

التكنولوجيا المالية والمخاطر المالية
الحديثة: بين سرعة الابتكار ومتطلبات
الحماية والامتثال

إعداد

د.علي جابر
د.شروق الحامد
د. زين المعاينة
آلاء العتيبي

هاتف: 00962790712522





الملخص

يتناول هذا البحث موضوع التكنولوجيا المالية والمخاطر المالية الحديثة بوصفه أحد أكثر الموضوعات حضوراً في الفكر المالي والمصرفي المعاصر؛ إذ لم تعد التكنولوجيا المالية مجرد قناة بديلة لتقديم الخدمة، بل أصبحت بيئة تشغيلية وتنظيمية متكاملة تعيد تشكيل المدفوعات والتمويل والائتمان وإدارة البيانات والرقابة. وقد أدى انتشار المحافظ الإلكترونية، والخدمات المصرفية المفتوحة، والذكاء الاصطناعي، وسلاسل الكتل، والتحقق الرقمي من الهوية، وتحليلات البيانات الضخمة، إلى تحسين سرعة الخدمة وتخفيض بعض تكاليفها وتوسيع فرص الوصول إليها، إلا أن هذا التحول أنتج في الوقت ذاته أنماطاً حديثة من المخاطر التي لا يمكن التعامل معها بالأدوات التقليدية وحدها.

وينطلق البحث من مشكلة منهجية مفادها أن سرعة الابتكار المالي الرقمي قد تسبق أحياناً قدرة المؤسسات والجهات الرقابية على بناء ضوابط كافية للحماية والامتثال، مما يفتح المجال أمام مخاطر تشغيلية وتقنية وسيرانية وتنظيمية ومخاطر بيانات واحتيال رقمي ومخاطر طرف ثالث. لذلك يعالج البحث الإطار المفاهيمي للتكنولوجيا المالية وخصائصها، ثم يبين طبيعة المخاطر المالية الحديثة في ظل التحول الرقمي، ويحلل العلاقة بين الابتكار وتسارع ظهور المخاطر، قبل أن ينتقل إلى مظاهر المخاطر المرتبطة بالتكنولوجيا المالية في التشغيل والتقنية والأمن السيرياني وحماية البيانات والامتثال والرقابة.

ويؤكد البحث أن التكنولوجيا المالية ليست مصدراً للخطر في ذاتها، كما أنها ليست حلاً كاملاً لكل مشكلات القطاع المالي، وإنما تتحدد قيمتها بمدى انضباطها ضمن إطار حوكمة واضح. فالابتكار قد يرفع الكفاءة ويعزز الشمول المالي ويطور إدارة المخاطر، لكنه قد يتحول إلى مصدر هشاشة إذا غابت الحماية منذ التصميم، أو ضعفت مراقبة مزودي الخدمات، أو توسع استخدام البيانات دون موافقة واضحة، أو

تم تسويق الخدمات الرقمية بطريقة لا تكشف حدودها ومخاطرها للعميل. ومن ثم فإن العلاقة بين الابتكار والحماية علاقة تكامل لا تعارض، لأن الابتكار المستدام لا ينفصل عن الثقة الرقمية. ويخلص البحث إلى أن مواجهة مخاطر التكنولوجيا المالية تقتضي بناء منظومة تجمع بين الحوكمة الرقمية، والأمن السيبراني، وإدارة الطرف الثالث، والامتثال الرقمي، وحماية المستهلك المالي، والتثقيف المالي الرقمي، وتعاون الجهات الرقابية محليا ودوليا. كما يوصي بضرورة انتقال المؤسسات المالية من الامتثال اللاحق إلى الامتثال منذ التصميم، ومن الأمن بوصفه وظيفة تقنية إلى الأمن بوصفه مسؤولية مؤسسية، ومن التسويق الرقمي الجاذب إلى الإفصاح الرقمي العادل. وبذلك يصبح التوازن بين سرعة الابتكار ومتطلبات الحماية والامتثال شرطا لازما لاستقرار النظام المالي واستدامة ثقة العملاء.

الكلمات المفتاحية: التكنولوجيا المالية، المخاطر المالية الحديثة، الأمن السيبراني، الامتثال الرقمي، الحوكمة الرقمية، حماية البيانات، الابتكار المالي.



Abstract

This study examines financial technology and modern financial risks as one of the most important issues in contemporary banking and financial thought. FinTech is no longer a secondary channel for delivering services; it has become an integrated operational and regulatory environment that reshapes payments, finance, credit, data governance, supervision, and customer interaction. The spread of e-wallets, open banking, artificial intelligence, blockchain, digital identity, and big data analytics has improved speed, accessibility, and cost efficiency, but it has also generated new forms of risk that cannot be addressed through traditional controls alone.

The study is built around a central problem: the speed of digital financial innovation may exceed the ability of institutions and regulators to develop adequate protection and compliance safeguards. This creates operational, technical, cyber, regulatory, data, fraud, and third-party risks. The study therefore develops the conceptual framework of FinTech and its characteristics, explains the changing nature of financial risks under digital transformation, analyzes the relationship between innovation and the acceleration of risk, and then examines the key manifestations of FinTech-related risks in operations, technology, cybersecurity, data protection, compliance, and supervision. The study argues that FinTech is neither a risk in itself nor a complete solution to the challenges of the financial sector. Its value depends on the extent to which it is governed by a clear framework of digital governance, cybersecurity, consumer protection, and regulatory compliance. Innovation may improve



efficiency, financial inclusion, and risk management, but it may also become a source of fragility if security by design is absent, third-party providers are weakly monitored, data is used without sufficient consent, or digital services are marketed without clear disclosure of their limits and risks.

The study concludes that managing modern FinTech risks requires an integrated system combining digital governance, cybersecurity, third-party risk management, compliance by design, financial consumer protection, digital financial literacy, and regulatory cooperation. It recommends that financial institutions move from ex-post compliance to compliance by design, from viewing cybersecurity as a purely technical function to treating it as an institutional responsibility, and from attractive digital marketing to fair digital disclosure. A practical balance between the speed of innovation and the requirements of protection and compliance is therefore essential for financial stability and sustainable customer trust.

Keywords: FinTech, modern financial risks, cybersecurity, digital compliance, digital governance, data protection, financial innovation.

المقدمة

شهد القطاع المالي خلال السنوات الأخيرة تحولا عميقا في طبيعة الخدمات والقنوات والأدوات. فلم تعد المؤسسة المالية تعتمد على الفرع التقليدي والموظف والوثيقة الورقية وحدها، بل أصبحت تعمل داخل شبكة رقمية مترابطة تجمع بين التطبيقات والمنصات وقواعد البيانات ومزودي الخدمات السحابية وشركات الدفع والتحقق الرقمي وخوارزميات التحليل. وقد جعل هذا التحول الخدمة المالية أسرع وأقرب إلى العميل، لكنه جعلها كذلك أكثر اعتمادا على التقنية وأكثر تعرضا لمخاطر يصعب حصرها في إطار المخاطر التقليدية.

وتتبع حساسية الموضوع من أن القطاع المالي يقوم أساسا على الثقة. فالعميل لا يتعامل مع التطبيق أو المحفظة أو منصة التمويل بوصفها واجهة تقنية فقط، بل بوصفها وعدا بحماية المال والبيانات والحقوق. وإذا تعرضت الخدمة الرقمية لتعطل متكرر، أو لاختراق، أو لاحتيال، أو لسوء استخدام للبيانات، فإن الضرر لا يبقى محصورا في الجانب التقني، بل يمتد إلى الثقة في المؤسسة وربما في النظام المالي كله.

ولا يعني ذلك أن التكنولوجيا المالية تمثل خطرا مطلقا أو أن الابتكار ينبغي أن يتوقف. فالابتكار المالي الرقمي أصبح ضرورة للتنافس، وتحسين الكفاءة، وتوسيع الشمول المالي، وتطوير أدوات إدارة المخاطر. لكن هذه الضرورة لا تلغي الحاجة إلى الحماية والامتثال، بل تجعلها أكثر إلحاحا؛ لأن الخدمة التي تنتشر بسرعة يمكن أن تنتشر معها الخلل بالسرعة نفسها إذا لم تكن محكومة بضوابط واضحة. ومن هنا يأتي هذا البحث لمعالجة العلاقة بين التكنولوجيا المالية والمخاطر المالية الحديثة من زاوية منهجية تجمع بين المفهوم والتطبيق، وبين الابتكار والحماية، وبين دور المؤسسة المالية ودور الجهة الرقابية. فالمقصود ليس سرد أدوات التكنولوجيا المالية فحسب، ولا تضخيم مخاطرها، وإنما بناء تصور يبين كيف يمكن أن تكون التكنولوجيا مصدرا للقيمة إذا ضبطت، ومصدرا للشاشة إذا

تركت بلا حوكمة وامثال.

مشكلة الدراسة وأسئلتها

تتمثل مشكلة الدراسة في أن التكنولوجيا المالية تتطور بسرعة كبيرة، بينما تحتاج الأطر التنظيمية والرقابية وإجراءات الامتثال إلى وقت أطول للتشريع والتطبيق والاختبار. وينشأ عن ذلك تفاوت بين قدرة المؤسسات المالية على إطلاق خدمات رقمية جديدة وبين قدرتها على حماية البيانات، وضمان استمرارية الأعمال، ومكافحة الاحتيال، وإدارة الطرف الثالث، والامتثال لمتطلبات مكافحة غسل الأموال وتمويل الإرهاب وحماية المستهلك المالي.

وتزداد المشكلة تعقيدا بسبب تعدد الأطراف المشاركة في الخدمة المالية الرقمية. فقد يتداخل البنك أو شركة التمويل مع شركة دفع، ومزود سحابي، ومنصة تحقق رقمي، ومزود ذكاء اصطناعي، وعميل يستخدم الخدمة من بلد آخر. وفي هذا الواقع تصبح المسؤولية موزعة، والبيانات متنقلة، والرقابة أكثر صعوبة، كما يصبح الخطأ الواحد قابلا للانتشار عبر سلسلة كاملة من الأطراف.

وتسعى الدراسة إلى الإجابة عن الأسئلة الآتية: ما مفهوم التكنولوجيا المالية وخصائصها في البيئة المالية المعاصرة؟ وما طبيعة المخاطر المالية الحديثة في ظل التحول الرقمي؟ وكيف يؤدي تسارع الابتكار المالي إلى ظهور مخاطر جديدة؟ وما أهم المخاطر التشغيلية والتقنية والسيبرانية ومخاطر البيانات والامتثال في تطبيقات التكنولوجيا المالية؟ وما متطلبات الحماية والحوكمة الرقمية اللازمة لمواجهتها؟ وما دور الجهات الرقابية في تحقيق التوازن بين الابتكار والاستقرار المالي؟

أهمية الدراسة

تتبع أهمية الدراسة من حادثة موضوعها واتصاله المباشر بتحولات القطاع المالي والمصرفي. فقد أصبحت التكنولوجيا المالية عنصرا مؤثرا في المدفوعات والتمويل والادخار والاستثمار والتأمين والرقابة،

ولم تعد مجرد أداة مساندة. ومن ثم فإن فهم مخاطرها ومتطلبات ضبطها يمثل ضرورة للباحثين والمؤسسات المالية والجهات الرقابية وصانعي السياسات.

كما تتجلى أهمية الدراسة في أنها تنظر إلى المخاطر الرقمية بوصفها مخاطر مالية ومؤسسية وتنظيمية، لا مخاطر تقنية فقط. فالاختراق السيرياني قد يبدأ من ثغرة تقنية، لكنه ينتهي بأثر مالي وسمعي وقانوني. وتعطل النظام قد يبدو خلاا تشغيليا، لكنه قد يؤدي إلى فقدان ثقة العملاء أو فرض غرامات رقابية أو توقف معاملات حيوية. وتفيد الدراسة في تقديم رؤية متوازنة لا ترفض الابتكار ولا تندفع وراءه دون ضوابط. فالمؤسسات المالية تحتاج إلى الابتكار حتى تبقى قادرة على المنافسة، لكنها تحتاج كذلك إلى حوكمة وامثال حتى لا يتحول الابتكار إلى مصدر خطر. ومن هنا تتضح أهمية البحث في بناء علاقة تكاملية بين سرعة التطوير ومتطلبات الحماية.

أهداف الدراسة

تهدف الدراسة إلى بيان مفهوم التكنولوجيا المالية وخصائصها ومجالاتها الرئيسية في البيئة المالية المعاصرة، مع توضيح الفرق بين التكنولوجيا بوصفها أداة تشغيل وبينها بوصفها عاملا يعيد تشكيل نموذج الخدمة المالية.

كما تهدف إلى تحليل طبيعة المخاطر المالية الحديثة التي نشأت أو تعاظمت في ظل التحول الرقمي، ولا سيما المخاطر التشغيلية والتقنية والسيريانية ومخاطر البيانات والاحتيال والامثال والرقابة العابرة للحدود.

وتسعى الدراسة كذلك إلى تحديد متطلبات الحماية والامثال في مواجهة هذه المخاطر، من خلال الحوكمة الرقمية، والأمن السيرياني، وإدارة الطرف الثالث، والإفصاح، والتحقق الرقمي من الهوية، وبناء الثقافة المالية الرقمية لدى العملاء والعاملين.

وتطمح الدراسة في نهايتها إلى تقديم تصور منهجي يساعد على تحقيق التوازن بين تشجيع الابتكار المالي وحماية الاستقرار المالي

وثقة العملاء، بحيث لا ينظر إلى الرقابة بوصفها عائقاً أمام الابتكار، بل بوصفها شرطاً لاستدامته.

منهجية الدراسة

تعتمد الدراسة المنهج الوصفي التحليلي؛ إذ تصف مفهوم التكنولوجيا المالية وخصائصها ومجالاتها، ثم تحلل المخاطر المالية الحديثة المرتبطة بها في ضوء الأدبيات والتقارير والدراسات الحديثة. ولا تقف الدراسة عند العرض الوصفي، بل تسعى إلى تفسير العلاقة بين الابتكار الرقمي ونشوء المخاطر ومتطلبات ضبطها. وتستعين الدراسة بالمنهج الاستقرائي في تتبع الدراسات والتقارير العربية والأجنبية الحديثة المتعلقة بالتكنولوجيا المالية والأمن السيبراني والامتثال الرقمي وإدارة المخاطر. كما تستعين بالمنهج التحليلي في ربط هذه الأدبيات بمباحث البحث، بحيث تكون الدراسات السابقة جزءاً من بناء المعالجة لا مجرد عرض منفصل. أما منهجية الكتابة فتقوم على الانتقال من الإطار المفاهيمي إلى مظاهر المخاطر ثم إلى متطلبات الحماية والامتثال. وهذا التدرج مقصود؛ لأن الحكم على آليات الحماية لا يكتمل إلا بعد فهم طبيعة الابتكار ومظاهر الخطر التي ينتجها أو يعمقها.

الدراسات السابقة

دراسة حشمان (٢٠٢٤) بعنوان «المخاطر السيبرانية في الصناعة المالية الإسلامية»: هدفت الدراسة إلى تسليط الضوء على المخاطر السيبرانية التي تواجه الصناعة المالية الإسلامية، وبيان ممارسات الأمن السيبراني التي تعتمد عليها المؤسسات المالية الإسلامية. وخلصت إلى أن المخاطر السيبرانية أصبحت أحد مهددات الثقة والاستقرار، وأن ضعف الوعي الأمني والاعتماد على الأنظمة الرقمية يزيدان من احتمالات التعرض للاختراق. وأوصت الدراسة بتعزيز الحوكمة السيبرانية، وتطوير التدريب، وربط الأمن السيبراني بإدارة المخاطر المؤسسية.



دراسة كعموش (٢٠٢٤) بعنوان «أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرين في أسهمها»: هدفت الدراسة إلى اختبار أثر الإفصاح عن إدارة مخاطر الأمن السيبراني في أحكام العملاء والمستثمرين. وخلصت إلى أن الإفصاح المنظم عن مخاطر الأمن السيبراني يعزز تقييم أصحاب المصلحة لقدرة البنك على إدارة المخاطر. وأوصت بتطوير الإفصاح السيبراني وربطه بتقارير الحوكمة وإدارة المخاطر.

دراسة مشاركة (٢٠٢٤) بعنوان «دور التكنولوجيا المالية في تحمل البنوك التجارية للمخاطر من خلال دور الكفاءة البنكية»: هدفت الرسالة إلى تحليل دور التكنولوجيا المالية في قدرة البنوك التجارية على تحمل المخاطر في ضوء الكفاءة البنكية. وخلصت إلى أن أثر التكنولوجيا المالية لا يظهر بمعزل عن كفاءة العمليات والإدارة، وأن التوسع الرقمي يحتاج إلى قدرة مؤسسية لضبط المخاطر. وأوصت بتطوير البنية التقنية وتعزيز الرقابة الداخلية قبل التوسع في الخدمات الرقمية.

دراسة حشروف (٢٠٢٥) بعنوان «تحديات واستراتيجيات الأمن السيبراني في البنوك الجزائرية»: هدفت الدراسة إلى بيان التحديات التي تواجه البنوك الجزائرية في مجال الأمن السيبراني في ظل التحول الرقمي. وخلصت إلى أن البنوك تحتاج إلى استراتيجية أمنية متكاملة تتضمن الوقاية والاستجابة والتوعية. وأوصت بتطوير التشريعات، وتكثيف التدريب، واعتماد اختبارات دورية للجاهزية السيبرانية.

دراسة السقاط (٢٠٢٥) بعنوان «تأثير الذكاء الاصطناعي على إدارة المخاطر في البنوك السعودية»: هدفت الدراسة إلى تحليل مدى تبني البنوك للذكاء الاصطناعي في إدارة المخاطر وتقييم أثره في تحسين الاستراتيجيات الرقابية. وخلصت إلى أن الذكاء الاصطناعي يساهم في كشف الاحتيال وتحسين التنبؤ بالمخاطر، لكنه يثير تحديات تتعلق بجودة البيانات والتحيز وقابلية التفسير. وأوصت بوضع ضوابط لاستخدام الذكاء الاصطناعي وربطه بالرقابة البشرية.

دراسة موساوي (٢٠٢٥) بعنوان «دور التكنولوجيا المالية الإسلامية

في تحسين الخدمات المصرفية»: هدفت الدراسة إلى بيان مساهمة التكنولوجيا المالية الإسلامية في تطوير جودة الخدمات المصرفية. وخلصت إلى أن التكنولوجيا المالية تعزز سرعة الخدمة وتنوعها، لكنها تحتاج إلى ضوابط أمثال وحوكمة حتى لا تفقد خصوصية الخدمة المالية الإسلامية. وأوصت بتطوير منصات رقمية متوافقة مع الضوابط الشرعية والرقابية.

دراسة بوخزر (٢٠٢٤) بعنوان «أهمية اعتماد تقنية البلوك تشين في تعزيز الأمن السيرياني في القطاع المصرفي»: هدفت الدراسة إلى إبراز إمكانات البلوك تشين في دعم أمن البيانات والمعاملات المصرفية. وخلصت إلى أن هذه التقنية قد تعزز الشفافية وسلامة السجلات، لكنها لا تلغي الحاجة إلى حوكمة المفاتيح الرقمية وحماية الخصوصية. وأوصت باعتماد تدريجي للتقنية ضمن أطر اختبار ورقابة واضحة.

دراسة بن عيسى (٢٠٢٥) بعنوان «تقييم تأثير التكنولوجيا المالية على النظام المالي العالمي»: هدفت الدراسة إلى تحليل أثر التكنولوجيا المالية في النظام المالي العالمي، مع التركيز على المخاطر السيريانية والخصوصية والطبيعة العابرة للحدود للمعاملات الرقمية. وخلصت إلى أن التكنولوجيا المالية تعزز الكفاءة لكنها توسع نطاق المخاطر النظامية. وأوصت بتعميق التعاون الرقابي الدولي.

دراسة غريب (٢٠٢٥) بعنوان «أثر استخدام التكنولوجيا المالية على تخفيض تكلفة الخدمات المصرفية: دراسة ميدانية»: هدفت الدراسة إلى اختبار أثر التكنولوجيا المالية في خفض تكلفة الخدمات المصرفية. وخلصت إلى أن التطبيقات الرقمية قد تسهم في تخفيض التكاليف وتحسين الكفاءة، غير أن ذلك مشروط بجاهزية البنية التحتية وقدرة العملاء على الاستخدام. وأوصت بتطوير الوعي الرقمي وتحسين أمن القنوات الإلكترونية.

دراسة الخوالدة (٢٠٢٥) بعنوان «أثر التكنولوجيا المالية في جودة الخدمات المصرفية: الدور الوسيط للشمول المالي في البنوك الإسلامية الأردنية»: هدفت الرسالة إلى دراسة أثر التكنولوجيا المالية



في جودة الخدمات المصرفية في البنوك الإسلامية الأردنية من خلال الشمول المالي. وخلصت إلى أن التكنولوجيا المالية تؤثر في جودة الخدمة وتعزيز الوصول، لكن الجودة لا تكتمل دون ثقة وأمان ووضوح. وأوصت بتوسيع الخدمات الرقمية الآمنة وتحسين الثقافة المالية للعملاء.

دراسة World Bank (٢٠٢٢) بعنوان «Fintech and the Future of Finance: Market and Policy Implications»: هدف التقرير إلى تحليل آثار التكنولوجيا المالية في الأسواق والسياسات المالية. وخلص إلى أن التكنولوجيا المالية تفتح فرصاً للشمول والمنافسة، لكنها تفرض تحديات في حماية المستهلك والبيانات والاستقرار المالي. وأوصى ببناء أطر تنظيمية مرنة قائمة على المخاطر.

دراسة Basel Committee (٢٠٢٤) بعنوان «Digitalisation of Finance»: ركز التقرير على آثار الرقمنة في البنوك والإشراف المصرفي. وخلص إلى أن الرقمنة تعيد تشكيل نماذج الأعمال والمخاطر التشغيلية والطرف الثالث. وأوصى بتعزيز الإشراف القائم على المخاطر وتطوير قدرات الرقابة على الابتكار الرقمي.

دراسة Javaheri et al. (٢٠٢٣) بعنوان «Cybersecurity threats in FinTech: A systematic review»: هدفت الدراسة إلى مراجعة منهجية للتهديدات السيبرانية في التكنولوجيا المالية. وخلصت إلى أن التصيد والبرمجيات الخبيثة وهجمات الفدية وتسرب البيانات من أكثر التهديدات تكراراً. وأوصت بتكامل أدوات الأمن السيبراني مع حوكمة المؤسسات ومراقبة الامتثال.

دراسة Waliullah et al. (٢٠٢٥) بعنوان «Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking»: هدفت الدراسة إلى تحليل أثر التهديدات السيبرانية في تبني ونمو الخدمات المصرفية الرقمية. وخلصت إلى أن الهجمات السيبرانية تخفض الثقة وتبطئ التبني، وأن المصادقة متعددة العوامل والذكاء الاصطناعي في كشف الاحتيال يعززان الأمان. وأوصت بتقوية الأطر الرقابية والتوعية الرقمية.

الفجوة البحثية

يتضح من الدراسات السابقة أن جزءا كبيرا من الأدبيات العربية تناول التكنولوجيا المالية من زاوية أثرها في جودة الخدمات أو تخفيض التكلفة أو الشمول المالي، بينما تناول جزء آخر الأمن السيبراني بوصفه موضوعا فنيا أو محاسبيا أو مصرفيا مستقلا. أما الأدبيات الأجنبية فقد ركزت بصورة أكبر على الرقمنة، ومخاطر الطرف الثالث، والمرونة التشغيلية، وحماية البيانات، وأثر التهديدات السيبرانية في تبني الخدمات الرقمية.

وتظهر الفجوة البحثية في أن الربط المنهجي بين سرعة الابتكار المالي الرقمي ومتطلبات الحماية والامتثال ما زال بحاجة إلى معالجة شاملة تجمع بين الجوانب التشغيلية والسيبرانية والتنظيمية والسلوكية. فكثير من الدراسات تقيس أثرا محددا أو تتناول خطرا منفردا، بينما تحتاج المؤسسات المالية إلى إطار يبين كيف تتداخل المخاطر عند إطلاق خدمة رقمية واحدة، وكيف يمكن بناء حماية منذ التصميم لا بعد وقوع المشكلة.

ومن هنا تتميز الدراسة الحالية بأنها لا تنظر إلى التكنولوجيا المالية بوصفها منفعة أو خطرا بصورة منفصلة، بل تعالجها ضمن علاقة توازن: ابتكار مطلوب للمنافسة والشمول، وحماية لازمة للثقة، وامتثال ضروري للاستقرار. وبذلك تسعى الدراسة إلى توظيف الدراسات السابقة في بناء معالجة منهجية للمباحث الثلاثة: الإطار المفاهيمي، ومظاهر المخاطر، ومتطلبات الحماية والامتثال.

المبحث الأول:

الإطار المفاهيمي للتكنولوجيا المالية والمخاطر المالية الحديثة

يمهد هذا المبحث لفهم الأساس الذي يقوم عليه البحث؛ لأن معالجة مخاطر التكنولوجيا المالية لا تستقيم قبل بيان مفهوم التكنولوجيا المالية وخصائصها، وتحديد طبيعة المخاطر المالية الحديثة، وفهم العلاقة بين سرعة الابتكار وتسارع ظهور المخاطر. فالبيئة الرقمية لا تضيف أدوات جديدة فحسب، بل تعيد ترتيب العلاقة بين المؤسسة والعميل والجهة الرقابية والطرف الثالث.

المطلب الأول: مفهوم التكنولوجيا المالية وخصائصها في البيئة المالية المعاصرة

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال.

يقصد بالتكنولوجيا المالية توظيف التقنيات الرقمية في تصميم وتقديم وإدارة الخدمات المالية، بما يشمل المدفوعات الرقمية، والمحافظ الإلكترونية، والتمويل الجماعي، والائتمان الرقمي، والخدمات المصرفية المفتوحة، والذكاء الاصطناعي، وسلاسل الكتل، والتحقق الرقمي من الهوية. ويظهر جوهر هذا المفهوم في أن التقنية لا تستعمل كأداة مساعدة فقط، بل تصبح جزءاً من نموذج العمل المالي نفسه (World Bank, ٢٠٢٢).

وتتميز التكنولوجيا المالية بسرعة الوصول إلى العميل وانخفاض الحاجز المكاني والزمني، إذ يستطيع العميل تنفيذ عملية مالية من

هاتفه دون زيارة الفرع. وهذه الخاصية تجعل الخدمة أكثر كفاءة وشمولا، لكنها تزيد في الوقت ذاته الحاجة إلى التحقق الرقمي، وحماية الحسابات، وتوعية المستخدم، لأن سهولة الوصول قد يستفيد منها العميل كما قد يستغلها المحتال (غريب، ٢٠٢٥). ومن خصائص التكنولوجيا المالية أنها تعتمد على البيانات بوصفها أصلا اقتصاديا. فالمنصة الرقمية لا تقدم الخدمة فقط، بل تجمع بيانات عن السلوك والتفضيلات والموقع والقدرة المالية. ولذلك أصبحت إدارة البيانات جزءا من إدارة المخاطر، لأن سوء استخدامها أو تسريبها قد يؤدي إلى ضرر مالي وقانوني وسمعي للمؤسسة (OECD، ٢٠٢٥).

وتتسم التكنولوجيا المالية كذلك بالترابط بين أطراف متعددة. فقد لا تقدم المؤسسة المالية الخدمة وحدها، بل تشترك معها شركات دفع ومزودون سحابيون وشركات تحقق رقمي ومطورون خارجيون. وهذا الترابط يوسع مجال الابتكار، لكنه يجعل إدارة المخاطر أكثر تعقيدا؛ لأن ضعف طرف واحد قد يؤثر في سلسلة الخدمة كاملة (Basel Committee، ٢٠٢٤).

وتظهر الخصوصية المعاصرة للتكنولوجيا المالية في أنها لا تكتفي برقمنة الخدمة التقليدية، بل قد تنشئ خدمة جديدة بالكامل؛ فالتمويل عبر المنصات، والائتمان القائم على الخوارزميات، والدفع الفوري، والخدمات المصرفية المفتوحة، كلها نماذج لا يمكن فهمها بالمنطق الورقي القديم. ولذلك فإن الرقابة عليها تحتاج إلى أدوات فنية وتنظيمية حديثة (بن عيسى، ٢٠٢٥).

ومن الناحية المالية، أسهمت التكنولوجيا المالية في تحسين المنافسة وتوسيع الشمول المالي، خاصة للفئات التي يصعب وصولها إلى الفروع التقليدية. إلا أن الشمول المالي الرقمي لا يعني مجرد فتح حساب أو تنزيل تطبيق، بل يعني قدرة العميل على استخدام الخدمة بأمان وفهم ووعي، حتى لا يتحول الوصول السهل إلى مديونية أو تعرض للاحتيال (عويسي، ٢٠٢٥).

وتشير الأدبيات الحديثة إلى أن المؤسسات المالية التي تنجح في



التكنولوجيا المالية هي التي تجمع بين الابتكار والحوكمة؛ فالسرعة وحدها لا تكفي، والتطبيق الجيد لا يعوض ضعف الحماية، والمنتج المبتكر لا يستدام إذا لم يكن واضحا ومفهوما ومحميا. ومن هنا يظهر أن مفهوم التكنولوجيا المالية يتضمن بعدا إداريا وتنظيميا إلى جانب بعده التقني (BIS, ٢٠٢٤).

المطلب الثاني: طبيعة المخاطر المالية الحديثة في ظل التحول الرقمي

يمثل هذا المطلب جزءا من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستمت المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال.

المخاطر المالية الحديثة في ظل التحول الرقمي لا تلغي المخاطر التقليدية، لكنها تعيد تشكيلها وتضيف إليها مصادر جديدة. فمخاطر الائتمان والسيولة والسوق والتشغيل ما زالت قائمة، غير أن البيئة الرقمية تجعلها أسرع انتقالا وأكثر ارتباطا بالبيانات والأنظمة والأطراف الخارجية (صندوق النقد العربي، ٢٠٢٣).

وتعد المخاطر التشغيلية الرقمية من أبرز هذه المخاطر؛ لأنها تتعلق بقدرة الأنظمة على العمل المستمر، ودقة البرمجيات، وسلامة قواعد البيانات، واستجابة المؤسسة للتعطّل. ففي الخدمات الرقمية، قد يؤدي خلل قصير إلى تعطيل آلاف المعاملات، وقد يتحول الخطأ البرمجي إلى أثر مالي واسع إذا لمس الأرصدة أو الرسوم أو صلاحيات الدخول (European Banking Authority, ٢٠٢٥).

أما المخاطر السيبرانية فتتجاوز مفهوم الاختراق البسيط إلى منظومة واسعة تشمل التصيد، والبرمجيات الخبيثة، وهجمات الفدية، وانتحال الهوية، وتسرب البيانات، والتلاعب بالمعاملات. وتزداد خطورتها في القطاع المالي لأنها تمس المال والبيانات والثقة معا، ولذلك أصبحت

جزءاً من إدارة الاستقرار المالي لا شأنًا فنياً داخلياً (حشمان، ٢٠٢٤). وتتصل المخاطر الحديثة كذلك بالبيانات والخصوصية؛ إذ أصبح جمع البيانات وتحليلها وتبادلها من أساسيات الخدمة الرقمية. وكلما توسعت المؤسسات في استخدام البيانات، زاد احتمال الخطأ في التصنيف، أو الاستخدام غير المشروع، أو مشاركة البيانات مع طرف ثالث دون موافقة كافية، مما يخلق مخاطر قانونية وأخلاقية ورقابية (Adegbite، ٢٠٢٥).

ومن المخاطر الحديثة مخاطر الاحتيال الرقمي، حيث يستغل المحتالون السرعة والثقة في الواجهة الرقمية لإيهام العميل أو الموظف بإجراء تحويل أو إفشاء رمز تحقق أو تحميل ملف خبيث. ومع تطور أدوات الذكاء الاصطناعي أصبحت عمليات الاحتيال أكثر دقة وقدرة على تقليد اللغة والصوت والصورة (اتحاد المصارف العربية، ٢٠٢٤). وتظهر كذلك مخاطر الامتثال عندما لا تستطيع المؤسسة إثبات التزامها بمتطلبات مكافحة غسل الأموال وتمويل الإرهاب، وحماية المستهلك، والإفصاح، وحماية البيانات، خاصة في الخدمات الفورية والعابرة للحدود. فالامتثال في البيئة الرقمية يحتاج إلى سجلات دقيقة، ومراقبة لحظية، وربط بين التقنية والقانون وإدارة المخاطر (IMF، ٢٠٢٤).

وبذلك يمكن القول إن طبيعة المخاطر الحديثة تتسم بالتداخل والسرعة والانتشار. فهي لا تقف عند إدارة واحدة، ولا تعالج بأداة واحدة، بل تحتاج إلى إطار مؤسسي يشترك فيه مجلس الإدارة، وإدارة المخاطر، والامتثال، وتقنية المعلومات، وخدمة العملاء، والجهة الرقابية (مشاركة، ٢٠٢٤).



المطلب الثالث: العلاقة بين الابتكار المالي وتسارع ظهور المخاطر

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامثال.

العلاقة بين الابتكار المالي والمخاطر علاقة مركبة؛ فكل ابتكار يفتح فرصة جديدة، لكنه في الوقت نفسه يفتح مجالاً جديداً للخطأ أو الاستغلال أو سوء الفهم. وعندما تكون الخدمة مالية ورقمية وسريعة، فإن الفاصل بين التجربة الناجحة والحادث المؤثر قد يكون قصيراً جداً (World Bank, ٢٠٢٢).

وتسارع الابتكار يؤدي إلى تسارع المخاطر بسبب اختصار دورة تطوير الخدمة. فالمؤسسة قد تنتقل من الفكرة إلى الإطلاق خلال مدة قصيرة، بينما تحتاج اختبارات الأمان والامثال وتجربة المستخدم إلى وقت وجهد. وإذا لم تدخل هذه الاختبارات منذ البداية، فقد تظهر الثغرات بعد وصول الخدمة إلى عدد كبير من العملاء (حشروف، ٢٠٢٥).

ومن أسباب تسارع المخاطر أثر الشبكة؛ فكلما زاد عدد المستخدمين والشركاء والواجهات المتصلة، زادت قيمة الخدمة، لكنها أصبحت أكثر حساسية للفشل. فإذا تعرض مزود مركزي للاختراق أو التعطل، فقد ينتقل الأثر إلى عدد واسع من المؤسسات والعملاء، مما يجعل الخطر التشغيلي الرقمي ذا بعد نظامي (Federal Reserve Board, ٢٠٢٥).

وتتسارع المخاطر أيضاً عندما يسبق الابتكار اللغة القانونية والتنظيمية. فقد تظهر نماذج عمل جديدة لا تنطبق عليها القواعد القديمة بصورة واضحة، فينشأ غموض حول الترخيص والمسؤولية وحماية العميل والبيانات. ولذلك اتجهت بعض الجهات الرقابية إلى



المختبرات التنظيمية والاختبار المحدود لتقليل الفجوة بين الابتكار والتنظيم (Gaviyau, ٢٠٢٥).

وقد يؤدي ضغط المنافسة إلى إطلاق حملات تسويقية تركز على السرعة والسهولة وقلّة التكلفة، دون توضيح كاف للمخاطر والرسوم وحدود المسؤولية. وفي هذه الحالة لا يكون الخطر تقنياً فقط، بل يتصل بالإفصاح وعدالة التعامل مع العميل. لذلك تعد الشفافية جزءاً من إدارة مخاطر الابتكار (كعموش، ٢٠٢٤).

ولا تعني هذه العلاقة أن الابتكار ينبغي أن يتباطأ دائماً، بل تعني أن الابتكار المسؤول هو الذي يجعل الحماية والامتثال جزءاً من التصميم. فالمنتج الرقمي الآمن لا يضاف إليه الأمن لاحقاً، بل يبنى على افتراضات واضحة حول الهوية والبيانات والصلاحيات والاستجابة للحوادث والرقابة الداخلية (Basel Committee, ٢٠٢٤).

المبحث الثاني:

مظاهر المخاطر المرتبطة بالتكنولوجيا المالية

بعد بيان المفهوم وطبيعة المخاطر، ينتقل هذا المبحث إلى تحليل المظاهر العملية للمخاطر المرتبطة بالتكنولوجيا المالية. وتكمن أهمية هذا التصنيف في أنه يساعد المؤسسة المالية على توزيع المسؤوليات وتحديد أدوات المعالجة. فالمخاطر لا تظهر دائما في صورة واحدة، بل تتداخل بين التشغيل والتقنية والأمن السيبراني والامتثال وحماية البيانات.

المطلب الأول: المخاطر التشغيلية والتقنية في تطبيقات التكنولوجيا المالية

يمثل هذا المطلب جزءا من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال.

تعد المخاطر التشغيلية والتقنية نقطة البداية في فهم مخاطر التكنولوجيا المالية؛ لأن الخدمة الرقمية تقوم على أنظمة وبرمجيات وشبكات وقواعد بيانات وتكامل بين منصات متعددة. فإذا اختل أحد هذه المكونات، فقد تتأثر الخدمة كاملة، خاصة في المدفوعات الفورية والمحافظ الإلكترونية والخدمات المصرفية عبر الهاتف (European Banking Authority, ٢٠٢٥).

ومن أبرز مظاهر هذه المخاطر تعطل الأنظمة. فالتوقف قد ينتج عن ضغط مرتفع، أو تحديث غير مختبر، أو فشل في الخادم، أو خطأ في الربط بين الأنظمة. ولا تقاس خطورة التعطل بمدته فقط، بل بعدد العملاء المتأثرين، وحجم المعاملات، ودرجة حساسية الخدمة، وطريقة التواصل مع العملاء وقت الحادث (مشاركة، ٢٠٢٤).

وتظهر مخاطر البرمجيات عندما تطلق المؤسسة تحديثا يحتوي خلافا، أو تعتمد على شيفرة غير آمنة، أو تفتح واجهات برمجة دون اختبار كاف. وقد يكون الخطأ الفني محدودا، لكنه يصبح ماليا خطيرا إذا أدى إلى احتساب رسوم خاطئة أو منح صلاحيات غير صحيحة أو تنفيذ معاملات مكررة (Basel Committee, ٢٠٢٤).

ومن المخاطر التقنية ضعف البنية التحتية الرقمية، خاصة إذا توسعت المؤسسة في التطبيقات والمنصات دون استثمار كاف في السعة والنسخ الاحتياطي والمرونة. فالتطبيق الجذاب لا يكفي إذا كانت البنية الخلفية عاجزة عن تحمل الطلب أو التعافي السريع من التعطل (غريب، ٢٠٢٥).

وتبرز مخاطر الطرف الثالث في اعتماد المؤسسة على مزودين خارجيين في السحابة أو الدفع أو التحقق الرقمي أو الذكاء الاصطناعي. وقد تكون المؤسسة أمام العميل هي المسؤولة عن الخدمة، رغم أن الخلل وقع لدى المزود. لذلك يتطلب الاعتماد على الطرف الثالث تقييما مسبقا، ومراقبة مستمرة، واتفاقيات واضحة للمسؤولية، وخطط خروج بديلة (World Bank, ٢٠٢٢).

وتتعلق مخاطر استمرارية الأعمال بقدرة المؤسسة على العمل أثناء الحوادث وبعدها. فالخطة المكتوبة لا تكفي إذا لم تختبر دوريا. وينبغي تحديد الزمن المقبول للتوقف، وحجم البيانات المقبول فقده، ومسارات الاتصال البديلة، وآليات تعويض العملاء عند الضرر. وهذا ما جعل المرونة التشغيلية محورا رئيسا في الرقابة الحديثة (Federal Reserve Board, ٢٠٢٥).

وتؤكد هذه المخاطر أن إدارة التقنية ليست مسألة تشغيلية بسيطة، بل هي جزء من إدارة المخاطر المالية. فالمؤسسة التي تفصل بين الابتكار والتشغيل والحماية قد تطلق خدمة جذابة لكنها هشة، بينما المؤسسة الرشيدة تجعل اختبار الأنظمة والمرونة والتوثيق جزءا من دورة حياة المنتج الرقمي (صندوق النقد العربي، ٢٠٢٣).

المطلب الثاني: المخاطر السيبرانية وحماية البيانات المالية

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستنتم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامثال.

المخاطر السيبرانية هي أكثر مظاهر مخاطر التكنولوجيا المالية وضوحاً؛ لأنها تمس المال والبيانات والسمعة في وقت واحد. فالاختراق قد يؤدي إلى تحويل أموال، أو تسريب معلومات، أو تشفير بيانات، أو تعطيل خدمة، أو ابتزاز مؤسسة، أو خداع العملاء عبر قنوات مزيفة (Javaheri et al, ٢٠٢٣).

وتبدأ كثير من الهجمات من الإنسان قبل النظام، من خلال التصيد والهندسة الاجتماعية وانتحال الهوية. فقد يرسل المهاجم رسالة تبدو صادرة من البنك، أو يتصل بالعميل طالباً رمز التحقق، أو يخدع الموظف بملف مرفق. ولذلك لا تكفي الجدران النارية إذا كان الوعي الأمني لدى العميل والعاملين ضعيفاً (اتحاد المصارف العربية، ٢٠٢٤). وتعد هجمات الفدية من التهديدات الخطيرة، لأنها لا تعطل البيانات فقط، بل قد تهدد بنشرها. وفي المؤسسات المالية يكون أثرها مضاعفاً؛ لأن توقف الخدمة قد يؤثر في المدفوعات والرواتب والالتزامات اليومية للعملاء. لذلك تحتاج المؤسسات إلى نسخ احتياطية معزولة، واختبارات استعادة، وسيناريوهات استجابة واضحة (Waliullah et al, ٢٠٢٥).

أما حماية البيانات المالية فتتطلب النظر إلى دورة حياة البيانات كاملة: الجمع، والتحقق، والاستخدام، والمشاركة، والتخزين، والحذف. وفي كل مرحلة توجد مخاطر تتعلق بالصلاحيات، أو التشفير، أو الاستخدام الزائد، أو الاحتفاظ غير المبرر، أو مشاركة البيانات مع طرف ثالث دون موافقة كافية (Adegbite, ٢٠٢٥).

وتزداد أهمية الخصوصية مع الخدمات المصرفية المفتوحة وواجهات

البرمجة، حيث يسمح العميل بمشاركة بياناته مع جهات أخرى. وهذه البيئة قد تعزز المنافسة والابتكار، لكنها تحتاج إلى موافقة واضحة، وصلاحيات محددة، وإمكانية إلغاء التفويض، وتحديد المسؤولية عند التسرب أو سوء الاستخدام (OECD، ٢٠٢٥). وتظهر أهمية الذكاء الاصطناعي في كشف الاحتيال وتحليل الأنماط غير المعتادة، لكنه في المقابل قد ينشئ مخاطر جديدة مثل التحيز، وضعف القابلية للتفسير، والاعتماد على بيانات غير دقيقة. ولذلك ينبغي أن يخضع استخدام الذكاء الاصطناعي في إدارة المخاطر لضوابط جودة البيانات والرقابة البشرية (السقاط، ٢٠٢٥). ومن الأدوات المهمة للحماية المصادقة متعددة العوامل، والتشفير، وإدارة الصلاحيات، والمراقبة اللحظية، واختبارات الاختراق، والتوعية المستمرة. غير أن هذه الأدوات يجب أن تعمل ضمن ثقافة مؤسسية تجعل الأمن مسؤولية الجميع، لا مسؤولية إدارة تقنية المعلومات وحدها (حشروف، ٢٠٢٥).

المطلب الثالث: مخاطر الامتثال والرقابة في البيئة المالية الرقمية

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك سيتم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال.

تظهر مخاطر الامتثال عندما تطلق المؤسسة خدمة رقمية دون قدرة كافية على إثبات الالتزام بالقوانين والتعليمات والمعايير. وفي التكنولوجيا المالية، تتسع هذه المخاطر بسبب سرعة المعاملات، وتعدد الأطراف، وكثافة البيانات، والطابع العابر للحدود (IMF، ٢٠٢٤). ومن أبرز مخاطر الامتثال تحديات مكافحة غسل الأموال وتمويل الإرهاب. فالمنصات الرقمية تسمح بفتح حسابات عن بعد، وتحويل



مبالغ صغيرة ومتكررة، واستخدام محافظ متعددة، والتنقل بين منصات مختلفة. وهذا يتطلب تحقق هوية قوي، ومراقبة سلوكية، وتحليلاً للأنماط غير المعتادة (البنك المركزي الأردني، ٢٠٢٥).

وتظهر مخاطر حماية المستهلك عندما لا يفهم العميل طبيعة الخدمة أو رسومها أو حدود الحماية أو إجراءات الاعتراض. فقد يظن أن كل عملية رقمية يمكن استرجاعها بسهولة، أو أن كل منصة مرخصة، أو أن كل إعلان رقمي آمن. لذلك ينبغي أن يكون الإفصاح واضحاً ومختصراً وفي وقت القرار (كعموش، ٢٠٢٤).

وتتصل مخاطر الامتثال بالخصوصية أيضاً؛ فقد تكون الخدمة صحيحة من حيث الترخيص لكنها تخالف قواعد استخدام البيانات أو التسويق أو المشاركة مع الأطراف الثالثة. ومع الذكاء الاصطناعي، قد تنشأ مخاطر إضافية إذا اتخذت الخوارزمية قرارات تمس العميل دون تفسير كاف أو آلية اعتراض فعالة (Bank of England، ٢٠٢٥).

وتبرز مشكلة الرقابة العابرة للحدود عندما يكون العميل في دولة، والمزود في دولة، والخادم في دولة ثالثة، والدفع عبر شبكة عالمية. في هذه الحالة تتعدد مسائل القانون الواجب التطبيق، وتبادل المعلومات، وتنفيذ العقوبات، وحماية العميل المحلي (بن عيسى، ٢٠٢٥).

ومن مظاهر المخاطر التنظيمية أن بعض الخدمات قد تقع في منطقة رمادية بين القطاع المصرفي وشركات التقنية، مما يخلق غموضاً في الترخيص والمسؤولية. وهنا تظهر أهمية التنظيم المرن القائم على المخاطر، بحيث لا يخنق الابتكار ولا يتركه بلا ضوابط (Gaviyau، ٢٠٢٥).

وتؤكد هذه المخاطر أن الامتثال في التكنولوجيا المالية يجب أن يكون أمثالاً رقمياً مدمجاً داخل النظام. فالتحقق، والإفصاح، وتسجيل الموافقات، ومراقبة المعاملات، وإدارة الشكاوى، ينبغي أن تكون جزءاً من رحلة العميل، لا إجراءات لاحقة منفصلة (OECD، ٢٠٢٥).

المبحث الثالث:

متطلبات الحماية والامتثال في مواجهة مخاطر التكنولوجيا المالية

يمثل هذا المبحث الجانب التطبيقي الحاكم للبحث؛ إذ لا يكفي تشخيص المخاطر دون بيان متطلبات الحماية والامتثال. فالهدف ليس إبطاء الابتكار، بل جعله أكثر أماناً واستدامة من خلال الحوكمة الرقمية، ودور الجهات الرقابية، وآليات بناء الثقة في الخدمات المالية الرقمية.

المطلب الأول: الحوكمة الرقمية كمدخل لضبط مخاطر التكنولوجيا المالية

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك ستنتم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال (obaod&t, ٢٠٢٣).

الحوكمة الرقمية هي الإطار الذي يحدد من يملك قرار الابتكار، ومن يراجع المخاطر، ومن يوافق على الإطلاق، ومن يتحمل المسؤولية عند الخلل. ومن دون هذا الإطار قد تتحول التكنولوجيا المالية إلى مبادرات متفرقة تقودها الحماسة التسويقية أو التقنية دون تقدير كاف للمخاطر (Basel Committee, ٢٠٢٤).

وتبدأ الحوكمة الرقمية من مجلس الإدارة والإدارة العليا؛ لأن المخاطر الرقمية قد تهدد الاستقرار والسمعة والامتثال. لذلك ينبغي أن لا تبقى القرارات التقنية في مستوى تشغيلي ضيق، بل يجب أن ترتبط باستراتيجية المؤسسة وشهيتها للمخاطر وقدرتها على التعافي (Federal Reserve Board, ٢٠٢٥).

ومن متطلبات الحوكمة تحديد المسؤوليات بين إدارة التقنية، وإدارة المخاطر، والامتثال، والتدقيق الداخلي، والأعمال. فالابتكار الرقمي لا



ينجح إذا صممه إدارة واحدة بمعزل عن الأخرى. وينبغي أن تتداخل هذه الوظائف منذ مرحلة الفكرة حتى الإطلاق والمتابعة (مشاركة، ٢٠٢٤).

وتتطلب الحوكمة الرقمية إدارة واضحة للطرف الثالث، تشمل التقييم السابق للتعاقد، وفحص الأمن والامتثال، ومراقبة الأداء، وحق التدقيق، وخطط الخروج. فالاعتماد على مزود خارجي لا ينقل المسؤولية الرقابية عن المؤسسة المالية، بل يضيف إليها واجبا في الرقابة والمتابعة (European Banking Authority، ٢٠٢٥).

ومن عناصر الحوكمة كذلك إدارة البيانات؛ إذ يجب تحديد من يملك البيانات، ومن يصل إليها، ولأي غرض تستخدم، وكم مدة الاحتفاظ بها، وكيف تحذف أو تشارك. ولا يمكن حماية العميل إذا بقيت البيانات متاحة بلا ضوابط أو استعملت لأغراض تسويقية لا يعلمها المستخدم (OECD، ٢٠٢٥).

كما تحتاج الحوكمة الرقمية إلى مؤشرات قياس واضحة، مثل عدد الحوادث، وزمن التعطل، وزمن الاستجابة، ومعدل الشكاوى الرقمية، ونتائج اختبارات الاختراق، ومؤشرات الاحتيال. فالحوكمة لا تكون فعالة إذا بقيت شعارات عامة، بل يجب أن تترجم إلى مؤشرات وتقارير ومساءلة (حشمان، ٢٠٢٤).

وبذلك تصبح الحوكمة الرقمية مدخلا لضبط العلاقة بين الابتكار والمخاطر. فهي لا تمنع المؤسسة من التطوير، لكنها تلزمها بأن تسأل قبل الإطلاق: هل الخدمة آمنة؟ هل الامتثال مدمج؟ هل البيانات محمية؟ هل العميل يفهم؟ هل توجد خطة عند التعطل؟ وهذه الأسئلة هي جوهر الابتكار المسؤول (صندوق النقد العربي، ٢٠٢٣).

المطلب الثاني: دور الجهات الرقابية في تحقيق التوازن بين الابتكار والحماية

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك سستتم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامثال.

تلعب الجهات الرقابية دوراً محورياً في تحقيق التوازن بين الابتكار والحماية؛ فهي مطالبة بتشجيع التطوير المالي وخفض عوائق الدخول، لكنها مطالبة في الوقت نفسه بحماية الاستقرار المالي والمستهلك والبيانات. ولذلك لم تعد الرقابة الحديثة تكتفي بالتفتيش التقليدي، بل تحتاج إلى فهم تقني وتنظيمي متقدم (IMF, ٢٠٢٤).

ومن أدوات الجهات الرقابية المختبرات التنظيمية، التي تسمح باختبار خدمات جديدة في نطاق محدود وتحت إشراف مباشر. وتساعد هذه المختبرات على فهم المخاطر قبل التوسع، كما تمنح المبتكرين فرصة للتجربة دون تعريض النظام المالي كله لخطر غير محسوب (Gaviyau, ٢٠٢٥).

وتظهر أهمية الترخيص المرحلي أو القائم على النشاط، بحيث لا تخضع كل الشركات لنموذج واحد، بل تنظم بحسب طبيعة الخدمة وحجم المخاطر. فشركة دفع صغيرة لا تشبه بنكا شاملا، ومنصة تمويل جماعي تختلف عن مزود بيانات، لكن الجميع يحتاج إلى حد أدنى من الحماية والشفافية (World Bank, ٢٠٢٢).

وتتطلب الرقابة الفعالة بناء قدرات داخل الجهات الرقابية نفسها، من خلال فرق متخصصة في الأمن السيبراني، وتحليل البيانات، والذكاء الاصطناعي، ومخاطر الطرف الثالث. فالجهة التي لا تفهم التقنية قد تتجه إما إلى منع مبالغ فيه أو تساهل غير مقصود (البنك المركزي الأردني، ٢٠٢٥).

وتبرز أهمية الرقابة الاحترافية في متابعة أثر التكنولوجيا المالية في

المخاطر النظامية، خاصة عندما تتجمع الخدمات حول مزودين كبار أو منصات مركزية. فإذا اعتمدت مؤسسات كثيرة على مزود واحد، فإن فشل هذا المزود قد يتحول إلى مشكلة تتجاوز مؤسسة بعينها (BIS، ٢٠٢٤).

كما أن حماية المستهلك المالي الرقمي تمثل جزءاً أساسياً من دور الجهات الرقابية، من خلال إلزام المؤسسات بإفصاحات واضحة، وآليات اعتراض سهلة، وحماية للبيانات، ومعالجة عادلة للشكاوى، وتوعية مستمرة بمخاطر الاحتيال الرقمي (اتحاد المصارف العربية، ٢٠٢٤).

ويحتاج التوازن بين الابتكار والحماية إلى تعاون دولي، لأن الخدمات الرقمية لا تقف عند الحدود. ويشمل ذلك تبادل المعلومات حول الحوادث السيبرانية، والتنسيق في مكافحة غسل الأموال، وتطوير معايير مشتركة للهوية الرقمية والخصوصية والإفصاح (OECD، ٢٠٢٥).

المطلب الثالث: آليات الامتثال وبناء الثقة في الخدمات المالية الرقمية

يمثل هذا المطلب جزءاً من البناء المنهجي للبحث؛ لأنه يربط بين التصور النظري والواقع العملي للمؤسسات المالية في بيئة رقمية متغيرة. ولذلك سيتم المعالجة من خلال بيان المفهوم، ثم تحليل المخاطر أو المتطلبات المرتبطة به، ثم إبراز أثر ذلك في الحماية والامتثال.

بناء الثقة في الخدمات المالية الرقمية لا يتحقق بالإعلان عن الأمان، بل بوجود آليات امتثال وحماية يشعر بها العميل وتستطيع المؤسسة إثباتها للجهة الرقابية. فالثقة الرقمية تتكون من تجربة متكررة تؤكد للعميل أن ماله وبياناته وحقوقه محمية (الخوالدة، ٢٠٢٥). ومن أهم آليات الامتثال التحقق الرقمي من الهوية، سواء عبر الوثائق الإلكترونية أو القياسات الحيوية أو الربط مع قواعد رسمية. غير أن

التحقق يجب أن يوازن بين الأمان والخصوصية وسهولة الاستخدام، لأن التعقيد المفرط قد يدفع العميل إلى تجنب القناة الرقمية أو البحث عن طرق أقل أماناً (OECD, ٢٠٢٥).

وتعد المصادقة متعددة العوامل أداة ضرورية، لكنها تحتاج إلى تصميم مناسب لطبيعة العملاء. فليس كل العملاء يمتلكون المعرفة التقنية نفسها، ولا يجوز أن تؤدي الحماية إلى إقصاء فئات معينة. ومن هنا يجب الجمع بين الأمان والتثقيف والدعم الفني السهل (Waliullah et al, ٢٠٢٥).

ومن آليات بناء الثقة الإفصاح الرقمي العادل، أي تقديم المعلومات الجوهرية في الوقت المناسب وبصيغة مفهومة. فلا يكفي إدراج الشروط في ملف طويل، بل ينبغي أن تظهر الرسوم، وحدود المسؤولية، ومخاطر الاحتيال، وطريقة الاعتراض، وبيانات التواصل بوضوح أثناء رحلة العميل (كعموش، ٢٠٢٤).

وتسهم الثقافة المالية الرقمية في تقليل المخاطر؛ لأن العميل الواعي أقل عرضة للتصيد وانتحال الهوية والعروض المضللة. لذلك ينبغي أن لا تقتصر مسؤولية المؤسسة على تقديم الخدمة، بل تشمل توعية العملاء بكيفية حماية رموزهم، والتحقق من الروابط، والإبلاغ عن العمليات المشبوهة (عويسي، ٢٠٢٥).

وتتطلب الثقة كذلك إدارة فعالة للحوادث. فعند وقوع خلل أو اختراق، يجب أن تكون المؤسسة قادرة على الاكتشاف السريع، والاحتواء، والتواصل مع العملاء، والإبلاغ للجهة الرقابية، ومعالجة الأثر. وطريقة إدارة الحادث قد تكون أحياناً أكثر تأثيراً في الثقة من الحادث نفسه (Federal Reserve Board, ٢٠٢٥).

كما ينبغي تطوير آليات امتثال قائمة على التقنية نفسها، مثل مراقبة المعاملات لحظياً، وتحليل السلوك غير المعتاد، وتسجيل الموافقات، وتتبع الوصول إلى البيانات، وأتمتة التنبيهات الرقابية. وهذا النوع من الامتثال يجعل الرقابة جزءاً من النظام لا عبئاً خارجياً عليه (نصير، ٢٠٢٦).

وفي النهاية، فإن الثقة الرقمية تبنى حين يدرك العميل أن المؤسسة



لا تطلب منه استخدام التطبيق لأنه أسرع فحسب، بل لأنها صممت الخدمة بما يحميه، ووضعت له حقوقه، ووفرت له طريقاً سهلاً للسؤال والاعتراض. وبذلك يتحول الامتثال من متطلب قانوني إلى قيمة تنافسية ومصدر استدامة (موساوي، ٢٠٢٥).

الخاتمة

تناول البحث موضوع التكنولوجيا المالية والمخاطر المالية الحديثة من زاوية العلاقة بين سرعة الابتكار ومتطلبات الحماية والامتثال. وقد ظهر من خلال المعالجة أن التكنولوجيا المالية لم تعد مجرد وسيلة مساندة، بل أصبحت بيئة عمل كاملة تعيد تشكيل الخدمة المالية وعلاقة المؤسسة بالعميل والجهة الرقابية والطرف الثالث. كما بين البحث أن المخاطر الحديثة لا تنحصر في الجانب السيبراني، رغم أهميته، بل تشمل التشغيل والتقنية والبيانات والخصوصية والاحتيال والامتثال وحماية المستهلك والرقابة العابرة للحدود. وهذه المخاطر متداخلة بطبيعتها؛ فقد يبدأ الخطر من خلل تقني، ثم يتحول إلى ضرر مالي، ثم إلى مخالفة رقابية، ثم إلى أزمة ثقة. وأكد البحث أن الحل لا يكون في رفض الابتكار أو إبطائه بصورة مطلقة، وإنما في جعله ابتكاراً مسؤولاً، تدخل فيه الحماية والامتثال منذ التصميم. فالمؤسسة المالية التي تدمج الأمن والحوكمة والشفافية في المنتج الرقمي تكون أقدر على المنافسة والاستدامة من مؤسسة تطلق الخدمات بسرعة ثم تعالج آثار الخلل لاحقاً.

النتائج

1. أظهرت الدراسة أن التكنولوجيا المالية توسع نطاق الخدمات المالية وتزيد سرعتها وكفاءتها، لكنها في الوقت نفسه توسع نطاق المخاطر إذا لم تخضع لحوكمة واضحة.
2. تبين أن المخاطر المالية الحديثة تتسم بالتداخل والسرعة والانتشار، ولا يمكن التعامل معها من خلال إدارة تقنية المعلومات وحدها.

3. أثبتت المعالجة أن مخاطر الطرف الثالث أصبحت من أهم مصادر الهشاشة في الخدمات المالية الرقمية بسبب اعتماد المؤسسات على مزودين خارجيين في التشغيل والبيانات والتحقق.
4. خلصت الدراسة إلى أن الأمن السيبراني لم يعد وظيفة فنية منفصلة، بل أصبح جزءاً من إدارة المخاطر المؤسسية والاستقرار المالي.
5. تبين أن حماية البيانات والخصوصية تمثلان محورين أساسيين في بناء الثقة الرقمية، خاصة مع انتشار الخدمات المصرفية المفتوحة وتحليل البيانات.
6. أظهرت الدراسة أن الامتثال الرقمي يجب أن يكون مدمجاً داخل رحلة العميل، لا مجرد مراجعة لاحقة للمعاملات أو النماذج.
7. أكدت الدراسة أن الجهات الرقابية تحتاج إلى أدوات مرنة مثل المختبرات التنظيمية والترخيص القائم على المخاطر حتى تحقق التوازن بين الابتكار والحماية.
8. خلصت الدراسة إلى أن الثقافة المالية الرقمية لدى العملاء والعاملين تعد خط دفاع رئيسياً ضد الاحتيال والتصيد وسوء استخدام الخدمات الرقمية.

التوصيات

1. ضرورة أن تعتمد المؤسسات المالية مبدأ الأمن والامتثال منذ التصميم عند تطوير أي خدمة مالية رقمية جديدة.
2. تعزيز دور مجالس الإدارة والإدارة العليا في متابعة مخاطر التكنولوجيا المالية وعدم حصرها في الإدارات الفنية.
3. تطوير سياسات واضحة لإدارة الطرف الثالث تشمل التقييم السابق، والمراقبة المستمرة، وحق التدقيق، وخطط الخروج.
4. إلزام الخدمات الرقمية بإفصاحات مختصرة وواضحة تظهر للعميل في وقت القرار، خاصة ما يتعلق بالرسوم والمخاطر وحدود المسؤولية.
5. تكثيف برامج التوعية بالاحتيال الرقمي والتصيد وانتحال الهوية،



- بحيث توجه إلى العملاء والموظفين بصورة مستمرة.
6. تطوير قدرات الجهات الرقابية في مجالات الذكاء الاصطناعي، وتحليل البيانات، والأمن السيبراني، والرقابة على المنصات الرقمية.
 7. تشجيع المختبرات التنظيمية والاختبار المحدود للخدمات الجديدة قبل تعميمها على نطاق واسع.
 8. تعزيز التعاون المحلي والدولي في تبادل المعلومات حول الحوادث السيبرانية ومخاطر غسل الأموال والاحتيال الرقمي.
 9. الاهتمام بالدراسات العربية التطبيقية حول التكنولوجيا المالية والمخاطر الحديثة، ولا سيما في البيئة المصرفية الأردنية والعربية.

المراجع

أولاً: المراجع باللغة العربية

- البنك المركزي الأردني. (٢٠٢٥). إطلاق المعسكر التدريبي للأمن السيبراني ٢٠٢٥ للقطاع المالي والمصرفي. عمّان: البنك المركزي الأردني.
- صندوق النقد العربي. (٢٠٢٣). تقرير الاستقرار المالي في الدول العربية. أبوظبي: صندوق النقد العربي.
- اتحاد المصارف العربية. (٢٠٢٤). تحديات الأمن السيبراني في أنظمة المدفوعات الإلكترونية. مجلة اتحاد المصارف العربية، بيروت.
- حشمان، ن. (٢٠٢٤). المخاطر السيبرانية في الصناعة المالية الإسلامية. مجلة الاقتصاد والتنمية المستدامة، الجزائر.
- كعموش، شريف علي خميس إبراهيم. (٢٠٢٤). أثر بدائل إفصاح البنوك عن إدارة مخاطر الأمن السيبراني على أحكام عملائها والمستثمرين في أسهمها: دراسة تجريبية. مجلة البحوث المحاسبية، مصر.
- مشارقة، نور سامي سعيد. (٢٠٢٤). دور التكنولوجيا المالية في تحمل البنوك التجارية للمخاطر من خلال دور الكفاءة البنكية. رسالة ماجستير، جامعة آل البيت، الأردن.
- السقاط، فراس محمد سعود. (٢٠٢٥). تأثير الذكاء الاصطناعي على إدارة المخاطر في البنوك السعودية. مجلة الاقتصاد والأعمال، السعودية.
- حشروف، ف. (٢٠٢٥). تحديات واستراتيجيات الأمن السيبراني في البنوك الجزائرية. مجلة دراسات اقتصادية، الجزائر.
- موساوي، ع. (٢٠٢٥). دور التكنولوجيا المالية الإسلامية في تحسين الخدمات المصرفية. مجلة البحوث الاقتصادية والمالية، الجزائر.
- بوخزر، م. (٢٠٢٤). أهمية اعتماد تقنية البلوك تشين في تعزيز الأمن السيبراني في القطاع المصرفي. مجلة الاقتصاد الحديث والتنمية المستدامة، الجزائر.

- بن عيسى، م. (٢٠٢٥). تقييم تأثير التكنولوجيا المالية على النظام المالي العالمي. مجلة الاقتصاد والتنمية، الجزائر.
- غريب، منى صلاح عبده. (٢٠٢٥). أثر استخدام التكنولوجيا المالية على تخفيض تكلفة الخدمات المصرفية: دراسة ميدانية. مجلة البحوث الإدارية والمالية والكمية، ١٥(١)، ٥٩٩-٦٤٩.
- الخوالدة، خالد ناصر عبد الكريم. (٢٠٢٥). أثر التكنولوجيا المالية في جودة الخدمات المصرفية: الدور الوسيط للشمول المالي في البنوك الإسلامية الأردنية. رسالة ماجستير، جامعة اليرموك، الأردن.
- عويسي، م. (٢٠٢٥). التكنولوجيا المالية كمحرك لتعزيز الشمول المالي في الجزائر. مجلة دفاتر اقتصادية، الجزائر.
- نصير، ع. (٢٠٢٦). دور التكنولوجيا الرقمية في التصدي لعمليات قرصنة البنوك. مجلة الدراسات القانونية والاقتصادية، مصر.

ثانياً: المراجع باللغة الإنجليزية

- World Bank. (2022). Fintech and the Future of Finance: Market and Policy Implications. Washington, DC: World Bank.
- Bank for International Settlements. (2024). Annual Economic Report 2024. Basel: BIS.
- International Monetary Fund. (2024). Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks. Washington, DC: IMF.
- Basel Committee on Banking Supervision. (2024). Digitalisation of Finance. Basel: Bank for International Settlements.
- European Banking Authority. (2025). Report on the Use of Digital Platforms and Operational Resilience in Banking. Paris: EBA.
- Federal Reserve Board. (2025). Cybersecurity and Financial System Resilience: Supervisory and Risk Management



- Considerations. Washington, DC: Board of Governors.
- Organisation for Economic Co-operation and Development. (2025). Digital Finance, Consumer Protection and Data Governance. Paris: OECD Publishing.
 - Bank of England. (2025). Artificial Intelligence, Data Governance and Financial Stability: Discussion Paper. London: Bank of England.
 - Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications, 120691, 231.
 - Obaid.S.Hanan, almusawi A mohammed Abdelwahab Nasser. (2023). The reality of the responsibility of the digital media marketing and its role in enhancing societal security for students of Jordanian public universities and development methods, INTERNATIONAL MINNESOTA JOURNAL OF ACADEMIC STUDIES, (VOL,1),(ISSUE,2), PP:40-15.
 - Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. arXiv preprint.
 - Adegbite, A. (2025). Data privacy, fraud analytics and regulatory compliance in digital banking. Journal of Financial Technology and Regulation, 67-44 ,(1)7.
 - Gaviyau, W. (2025). Regulatory sandboxes and financial innovation: Balancing consumer protection and innovation. Journal of Banking Regulation, 121-103 ,(2)26.



الجامعة الإسلامية بنيسوتا

Islamic University of Minnesota

المركز الرئيسي IUM