركة أوبر، "ترافيس كالانيك"، وسط سلسلة من الجدل، مثالاً على كيف يمكن لقضايا القيادة أن تصبح مخاطر على السمعة.⁷³

ثانياً: المخاطر البيئية

- **أشكال المخاطر البيئية:** المخاطر البيئية تشير إلى التأثيرات أو التحديات البيئية التي قد تتجم عن استخدام التكنولوجيا، ومن بين أسباب هذه المخاطر فشل المعدات مثل التسريبات من الخزانات أو خطوط

⁷³ إدارة السمعة مخاطر السمعة، التخفيف من مخاطر السمعة، استراتيجيات الوقاية والاستجابة، [http:// www. Faste. capital. com](http://www.Faste.capital.com). (6 أبريل 2025، 13:00).

الأنابيب أو الكمبيوتر وتستغل هذه المخاطر من قبل القراصنة حيث يستهدفون الأنظمة المالية المعطلة لشن هجمات إلكترونية لها عدة أشكال نذكر منها:⁷⁴

- **التلوث:** يشمل العديد من المجالات نذكر منها نفقات التنظيف والعلاج، والاستهلاك غير المستدام للموارد يمكن أن يشمل ذلك الحوادث التي تنطوي على النفايات الخطرة وغيرها من الملوثات.
- **الكوارث الطبيعية:** يمكن أن تنشأ المخاطر البيئية أيضاً من الكوارث الطبيعية، مثل الأعاصير والفيضانات والزلازل أو حرائق الغابات كما تحدث التحولات الجيولوجية مثل تآكل التربة والتصحر.
- **فشل المعدات:** يمكن أن يؤدي فشل المعدات أيضاً إلى مخاطر بيئية، مثل التسريبات من الخزانات أو خطوط الأنابيب أو الكمبيوتر وتستغل هذه المخاطر من قبل القراصنة حيث يستهدفون الأنظمة المالية المعطلة لشن هجمات إلكترونية.

- **الخطأ البشري:** الخطأ البشري هو سبب شائع للمخاطر البيئية، بسبب الأفعال الغير المقصودة أو القرارات الخاطئة التي يتخذها الفرد، أي الناتجة عن التعامل مع المواد الغير سليمة أو تخزينها، تحدث نتيجة قلة الوعي البيئي.⁷⁵

■ أمثلة حول النفايات الإلكترونية:

- نفايات أجهزة التبريد والتسخين، مثل الثلاجات والتدفئة والمكيفات الهواء. والتي تبلغ كمية إنتاجها في سنة 2019 حوالي 10.8 مليون طن متري؛
- نفايات الشاشات العرض بمختلف أنواعها للحواسيب والتلفزيونات وأي باد وغيرها والتي بلغت كمياتها سنة 2019 حوالي 6.7 مليون طن متري؛
- نفايات الأجهزة الاتصالات الصغيرة المستعملة في منظومات تقنية المعلومات والاتصالات مثل النقالات والساعات الذكية وغيرها، والتي بلغت كمياتها المنتجة حوالي 4.7 مليون طن متري في سنة 2019.⁷⁶
- بحيث تحتوي النفايات الإلكترونية على مواد مضافة سامة أو مواد خطرة، مثل الزئبق، ومركبات الكلوروفلوروكربون (CFCs) حيث أن التخلص الغير الفعال لها وسوء المعاملة تعرض البيئة وصحة الإنسان للخطر.

⁷⁴ جميع المخاطر البيئية، ومعالجة المخاطر البيئية، <http://www.Fastercapital.COM>، (15 أبريل 2025، 18:00).

⁷⁵ جميع المخاطر البيئية، ومعالجة المخاطر البيئية، <http://www.Fastercapital.COM>، (11 أبريل 2025، 17:00).

⁷⁶ النفايات الإلكترونية، أنواعها، تأثيراتها على البيئة، <http://www.medicalwaste.org>، (11 أبريل 2025، 19:00).

المطلب الثالث: مخاطر السوق والمخاطر التشغيلية.

ترتبط المخاطر التشغيلية بمخاطر السوق بشكل وثيق، حيث تؤدي الأعطال التقنية أو الاختراقات إلى اضطراب الأسواق وتقلب الأسعار.

أولاً: مخاطر السوق

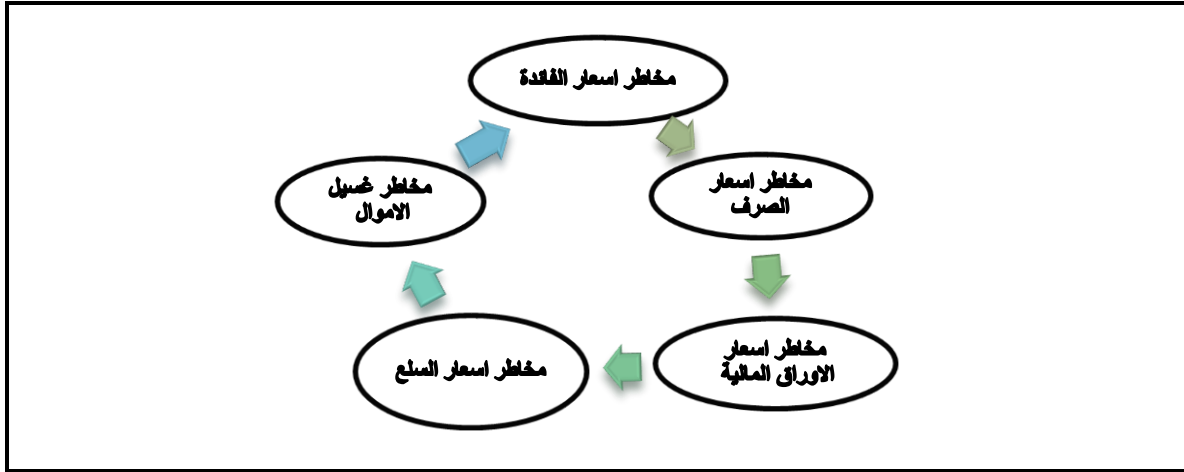
- **التعريف الأول:** هي مخاطر الانحرافات السلبية لقيمة مراقبة تحركات السوق لمحفظه التداول أثناء الفترة المطلوبة لتصفية المعاملات.
 - **التعريف الثاني:** هو خسارة المحتملة الناجمة عن تقلبات أسعار الفائدة، أسعار السلع، أسعار الأوراق المالية وذلك بسبب التطورات غير مناسبة لعوامل السوق، بمعنى أن مخاطر السوق تنتج عن التغيرات المعاكسة أو التي ليست في صالح المصرف لأسعار السوق⁷⁷.
 - **التعريف الثالث:** تعرف مخاطر السوق هي المخاطر الناتجة عن التحركات العكسية في القيمة السوقية لأصل ما قد تكون سلعة أو عملة أو صك استثماري أو غير ذلك.⁷⁸
- ومن هذه التعاريف السابقة نستنتج أن مخاطر السوق تلك التقلبات التي تحدث في سعر الفائدة والخسائر التي يتكبدها المصرف كما تتميز مخاطر السوق إلى احتمالية تكبد خسائر بسبب تقلبات أسعار الأصول المالية.
- **أنواع مخاطر السوق:**
- يمكن توضيحها في الشكل التالي:

شكل رقم 12: أهم أنواع مخاطر السوق.

المصدر: عياش زويير، العايب سناء، تسيير مخاطر السوق وفق مقررات بازل 2 واصلاحات بازل 3، مجلة دراسات اقتصادية، المجلد 6، العدد 02، ديسمبر 2019، ص 89.91.

⁷⁷لوييزة أوصغير، مرجع سابق، ص 71.

⁷⁸ طبيب سارة، أساليب تعامل المؤسسات الصناعية الجزائرية مع مخاطر السوق، مجلة العلوم الاقتصادية و التسيير و العلوم التجارية، العدد 14، 2015، ص 35 .



من الشكل رقم 12: تحدث مخاطر السوق إما لأسباب متعلقة بالمتغيرات الاقتصادية أو نتيجة تغير أحوال المؤسسات الاقتصادية على المستوى الجزئي ومنه يمكن تصنيف مخاطر السوق إلى:

- **مخاطر أسعار الفائدة Interest rate risk**: يتعرض لهذا النوع من المخاطر كل الأدوات المالية (سندات، أوراق مالية....) ذات أسعار الفائدة الثابتة والمتغيرة، وكذلك المشتقات مثل المستقبلات، عقود الصرف ويقسم إلى الخطر الخاص والخطر العام بحيث:
 - ✓ **الخطر الخاص**: ينتج عن تغير غير مناسب في سعر السند لسبب يعود على مصدره الخاص.
 - ✓ **الخطر العام**: ينتج من خلال قياس الخسارة الناتجة عن تغير في سعر الفائدة في السوق.⁷⁹
- **مخاطر أسعار الصرف Foreign Exchange Risk**: تنشأ هذه المخاطر في سوق النقد، وتعرف على أنها المخاطر الناتجة عن تقلب أسعار صرف العملات في التعاملات الآجلة التي تقعدها المؤسسة الدولية النشاط.
- **مخاطر أسعار الأوراق المالية Securities Prices Movement**: تنشأ هذه المخاطر نتيجة تقلبات أسعار الأوراق المالية في أسواق رأس المال استجابة لإحداث خارجية سواء بفعل عوامل حقيقية أو عوامل مصطنعة وغير أخلاقية.
- **مخاطر أسعار السلع Commodity Prices Fluctuations Risk**: وتسمى بمخاطر التضخم الناتجة عن ارتفاع العام والمستمر في سلة السلع المختلفة، ومن ثم انخفاض القدرة الشرائية للعملة.⁸⁰
- **مخاطر غسل الأموال**: يعد غسل (تبييض) الأموال جريمة اقتصادية عابرة للحدود، تهدد استقرار الأنظمة المالية والاقتصادية في دول العالم، فهو عملية معقدة تهدف إلى إخفاء المصدر الحقيقي للأموال غير المشروعة ويمكن تعريف غسل الأموال كما يلي:

⁷⁹ عياش زويبر، العايب سناء، تسيير مخاطر السوق وفق مقررات بازل 2 وإصلاحات بازل 3، مجلة دراسات اقتصادية، المجلد 6، العدد 02، ديسمبر 2019، ص 89، 91.

⁸⁰ فخاري فاروق، أهمية النماذج الرياضية في إدارة وقياس مخاطر السوق مع الإشارة لتجربة استخدام نموذج القيمة المعرضة للخطر VAR على مستوى البنوك المصرية، مجلة التكامل الاقتصادي، المجلد 08، 2020، ص 180.

- **التعريف الأول:** غسيل الأموال هي مجموعة العمليات ذات الطبيعة الاقتصادية تتبع لتغيير صفة مال وإخفاء طبيعته وتمويه مصدره الذي أتى من مصدر غير مشروع، ليظهر وكأنه نشأ عن مصدر مشروع بإخفاء الشرعية عليها.⁸¹
- **التعريف الثاني:** يتمثل في تحويل السيولة النقدية الناتجة عن الأعمال غير القانونية، إلى أشكال أخرى من الأصول، بما يساعد على تأمين تدفق العائدات المالية غير المشروعة، وبحيث يمكن استخدامها فيما بعد في أنشطة مشروعة تزيل أي شبهات عنها.⁸²
- ومن التعريفين السابقين نستنتج أن غسيل الأموال هي جريمة اقتصادية تهدف إلى إخفاء شرعية القانونية على أموال محرمة، لغرض حيازتها أو التصرف فيها أو إدارتها، حفظها، استبدالها، أو تلاعب في قيمتها إذا كانت متحصلة من جرائم.
- ✓ **مراحل غسيل الأموال:** تعتبر عملية غسيل (تبييض) الأموال عملية ديناميكية، ويمكن تصنيفها على ثلاث مراحل فيما يلي:⁸³
- **مرحلة التوظيف أو الإيداع:** وذلك من خلال إدخال المال في الدورة المالية أي تحويل المال القدر إلى ودائع مصرفية وفي عدة حسابات في مصرف واحد أو أكثر، وتعتبر سلسلة العمليات هذه عند انتهائها بدء عملية التبييض. ففي هذه المرحلة يتم التخلص المادي من الأموال غير المشروعة، غير أن من البديهي إن الكميات الكبيرة من السيولة النقدية، يمكن أن تجلب الانتباه، فالهدف من هذه المرحلة هو التخلص من السيولة النقدية، التي أصبحت ثقلاً على كاهل المجرمين، ويتم ذلك عادة عندما يتمكن مبيضو الأموال إيداع متحصلات النشاط الإجرامي إلى داخل النظام المصرفي والنقدي.
- **مرحلة إخفاء مصدر الأموال:** يتمثل في قيام أصحاب الأموال الناتجة عن أنشطة إجرامية بإجراء العديد من العمليات على حساباتهم وذلك لقطع الصلة بمصادرها الأصلية مثل شراء أسهم وسندات أو تحويلها من شركات حقيقية متواطئة معهم وهنا يضيع الأثر الإجرامي لمصدر الأموال وإخفاء مصدر المال وإعطائها غطاءً شرعياً ويصبح المال جاهز للدخول بمشاريع اقتصادية بشكل قانوني.

⁸¹ أحمد عازب الشيخ، عبد الجليل هويدي، مخاطر ظاهرة غسيل الأموال على الأمن الاقتصادي الجزائري، جامعة الوادي، الجزائر، المجلد 01، العدد 01، 2019، ص 37.

⁸² عبد الله عزت بركات، ظاهرة غسيل الأموال وأثارها الاقتصادية والاجتماعية، جامعة الزرقاء الأهلية، الأردن، مجلة اقتصاديات شمال إفريقيا، العدد 04، ص 218.

⁸³ مسعداوي يوسف، دور البنوك في محاربة عمليات غسيل الأموال غير المشروعة، جامعة البليدة 2، الجزائر، مجلة الإدارة والتنمية للبحوث والدراسات، العدد 5، ص 37/36.

ومع التطور التكنولوجي أصبح غاسلوا الأموال يلجأون إلى الوسائل الالكترونية الحديثة لتمويه نشاطاتهم من أجل محو آثار الجريمة وذلك كون تلك العمليات تتسم بالسرعة والمسافات البعيدة والقدرة على إخفاء الاسم ومحو أية آثار محاسبية في هذا الإطار.

- **مرحلة دمج الأموال المغسولة بالأموال الشرعية:** تعتبر هذه المرحلة الأخيرة في عمليات غسل الأموال وتمتاز بعلنية نشاطاتها، وذلك من خلال دمج هذه الأموال في الدورة الاقتصادية وخطها في الاقتصاد الكلي بحيث يصعب معها التمييز بين الثروة ذات المصدر المشروع وغيرها من الثروات ذات المصادر غير المشروعة وإضفاء الطابع القانوني على أعمالها، بحيث يصعب معها اكتشاف أمرها باعتبارها قد خضعت لعدة مستويات من التدوير وعلى مراحل زمنية متباعدة ولا يمكن في هذه الحالة كشفها إلا من خلال أعمال الجاسوسية والمخبرين السريين والأعمال الاستخباراتية وحظوظ المصادقة والتي لا يمكن الركون عليها كأساس لمكافحة عمليات غسل الأموال .
- **غسيل الأموال عن طريق العملات المشفرة:** يتبع غسل الأموال باستخدام العملات المشفرة النمط العام المتمثل في الإيداع، تمويه، الأثر، الاندماج ولكنه يتسم ببعض الميزات المحددة:
- العملات المشفرة تخفي الهوية في نقطة إنشائها، وبالتالي فإن مرحلة الإيداع من غسل الأموال تكون غائبة؛
- يمكن بتكلفة منخفضة وضع مخطط كبير لغسل الأموال ينطوي على آلاف التحويلات، وتنفيذه باستخدام برنامج حاسوبي نصي؛
- نظرا للزيادات السريعة في أسعار الصرف، ومع ظهور نمو في بعض العملات المشفرة 10000 في المائة، يسهل كثيرا تبرير كسب الثروة غير متوقعة من العملات المشفرة.⁸⁴

ثانيا: المخاطر التشغيلية

- **التعريف الأول:** يعرف معهد التمويل الدولي المخاطر التشغيلية بأنها " خطر الخسارة الناتجة من الإخفاق أو الفشل في الإجراءات الداخلية والأفراد والأنظمة أو حتى الأحداث الخارجية، التي لم تغطى

⁸⁴ غسيل الاموال عن طريق العملات المشفرة، الموقع الالكتروني، <https://syntheticdrugs.unodc.org>، (12:30، 3/4/2025).

مسبقا بموجب احتياطات رأسمالية أخرى مثل مخاطر الفائدة وتلاحظ عدم اهتمام المصارف بمخاطر السيولة، السمعة، وعدم وجود استراتيجية للعمل وخسائر قريبة الحدوث.

- **التعريف الثاني للجنة بازل للرقابة المصرفية:** هيا الخسائر الناجمة عن إخفاق أو عدم كفاية الإجراءات الداخلية أو العنصر البشري والأنظمة لدى البنوك لأحداث خارجية.⁸⁵
- من التعاريف السابقة يمكن أن نعرف المخاطر التشغيلية على أنها الفشل والقصور في العمليات الداخلية للمؤسسة وتشمل هذه المخاطر الاحتيال والأعطال التقنية.

■ أسباب المخاطر التشغيلية:

- هناك جملة من الأسباب التي جعلت البنوك أكثر عرضة للمخاطر التشغيلية في الآونة الأخيرة أهمها:
- ضعف مقدرة البنوك في التحكم في التقنيات الآلية المتطورة المستخدمة في تنفيذ العمليات المصرفية؛
- النمو في التجارة الالكترونية والتي تتطوي على مخاطر محتملة مازالت أبعادها غير معروفة تماما؛
- ضعف السياسات الأمنية المصاحبة للعمل المصرفي الالكتروني، حيث تنشأ المخاطر من جراء أخطاء المرخص لهم مثل تجاوزات الموظفين في البنك أو تنشأ من غير المرخص لهم.⁸⁶

■ أنواع المخاطر التشغيلية:

- **العنصر البشري:** تتمثل في الخسائر التي يتسبب بها الموظفون أو تتعلق بالموظفين بقصد أو بدون قصد كما تشمل الأفعال التي يكون الهدف منها الغش أو استعمال الممتلكات أو التحايل على القانون واللوائح التنظيمية أو سياسية الشركة من قبل المسؤولين، أو الموظفين وكذلك الخسائر الناشئة عن العلاقة مع العملاء المساهمين الجهات الرقابية أو أي طرف ثالث من الأمثلة عليها:
- **عمليات الاحتيال الداخلي من قبل الموظفين:** كالاختلاس المالي، والتعمد في إعداد تقارير خاطئة عن أوضاع البنك، التجارة الداخلية لحسابات الموظفين الخاصة، إساءة استخدام بيانات العملاء السرية، الابتزاز، الرشاوي، التهريب الضريبي المتعمد.
- من التوضيحات السابقة نجد أنها عبارة عن الممارسات المتعلقة بالعملاء والمنتجات والأعمال أي الإخفاق غير متعمد أو الناتج عن الإهمال في الوفاء بالالتزامات المهنية تجاه عملاء محددين.

⁸⁵ محريق عدنان، أساليب قياس مخاطر التشغيل وفقا لاتفاق بازل 2، مجلة الدراسات الاقتصادية والمالية، جامعة الوادي، العدد 08، المجلد 03، ص 172.

⁸⁶ مصداق راضية، إدارة المخاطر التشغيلية وفقا لاتفاقية بازل 2 في البنوك التجارية الجزائرية، دراسة حالة بنك الفلاحة والتنمية الريفية، مجلة الاستراتيجية والتنمية، العدد 13، المجلد 07، جامعة فرحاب عباس، سطيف 01، ص 14.

- **الأحداث المتعلقة بالبيئة الخارجية:** الخسائر الناشئة عن أعمار طرف ثالث بما يشمل الاحتيال الخارجي وأي أضرار تصيب الممتلكات والأصول وخسائر نتيجة تغيير في القوانين، بما يؤثر على قدرة المصرف في مواصلة العمل وتشمل الاحتيال الخارجي كالسرقة والسطو المسلح، وكذا تزييف العملات والتزوير والقرصنة التي تؤدي إلى تدمير الحواسيب سرقة البيانات الاحتيال عبر بطاقات الائتمان الاحتيال عبر شبكات الكمبيوتر والإرهاب والابتزاز
- **الإخفاق الإلكتروني:** الخسائر الناتجة عن تعطل العمل أو فشل الأنظمة بسبب البنية التحتية لتكنولوجيا المعلومات أو عدم توفر الأنظمة وأي عطل أو خلل في الأنظمة، وتشمل انهيار أنظمة الكمبيوتر الأعطال في أنظمة الاتصالات أخطاء البرمجة وفيروسات الحاسب.
- **تنفيذ وإدارة العمليات:** هيا الخسائر الناتجة عن المعالجة للعمليات وحسابات العملاء مثل عمليات المصرف اليومية والضعف في أنظمة الرقابة والتدقيق الداخلية والإخفاق في تنفيذ المعاملات وإدارة العمليات ومثال ذلك الأخطاء في إدخال البيانات بحيث الدخول إلى البيانات لغير المصرح لهم يسبب خسائر وإتلاف أصول العملاء.
- **العوامل التي ساعدت على زيادة الاهتمام بالمخاطر التشغيلية:**
 - التطورات المتسارعة على صعيد تحرير وعولمة الخدمات المالية وازدياد المنافسة؛
 - تطور الخدمات والمنتجات المصرفية وزيادة درجة تعقيدها؛
 - زيادة استخدام التكنولوجيا والتطوير المستمر في أنظمة المعلومات المتكاملة؛
 - ازدياد اهتمام الجهات الرقابية وخاصة لجنة بازل بهذا النوع من المخاطر؛
 - تعرض العديد من البنوك لحالات من المخاطر التشغيلية أدى إلى تحميل البنوك خسائر كبيرة ساهمت في خروج بعضها من السوق من بنك "بيرينغر البريطاني" 1995 حيث بلغت الخسائر الناتجة عن التداولات غير المصرح بها حوالي 1.4 مليار دولار مما أدى لإفلاس البنك.⁸⁷

خلاصة الفصل الثاني:

⁸⁷ عائشة بوقليمينة، واقع مخاطر التشغيل في البنوك الجزائرية وتأثيرها على الربحية دراسة تطبيقية، المجلد 09، العدد 01، جامعة غرداية (الجزائر)، ص 225.

تشهد التكنولوجيا المالية تطوراً سريعاً يجعلها أكثر كفاءة، ورغم ما تحمله من مزايا فإنها في المقابل تولد مجموعة من المخاطر التي تؤثر على استقرار النظام المالي، فهناك مخاطر تتعلق بضعف حماية البيانات الحساسة ما يجعلها عرضة للسرقة أو التسريب أو التلاعب، كما توجد مخاطر تنجم عن أعطال الأنظمة التقنية أو فشل البنية التحتية، الرقمية ومخاطر ترتبط بتقلبات أسعار الأصول الرقمية أو تغيرات مفاجئة في العرض والطلب على خدمات التكنولوجيا المالية، كما توجد مخاطر أخرى تظهر عند حدوث خروقات أمنية أو إخفاقات تنظيمية تؤدي إلى تآكل ثقة العملاء والمستثمرين.

الفصل الثالث:

آليات الحد من مخاطر التكنولوجيا المالية

تمهيد:

رافق التطور السريع للتكنولوجيا المالية العديد من المخاطر التي أثارت تحديات كبيرة أمام الجهات التنظيمية والمؤسسات المالية، وفي هذا السياق أصبح من الضروري تطوير آليات فعالة للحد من هذه المخاطر بما يضمن تحقيق التوازن والحفاظ على الاستقرار المالي، ويهدف هذا الفصل إلى استعراض أبرز الآليات التي تشمل تعزيز حوكمة تكنولوجيا المعلومات، وتطوير الأطر القانونية والرقابية وتبني استراتيجيات الأمن السيبراني بالإضافة إلى دعم التعاون بين الفاعلين في المنظومة المالية، بما يعزز الثقة ويقلل من الأضرار المحتملة على المؤسسات والأفراد، من خلال المباحث التالية:

المبحث الأول: المتطلبات الأمنية للحد من مخاطر التكنولوجيا المالية.

المبحث الثاني: سبل مواجهة المخاطر التنظيمية والتشريعية.

المبحث الثالث: حوكمة تكنولوجيا المعلومات.

المبحث الأول: المتطلبات الأمنية للحد من مخاطر التكنولوجيا المالية

إن مخاطر التكنولوجيا المالية تبرز الحاجة الملحة لوضع متطلبات أمنية صارمة وشاملة، تضمن حماية البنية التحتية الرقمية وتأمين بيانات المستخدمين وضمان استمرارية الأنظمة المالية وفي هذا المبحث سنتطرق إلى سبل مواجهة الهجمات السيبرانية وكذلك مكافحة ظاهرة غسيل الأموال.

المطلب الأول: سبل مواجهة الهجمات السيبرانية وآليات مكافحة غسيل الأموال.

سبب تزايد عمليات غسيل الأموال والهجمات السيبرانية ضرورة تطوير آليات فعالة للتصدي لهذه الجرائم التي تهدد أمن المعلومات وسلامة الأنظمة، وفي هذا المطلب سنسلط الضوء على أهم هذه الآليات.

أولاً: مواجهة الهجمات السيبرانية.

تتعدد سبل مواجهة الهجمات السيبرانية، يمكن حصرها فيما يلي:⁸⁸

- **جدران الحماية:** تعد من أقوى السبل الوقائية لمثل هذه الهجمات الحادة التي تمس أنظمة الكمبيوتر والشبكات، والتي تعرف كذلك بتسمية الجدران النارية، أما عن بداية هذه التقنية فقد ظهرت في أواخر عقد الثمانينات استجابة لعدد من الاختراقات لشبكة الانترنت المستجدة، وقد تم استخدام أول الجدران النارية لتحقيق الأمن في أوائل التسعينات، وكانت عبارة عن موجّهات لبروتوكول مع قوانين فلترة كانت تبدو كالتالي: أسمح لفلان بالدخول والنفاذ إلى الملف التالي أو أمنع فلان من الدخول للمناطق التالية. وقد ظهر منها عدة أجيال لأنها محدودة نذكر منها:

⁸⁸بوزادية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر 03، كلية العلوم السياسية والعلاقات الدولية، ص74، 2021/2020.

الجيل الأول يعرف بمرشحات العبوة حيث يقوم مبدأ عمله على ترشيح العبوة والتي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الانترنت فإذا كانت العبوة تطابق مجموعة شروط الجدار فإنه يسمح بمرور العبوة أو يرفضها ويتخلص منها ويرسل إشارة خطأ للمصدر في حال لم تكن مطابقة.

- **التطبيقات المضادة للفيروسات:** هي برامج يتم استخدامها لاكتشاف البرمجيات الضارة ومنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، وذلك عن طريق إزالتها أو إجراء التعديلات عليها أو إصلاحها، بحيث يمكن لهذا البرنامج أن يتصدى لبرنامج التجسس أو برنامج أحصنة الطروادة.

- **الوسائل الأمنية المتعلقة بالتعريف بشخص المستخدم والتأكد من مشروعيتها:** هي الوسائل التي تهدف إلى ضمان استخدام النظام والشبكات من قبل الشخص المخول بهذا الاستخدام، وتضم كلمات السر بأنواعها والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آنية أو وقتية متغيرة الكترونياً، و المفاتيح المشفرة، بل تضم بما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ، وحتى يتحقق الغرض ويتأكد من فعالية هذه الوسيلة يجب ما يلي:

✓ **التحكم في الدخول والنفاذ إلى الشبكة:** التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة وتشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين أو قوائم أشخاص المستخدمين أنفسهم أو تحديد المزايا الاستخدامية أو غير ذلك من الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة.

✓ **منع إفشاء المعلومات لغير المخولين بذلك وتهدف إلى تحقيق سرية المعلومات:** وتشمل هذه الوسائل من بين ما تشمل تقنيات تشفير المعطيات والملفات وإجراءات حماية نسخ الحفظ الاحتياطية، والحماية المادية للأجهزة ومكونات الشبكات.

✓ **منع الإنكار:** ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي قام بالتصرف، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات عل الخط، وترتكز هذه الوسائل على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.⁸⁹

ثانياً: آليات الحد من غسيل الأموال.

- **الامتثال لمكافحة غسيل الأموال:** يستند برنامج الامتثال لمكافحة الجرائم المالية في المصارف إلى سياسات مواجهة غسيل الأموال ومكافحة تمويل الإرهاب والعقوبات ومكافحة الرشوة والفساد، وتكون تحت إشراف لجنة التدقيق والالتزام التابعة لمجلس الإدارة فيما يتماشى مع إرشادات لجنة بازل وقوانين المصرف، وكذلك استعمال خاصية

⁸⁹ محمد الصغير كاوجة، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 03، سبتمبر 2022، ص114.

"اعرف عميلك"، وهي عملية التحقق من هوية العملاء وتقييم مدى ملاءمتها إلى جانب المخاطر المحتملة للنوايا غير القانونية⁹⁰.

- **حلول نيس أكتمايز:** هي مؤسسة تقوم بتزويد الشركات والبنوك والمؤسسات بأنظمة حماية لمكافحة غسيل الأموال من بين إيجابياتها:⁹¹

- ✓ إدارة برنامج مراقبة نظام مكافحة غسيل الأموال الكامل على منصة واحدة؛
- ✓ تحديد أي نشاط مشبوه على نحو أكثر فعالية؛
- ✓ ترشيد وتبسيط العمليات وتحسين الكفاءة؛
- ✓ النشر بسرعة وخفض التكلفة الإجمالية للملكية.

- **كومباس إي إم إل:** أول نظام إلكتروني متكامل لمكافحة جرائم غسيل الأموال موجه إلى جميع المؤسسات المالية من بنوك ومؤسسات مالية، كما يعزز النظام الإجراءات المتعلقة باكتساب عملاء جدد والتحقق من بياناتهم، ويتضمن أيضا وظائف تعالج كافة جوانب مكافحة غسيل الأموال مثل مطابقة الأسماء مع الواردة في القوائم السوداء بأنواعها حسب الدقة المرغوبة باللغتين العربية والإنجليزية مع التشابهات الصوتية للتهجئة أي مبادئ اعرف عميلك ونظام تنبيه دقيق.⁹²

المطلب الثاني: آليات مواجهة الجرائم السيبرانية في الجزائر

في ظل تنامي التهديدات السيبرانية وتأثيراتها المتزايدة على الأمن القومي للجزائر، سارعت الجزائر إلى تبني العديد من الجهود والآليات الكفيلة بمواجهة مختلف التهديدات والجرائم السيبرانية نذكر منها عدة جوانب:

أولاً: الجانب القانوني

استدرك المشرع الجزائري الفراغ القانوني في مجال الجريمة الإلكترونية، وذلك لما أصدر القانون 04_15 المتضمن تعديل قانون العقوبات، لذا وجب عليها استحداث العديد من التشريعات والقوانين الكفيلة بمحاربة التهديدات والجرائم السيبرانية، وذلك من أجل تعزيز أمنها السيبراني، ومن ذلك نجد القانون 05_10 الصادر في 20 جوان 2005 المتضمن الدليل الإلكتروني، إضافة إلى قانون الإجراءات الجزائية، وقانون العقوبات لاسيما في المواد 303،333،394،396، المتضمنة تجريم وتسليط العقوبات على كل من يثبت في حقه اختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية، كما صدر سنة 2009 القانون 09_04 المتضمن القواعد الخاصة للوقاية

⁹⁰ الامتثال لمكافحة غسيل الأموال واعرف عميلك، الموقع الإلكتروني، <https://wikipedia.com>، (28/3/2025، 14:00).

⁹¹ شايب محمد، مخاطر غسيل الأموال في البنوك والمؤسسات المالية العربية ودور التكنولوجيا الحديثة في مكافحتها، المجلة الجزائرية للأبحاث الاقتصادية، ماي 2018، ص 13.

⁹² شايب محمد، مرجع سابق، ص 13.

من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها واستهل بالهدف الاسمي منه وهو الوقاية من الجريمة المعلوماتية ليرصد في المادة الرابعة منه الحالات التي يسمح بها باللجوء إلى المراقبة الالكترونية وحددها في الآتي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم الماسة بأمن الدولة؛
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو الاقتصاد الوطني؛
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، وأكد المشرع على أنه لا يمكن إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة، واستثنى الحالة الواردة في الفقرة (1) وخصها بإذن من النائب لدى مجلس قضاء الجزائر.

فالإطار القانوني مهم في الحد من انتشار التهديدات السيبرانية، بحيث أن النظم القانونية تسعى إلى تنظيم ممارسة واستخدام تكنولوجيا الإعلام والاتصال في الإطار الشرعي، لكن من الجانب الآخر تعمل على معاقبة كل من يسيئ استخدامها في الأطر الغير الشرعية، باعتبار أن أمن المؤسسات والأفراد هو من قبيل المحافظة على الأمن القومي الجزائري، والمحافظة عليه يستوجب إصدار القوانين والتشريعات الكفيلة بذلك، فقد بين المشرع الجزائري فصلا كاملا متعلق بالتهديدات والجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث بين القسم السابع من قانون العقوبات كل أشكال المساس بأنظمة المعالجة الآلية للمعطيات المترتبة عنها.⁹³

ثانيا: الجانب الأمني

في هذا الجانب عمدت الجزائر من خلال أجهزتها الأمنية إلى استحداث مؤسسات أمنية متخصصة ضمن أسلاك الأمن وأوصت باحترام الحريات في إطار الشرعية الدستورية والمواثيق الدولية ومن ين الهيئات نذكر:⁹⁴

- مصلحة الدفاع السيبراني ومراقبته أمن الأنظمة: وهي مصلحة تابعة لقيادة الجيش الوطني الشعبي على مستوى دائرة الاستعمال والتحضير، هدفها تأمين وحماية المنشآت الجوية للقوات المسلحة الجزائرية ضد أي تهديد أمني سيبراني، حيث تعمل هذه المصلحة على تطبيق السياسة العامة للدفاع السيبراني وهي بذلك تعد طرفا فاعلا في العمليات العسكرية حيث تتمحور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي على محاور أساسية تتمثل في الجوانب التالية:

⁹³بارة سمير، مرجع سابق، ص 115.

⁹⁴ عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، مرجع سابق، ص 250.

- ✓ الجانب الوظيفي: من أجل ضمان فعالية وتناسق أعمال الدفاع السيبراني.
- ✓ الجانب القانوني: من خلال تعزيز وتحسين الأطر القانونية التي تضمن التطور المتعلق باستعمال تكنولوجيا الإعلام والاتصال وتأمين منظومات الإعلام.
- ✓ الجانب البشري: من خلال تكوين وكفاءة وجاهزية الموارد البشرية لأي هجوم سيبراني يهدد الأمن الجزائري.
- ✓ الجانب التقني: يتعلق بمدى كفاءة الأجهزة والوسائل المستعملة مع ضمان اليقظة للكشف والرد على الهجمات السيبرانية.

- المصلحة المركزية لمكافحة الجريمة المعلوماتية: وهي مؤسسة تابعة للأمن الوطني أنشئت سنة 2011 لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني حيث عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والإيصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جافى 2015.
 - مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني: حيث أنشئ هذا المركز في 2008، بالجزائر العاصمة تتمثل أهدافه في تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق يقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة ومحاولة تحديد أصحابها مما يؤمن الأنظمة المعلوماتية للمؤسسات والبنوك والشركات، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى.
- ثالثا: من الناحية العلمية**

حتى تتمكن الهيئات العمومية من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبراني وفق ما تم ترسيمه في الاستراتيجية الوطنية توجّهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع، المؤسسات الأمنية) إلى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما ساهمت الجامعات ومؤسسات البحث العلمي من تنظيم أيام دراسية وملتقيات أكاديمية، نذكر على سبيل المثال الملتقى الدولي الذي نظّمته كلية الحقوق جامعة برج بوعريّيج بتاريخ 2017/04/12 تحت عنوان الإجرام السيبراني، المفاهيم والتحديات وكذا الملتقى الدولي الذي نظّمه كل من الجيش الوطني الشعبي وقيادة الدرك الوطني في الفترة الممتدة بين شهر مارس وماي 2017، كل التوصيات التي انتهت إليها اللقاءات العلمية تجتمع حول نقاط مشتركة يمكن استخلاصها في العناصر التالية: تنسيق الجهود، الاعتماد على الكفاءات، إنشاء هيئة مديرة، تعزيز الجانب المادي والبشري، إطلاق مشاريع بحثية، تعزيز التعاون الدولي⁹⁵.

المبحث الثاني: سبل مواجهة مخاطر التنظيمية والتشريعية

⁹⁵بوازديّة جمال، مرجع سابق، ص 85.

مع تنامي في استخدامات بالتكنولوجيا المالية وتوسع نطاقها، برزت المخاطر من أبرز التحديات التي تواجه هذا القطاع، ويجب وضع طرق وأساليب لإتباع القواعد واللوائح بشكل سهل وسريع وفي هذا المبحث سنفصل فيه.

المطلب الأول: الحماية من المخاطر التشريعية والتنظيمية

تعد البيئة التشريعية والتنظيمية أحد العوامل الأساسية التي تؤثر في استقرار الأعمال واستمرارها، ومع تطور الأنظمة القانونية وتعدد القوانين واللوائح المنظمة باتت المؤسسات عرضة لمجموعة من المخاطر التشريعية والتنظيمية.

أولاً: الامتثال للقوانين

شكل الامتثال للأنظمة واللوائح والقوانين أساساً لضمان حسن سير الأعمال والمؤسسات، وهو ركيزة ضرورية لتحقيق الشفافية، النزاهة والمسؤولية القانونية. ويكتسب هذا الامتثال أهمية مضاعفة في ظل التطورات التقنية والاقتصادية المتسارعة، مما يستدعي أطر تنظيمية متطورة وقادرة على ملاحقة تلك التغيرات دون المساس بمبادئ الحوكمة.

- مفهوم الامتثال: هي عمليات فحص منهجية ومستقلة لأنظمة وعمليات وسجلات الامتثال، يتم إجراؤها بواسطة مدققين أو مراجعين داخليين أو خارجيين يمكنهم المساعدة في التحقق من صحتها.⁹⁶
- مجالات الامتثال للأنظمة واللوائح:

يشكل الامتثال للأنظمة واللوائح حجر الزاوية في عمل أي منظمة تسعى إلى تحقيق الاستدامة والنجاح على المدى الطويل، فهو ليس مجرد التزام قانوني، بل يعتمد على مجموعة واسعة من المسؤوليات التي تضمن سير العمليات بكفاءة وشفافية وأخلاقية، ويمكن التفصيل حول مجالات الامتثال فيما يلي:

- الامتثال المالي: هو مجموعة من الإجراءات والسياسات التي تضعها الشركات والمؤسسات لضمان التزامها باللوائح والقوانين المالية والمحلية والدولية. يهدف الامتثال المالي إلى تعزيز الشفافية والحوكمة الجيدة، وتقليل المخاطر المالية والقانونية، مع ضمان أن جميع العمليات المالية تتم وفق المعايير الأخلاقية والمهنية.⁹⁷
- الامتثال الإداري: هي عملية تتضمن مجموعة من المهام والأنشطة التي تهدف إلى تحقيق الالتزام بالقوانين والتشريعات المحلية والدولية. وتضمن سلامة العمل والموظفين وتعزز الثقة بين المؤسسة والعملاء.⁹⁸

⁹⁶ مفهوم الامتثال، الموقع الإلكتروني، <http://fastercapita.com>، (254/03/2025، 15:27).

⁹⁷ مفهوم الامتثال المالي، الموقع الإلكتروني، <https://gadwalah.com>، (16،17:53/4/2025).

⁹⁸ الامتثال الإداري، الموقع الإلكتروني، <https://www.rmgasa.com>، (2،18:07/4/2025).

- **الامتثال القانوني:** يشير إلى عملية ضمان التزام الشركة أو الفرد بجميع القوانين واللوائح المعمول بها، ويتضمن تحديد وتقييم المخاطر المرتبطة بنشاط أو معاملة معينة. وتنفيذ التدابير اللازمة للتخفيف من تلك المخاطر ويعد الامتثال القانوني جزءا أساسيا من ممارسة الأعمال، لأنه يساعد على حماية الشركات من المسؤوليات القانونية والحفاظ على سمعتها وحماية الفرد.⁹⁹

ثانيا: تنفيذ القوانين وفاعلية التشريعات

يأتي هنا وهو تقاعس الإدارات في تنفيذ القوانين التي وضعت آليات تنفيذها، كما هو الحال مع القوانين حماية، حيث تنتشر ظاهرة قرصنة البرامج بشكل كثيف في مختلف الدول العربية، ويعود ذلك إما لغياب إدارة المتخصصة بالملاحقة، وإما لعدم إمكانية الإدارة المعنية متابعة الوضع بشكل فاعل، نتيجة عدم توافر الإمكانيات التقنية والمادية والبشرية، غياب القدرة على الضبط والتحقق، من رغم إنشاء عدد من مراكز الاستجابة لطوارئ الانترنت في البلدان العربية فان بعضها غير فاعل بشكل كاف، يجب وضع إطار عالمي للتعاون والتوعية على الصعيدين الإقليمي والوطني من أجل إرساء ثقافة عالمية ومساعدة في توعية المستعملين في مجال التجارة الالكترونية ومعاملات المتنقلة، وضع آليات مؤسسية وتنظيمية لتسيير والتنفيذ الفعال.¹⁰⁰

المطلب الثاني: القرارات السياسية للتعاون الدولي

بسبب تطورات التكنولوجيا المالية أصبحت تمثل محورا أساسيا للتنمية الاقتصادية والتجارية في العالم، ومع تنامي دور هذه التكنولوجيا في تغيير أنماط المعاملات المالية ازداد وعي الدول بأهمية التعاون الدولي في هذا المجال.

أولاً: إقرار سياسات وقائية ودفاعية

تتمثل في الأمن في استعمال الاتصالات والتكنولوجيا المعلومات فضلا عن حماية البيانات الشخصية وهي من الأولويات التي تستدعي تعاوننا وتنسيقا دوليين بين الحكومات والمنظمات ذات الصلة وشركات القطاع الخاص والكيانات المعنية في مجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامة والتدابير القانونية والتنظيمية والتقنية التي تتناول حماية البيانات الشخصية، لضمان موثوقية وأمن شبكات وخدمات التكنولوجيا، ولذلك اتجهت مع الدول المتقدمة، إلى إقرار سياسات وقائية ودفاعية، هجمات التي تتعرض لها وخصصت بعض الدول مثل الولايات المتحدة الأمريكية، استراليا، انجلترا مبالغ طائلة لمعالجة تلك الهجمات ، وليست هذه الحقيقة سوى مؤشر إلى مدى اهتمام الذي توليه هذه الدول، لإرساء الثقة والاستقرار بالعلاقات الدولية،

⁹⁹ مفهوم الامتثال القانوني، الموقع الالكتروني، https://www.noor_book.com، (24/03/2025، 12:30).

¹⁰⁰ إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، مجلة الاجتماعية القومية، جامعة دنبور، المجلد

مهدة في كل لحظة إلى نتيجة الاختراقات والاعتداءات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية، وقواعد المعلومات ولم تتأخر الإدارة الأمريكية عن استحداث قيادة عسكرية جديدة مختصة بحماية الفضاء السيبراني.¹⁰¹

ثانيا: نشر ثقافة الأمن السيبراني

تعترف حكومات عديدة بأن التعليم العام وتوعية الجمهور من الأساليب القوية للدفاع السيبراني وتساعد برامج التوعية الوطنية التي تنفذها الحكومة أو الكيانات الخاصة على تعزيز الوعي على مستوى القاعدة الجماهيرية ونذكر مايلي:¹⁰²

- برنامج الأمن السيبراني العالمي: وهو إطار للتعاون الدولي يهدف إلى تعزيز الثقة والأمن في مجتمع المعلومات، ويهدف لتحقيق خمس ركائز لتوجيه أنشطة وهي: التدابير القانونية، التدابير الإجرائية والتقنية، الهياكل التنظيمية، بناء القدرات، التعاون الدولي؛
 - إعلان ايريتشي لمبادئ الاستقرار والسلام السيبراني: وهو إعلان يدعو إلى تضافر العمل والترويج لمفهوم السلام السيبراني العالمي ويدعو لما يلي:
 - فحص الطريقة التي تعمل بها تكنولوجيا المعلومات على دعم الحياة اليومية؛
 - تقييم التهديدات السيبرانية؛
 - تقييم صحة الأطر القانونية الجارية؛
 - رسم مسار العمل في المستقبل.
- لذا يعد إعلان ايريتشي انجازا علميا، آذ يصبح بحوزة البشرية الوسائل اللازمة لبسط المواد الاقتصادية وتعزيز القدرات الفكرية وثقافية.

ثالثا: التعاون الدولي

نظرا لطبيعة التعاون الدولي في تعزيز الموثوقية في استخدام التكنولوجيا المعلومات وتوافر هذه التكنولوجيات وامن استخدامها، فإن قطاع تنمية الاتصالات بالحاجة الملحة لدعم الدول لوضع تدابير محددة لتنفيذ أطرها الوطنية المتعلقة بالمخاطر من اجل معالجة شواغل أصحاب المصلحة المختلفة بهذا الشأن، ومن اجل إفساح المجال أمام تبادل أفضل الممارسات على المستوى العالمي، ويتطلب التعاون الدولي المساعدة في التحقيق

¹⁰¹إسلام فوزي، المرجع نفسه، ص117.

¹⁰²سي عبد القادر حنان، الأمن السيبراني وأثره على دول العالم، جامعة بسوسة، تونس، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 04، العدد 07، 2024، ص30.

والأحكام الإجرائية والموضوعية المشتركة لمعالجتها على النحو الملائم، وإضافة إلى ذلك من المعترف به على نطاق واسع أن التعاون الدولي يمثل احد المتطلبات الرئيسية لضمان الأمن على المستوى الصعيد العالمي، ولذلك ينبغي أن يكون هذا التعاون بدافع الرغبة المشتركة لكل بلد.¹⁰³

المبحث الثالث: حوكمة تكنولوجيا المعلومات

مع التطور السريع لتطبيقات وممارسات تكنولوجيا المعلومات في جميع أنحاء المنظمة، أصبحت ضرورية لنجاح أي مؤسسة، حيث برزت هذه الأخيرة كآلية من آليات التحكم والتوجيه الأمثل في تكنولوجيا المعلومات وضمان الحد الأقصى من الاستفادة منها من خلال اتخاذ أفضل القرارات بشأنها. وفي هذا المبحث سنتطرق إلى مطلبين يركز المطلب الأول على مفاهيم أساسية حول تكنولوجيا المعلومات أما المطلب الثاني فيركز على ركائز حوكمة تكنولوجيا المعلومات.

المطلب الأول: مفاهيم أساسية حول حوكمة تكنولوجيا المعلومات

تمثل تكنولوجيا المعلومات أحد الركائز التي تعتمد عليها المؤسسات في جميع مجالاتها، يشير مصطلح تكنولوجيا المعلومات إلى استخدام الحواسيب، البرمجيات والشبكات وأنظمة الاتصالات لتخزين المعلومات ومعالجتها بطريقة فعالة وأمنة في هذا مطلب سنتم التعرف على مفهوم تكنولوجيا المعلومات وأهدافها وجوانبها.

أولاً: تعريف حوكمة تكنولوجيا المعلومات

لقد تعددت تعاريف تكنولوجيا المعلومات سنتم تعريفها على النحو التالي:

- **التعريف الأول:** تعرف وفق المعهد الاسترالي لمعايير حوكمة الشركات هي نظام يتم من خلاله توجيه ورقابة الاستخدامات الحالية والمستقبلية لتقنية المعلومات وتقييم وتوجيه الخطط لاستخدام تقنيات معلومات في تدعيم المؤسسة، لإنجاز الخطط المقررة.¹⁰⁴
- **التعريف الثاني:** هي وسيلة أو أداة فعالة في المؤسسة من خلال خلق مرونة في تكنولوجيا المعلومات وفي هيكليات وعمليات نظم المعلومات، حيث يُنظر إليها على أنها القدرة التنظيمية لرقابة تركيب وتطبيق استراتيجية تكنولوجيا المعلومات وتعتبر دليل للاتجاه المناسب بغرض تحقيق ميزة تنافسية للمؤسسة.¹⁰⁵

¹⁰³ سامي محمد بونيف، دور الاستراتيجيات الاستباقية في الهجمات السيبرانية الردع السيبراني نموذجاً، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة احمد بن يحيى الوشرسي تيسمسيلت، الجزائر، المجلد 04، العدد 07، 30 جوان 2019، ص 131.

¹⁰⁴ فايزة جيجخ، سميرة فرحات، حوكمة تكنولوجيا المعلومات ودورها في الوقاية من الأزمات، مجلة الاقتصاديات المالية البنكية وإدارة الأعمال، جامعة بسكرة، الجزائر، العدد 01، 2016، ص 117.

¹⁰⁵ اوانان محمد، وآخرون، آليات وقاية المعاملات الالكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة les cahiers du mecas، جامعة جيلالي ليايس، سيدي بلعباس، الجزائر، العدد 12، جوان 2016، ص 383.

ومن التعريفين السابقين يمكن تعريف حوكمة تكنولوجيا المعلومات بأنها هي مجموعة من المبادئ والمعايير الهادفة إلى وضع ورسم سياسات وإجراءات لتحسين عمليات وأنشطة تكنولوجيا المعلومات والرقابة عليها.

ثانياً: أهداف حوكمة تكنولوجيا المعلومات

تسعى المؤسسات ومنظمات الأعمال من خلال تجسيد حوكمة تكنولوجيا المعلومات إلى تحقيق جملة من الأهداف نذكر منها ما يلي:¹⁰⁶

- وضع رقابة مادية على أجهزة الحسابات الالكترونية مثل استعمال نظام إنذار مني للكشف عن أي دخول في مصرح إلى النظام؛
- تقييم أداء الإدارة العليا وتعزيز المساءلة ورفع درجة الثقة؛
- المساهمة في وضع الخطط اللازمة للحد من مخاطر تكنولوجيا المعلومات ومواجهة تحدياتها، بهدف تحقيق امن المعلومات لكافة عمليات وإدارات المصرف؛
- إدارة مخاطر تكنولوجيا المعلومات وتحقيق الأمن المعلوماتي؛
- اتخاذ التدابير اللازمة لتحقيق أقصى معايير جودة المعلومات لنظام تكنولوجيا المعلومات، والتي تتمثل في المعايير الأساسية التالية: الكفاءة، السرية، التكامل والسلامة، الإتاحة والموثوقية، الامتثال والتوافق؛
- ادارة المخاطر وحالة عدم التأكد ناتجة عن التحول الرقمي واستخدام تكنولوجيا المعلومات، من خلال تحديد الهدف ونطاق ووظيفة كل نشاط يعتمد على تكنولوجيا المعلومات بشكل دقيق وهذا لتسهيل عملية مراقبتها والسيطرة عليها بما يضمن تحقيق أهداف المؤسسة التنظيمية والاستراتيجية والتقليل من مخاطر المحتملة.

ثالثاً: مقومات ومتطلبات نجاح حوكمة تكنولوجيا المعلومات

تحتاج عملية تطبيق حوكمة تكنولوجيا المعلومات في المؤسسات والمنشآت متطلبات ومقومات عديدة، وشروط لا بد من توفرها لنجاح تجسيدها نذكر منها ما يلي:¹⁰⁷

- تحقيق المواءمة بين الاستراتيجية العامة للمؤسسة، وخطط التشغيل اللازمة لتحقيق هذه الأهداف، وبين الاستراتيجية لتكنولوجيا المعلومات؛
- وضع خطة تشغيل واضحة المعالم والأهداف لتكنولوجيا المعلومات؛
- وضع خطة مالية وتمويلية بالقدر الكافي لتكنولوجيا المعلومات؛

¹⁰⁶ أحمد خليفة، وآخرون، أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبين، مجلة الدراسات المالية والمحاسبة والإدارية، المجلد 08، العدد 01، مارس 2021، ص 205.

¹⁰⁷ قوريش زكرياء، بلعدي عبد الله، حوكمة تكنولوجيا المعلومات . تقنية الكوبيت 5 نموذجاً .، مجلة الأصيل للبحوث الاقتصادية والإدارية، جامعة عباس لغرور، خنشلة، الجزائر، المجلد 07، العدد 01، أبريل 2023، ص 309.

- وضع إطار عام لتطبيق حوكمة تكنولوجيا المعلومات والرقابة الدائمة عليها، مع الأخذ في الاعتبار ما تقرضه جهات الرقابة والإشراف والتشريعات المنظمة للعمل بالمؤسسات والمنظمات واختيار البدائل العملية المطروحة مثل نموذج الكويت؛
- القيام بتشكيل اللجان المختصة في توجيه وإدارة تكنولوجيا المعلومات مع وضع الاستراتيجية الخاصة بها، ويتعين أن يكون مستوى تلك اللجان من أعضاء مجلس الإدارة؛
- تعتبر التشريعات العنصر الأساسي لتفعيل حوكمة تكنولوجيا المعلومات باعتبارها هدف الإدارة الإلكترونية من خلال وضع القوانين والتشريعات اللازمة التي تسمح بقيامها وتجسيدها، وذلك عن طريق وضع الإطار القانوني المناسب الذي ينص على هذا التحول، سواء من حيث التعامل بها أو من خلال ضبط المصطلحات القانونية التقنية المرتبطة بها، فالقوانين التقليدية لا تصلح في مجال حوكمة تكنولوجيا المعلومات، كون التعامل الإلكتروني يرتبط بعدة جوانب قانونية يجب مراعاتها، كحجية الوثائق الإلكترونية، الخصوصية والسرية، وبالتالي وجب تكييف الأطر التشريعية بما يتماشى ومتطلبات تطبيق حوكمة تكنولوجيا المعلومات.

المطلب الثاني: ركائز ومعايير حوكمة تكنولوجيا المعلومات.

تعد حوكمة التكنولوجيا المالية إطاراً تنظيمياً وإدارياً، يهدف إلى تحقيق التوازن بين الابتكار والرقابة، من خلال وضع قواعد واضحة لإدارة المخاطر وضمان الشفافية، ويركز هذا المطلب على دراسة الركائز الأساسية والمعايير المعتمدة في حوكمة التكنولوجيا المالية، والتي تمثل عناصر محورية لضمان سلامة العمليات الرقمية.

أولاً: ركائز حوكمة تكنولوجيا المعلومات

وفقاً لتوصيات معهد حوكمة تكنولوجيا المعلومات ITGI فإن مبادئ حوكمة تكنولوجيا المعلومات يمكن حصرها في خمس مبادئ أساسية، وهذه المبادئ هي: ¹⁰⁸

- **التوافق الاستراتيجي (Alignment It Strategic):** يقصد به المشاركة المشتركة لجميع استراتيجيات وحدات تكنولوجيا المعلومات بخططها وعملياتها واستثماراتها وقراراتها لدعم المهام والأهداف التي تسعى المؤسسة لتحقيقها.
- **إضافة القيمة (It Value):** يجب أن يضيف تنفيذ تطبيقات تكنولوجيا المعلومات الجديدة قيمة إلى المنظمة من خلال جودة الخدمات، وتحسين التكاليف، وتقديم المعلومات والبيانات ذات الصلة والمفيدة في الوقت المناسب لجميع أنحاء المؤسسة.

¹⁰⁸ بوكفوس سمية، بوعبد الله فاطمة الزهراء، أثر حوكمة تكنولوجيا المعلومات على الاداء المالي للمؤسسة الاقتصادية دراسة حالة . الصندوق الوطني لضمان الاجتماعي لغير الأجراء casnos، مذكرة مكملة لنيل شهادة الماستر، تخصص إدارة مالية، المركز الجامعي عبد الحفيظ بوصوف، ميلة، الجزائر، 2022/2023، ص 18.

- إدارة الموارد (It Resource): يقصد بإدارة الموارد، موارد تكنولوجيا المعلومات الأساسية مثل المعلومات والتطبيقات والأشخاص والبنى التحتية ومساعي استثمارها وإدارتها بأفضل طريقة مناسبة.
- إدارة المخاطر (ItRisk): وتتمثل المخاطر هنا في مختلف التهديدات التي تمس بأمن المعلومة وسلامتها وموثوقيتها باعتبار تكنولوجيا المعلومات مجالا خصباً لهذا اختراقات أمنية.
- قياس الأداء (It Performance Measurement) : يعني رصد ومراقبة تنفيذ الاستراتيجية وكيفية استخدام الموارد بشكل عقلاني بشكل دوري من أجل تصحيح مختلف الثغرات، سواء بطرق إحصائية مضبوطة أو عن طريق التقارير الدورية.

ثانياً: معايير حوكمة تكنولوجيا المعلومات

يمكن توفير حوكمة تكنولوجيا المعلومات عن طريق العديد من المعايير الدولية والبرامج أهمها مكتبة البنية التحتية الخاصة بقطاع تكنولوجيا المعلومات (ITIL) ومقترحات التحكم الخاصة بالمعلومات والتكنولوجيا ذات الصلة (COBIT) ومعايير الجودة الشاملة (ISO)، وتشمل الفوائد الخاصة بهذه التطبيقات قدرتها على الحد من التعرض للمخاطر وتتمثل هذه المعايير في:¹⁰⁹

أولاً: معيار كوبيت cobit

يعد من أشهر الآليات انتشاراً واستخداماً والكلمة اختصاراً أي أهداف التحكم في المعلومات والتكنولوجيا ذات الصلة وهو عبارة عن إطار عمل مفتوح وأداة تستخدم للرقابة والسيطرة على التكنولوجيا المعلومات قد طور هذا المقياس بواسطة منظمة التدقيق والتحكم في نظم المعلومات، ويحدد إطار العمل هذا 34 هدفاً ذات مستوى عالٍ للرقابة على عمليات تكنولوجيا المعلومات وممارسات للرقابة من أجل تدعيم احتياجات الإدارة في تحديد ومتابعة المستوى المناسب لتأمين تكنولوجيا المعلومات.

■ مبادئ نموذج كوبيت cobit:

يستند كوبيت على خمس مبادئ رئيسية وهي كما يلي:¹¹⁰

- تلبية احتياجات أصحاب المصلحة: وذلك من خلال الحفاظ على التوازن بين تحقيق الفوائد وتقليل المخاطر من جهة، واستخدام الموارد بشكل أمثل من جهة أخرى.

¹⁰⁹ بوكفوس سمية، بوعبد الله فاطمة الزهراء، أثر حوكمة تكنولوجيا المعلومات على الأداء المالي للمؤسسة الاقتصادية دراسة حالة الصندوق الوطني للضمان الاجتماعي لغير الأجراء، مذكرة مكملة لنيل شهادة الماستر، جامعة عبد الحفيظ بوالصوف، ميله، السنة الجامعية 2023/2022، ص16.

¹¹⁰ هاجر محبوب، متطلبات حوكمة تكنولوجيا المعلومات وفقاً لنموذج كوبيت دراسة حالة شركة اتصالات الجزائر، مجلة العلوم الإدارية والمالية، المجلد 5، العدد 01، سنة 2021، ص369.

- **التغطية الكاملة للمؤسسة:** يجب أن تكون جميع عوامل التمكين الخاصة بالإدارة والحوكمة المتعلقة بتكنولوجيا المعلومات شاملة لجميع المؤسسة، أي جميع العوامل الداخلية والخارجية على مستوى بيئة المؤسسة.
- **تطبيق إطار عمل موحد ومتكامل:** هناك العديد من المعايير والممارسات المتعلقة بتكنولوجيا المعلومات كل منها توفر إرشادات حول مجموعة فرعية من أنشطة تكنولوجيا المعلومات التي تتوافق مع cobit5 وبالتالي يمكن أن يكون بمثابة نموذج شامل لحوكمة وإدارة تكنولوجيا المعلومات في المؤسسة.
- **تمكين أسلوب شامل:** تتطلب الإدارة الفعالة والكفاءة لإدارة تكنولوجيا المعلومات في المؤسسة إتباع أسلوب شامل مع مراعاة العديد من المكونات المتفاعلة (المبادئ والسياسات والأطر العمليات الهياكل التنظيمية الثقافة والأخلاق والسلوك المعلومات الخدمات والبنية التحتية والتطبيقات الأفراد والمهارات والكفاءات) يحدد cobit مجموعة من العوامل التمكينية لدعم تنفيذ نظام شامل لحوكمة والإدارة لتكنولوجيا المعلومات في المؤسسة ما يساعد في تحقيق أهداف المؤسسة.
- **فصل الحوكمة عن الإدارة:** يميز إطار cobit بين الحوكمة والإدارة حيث يشمل هذان المجالين أنواعا مختلفة من الأنشطة ما يجعلها تتطلب هياكل تنظيمية مختلفة ما يخدم أعراض إدارة وحوكمة تكنولوجيا المعلومات.
- **المزايا التي يقدمها:** للمعيار عدة مزايا نذكر منها:¹¹¹
 - السيطرة المحكمة على المعلومات المنظمة والتكنولوجيا المرتبطة بها؛
 - مراقبة ومتابعة ما تم إنجازه من أهداف؛
 - إدارة الموارد التكنولوجية المعلومات بشكل أفضل؛
 - إدارة المخاطر التي تحيط بتكنولوجيا المعلومات؛
 - تحقيق قيمة مضافة لأعمال المنظمة.

ثانيا: معيار ITIL

هو اختصار لـ "the information technology infrastructure Library" تم إنشائه وتطويره سنة 1989 من قبل مكتبة التجارة الحكومية البريطانية OGC، وهو عبارة عن إطار مفصل لأفضل ممارسات تكنولوجيا المعلومات مع قوائم مراجعة شاملة ومهام وإجراءات ومسؤوليات مصممة لتناسب أي وظيفة في مجال تكنولوجيا المعلومات يحدد سلسلة من أفضل الممارسات الضرورية لحوكمة التكنولوجيا المعلومات إضافة إلى إمكانية تعديل المهام والإجراءات بما يلاءم المنظمة واحتياجاتها.

¹¹¹ يوفوكوس سمية، بوعبد الله فاطمة الزهراء، مرجع نفسه، ص15.

أصبح ITIL اليوم مجموعة مستقلة ومحدثة بانتظام لأفضل ممارسات تكنولوجيا المعلومات التي تم الاعتراف بها على نطاق واسع لأول مرة من قبل عمليات تكنولوجيا المعلومات في المملكة المتحدة، يليها الاتحاد الأوروبي، وهي الآن بشكل متزايد في الولايات المتحدة.

■ المراحل الأساسية لمعيار ITIL:

حيث تضم سبع خطوات تغطي ما يمكن وينبغي قياسه وجمع ومعالجة وتحليل البيانات وتقديم المعلومات واستخدامها نذكر منها ما يلي:¹¹²

- **مرحلة استراتيجية الخدمة:** تركز هذه المرحلة على دورة حياة خدمة ITIL وتصف كيفية تصميم وتطوير وتنفيذ إدارة خدمات تكنولوجيا المعلومات.
- **مرحلة تصميم الخدمة:** تصف هذه المرحلة كيفية تصميم الخدمات والعمليات.
- **مرحلة نقل الخدمة:** تشرح هذه المرحلة كيفية إدارة انتقال خدمة جديدة أو متغيرة مع التركيز على ضمان توازن جميع عمليات إدارة الخدمة.
- **مرحلة تشغيل الخدمة:** ترشد هذه المرحلة إلى طرق ضمان تقديم الخدمات وتشغيلها بسلاسة وموثوقية.
- **مرحلة التحسين المستمرة للخدمة:** تغطي هذه المرحلة كيفية إعادة مواءمة خدمات تكنولوجيا المعلومات مع تغير احتياجات العمل.

■ المزايا التي يقدمها معيار ITIL:

يوفر إطار ITIL لحوكمة تكنولوجيا المعلومات ويركز على القياس والتحسين المستمر لجودة خدمات تكنولوجيا المعلومات المقدمة من منظور الأعمال والعملاء كان هذا التركيز عاملاً رئيسياً في النجاح ITIL في جميع أنحاء العالم وساهم في استخدامه، ومن الفوائد الرئيسية التي حصلت عليها المنظمات التي استخدمت تقنيات وعمليات ITIL في جميع أنحاء مؤسساتها والتي تتمثل فيما يلي:¹¹³

زيادة رضا المستخدمين والعملاء عن خدمات تكنولوجيا مقدمة؛

- تحسين إتاحة الخدمة مما يؤدي مباشرة إلى زيادة محتملة في أرباح الأعمال وإيراداتها؛
- التوفيرات المالية الجديدة الناتجة عن تقليل إعادة العمل والوقت الضائع وتحسين إدارة الموارد واستخدامها؛
- تحسن الوقت اللازم لتسويق جوانب تكنولوجيا المعلومات للمنتجات والخدمات الجديدة؛
- تحسين عملية اتخاذ القرار وتحسين المخاطر لجميع العمليات المتعلقة بتكنولوجيا المعلومات؛

ثالثاً: معيار iso38500

¹¹² مراحل معيار ITIL، الموقع الإلكتروني <http://www.rmg-sa.com>، (29/5/2025، 19:30).

¹¹³ يوفكوس سمية، بوعبد الله فاطمة الزهراء، مرجع نفسه، ص 16.

أتى هذا المعيار في طبعته الثانية سنة 2015 في كتيب من 12 صفحة تحت عنوان "حكومة تكنولوجيا المعلومات للمؤسسات" وهو من تعريف المنظمة الدولية للتقييس (ISO) واللجنة الكهرو تقنية الدولية (IEC)، ويوفر المعيار إطاراً من المبادئ التوجيهية للمديرين لاستخدامه عند تقييم وتوجيه ومراقبة استخدام تكنولوجيا المعلومات داخل مؤسساتهم.

■ **مبادئ معيار iso38500:** يركز معيار على ستة مبادئ أساسية لحكومة تكنولوجيا المعلومات داخل المنظمة هي: ¹¹⁴

- **المبدأ الأول:** تحديد مسؤوليات مفهومة وواضحة فيما يتعلق بتكنولوجيا المعلومات؛
- **المبدأ الثاني:** ضرورة التخطيط لتكنولوجيا المعلومات لتقديم دعم أفضل للمنظمة؛
- **المبدأ الثالث:** التمكن من تكنولوجيا المعلومات بطريقة صحية؛
- **المبدأ الرابع:** التأكد من أن أداء تكنولوجيا المعلومات يعمل بكفاءة كلما لزم الأمر ذلك؛
- **المبدأ الخامس:** التأكد من توافق تكنولوجيا المعلومات يحترم العوامل البشرية؛
- **المبدأ السادس:** التأكد من أن استخدام تكنولوجيا المعلومات يحترم العوامل البشرية.

■ **أهداف معيار iso38500:** يهدف إلى تعزيز لاستخدام الفعال والكفاء والمقبول لتكنولوجيا المعلومات في جميع المؤسسات من خلال: ¹¹⁵

- طمأنة أصحاب المصلحة (المديرين والموظفين والزبائن) أنه في حالة إتباع المبادئ والممارسات التي يقترحها المعيار يمكنهم الوثوق في حوكمة تكنولوجيا المعلومات في المنظمة؛
- إعلام وتوجيه المديرين ومرافقهم لحكومة تكنولوجيا المعلومات في مؤسساتهم؛
- إنشاء نموذج مفاهيمي لاستيعاب مفردات حوكمة تكنولوجيا المعلومات؛
- توفير قاعدة للتقييم الموضوعي لحكومة تكنولوجيا المعلومات داخل المؤسسة.

خلاصة الفصل الثالث:

تناول هذا الفصل الوسائل والآليات التي يمكن من خلالها مواجهة المخاطر المتزايدة المرتبطة باستخدام تقنيات التكنولوجيا المالية، وفي هذا الإطار برزت حوكمة التكنولوجيا المعلومات كأحد الحلول الرئيسية حيث تساهم في ضبط استخدام النظم الرقمية، كما أن تعزيز الأطر القانونية والتشريعية يعد أمراً أساسياً من خلال سن قوانين مرنة، من جهة أخرى إشارة الفصل على أهمية تعزيز الأمن السيبراني عبر تبني تقنيات متقدمة في حماية

¹¹⁴ مبادئ معيار ISO، الموقع الإلكتروني <http://www.rmg-sa.com>، (30/5/2025، 4:40).

¹¹⁵ يوفكوس سمية، بوعبد الله فاطمة الزهراء، مرجع نفسه، ص 20.

البيانات ونشر ثقافة التوعية والأمنية، كما تم التطرق إلى دور التعاون بين الجهات الرقابية والتنظيمية محليا ودوليا وفي الختام أكد الفصل أن التصدي لمخاطر التكنولوجيا المالية لا يتطلب إيقاف التقدم الرقمي بل يتطلب تأطيره من خلال حوكمة رشيدة وقوانين فعالة وأدوات تقنية متطورة تضمن تحقيق التوازن بين الابتكار والاستقرار.

الخاتمة

تعد التكنولوجيا المالية قوة دافعة نحو التحول الجذري في القطاع المالي، والتي أصبحت أحد المحركات الرئيسية للتغيير في الخدمات المصرفية للمعاملات المالية لها، حيث ساهمت في تطوير القطاع المصرفي عبر نماذج الأعمال الحديثة والمستحدثة المتعلقة بخدمات الدفع والتحويل، والتي من خلالها استطاعت المصارف التوجه إلى تقديم حزم من الخدمات والعروض بأقل التكاليف المادية والمعنوية وأكثر فعالية وكفاءة، ومع تنامي الاعتماد على هذه التقنيات الحديثة برزت العديد من المخاطر، مما يجعل إدارة المخاطر المالية والمصرفية أمام تحدي دائم لمواكبة التطور في مجال التكنولوجيا المالية، إذ أصبحت البنوك عرضة للعديد من المخاطر منها مخاطر الاختراق والقرصنة عبر هجمات سيبرانية حيث تعتمد على فكرة الهجوم التكنولوجي الافتراضي، الذي أصبح أكثر خطورة إذ يهدد أمن وسرية وخصوصية البيانات، وقد يؤدي التأخر وعدم ملائمة الأطر القانونية مع طبيعة الابتكارات الرقمية إلى خلق فراغ تشريعي تستغله بعض الجهات في مزاوله أنشطة غير خاضعة للرقابة وهذا ما يسمى بالمخاطر التشريعية والتنظيمية للتكنولوجيا المالية، كما تظهر مخاطر السوق نتيجة تقلبات الأسعار وفشل الأنظمة الرقمية في مواجهة المنافسة، وإلى جانب مخاطر السوق نجد مخاطر غسيل الأموال وتهريب الإرهاب الذي أصبح قضية عالمية، ولا تقل المخاطر البيئية أهمية خاصة في ظل الاعتماد المكثف على مراكز البيانات واستهلاك الطاقة مما يثير التساؤلات حول الأثر البيئي لهذا النوع من التكنولوجيا، كما أن مخاطر السمعة تشكل تهديدا حقيقيا حيث تؤدي هذه المخاطر لفقدان الثقة في المؤسسة المالية وهو ما يصعب استرجاعه في البيئة التنافسية، مما جعل البحث عن آليات تواجه هذه المخاطر ضرورة ملحة لضمان استقرار النظام المالي وحماية حقوق المستخدمين، وتشمل هذه الآليات مجموعة من التدابير التنظيمية والتقنية إلى جانب التعاون بين الجهات التنظيمية والمؤسسات المالية لتطوير بيئة آمنة ومبتكرة، كما تعتبر حوكمة تكنولوجيا المعلومات أداة فعالة لضبط العمليات الرقمية وضمان الامتثال للمعايير القانونية، حيث التكامل بين هذه الآليات يوفر بيئة مالية أكثر أمانا واستدامة ويعزز ثقة المستخدمين في نظم التكنولوجيا المالية.

🔗 نتائج الدراسة:

من خلال ما تم عرضه في الدراسة من محاولتنا للإجابة على الإشكالية خلصنا إلى النتائج التالية منها
نتائج تختبر صحة فرضياتنا:

- تتنوع مخاطر التكنولوجيا المالية بين مخاطر سيبرانية كالهجمات الإلكترونية ومخاطر تنظيمية وقانونية (غياب الأطر القانونية المناسبة)، وأخرى تشغيلية (أعطال الأنظمة أو الأخطاء البشرية)؛
- استخدام بعض تقنيات التكنولوجيا المالية في غسيل الأموال وتمويل الإرهاب بسبب ضعف الرقابة؛
- ضعف البنية التحتية الرقمية يعيق تبني التكنولوجيا المالية بشكل آمن؛

- وجود تأخر في مواكبة التشريعات المحلية للتطور في مجال التكنولوجيا المالية، ما يخلق فراغا قانونيا وقصوراً تشريعياً يمكن أن يستغل؛
- ضعف الوعي الأمني، حيث لا يزال العديد من المستخدمين والشركات الناشئة يفتقرون إلى الوعي الكافي بالمخاطر المرتبة باستخدام التقنيات المالية؛
- عدم وجود استراتيجية وطنية متكاملة لإدارة مخاطر التكنولوجيا المالية بشكل صحيح؛
- قلة التكوين والتدريب المتخصص في مجال إدارة مخاطر التكنولوجيا المالية.

🚩 الاقتراحات:

- بناءً على النتائج السابقة ومن أجل التقليل من أثر هذه المخاطر نقترح جملة من التوصيات التالية:
- الانخراط في الاتفاقيات الدولية الخاصة بالأمن السيبراني ومكافحة غسل الأموال؛
 - تطوير أدوات اكتشاف مبكر للهجمات الإلكترونية؛
 - وضع معايير وطنية لتقييم أمن المنصات الرقمية ومراقبة مدى التزامها بتلك المعايير؛
 - إطلاق حملات وطنية للتوعية الرقمية والتكوين المستمر للمستخدمين والعاملين؛
 - تحديث وتطوير الأطر القانونية والتنظيمية؛
 - الاستمرار في تحديث البرامج والتطبيقات الخاصة بمكافحة البرمجيات الخبيثة؛
 - تجنب استخدام أو تنزيل البرامج والملفات دون التأكد من مصداقيتها، والاعتماد على كلمات مرور قوية وغير مألوفة.

🚩 آفاق الدراسة:

لا شك أنه رغم الجهد المبذول في إتمام هذا البحث، فإن هذا الأخير لا يخلو من النقائص بسبب عدم قدرتنا على تناول كل نواحي الموضوع بالتفصيل، إلا أنه يمكن أن يكون هذا البحث جسراً يربط بين بحوث سبقت فأضاف إليها بعض المستجدات لإثرائها وبعثها من جديد، وبحوث مقبلة كتمهيد لمواضيع يمكنها أن تكون إشكالية لأبحاث أخرى نذكر منها:

- تقييم فعالية الأطر التنظيمية المتعلقة بالتكنولوجيا المالية المعتمدة في الدول العربية (إلى أي مدى تستطيع مواكبة تطور مخاطر التكنولوجيا المالية؟)؛
- دراسة تحليلية حول مدى استجابة الجزائر لآليات الحد من مخاطر التكنولوجيا المالية؛
- دراسة التوازن بين تشجيع الابتكار المالي وضمان الحماية من المخاطر السيبرانية.

قائمة المراجع

المراجع باللغة العربية

أولاً: الكتب

- بن قيده مروان وآخرون، التكنولوجيا المالية الابتكارات والحلول الرقمية، كتاب جماعي، مخبر التنمية المحلية المستدامة، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة يحي فارس، المدينة، 2022.

ثانياً: الرسائل الجامعية

- أطروحات الدكتوراه:
 - حجيرة الهام، دور التكنولوجيا المالية في تطوير الأداء المصرفي، أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث ل م د في الاقتصاد النقدي والبنكي، جامعة غرداية، الجزائر، 2024/2023.
 - خولة واصل، أثر تبني الحوسبة السحابية على الأداء الوظيفي دراسة حالة المؤسسة الجزائرية للتأمين، أطروحة دكتوراه لنيل شهادة دكتوراه علوم فرع علوم التسيير، تخصص أنظمة المعلومات ومراقبة التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2020/2019.

▪ مذكرات الماستر:

- بوكفوس سمية، بوعبد الله فاطمة الزهراء، أثر حوكمة تكنولوجيا المعلومات على الأداء المالي للمؤسسة الاقتصادية دراسة حالة الصندوق الوطني للضمان الاجتماعي لغير الأجراء، مذكرة مكملة لنيل شهادة الماستر، جامعة عبد الحفيظ بوالصوف، ميلة، السنة الجامعية 2023/2022.
- حفيان جهاد، إدارة المخاطر الائتمانية في البنوك التجارية دراسة استبائية مجموعة من البنوك التجارية العاملة بولاية ورقلة خلال سنة 2012، مذكرة مقدمة لنيل شهادة الماستر في العلوم المالية، جامعة قاصدي مرباح، 2012/2011.
- خليل عبير، علواني نوال، دور تقنية البلوك تشين في التعاملات التجارية، مذكرة مكملة لنيل شهادة الماستر في القانون، تخصص قانون أعمال، جامعة 8 ماي 1945، قالمة، الجزائر، 2023/2022.

ثالثاً: المجلات والملتقيات العلمية

- ابتهاج إسماعيل يعقوب، وآخرون، مؤشر مقترح لإفصاح المحاسبي عن مخاطر السيبرانية في سوق العراق للأوراق المالية على وفق متطلبات الدولية: دراسة اختيارية، جامعة المستنصرية، العراق، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 09، العدد 01، 2022.
- أحلام بوعلي، ثريا سعيد، إدارة المخاطر التشغيلية في البنوك التجارية: دراسة حالة لعينة من البنوك التجارية في الجزائر . المجلة الجزائرية للتنمية الاقتصادية، المجلد 02، عدد 03، 2015.
- أحمد خليفة، وآخرون، أثر حوكمة تكنولوجيا المعلومات على الحد من مخاطر نظام المعلومات المحاسبين، مجلة الدراسات المالية والمحاسبة والإدارية، المجلد 08، العدد 01، مارس 2021.
- احمد عازب الشيخ، عبد الجليل هويدي، مخاطر ظاهرة غسل الأموال على الأمن الاقتصادي الجزائري، جامعة الوادي، الجزائر، المجلد 01، العدد 01، 2019.
- إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي، مجلة الاجتماعية القومية، جامعة دنبور، المجلد 10، العدد 4، 2019.

- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أفريل 2019.
- أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، المجلد 32، العدد 35، الجزء الثالث، 2020.
- أونان محمد، وآخرون، آليات وقاية المعاملات الالكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة les cahiers du mecas، جامعة جيلالي ليايس، سيدي بلعباس، الجزائر، المجلد 12، العدد 01، جوان 2016.
- برا هيمي فائزة، مساهمة تقنية سلسلة الكتل في تعزيز التكنولوجيا المالية، مجلة التنمية والاستشراف للبحوث والدراسات، المجلد 06، العدد 02، ديسمبر 2021.
- بن صابر بالقاسم، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، المجلد 02، العدد 04، جوان 2017.
- بن علي صليحة، تقنية البلوك تشين أساس تفعيل آلية عمل العقود الذكية، مجلة العلوم القانونية والاجتماعية، جماعة زيان عاشور، الجلفة، الجزائر، المجلد 07، العدد 02، جوان 2022.
- حيدر عبد الحسين حميد المستوفي، أهمية الإفصاح عن المخاطر خلال دورة حياة المؤسسة المالية، المركز الجامعي بريكة، الجزائر، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، 2022.
- خليل غربي، محفوظ جبار، إدارة المخاطر المالية ودورها في التنبؤ بالفشل المالي باستخدام نموذج sherrod للبنك الوطني الجزائري 2016/2019، مجلة المنهل الاقتصادي، جامعة فرحات عباس سطيف، الجزائر، المجلد 5، العدد 1، ماي 2022.
- ربيعي حسين، وسمر محمود، الحروب السيبراني المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والخارجي، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 02، جويلية 2022.
- زعموكي سالم، مرزق فتيحة حبال، الذكاء الاصطناعي وانعكاساته الاقتصادية على العالم، جامعة زيان عاشور جلفة، الجزائر، مجلة التراث، المجلد 13، العدد 04، ديسمبر 2023.
- ساعد بوقرص، الأمن السيبراني مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا هواري بومدين، المجلد 3، العدد 1، 2022.
- سامي محمد بونيف، دور الاستراتيجيات الاستباقية في الهجمات السيبرانية الردع السيبراني نموذجاً، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة احمد بن يحيى الونشريسي تيسمسيلت، الجزائر، المجلد 04، العدد 07، 30 جوان 2019.
- سعاد بوبجة، الذكاء الاصطناعي: تطبيقات وانعكاسات، مجلة اقتصاد المال والأعمال، المجلد 06، العدد 04، ديسمبر 2022.
- سلطان احمد خليف، المخاطر التنظيمية والسلوك القيادي دراسة لآراء عينة من القيادات الإدارية في جامعة الموصل، مجلة جامعة الانبار للعلوم الاقتصادية والإدارية، المجلد 5، العدد 10، 2013.
- سليمان عبد الواحد يوسف، أمل محمد غنايم، اتجاهات الباحثين نحو توظيف تطبيقات الذكاء الاصطناعي في البحث النفسي والتربوي، جامعة قناة السويس، مصر، مجلة التراث، المجلد 13، العدد 04، ديسمبر 2023.
- سي عبد القادر حنان، الأمن السيبراني وأثره على دول العالم، جامعة بسوسة، تونس، مجلة البصائر للدراسات القانونية والاقتصادية، المجلد 04، العدد 07، 2024.

- شايب محمد، مخاطر غسيل الأموال في البنوك والمؤسسات المالية العربية ودور التكنولوجيا الحديثة في مكافحتها، المجلة الجزائرية للأبحاث الاقتصادية، المجلد 01، العدد 01، ماي 2018.
- صفار محمد، شرشم محمد، واقع وتحديات تكنولوجيا البلوك تشين في القطاع المالي والمصرفي (تجربة بعض الدول العربية)، مجلة الاقتصاد والتنمية المستدامة، جامعة وهران، الجزائر، المجلد 05، العدد 02، 2022.
- طبيب سارة، أساليب تعامل المؤسسات الصناعية الجزائرية مع مخاطر السوق، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، المجلد 09، العدد 14، 2015.
- طروبيا ندير، تكنولوجيا البلوك تشين وتأثيراتها على المستقبل الرقمي للعمليات الاقتصادية . الفرص والتحديات، جامعة احمد دراية (الجزائر)، مجلة أبحاث اقتصادية معاصرة، المجلد 03، العدد 01، 2020.
- عبد الحفيظ احمد، صديقي مليكة، دور الحوكمة في الحد من مخاطر السمعة في البنوك التجارية، مجلة إدارة الأعمال والدراسات الاقتصادية، مجلد 05، عدد 02، 2019.
- عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد إدراج، الجزائر، المجلد 06، العدد 02، 2022.
- عبد الله عزت بركات، ظاهرة غسيل الأموال وأثارها الاقتصادية والاجتماعية، جامعة الزرقاء الأهلية، الأردن، مجلة اقتصاديات شمال إفريقيا، المجلد 03، العدد 04، 2006.
- علاش أحمد، دور التكنولوجيا المالية في دعم النشاط المالي والابتكار تجربة البحرين، مجلة الإبداع، المجلد 9، العدد 1، 2019.
- علياء زامل مشتت، أثر التصيد الاحتيالي في الاعتداء على الخصوصية في المجال الرقمي، مجلة كلية الإمام الكاظم، المجلد 8، العدد 1، 2022.
- عمارية بخته، غنية مجاني، دور تكنولوجيا المالية في دعم القطاع المصرفي، مجلة (المدير) المجلد 07، العدد 02، 2020.
- عياش زوبير، العايب سناء، تسيير مخاطر السوق وفق مقررات بازل 2 واصلاحات بازل 3، مجلة دراسات اقتصادية، المجلد 6، العدد 02، ديسمبر 2019.
- العياشي زرزار، حمزة بن وريدة، الحوسبة السحابية: المفهوم والخصائص (تجارب دول وشركات رائدة)، مجلة أرصاد للدراسات الاقتصادية والإدارية، جامعة 20 أوت 1955 سكيكدة، الجزائر، مجلد 02، العدد 02، ديسمبر 2019.
- فايزة جيجخ، سميرة فرحات، حوكمة تكنولوجيا المعلومات ودورها في الوقاية من الأزمات، مجلة الاقتصاديات المالية البنكية وإدارة الأعمال، جامعة بسكرة، الجزائر، المجلد 05، العدد 01، 2016.
- فخاري فاروق، أهمية النماذج الرياضية في إدارة وقياس مخاطر السوق مع الإشارة لتجربة استخدام نموذج القيمة المعرضة للخطر VAR على مستوى البنوك المصرية، مجلة التكامل الاقتصادي، المجلد 08، العدد 01، 2020.
- قوريش زكرياء، بلعبيدي عبد الله، حوكمة تكنولوجيا المعلومات . تقنية الكوبيت 5 نموذجا، مجلة الأصل للبحوث الاقتصادية والإدارية، جامعة عباس لغرور، خنشلة، الجزائر، المجلد 07، العدد 01، أفريل 2023.
- كريم لخضر، الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية، مجلة طبنة، المركز الجامعي بريكة، الجزائر، المجلد 02، العدد 02، ديسمبر 2019.

- كلاش مريم، بهلول نور الدين، دور إدارة المخاطر المالية في تقييم الأداء المالي للمؤسسة الاقتصادية، دراسة حالة مجمع صيدال، جامعة سوق أهراس، الجزائر، المجلد 11، العدد 03، افريل 2021.
- كوثر طلحي، نهاد زوادي، دور ابتكارات التكنولوجيا المالية في تطوير الخدمات المالية الإسلامية، مجلة دراسات في المالية الإسلامية والتنمية، المجلد 04، العدد 7، 2023.
- لطرش ذهبية، دراسة تحليلية لفرص ومخاطر التكنولوجيا المالية على الاستقرار المالي، مجلة اقتصاد المال والأعمال، جامعة الشهيد حمه لخضر الوادي، الجزائر المجلد 8، العدد 01، مارس 2023.
- لويظة أوصغير، مخاطر السوق في البنوك الدولية واستراتيجيات إدارتها حسب المعايير الدولية للجنة بازل مجموعة سوسيتي جنرال نموذجاً، مجلة نور للدراسات الاقتصادية، مجلد 06، العدد 10، 2020.
- ليندة صيمود، سهيلة دهماني، الذكاء الاصطناعي تقنية رقمية تقود إلى ابتكار تجربة تعليمية ناشئة في الجزائر. شركة انكيديا نموذجاً، مجلة الدراسات الإعلامية والاتصالية، المجلد 02، العدد 02، أكتوبر 2022.
- المبارك رعاش، وآخرون، توظيف الحوسبة السحابية في النشر الإلكتروني الأكاديمي للبحوث العلمية، جامعة الجزائر 2، الجزائر، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 07، العدد 06، أكتوبر 2022.
- محريق عدنان، أساليب قياس مخاطر التشغيل وفقاً لاتفاق بازل 2، مجلة الدراسات الاقتصادية والمالية، جامعة الوادي، المجلد 03، العدد 08، 2015.
- محمد الصغير كاوجة، الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 03، سبتمبر 2022.
- محمد عبد الله مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، المجلد 01، العدد 6، يناير 2015.
- مسعداوي يوسف، دور البنوك في محاربة عمليات غسيل الأموال غير المشروعة، جامعة البليدة 2، الجزائر، مجلة الإدارة والتنمية للبحوث والدراسات، المجلد 03، العدد 5، 2014.
- مصداق راضية، إدارة المخاطر التشغيلية وفقاً لاتفاقية بازل 2 في البنوك التجارية الجزائرية، دراسة حالة بنك الفلاحة والتنمية الريفية، مجلة الاستراتيجية والتنمية، جامعة فرحاب عباس، سطيف 01، المجلد 07، العدد 13، 2017.
- نور الدين كروش، مستقبل الصناعة المصرفية الإسلامية في ظل تطورات التكنولوجيا المالية، مجلة الدراسات المحاسبية والمالية المتقدمة، المجلد 04، العدد 02، أكتوبر 2020.
- هاشمي رشيدة، ملياني عبد الوهاب، الإطار المفاهيمي للذكاء الاصطناعي، جامعة عمار ثليجي الاغواط، الجزائر، مجلة التراث، المجلد 14، العدد 02، جوان 2024.
- هشام معيري، مراد زايد، المخاطر الاجتماعية للمؤسسات (المفهوم واستراتيجيات الوقاية)، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، المجلد 28، العدد 05، 2024.
- واصل خولة، رجم خالد، واقع استخدام خدمة الحوسبة السحابية بمؤسسة موبليس، جامعة ورقلة، الجزائر، مجلة العلوم الإنسانية، المجلد 09، العدد 01، 2019.
- ياسع ياسمين، المخاطر المالية من خلال العمليات المصرفية الإلكترونية، مجلة دراسات اقتصادية، جامعة بومرداس، الجزائر، المجلد 08، العدد 01، 2022.

رابعاً: التقارير

- تقرير كاسبرسكس يكشف عن تضاعف هجمات سرقة البيانات المصرفية التي تستهدف الهواتف الذكية،
4مارس2025، <http://me.kaspersky.com>

خامساً: المطبوعات الجامعية

- بوزادية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات إستراتيجية وأمنية، جامعة الجزائر 03، كلية العلوم السياسية والعلاقات الدولية، 2021/2020.

المراجع باللغة الأجنبية

- Karbnache houri، abderrazak habbar،the importance of using informatio technology in managing liquity risk in chalef cement compan,volume 08, N 02,2014.

المواقع الإلكترونية

- مفهوم الامتثال، الموقع الالكتروني، . <http://fastercapita.com> .
- <https://www.axio,Chainalysis> (2024) Ransomware trends and Financial Crime Analysis,com.
- إدارة السمعة مخاطر السمعة، التخفيف من مخاطر السمعة، استراتيجيات الوقاية والاستجابة،<http://www.Fastercapital.com>.
- إدارة السمعة ومخاطر المنافسة في الأعمال التجارية، مقال 100 من سلسلة إدارة وتطوير الأعمال، من موقع، business insight .
- الامتثال الإداري، الموقع الالكتروني، <https://www.rmgsa.com> .
- الامتثال لمكافحة غسيل الاموال واعرف عميلك، الموقع الالكتروني، <https://wikipedia.com>.
- برامج الفدية، موقع إلكتروني، <http://www.Vic.Gov.Au> .
- جميع المخاطر البيئية، ومعالجة المخاطر البيئية،<http://www.Fastercapital.COM>.
- خالد، بن سليمان الغنبر،الاصطياد الإلكتروني، الأساليب والإجراءات المضادة، مركز التميز لأمن المعلومات، <http://COEIA,EDU,S A> .
- دور التكنولوجيا في إدارة مخاطر الامتثال،<https://Fastercapital.Com>.
- سمعة الشركة كيف تتجنب المخاطر. <http://www.Rowadalaamal.com>.
- غسيل الاموال عن طريق العملات المشفرة، الموقع الالكتروني، <https://syntheticdrugs.unodc.org> .
- القوة العمياء والحماية الرقمية 28.2019، <http://digital,protection,Tech> , apr.
- ما المقصود بالتصيد الاحتيالي، موقع إلكتروني، <http://www.microsoft.com> .
- ما هي برامج الفدية، موقع إلكتروني، <http://www.microsoft.com> .
- مفهوم الامتثال القانوني، الموقع الالكتروني، https://www.noor_book.com .
- مفهوم الامتثال المالي، الموقع الالكتروني، <https://gadwalah.com> .
- مفهوم المخاطر التنظيمية، موقع الكتروني <https://albarakatilaw.com> .
- مفهوم المخاطر المالية، موقع الالكتروني، [HTTPS://BAKKAH.COM](https://BAKKAH.COM) .
- مفهوم مخاطر الامتثال، موقع الالكتروني، <https://ar.lpcentre.com> .
- مفهوم مخاطر العملة، موقع الالكتروني <https://www.argaam.com> .

- مؤسسة دعائم التقنية للحاسب الآلي، ما هو فيروس الفدية و أنواعه، وكيف يمكن حماية نفسك ومؤسستك من الاختراق ; http://www.it_pillae.com.
- النفايات الالكترونية، أنواعها، تأثيراتها على البيئة، <http://www.medicalwaste.org.Ly>.
- هجوم القوة العمياء، منصة مجرة، <https://mhbarabic.com>, harvard , business , revie .
- هشام حمزة، التكنولوجيا المالية (مفهوم، تطور، مخاطر)، مجلة الكترونية تصدر عن المعهد المصرفي المصري لمتابعة مستجدات القطاع المصرفي ورصد آراء القائمين على الصناعة المصرفية المصرية، <http://www.masrafeyou.Ebi.Gov.eg>.
- وليد أبو سعد، أمن المعلومات، الموسوعة العربية للكمبيوتر، قسم دورات التعليمية سلسلة كتب الدورات التعليمية الإلكترونية، <http://www.c4arab.com>.

فهرس المحتويات

الصفحة	العنوان
-	الإهداء
-	شكر وعرفان
I	ملخص الدراسة
II	قائمة المحتويات
III	قائمة الجداول
VI	قائمة الأشكال
أ-ج	مقدمة
05	الفصل الأول: الإطار المفاهيمي حول التكنولوجيا المالية
05	تمهيد
09-05	المبحث الأول: مفاهيم أساسية للتكنولوجيا المالية
07-05	المطلب الأول: تعريف التكنولوجيا المالية وخصائصه
09-08	المطلب الثاني: التطور التاريخي للتكنولوجيا المالية
11-09	المطلب الثالث: أهمية ودوافع تبني التكنولوجيا المالية
18-11	المبحث الثاني: تقنيات التكنولوجيا المالية
13-11	المطلب الأول: تقنية البلوك تشين
15-13	المطلب الثاني: الحوسبة السحابية
18-16	المطلب الثالث: الذكاء الاصطناعي
21	الفصل الثاني: مخاطر التكنولوجيا المالية
21	تمهيد
25-21	المبحث الأول: مفاهيم أساسية حول التكنولوجيا المالية
22-21	المطلب الأول: مفهوم مخاطر التكنولوجيا المالية.
25-22	المطلب الثاني: أشكال مخاطر التكنولوجيا المالية
41-26	المبحث الثاني: مخاطر أمن المعلومات
29-26	المطلب الأول: مفهوم المخاطر السيبرانية والفضاء السيبراني
31-29	المطلب الثاني: الإطار المفاهيمي للأمن السيبراني

41-32	المطلب الثالث: أنواع المخاطر السيبرانية
58-42	المبحث الثالث: المخاطر الأخرى
47-42	المطلب الأول: المخاطر التشريعية والتنظيمية
52-48	المطلب الثاني: مخاطر السمعة والمخاطر البيئية
58-53	المطلب الثالث: مخاطر السوق والمخاطر التشغيلية
61	الفصل الثالث: آليات الحد من مخاطر التكنولوجيا المالية
61	تمهيد
66-61	المبحث الأول: المتطلبات الأمنية في الحد من مخاطر التكنولوجيا المالية
63-61	المطلب الأول: سبل مواجهة الهجمات السيبرانية وآليات مكافحة غسيل الأموال
66-64	المطلب الثاني: جهود الجزائر في مواجهة تهديدات والجرائم السيبرانية
69-66	المبحث الثاني: سبل مواجهة المخاطر التنظيمية والتشريعية
67-66	المطلب الأول: الحماية من المخاطر التنظيمية والتشريعية
69-68	المطلب الثاني: القرارات السياسية للتعاون الدولي
76-70	المبحث الثالث: حوكمة التكنولوجيا المعلومات
72-70	المطلب الأول: مفاهيم أساسية حول حوكمة تكنولوجيا معلومات
76-72	المطلب الثاني: ركائز ومعايير حوكمة تكنولوجيا المعلومات
78-76	الخاتمة
85-80	قائمة المراجع
88-87	فهرس المحتويات

هدفت هذه الدراسة إلى إبراز المخاطر المختلفة الناشئة عن استخدام التكنولوجيا المالية بتقنياتها المعتمدة في القطاع المصرفي، سواء كانت سيبرانية، تنظيمية وتشريعية، أو متعلقة بالسوق والبيئة والسمعة، من أجل فهم أثارها المحتملة على سلامة واستقرار البيئة المالية في المؤسسات المالية، كما سعت إلى استعراض أبرز الآليات الوقائية والضوابط التي يمكن اعتمادها للتقليل من حدة هذه المخاطر، كتفعيل حوكمة تكنولوجيا المعلومات وتطوير الأطر القانونية وتعزيز التعاون بين مختلف الجهات الرقابية والتنظيمية لضمان بيئة مصرفية آمنة ومستدامة في ظل التحول الرقمي المتسارع.

وقد توصلت الدراسة إلى جملة من النتائج تمحورت حول أن التكنولوجيا المالية على الرغم من مزاياها العديدة في تطوير القطاع المصرفي إلا أنها تحمل معها مخاطر متعددة بإمكانها أن تكون لها آثار عكسية لذا وجب العمل بشكل مستمر على تقديم آليات تسمح بتقليل أو تفادي تلك المخاطر مع الحفاظ على المزايا والآثار الإيجابية التي تتميز بها.

الكلمات المفتاحية: التكنولوجيا المالية، الأمن السيبراني، آليات الحد من المخاطر، حوكمة تكنولوجيا المعلومات.

Abstract:

This study aimed to highlight the various risks arising from the use of financial technology and its adopted techniques in the banking sector, whether they are cyber, regulatory and legislative, or related to the market, environment, and reputation, in order to understand its potential impact on the safety and stability of the financial environment within financial institutions , It also sought to review the key preventive mechanisms and controls that can be adopted to mitigate the severity of these risks, such as implementing information Technology governance, developing legal frameworks, and enhancing cooperation among various regulatory and supervisory authorities, in order to ensure a secure and sustainable banking environment amid the accelerating digital transformation The study reached a set of conclusions, centered around the fact that, despite the numerous advantages of financial technology in advancing the banking sector, it also carries multiple risks that could have adverse effects Therefore, it is essential to continuously provide mechanisms that help reduce or avoid these risks while preserving the benefits and positive impacts that financial technology offers .

Key words: financial technology, Cyber security, information technology Governance, Risk Mitigation Mechanisms.