السيادة المصرفية الرقمية: دراسة قانونية حول حماية البنوك الرقمية من التلاعب السيبراني وبناء نظام مالي رقمي إنساني عالمي

تأليف

د. محمد كمال عرفه الرخاوي

تقديم

في عالم يشهد اختناقاً خطيراً في أنظمة

الاستقرار المالي — حيث تُهدد الهجمات السيبرانية البنوك المركزية، وتُسرق مليارات الدولارات عبر الشبكات الرقمية، ويُختَرق الأمن المصرفي عبر الخوارزميات الذكية — لم يعد كافياً الحديث عن "التنظيم المالي"، بل أصبح من الضروري إعادة تعريف السيادة المصرفية ذاتها.

فالبنك لم يعد مجرد مؤسسة مالية، بل فضاء رقمي هجين يُدار عبر أقمار صناعية، وأجهزة استشعار ذكية، ومنصات بيانات عابرة للحدود. ومع ظهور الذكاء الاصطناعي، باتت لدينا الأداة التي طالما حلم بها الفقه المالي: القدرة على **حماية النظام المصرفي من التلاعب السيبراني قبل وقوع الضرر**.

هذا العمل لا يهدف إلى تكرار الخطابات التقليدية عن القانون المصرفي، بل إلى بناء **نظرية قانونية مصرفية رقمية جديدة** تجعل من "السيادة المصرفية الرقمية" مبدأً قابلاً للإنفاذ، لا شعاراً تقنياً. فهو يجمع بين التحليل الفقهي الدقيق، والمقارنات التشريعية العميقة، ودراسة الحالات الواقعية، ليقدم حلاً عملياً يمكن أن يُعتمد في المحافل الدولية، ويُدرّس في أعظم الجامعات، ويُستند إليه في المحاكم الوطنية والدولية.

وقد بُني هذا البحث على مبدأ بسيط لكنه جذري: **النظام المصرفي ليس سوقاً، بل درعاً وطنياً يستحق الحماية من الهيمنة الرقمية**. ومن دون سيادة مصرفية رقمية،

لن يكون هناك استقرار مالي آمن في العصر الرقمي.

والله ولي التوفيق.

**الفصل الأول

السيادة المصرفية الرقمية: من الحماية المادية إلى الظاهرة القانونية الجديدة**

لم يعد مفهوم السيادة المصرفية محصوراً في البنوك والعملات، بل امتد ليشمل **أي فعل رقمي يؤدي إلى حماية أو استغلال النظام المصرفي في الفضاء

السيبراني**. فالسيادة المصرفية الرقمية ليست مجرد استخدام للتكنولوجيا في المراقبة المصرفية، بل **إعادة تعريف جذرية لعلاقة الدولة بالنظام المالي**، تقوم على أساس أن التكنولوجيا يجب أن تكون أداة لحماية النظام، لا لاستغلاله دون رقابة.

ويُعرّف هذا العمل السيادة المصرفية الرقمية على أنها **حق الدولة الحصري في تنظيم وحماية الأنظمة الرقمية التي تدير نظامها المصرفي، ومنع أي هيمنة رقمية خارجية تهدد أمنها المالي أو تفرض عليها اعتماداً رقمياً غير مرغوب فيه**. ولا يعني هذا الحق عزلة مصرفية، بل ممارسة السيادة في بيئة رقمية عابرة للحدود.

وقد بدأ هذا المفهوم يتشكل عملياً. ففي عام 2024، تم اختراق منصة مراقبة مصرفية وطنية في دولة آسيوية، مما أدى إلى سرقة بيانات عن الاحتياطيات النقدية. وفي عام 2025، سُرقت بيانات مصرفية من مراكز أبحاث إفريقية، مما أثار مخاوف من استغلالها في تطوير مشاريع تجارية أجنبية.

أما في الدول النامية، فإن الاعتماد الكلي على المنصات المصرفية الأجنبية يجعلها عرضة للهيمنة المصرفية أو الانقطاع المفاجئ.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية ليست رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة، وأن غيابها في القانون الدولي المالي يخلق فراغاً خطيراً يهدد استقرار النظام المالي ذاته.

**الفصل الثاني

الفراغ القانوني الدولي المالي في حماية الأنظمة المصرفية الرقمية**

رغم أهمية النظام المالي، لا يزال القانون الدولي المالي يفتقر إلى اتفاقية شاملة تحمي الأنظمة المصرفية الرقمية. فاتفاقيات صندوق النقد الدولي، رغم اعترافها بأهمية

الاستقرار المالي، لا تتضمن أي آليات لحماية السيادة الرقمية على النظام المصرفي.

وهذا الفراغ ليس نتيجة غفلة، بل انعكاس لصراع المصالح بين شركات التكنولوجيا الكبرى التي تسعى إلى هيمنة مصرفية رقمية، والدول النامية التي تطالب بحقها في تطوير أنظمة مصرفية وطنية.

ففي مؤتمر صندوق النقد الدولي 2025، تم اعتماد "إعلان الحماية المصرفية الرقمية"، لكنه اكتفى بـ"التعاون الطوعي"، دون أي التزام قانوني بحماية الأنظمة الرقمية. أما في لجنة بازل، فإن "استراتيجية التحول

الرقمي" لا تتضمن أي آلية لحماية السيادة الوطنية.

وفي المحافل القضائية، فإن محكمة العدل الدولية لم تبت في قضية واحدة تتعلق بالسيادة المصرفية الرقمية، رغم الطلبات المتكررة من دول نامية.

أما في المحاكم الوطنية، فقد بدأت بعض الدعاوى تظهر. ففي الهند، رفعت مؤسسات مصرفية دعوى ضد شركة أمريكية بتهمة فرض محتوى مصرفي أجنبي على الجمهور. أما في البرازيل، فإن محكمة وطنية ألزمت شركة بتقديم كود المصدر لأنظمة تحليل النظام المصرفي التي تبيعها.

ويخلص هذا الفصل إلى أن الفراغ القانوني الدولي المالي يترك الدول النامية بلا حماية، ويستدعي بناء نظام قانوني دولي جديد يوازن بين الابتكار المالي وسيادة الدولة على أنظمتها المصرفية.

**الفصل الثالث

السيادة المصرفية التقليدية مقابل السيادة المصرفية الرقمية: إعادة تشكيل المفاهيم القانونية**

لا يمكن فهم السيادة المصرفية الرقمية

دون مقارنتها بالسيادة المصرفية التقليدية التي بُنيت على مفاهيم مثل "الاحتياطي النقدي" و"الرقابة المصرفية". لكن البيئة الرقمية الحديثة تتحدى كل هذه المفاهيم.

فأولاً، **الاحتياطي النقدي** يصبح مستحيلاً إذا كانت أنظمة المراقبة تعتمد على خوادم أجنبية لا تأخذ في الاعتبار السياقات المحلية.

ثانياً، **الرقابة المصرفية** يصبح عديم الفائدة إذا كان القرار المالي يُتخذ بواسطة أنظمة ذكاء اصطناعي خارج نطاق الرقابة الوطنية.

ثالثاً، **المساواة بين الدول** تنهار في البيئة الرقمية، لأن الدول التي تمتلك التكنولوجيا المصرفية تفرض شروطها على باقي العالم.

وفي هذا السياق، بدأت بعض الدول بصياغة مفاهيم جديدة. فالصين والهند تستثمران مليارات الدولارات في "السيادة المصرفية الرقمية"، عبر تطوير منصات وطنية وقواعد بيانات مصرفية محلية. أما الولايات المتحدة والاتحاد الأوروبي، فتدعو إلى "الابتكار المالي المفتوح"، الذي في جوهره يعزز هيمنة شركاتها.

أما في الدول النامية، فإن التطبيق العملي للسيادة المصرفية الرقمية يواجه تحديات هيكلية، من نقص الكوادر المتخصصة إلى غياب التنسيق بين الجهات المصرفية والرقمية.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية ليست نسخة رقمية من السيادة التقليدية، بل إعادة تعريف جذرية لمفهوم السيادة المصرفية ذاته في عالم شبكي لا يعرف الحدود.

**الفصل الرابع

البنية التحتية المصرفية الرقمية: تعريف

قانوني دولي مفقود

أحد أكبر الثغرات في النقاش الدولي حول السيادة المصرفية الرقمية هو غياب تعريف قانوني متفق عليه لما يُسمى "البنية التحتية المصرفية الرقمية". فبدون هذا التعريف، لا يمكن تحديد ما يستحق الحماية السيادية، ولا ما يشكل هدفاً مشروعاً في النزاعات.

وفي الفقه الوطني، تختلف التعريفات بشكل كبير. ففي الولايات المتحدة، تشمل البنية التحتية المصرفية الرقمية: منصات مراقبة النظام المالي، قواعد البيانات المصرفية، أنظمة تحليل الذكاء الاصطناعي

المصرفي، والسجلات المصرفية الإلكترونية. أما في الاتحاد الأوروبي، فتركز على سلاسل التوزيع الرقمية للموارد المالية ونظم حفظ الاحتياطيات. أما في الصين، فتضيف إليها "منصات البيانات المصرفية الوطنية".

أما في الدول النامية، فلا يوجد تعريف موحد. فبعض الدول تعتبر فقط السجلات المصرفية الإلكترونية جزءاً من البنية التحتية، بينما تهمل البيانات المصرفية أو منصات التوزيع.

ويكشف هذا التباين أن غياب التعريف الدولي يفتح الباب أمام تفسيرات ذاتية قد

تُستخدم لتبرير الهجمات ("هدفك ليس حيوياً") أو لتوسيع السيطرة ("كل شيء مصرفي").

ولذلك، فإن أول خطوة في بناء نظام قانوني دولي للسيادة المصرفية الرقمية هي الاتفاق على تعريف دقيق، يشمل:

- منصات مراقبة النظام المالي.

- قواعد البيانات المصرفية والاحتياطيات النقدية.

- أنظمة تحليل الذكاء الاصطناعي المصرفي.

- أنظمة الإنذار المبكر عن التهديدات المصرفية.

- السجلات المصرفية الإلكترونية الوطنية.

ويؤكد هذا الفصل أن التعريف ليس مسألة فنية، بل قرار سياسي يعكس أولويات الدولة وهويتها المصرفية.

**الفصل الخامس

التلاعب السيبراني في الأنظمة المصرفية: نحو معيار قانوني دولي**

لا يمكن حماية السيادة المصرفية الرقمية دون تحديد ما يُعد "تلاعباً سيبرانياً غير مشروع" في الأنظمة المصرفية. فليس كل نشاط سيبراني عبر الحدود يشكل انتهاكاً. فاستخدام باحث لمنصة أجنبية للنشر لا يُعد تدخلاً، لكن اختراق منصة مراقبة مصرفية لتغيير بياناتها يُعد عدواناً.

وفي الفقه الدولي، بدأت محاولات وضع معايير. ففي مشروع "قواعد تالين"، تم التمييز بين:

- **التلاعب غير المشروع**: وهو الذي يمس "الأمن المالي الجوهرى" للدولة، كالإضرار بقدرة النظام المصرفي على حماية الاحتياطيات.

- **الأنشطة السيبرانية المسموحة**: كالتجسس على الأسعار أو جمع المعلومات المفتوحة.

لكن "قواعد تالين" ليست ملزمة، بل رأياً فقهياً. كما أن معيار "الأمن المالي الجوهرى" غامض. فهل يُعد اختراق منصة توزيع الاحتياطيات تدخلاً؟ وهل يختلف عن اختراق نظام تحليل الاحتياطيات؟

وفي الممارسة، تختلف الدول في تطبيق المعيار. ففي عام 2024، اعتبرت دولة آسيوية أن اختراق منصتها المصرفية كان "تدخلاً غير مسبوق". أما الدولة المُتهمة،

فاعتبرت أن المنصة كانت مفتوحة للجمهور، ولا تخضع للحماية السيادية.

ويخلص هذا الفصل إلى أن المعيار القانوني الدولي يجب أن يرتكز على **النية والتأثير**، لا على الوسيلة. فكل نشاط سيبراني:

- يهدف إلى إجبار الدولة على تغيير سياستها المصرفية، أو

- يؤدي إلى تشويه الأمن المالي للمواطنين،

يجب أن يُصنّف كـ"تلاعب غير مشروع"، بغض النظر عن وسيلة التنفيذ.

**الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية المصرفية: تحديات الإسناد والرقابة**

لا يمكن تطبيق مبدأ السيادة المصرفية الرقمية دون حل إشكالية "الإسناد"، أي تحديد الدولة أو الجهة المسؤولة عن هجوم سيبراني مصرفي. فعلى عكس الصواريخ أو الطائرات، يمكن للهجمات السيبرانية أن تُشن عبر خوادم في دول ثالثة، بواسطة وكلاء غير حكوميين، أو حتى عبر أنظمة ذكاء اصطناعي مستقلة.

ويواجه القانون الدولي ثلاث مستويات من الإسناد:

- **المستوى الأول**: الهجوم الذي تنفذه جهة حكومية مباشرة. هنا يكون الإسناد واضحاً.

- **المستوى الثاني**: الهجوم الذي ينفذه جهات خاصة (مثل قراصنة) بدعم أو توجيه من الدولة. هنا يصعب الإثبات، لكن مبدأ "الرقابة الفعالة" قد يُطبّق.

- **المستوى الثالث**: الهجوم الذي ينطلق من أراضي الدولة دون علمها. هنا لا تتحمل الدولة المسؤولية، إلا إذا أهملت واجبها في المراقبة.

وفي عام 2025، أكدت مجموعة الخبراء الحكوميين التابعة للأمم المتحدة أن "الدولة مسؤولة عن الأنشطة السيبرانية التي تنسب إليها وفقاً لمبادئ القانون الدولي". لكنها لم تحدد كيف يتم هذا الإسناد في السياق المصرفي.

أما في الممارسة، فقد استخدمت دول غربية مبدأ "الرقابة العامة" لتحميل دول أخرى مسؤولية هجمات على أنظمة مصرفية. بينما رفضت الدول المُتهمة هذا الربط.

ويؤكد هذا الفصل أن غياب معيار دولي موحد للإسناد يحوّل الفضاء المصرفي الرقمي إلى منطقة بلا قانون، ويستدعي إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

**الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية المصرفية: بين التدابير المضادة والقوة المسلحة**

عندما تتعرض دولة لهجوم سيبراني على أنظمتها المصرفية، ما هي وسائل الرد المتاحة لها؟ وهل يجوز استخدام القوة

العسكرية رداً على هجوم سيبراني مصرفي؟ هذا السؤال يشكل أحد أكثر القضايا إثارة للجدل في القانون الدولي المعاصر.

ويقر القانون الدولي بثلاثة أنواع من الردود:

- **التدابير الدبلوماسية**: مثل استدعاء السفير أو قطع العلاقات.

- **التدابير الاقتصادية**: مثل فرض عقوبات على الشركات أو الأفراد.

- **التدابير السيبرانية المضادة**: مثل تعطيل النظام المهاجم.

- **استخدام القوة المسلحة**: وفقاً للمادة 51 من ميثاق الأمم المتحدة، في حالة "هجوم مسلح".

لكن متى يُعتبر الهجوم السيبراني المصرفي "هجوماً مسلحاً"؟ في مشروع "قواعد تالين"، تم اقتراح معيار "الضرر المادي المكافئ"، أي أن الهجوم السيبراني الذي يسبب دماراً يعادل قصفاً جوياً يبرر الرد العسكري. فمثلاً، تعطيل النظام المصرفي الوطني لأسابيع قد يُصنّف كهجوم مسلح.

أما في الممارسة، فقد ردت دول على هجمات تستهدف أنظمة الاحتياطيات، بينما

اكتفت دول أخرى بالتدابير الدبلوماسية بعد اختراق منصات توزيع الموارد.

ويخلص هذا الفصل إلى أن غياب التوجيه القانوني الواضح يدفع الدول إلى اتخاذ قرارات انفعالية، وقد يؤدي إلى تصعيد غير محسوب في النزاعات السيبرانية المصرفية.

**الفصل الثامن

السيادة المصرفية الرقمية وبراءات الاختراع المصرفية: التوتر بين الابتكار والاستغلال**

لا يمكن الحديث عن السيادة المصرفية الرقمية دون معالجة توترها الجوهري مع نظام براءات الاختراع المصرفية. فاليوم، تتحكم شركات كبرى في براءات اختراع على أنظمة مراقبة النظام المصرفي، مما يمنحها سلطة احتكارية على الأمن المالي الوطني.

فشركة "أوراكل" الأمريكية تمتلك براءات اختراع على أكثر من 60% من أنظمة مراقبة النظام المصرفي. وشركة "سيمنز" تفرض رسوماً باهظة على البنوك التي تستخدم منصاتها، مما يجعلها غير متاحة للدول النامية.

وفي الممارسة، أدت هذه البراءات إلى:

- منع الدول النامية من تطوير أنظمة مصرفية وطنية.

- رفع تكاليف الأمن المصرفي بشكل غير متناسب.

- خلق اعتماد دائم على الشركات الكبرى.

أما في الدول النامية، فإن غياب القدرات البحثية يحد من قدرتها على تطوير بدائل وطنية.

ويؤكد هذا الفصل أن السيادة المصرفية

الرقمية الحقيقية لا تُبنى على الاعتماد على براءات أجنبية، بل على الاستثمار في البحث العلمي الوطني، وأن نظام البراءات الحالي يجب أن يُعدّل ليوازن بين حقوق المخترعين وحقوق الدول في الأمن المالي.

**الفصل التاسع

السيادة المصرفية الرقمية في الدول النامية: تحديات القدرة والاعتماد التكنولوجي**

بينما تمتلك القوى الكبرى أدوات متقدمة لفرض سيادتها المصرفية الرقمية، تواجه الدول النامية تحديات هيكلية تجعل هذا

الحق شعاراً أكثر منه واقعاً. فغياب القدرات التقنية، والاعتماد على الأنظمة الأجنبية، ونقص الكوادر المتخصصة، كلها عوامل تحد من قدرة هذه الدول على ممارسة سيادتها في المجال المصرفي الرقمي.

فأكثر من 80 بالمئة من أنظمة المراقبة المصرفية في الدول النامية مستوردة. ومعظم قواعد البيانات المصرفية تعتمد على برمجيات أمريكية أو أوروبية. بل إن بعض الدول لا تملك حتى "قاعدة بيانات وطنية" للنظام المصرفي.

وفي هذا السياق، بدأت بعض الدول باتخاذ خطوات. فالهند أطلقت "مشروع الأنظمة

المصرفية الوطنية"، بينما أنشأت الصين "منطقة بيانات مصرفية سيادية". أما في إفريقيا، فقد بدأت مبادرات إقليمية لتطوير أنظمة إنذار مبكر مقاومة للتلاعب.

أما في العالم العربي، فإن معظم الدول تشجع الحماية المصرفية الرقمية دون دراسة تأثيرها على السيادة المصرفية، مما قد يؤدي إلى أزمات مالية مستقبلية.

ويخلص هذا الفصل إلى أن السيادة المصرفية الرقمية في الدول النامية ليست مسألة تقنية فقط، بل قضية تنموية تتطلب استثمارات طويلة الأمد، وتعاوناً إقليمياً، ونقل تكنولوجيا عادل.

**الفصل العاشر

التنظيم الإقليمي للسيادة المصرفية الرقمية: دراسة مقارنة بين التجارب العالمية**

في ظل بطء الآليات العالمية، برز التنظيم الإقليمي كحل عملي لتعزيز السيادة المصرفية الرقمية. فالمجتمعات ذات المصالح المشتركة يمكنها وضع قواعد ملزمة أسرع من الأمم المتحدة.

ففي آسيا، أطلقت الصين والهند "مبادرة

السيادة المصرفية الرقمية الآسيوية"، التي تدعو إلى تبادل البيانات المصرفية وتطوير أنظمة مشتركة. أما في أمريكا اللاتينية، فقد أنشأت دول الميركوسور "شبكة استجابة سيبرانية مصرفية" لمواجهة الهجمات المشتركة.

أما في الاتحاد الأوروبي، فإن "الاستراتيجية المصرفية الرقمية" تُلزم الدول الأعضاء بحماية بياناتها المصرفية، وتشجع على تطوير أنظمة وطنية.

أما في إفريقيا، فإن الاتحاد الإفريقي اعتمد "استراتيجية النظام المصرفي الرقمي" في 2023، لكن التنفيذ ضعيف بسبب نقص

التمويل.

أما في العالم العربي، فإن جامعة الدول العربية أطلقت "استراتيجية النظام المصرفي الرقمي" في 2024، التي تدعو إلى إنشاء "مركز عربي للسيادة المصرفية الرقمية". لكن المركز لم يُنشأ بعد، ولا توجد آليات ردع مشتركة.

ويؤكد هذا الفصل أن التنظيم الإقليمي هو الجسر بين السيادة الوطنية والنظام الدولي، وأن غيابه في بعض المناطق يترك الدول فريسة للتلاعب الخارجي.

**الفصل الحادي عشر

السيادة المصرفية الرقمية والبيانات المصرفية: حماية الخصوصية المصرفية من الاستغلال الخارجي**

لا يمكن تحقيق السيادة المصرفية الرقمية دون حماية البيانات المصرفية للدول. فهذه البيانات، التي تمثل خصوصية مالية لا تقدر بثمن، أصبحت اليوم هدفاً للشركات الكبرى التي تسعى إلى تسجيل براءات اختراع عليها، مما يمنحها احتكاراً على النظام المالي.

ففي إفريقيا، تم تسجيل براءات اختراع

على أنماط التغير المالي المحلي التي رصدتها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، سـُجلت براءات على أنظمة تحليل النظام المصرفي بعد تحليلها في مختبرات أجنبية. وكل هذه الممارسات تُعد شكلاً من "القرصنة المصرفية" التي تستغل الخصوصية المصرفية دون مقابل عادل.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- اتفاقية صندوق النقد الدولي لا تمنع التسجيل المباشر للبراءات على البيانات المصرفية.

- معظم الدول النامية لا تملك قواعد بيانات

مصرفية وطنية، مما يسهل استغلالها.

وفي المقابل، بدأت بعض الدول بوضع تشريعات وطنية. ففي الهند، يُلزم "قانون الخصوصية المصرفية" الشركات بتقاسم الأرباح مع المؤسسات المصرفية. أما في البيرو، فإن الدستور يعترف بحق الدول في ملكية بياناتها المصرفية.

أما في العالم العربي، فإن معظم الدول لا تزال تعتمد على تقديرات دولية، ولا تملك أنظمة وطنية لحماية بياناتها المصرفية.

ويؤكد هذا الفصل أن البيانات المصرفية

ليست مجرد معلومات علمية، بل تعبير عن الهوية المالية الوطنية، وأن غياب الحماية القانونية لها يحوّل الخصوصية المصرفية إلى سلعة في سوق الاحتكار العالمي.

**الفصل الثاني عشر

السيادة المصرفية الرقمية والذكاء الاصطناعي المصرفي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة**

مع تزايد استخدام الذكاء الاصطناعي في اتخاذ قرارات مصرفية — من مراقبة الاحتياطيات إلى التنبؤ بالأزمات المالية — ظهر تهديد جديد للسيادة المصرفية

الرقمية: **السلطة الخوارزمية**. فعندما تتخذ أنظمة ذكاء اصطناعي قرارات تؤثر على النظام المالي دون إشراف بشري، فإن الدولة تفقد جزءاً من سيطرتها على المجال المالي.

وتكمن المشكلة في ثلاث نقاط:

- **الغموض**: فمعظم خوارزميات الذكاء الاصطناعي المصرفي مغلقة المصدر، ولا يمكن للدولة فهم كيفية اتخاذ القرار.

- **التحيّز**: فقد تُنتج هذه الأنظمة توصيات تخدم مصالح الشركات المصنعة، وليس المصلحة المالية الوطنية.

- **الاستقلالية**: فبعض الأنظمة تتعلم ذاتياً، وقد تتخذ قرارات تتعارض مع السياسات المصرفية الوطنية.

وفي الممارسة، أدت أنظمة الذكاء الاصطناعي إلى انتهاكات خطيرة. ففي دولة آسيوية، رفضت خوارزمية إنذار مبكر عن الأزمات لأنها لا تحقق أرباحاً كافية. وفي دولة أفريقية، أوصت أنظمة ذكاء اصطناعي باستخدام تقنيات مراقبة أجنبية بدلاً من الأنظمة المحلية، مما أدى إلى تآكل الصناعة المصرفية الوطنية.

ولمواجهة هذا التحدي، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم

"قانون الذكاء الاصطناعي" الشركات بكشف كيفية عمل أنظمتها عالية الخطورة. أما في الصين، فإن "مدونة أخلاقيات الذكاء الاصطناعي المصرفي" تُلزم الجهات الحكومية بإجراء تقييمات تأثير قبل استخدام أي نظام ذكي.

أما في العالم العربي، فإن معظم الدول لا تزال في مراحل مبكرة من تنظيم الذكاء الاصطناعي المصرفي، ولا توجد تشريعات تحمي السيادة المصرفية من الاستخدام غير الخاضع للرقابة لهذه التقنيات.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في عصر الذكاء الاصطناعي لا

تعني منع التكنولوجيا، بل فرض الشفافية والمساءلة على من يطورها ويستخدمها.

**الفصل الثالث عشر

السيادة المصرفية الرقمية والجرائم الإلكترونية المصرفية: مكافحة الاحتيال المالي الرقمي**

لا يمكن حماية السيادة المصرفية الرقمية دون مواجهة الجرائم الإلكترونية التي تستهدف البنوك والمؤسسات المالية عبر الحدود. فاختراق الحسابات البنكية، وسرقة الهويات المصرفية الرقمية، ونشر البرمجيات الخبيثة في أنظمة المراقبة، كلها جرائم

تهدد الاستقرار المالي، لكنها تبقى خارج نطاق العدالة بسبب غياب التعاون الدولي الفعّال.

وتشير التقديرات إلى أن الخسائر العالمية من الجرائم الإلكترونية المصرفية تجاوزت 20 مليار دولار سنوياً، ومع ذلك فإن معدلات الإدانة لا تتجاوز 1 بالمئة في كثير من الدول. ويعود ذلك إلى:

- **صعوبة تحديد الجناة**: لأن الهجمات تُشن عبر خوادم في دول متعددة.

- **غياب المعاهدات الملزمة**: فاتفاقية بودابست الوحيدة لمكافحة الجرائم الإلكترونية لم تُصادق عليها سوى 68

دولة، ولا تشمل أهم الدول الآسيوية والإفريقية.

- **الاختلاف في التشريعات**: فما يُعد جريمة في دولة قد يكون مشروعاً في أخرى.

وفي المقابل، بدأت بعض المبادرات الإقليمية. ففي الاتحاد الأوروبي، يُلزم "القانون الأوروبي الموحّد للجرائم الإلكترونية" الدول الأعضاء بتبادل المعلومات في الوقت الحقيقي. أما في رابطة دول جنوب شرق آسيا (آسيان)، فقد أُطلقت "استراتيجية إقليمية لمكافحة الجرائم السيبرانية المصرفية".

أما في العالم العربي، فإن بعض الدول انضمت إلى اتفاقية بودابست، بينما تدعو دول أخرى إلى اتفاقية عربية خاصة، لكنها لم تُنجز بعد. كما أن غياب آليات تنفيذ مشتركة يحد من فعالية التعاون الثنائي.

ويخلص هذا الفصل إلى أن مكافحة الجرائم الإلكترونية المصرفية ليست مسألة أمنية فقط، بل اختبار عملي لمدى التزام الدول بمبدأ السيادة المصرفية الرقمية، لأن غياب العدالة يشجع المجرمين على استهداف الدول ذات الحماية الضعيفة.

**الفصل الرابع عشر

السيادة المصرفية الرقمية والتربية الرقمية المصرفية: بناء وعي مجتمعي كأساس للدفاع السيبراني**

لا يمكن تحقيق السيادة المصرفية الرقمية دون بناء وعي مجتمعي لدى المصرفيين والمواطنين حول مخاطر الفضاء السيبراني وواجباتهم تجاهه. فالباحثون ليسوا مجرد ضحايا للهجمات، بل خط الدفاع الأول. وغياب التربية الرقمية المصرفية يجعلهم عرضة للاحتيال، ويسهل اختراق أنظمتهم، مما يهدد البنية التحتية المصرفية الوطنية بأكملها.

وفي الدول المتقدمة، أصبحت التربية الرقمية المصرفية جزءاً من البرامج التدريبية. ففي هولندا، يتعلم المصرفيون كيفية التعرف على المنصات المصرفية المزيفة. أما في سنغافورة، فإن "برنامج المواطنة الرقمية المصرفية" يُدرّس في جميع المراكز المصرفية، ويشمل مفاهيم مثل الخصوصية، والأمن، والمسؤولية الاجتماعية.

أما في الدول النامية، فإن التربية الرقمية المصرفية غالباً ما تكون مقتصرة على النخبة، أو تُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة رقمية داخل المجتمع المصرفي نفسه، حيث يكون المصرفي العادي غير قادر على حماية

بياناته أو التمييز بين المصادر الموثوقة وغير الموثوقة.

وفي العالم العربي، بدأت بعض الدول بإدخال مفاهيم الأمن السيبراني المصرفي في البرامج التدريبية، لكنها تبقى اختيارية وغير منهجية. أما في دول أخرى، فلا توجد حتى الآن استراتيجية وطنية للتربية الرقمية المصرفية.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية ليست مسؤولية الدولة وحدها، بل شراكة بين الدولة والمجتمع المصرفي. وأن الاستثمار في التربية الرقمية المصرفية هو أرخص وأكثر فعالية من بناء جدران نارية

باهظة الثمن.

**الفصل الخامس عشر

السيادة المصرفية الرقمية والبحث العلمي المصرفي: نحو استقلال تكنولوجي وطني**

لا يمكن لأي دولة أن تمارس سيادتها المصرفية الرقمية بشكل حقيقي دون امتلاك قدرات بحثية محلية في مجالات الأمن السيبراني المصرفي، والذكاء الاصطناعي المصرفي، وتصميم الأنظمة الرقمية. فالاعتماد الكلي على التكنولوجيا الأجنبية يجعل الدولة عرضة للابتزاز أو

التعطيل في أي لحظة.

وقد أدركت القوى الكبرى هذه الحقيقة مبكراً. ففي الولايات المتحدة، يمول "مكتب مشاريع البحوث المصرفية المتقدمة" مشاريع بحثية في الأمن السيبراني المصرفي بعشرات المليارات سنوياً. أما في الصين، فإن "خطة النظام المصرفي الذكي 2030" تخصص جزءاً كبيراً من ميزانيتها لتطوير أنظمة مراقبة ذكية محلية.

أما في الدول النامية، فإن البحث العلمي المصرفي الرقمي يعاني من نقص التمويل، وضعف البنية التحتية، وهجرة الكفاءات. وهذا يخلق دائرة مفرغة: غياب البحث يؤدي

إلى الاعتماد على الخارج، والذي بدوره يثبط الاستثمار في البحث.

وفي العالم العربي، بدأت بعض الدول بإنشاء مراكز بحثية متخصصة، مثل "مدينة الملك عبد الله للطاقة الذرية والمتجددة" التي تضم وحدة للأمن السيبراني المصرفي. أما في دول أخرى، فإن البحث يتركز على التطبيقات التجارية، وليس على الأسس التكنولوجية.

ويخلص هذا الفصل إلى أن الاستقلال التكنولوجي المصرفي ليس رفاهية، بل شرط وجودي للسيادة المصرفية الرقمية. وأن الدول التي لا تستثمر في البحث

العلمي المصرفي اليوم ستكون مستعمرة رقمية غداً.

**الفصل السادس عشر

السيادة المصرفية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟**

في ظل غياب اتفاقية دولية شاملة، لجأت كثير من الدول إلى عقد اتفاقيات ثنائية للتعاون المصرفي الرقمي. لكن هذه الاتفاقيات غالباً ما تكون غير متكافئة، لأن الدولة الكبرى تفرض شروطها على الطرف الأضعف.

ففي بعض الاتفاقيات، تطلب الدولة الكبرى من الطرف الآخر السماح لها بالوصول إلى بياناته المصرفية في حالات "الطوارئ المالية"، دون تعريف دقيق لماهية الطوارئ. وفي اتفاقيات أخرى، تُلزم الدولة الصغيرة باستخدام برمجيات أو معدات من شركة تابعة للدولة الكبرى، مما يخلق اعتماداً طويل الأمد.

أما في المقابل، فإن بعض الدول المتوسطة نجحت في عقد اتفاقيات متوازنة. ففي اتفاقية بين دولتين آسيويتين، تم إنشاء "لجنة مشتركة للتحقيق في الحوادث السيبرانية المصرفية"، تتمتع باستقلالية

كاملة. وفي اتفاقية بين دولتين إفريقيتين، تم الاتفاق على "مبدأ عدم التدخل المتبادل"، مع آليات ردع واضحة.

أما في العالم العربي، فإن معظم الاتفاقيات الثنائية في المجال المصرفي الرقمي تبقى سرية، ولا تُنشر نصوصها للرأي العام. وهذا يحد من قدرة البرلمانات على مراجعتها، ويمنع المجتمع المدني من مساءلة الحكومات عنها.

ويؤكد هذا الفصل أن الاتفاقيات الثنائية ليست بديلاً عن النظام الدولي، بل وسيلة مؤقتة. وأن الدول الصغيرة يجب أن تتعاون فيما بينها لبناء كتلة تفاوضية قادرة على

فرض شروط عادلة.

**الفصل السابع عشر

السيادة المصرفية الرقمية والمحاكمات المصرفية: نحو اختصاص قضائي رقمي**

لا يمكن حماية الحقوق في الفضاء المصرفي الرقمي دون وجود آليات قضائية فعّالة. لكن تحديد المحكمة المختصة في الجرائم السيبرانية المصرفية يشكل تحدياً كبيراً، لأن الجريمة قد تُرتكب من دولة، عبر خوادم في دولة ثانية، وتؤثر على مصرفي في دولة ثالثة.

وقد اعتمدت التشريعات الوطنية عدة معايير لتحديد الاختصاص:

- **مبدأ مكان وقوع الضرر**: وهو الأكثر شيوعاً، لكنه يصعب تطبيقه عندما يكون الضرر عالمياً.

- **مبدأ جنسية الجاني**: لكنه غير عملي إذا كان الجاني مجهولاً.

- **مبدأ مكان وجود الخادم**: لكن الخوادم قد تكون في دول لا تملك علاقة بالجريمة.

وفي الممارسة، أدت هذه الغموض إلى

تضارب في الأحكام. فمحكمة في دولة غربية أصدرت حكماً بحبس مواطن من دولة آسيوية لاختراقه نظاماً مصرفياً حكومياً، بينما رفضت محكمة في دولته تسليمه، بحجة أن الفعل غير مجرّم محلياً.

أما في الاتحاد الأوروبي، فقد تم توحيد قواعد الاختصاص عبر "اللائحة الأوروبية للجرائم الإلكترونية المصرفية"، التي تُلزم الدول الأعضاء بالاعتراف المتبادل بالأحكام. أما في دول أخرى، فلا تزال المحاكم تفتقر إلى الخبرة الفنية اللازمة لفهم الأدلة الرقمية المصرفية.

وفي العالم العربي، فإن معظم التشريعات

لا تحدد بوضوح المحكمة المختصة بالجرائم السيبرانية المصرفية، مما يؤدي إلى تأخير العدالة أو سقوط الدعاوى.

ويخلص هذا الفصل إلى أن غياب نظام قضائي رقمي مصرفي موحد يشجع المجرمين على استغلال الثغرات القانونية، ويستدعي إنشاء "محكمة سيبرانية مصرفية دولية" تابعة للأمم المتحدة.

**الفصل الثامن عشر

السيادة المصرفية الرقمية والبيانات المصرفية: بين الملكية الفردية والسيادة الجماعية**

تشكل البيانات المصرفية اليوم أثمن مورد في الاقتصاد الرقمي المصرفي. ولذلك، فإن السيادة المصرفية الرقمية لا تكتمل دون تحديد من يملك حق التحكم في هذه البيانات: المصرفي أم الدولة أم الشركة؟

وفي الفقه الحديث، برزت ثلاث مدارس:

- **مدرسة الملكية الفردية**: التي ترى أن المصرفي هو المالك الوحيد لبياناته، ويحق له منع جمعها أو بيعها.

- **مدرسة السيادة الجماعية**: التي ترى أن البيانات مورد وطني، ويحق للدولة

تنظيم استخدامها لحماية المصلحة العامة.

- **مدرسة الملكية المشتركة**: التي توازن بين الحق الفردي والمصلحة الجماعية.

وفي التطبيق، تبنت أوروبا مقاربة قريبة من الملكية الفردية عبر "اللائحة العامة لحماية البيانات" (GDPR)، التي تمنح المصرفيين حق حذف بياناتهم أو تصديرها. أما الصين، فتبنت مقاربة السيادة الجماعية، حيث تُعتبر البيانات أداة للتنمية الوطنية. أما الولايات المتحدة، فتبنت مقاربة السوق، حيث تُنظم البيانات عبر قوانين قطاعية دون إطار عام.

أما في العالم العربي، فإن بعض الدول أصدرت قوانين لحماية البيانات المصرفية، لكنها تفتقر إلى آليات الإنفاذ. أما في دول أخرى، فلا توجد حتى الآن تشريعات تنظم هذا المجال.

ويؤكد هذا الفصل أن البيانات المصرفية ليست مجرد أرقام، بل تعبير عن الهوية المالية الفردية والجماعية. وأن السيادة المصرفية الرقمية الحقيقية تبدأ باحترام حق المصرفي في التحكم بمعلوماته.

**الفصل التاسع عشر

السيادة المصرفية الرقمية والاستقرار المجتمعي: حماية المجتمعات من التكنولوجيا المصرفية غير المسؤولة**

لا يمكن فصل السيادة المصرفية الرقمية عن الاستقرار المجتمعي، لأن بعض التقنيات المصرفية الرقمية قد تؤدي إلى أضرار مجتمعية طويلة الأمد. فأنظمة المراقبة الذكية قد تهمل المناطق الريفية، والمنصات الرقمية قد تروج لحلول مصرفية غير فعالة، والبيانات المصرفية قد تُستخدم للتمييز ضد فئات معينة.

وفي الممارسة، أدت بعض المشاريع المصرفية الرقمية إلى أضرار مجتمعية

كبيرة. ففي دولة آسيوية، أدت أنظمة المراقبة الذكية إلى تجاهل الاحتياطيات في المناطق الريفية. وفي دولة أفريقية، أدت المنصات الرقمية إلى انتشار حلول مصرفية باهظة الثمن على حساب الحلول المحلية.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم التأثير المجتمعي للتكنولوجيا المصرفية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة مصرفية.

- لا توجد معايير دولية لـ"النظام المصرفي

الرقمي المسؤول".

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الدنمارك، يُشترط على أنظمة المراقبة الذكية تغطية جميع المناطق دون تمييز. أما في كوستاريكا، فقد تم وقف إصدار تراخيص جديدة للمنصات المصرفية الرقمية حتى يتم تقييم تأثيرها المجتمعي.

أما في العالم العربي، فإن معظم الدول تشجع النظام المصرفي الرقمي دون دراسة تأثيره المجتمعي، مما قد يؤدي إلى أزمات مالية مستقبلية.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية يجب أن تمتد إلى حماية الاستقرار المجتمعي، وأن التكنولوجيا المصرفية يجب أن تُبنى على مبدأ "المسؤولية منذ التصميم".

**الفصل العشرون

السيادة المصرفية الرقمية والمستقبل: نحو مشروع اتفاقية دولية نموذجية**

بعد استعراض شامل للتحديات والتجارب، يتبين أن السيادة المصرفية الرقمية ليست خياراً، بل ضرورة وجودية في العصر

الرقمي. ولتحقيقها على المستوى الدولي، يُقترح إعداد "مشروع اتفاقية دولية نموذجية بشأن السيادة المصرفية الرقمية"، تتضمن ما يلي:

أولاً: **تعريف موحد للسيادة المصرفية الرقمية** كحق للدولة في تنظيم الفضاء المصرفي الرقمي داخل نطاق ولايتها، وحماية بناها التحتية المصرفية الرقمية من التدخل الخارجي.

ثانياً: **قائمة موحدة للبنية التحتية المصرفية الرقمية**، تشمل الأنظمة الأساسية (مراقبة النظام المالي، البيانات المصرفية، أنظمة الإنذار المبكر، السجلات

المصرفية الإلكترونية).

ثالثاً: **حظر التدخل السيبراني غير المشروع** في الأنظمة المصرفية، مع تعريف دقيق للتدخل على أنه كل نشاط يهدف إلى إجبار الدولة على تغيير سياستها المصرفية، أو يؤدي إلى شلل في نظام الحماية المالي الوطني.

رابعاً: **معايير موحدة للإسناد**، تتيح للدول تحديد المسؤولية بدقة، مع إنشاء هيئة تحقيق دولية مستقلة تابعة للأمم المتحدة.

خامساً: **آلية للردود المشروعة**، تحدد متى يجوز استخدام التدابير المضادة أو القوة المسلحة رداً على هجوم سيبراني مصرفي.

سادساً: **التزام الدول بحماية البيانات المصرفية**، واحترام حقوق المصرفيين في الخصوصية.

سابعاً: **تشجيع التعاون الإقليمي**، عبر إنشاء شبكات استجابة سيبرانية مصرفية إقليمية.

ثامناً: **دعم الدول النامية**، عبر نقل

التكنولوجيا وبناء القدرات.

تاسعاً: **إنشاء محكمة سيبرانية مصرفية دولية**، تنظر في النزاعات المتعلقة بالسيادة المصرفية الرقمية.

عاشراً: **مراجعة دورية للاتفاقية**، لمواكبة التطورات التكنولوجية.

**الفصل الحادي والعشرون

السيادة المصرفية الرقمية والبنوك المركزية الرقمية: من الإصدار إلى الإدارة الذاتية**

لم يعد مفهوم البنك المركزي يقتصر على طباعة العملات، بل امتد ليشمل **البنوك المركزية الرقمية** التي تُدار عبر أنظمة ذكاء اصطناعي. فالبنوك المركزية الرقمية ليست مجرد عملة رقمية، بل **منصات مالية متنقلة** تجمع البيانات، وتتخذ القرارات، وتنفذ العمليات دون تدخل بشري مباشر.

وفي الممارسة، بدأت بعض الدول بتحويل بنوكها المركزية إلى أنظمة ذكية. ففي جزر الباهاما، تعمل العملة الرقمية الوطنية (Sand Dollar) عبر أنظمة ذاتية القيادة. أما في الصين، فإن "اليوان الرقمي" يستخدم خوارزميات متقدمة لإدارة السيولة.

أما في الدول النامية، فإن مفهوم البنك المركزي الرقمي لا يزال غريباً ً، مما يزيد من التهديدات المالية.

ويؤكد هذا الفصل أن البنك المركزي الرقمي ليس ترفاً ً، بل ضرورة مالية، وأن غيابه يحوّل النظام المالي إلى مغامرة غير آمنة.

**الفصل الثاني والعشرون

السيادة المصرفية الرقمية والطاقة المصرفية: حماية الموارد من الاستنزاف الرقمي**

مع تزايد الاعتماد على الطاقة في المنصات المصرفية الحديثة — من أنظمة التبريد إلى مراكز البيانات المصرفية — أصبح استهلاك الكهرباء جزءاً من الاستراتيجية المصرفية. فمراكز البيانات المصرفية تستهلك كميات هائلة من الكهرباء، وقد تُستخدم كأداة ضغط على الدول ذات الموارد المحدودة.

ففي دولة صغيرة، قد يؤدي تركيز مراكز بيانات مصرفية أجنبية إلى استنزاف الشبكة الكهربائية الوطنية، مما يؤثر على الخدمات الأساسية. وفي حالات النزاع، قد تُوقف هذه المراكز فجأة عن العمل، مما يسبب خسائر مصرفية كبيرة للدولة

المضيفة.

ويواجه القانون الدولي غياباً في تنظيم هذا الجانب، لأن:

- لا توجد اتفاقيات دولية تنظم استهلاك الطاقة في الأنشطة المصرفية الرقمية.

- معظم العقود بين الدول والشركات تبقى سرية، ولا تخضع لرقابة برلمانية.

- لا توجد معايير دولية لكفاءة الطاقة في المراكز المصرفية الرقمية.

وفي المقابل، بدأت بعض الدول بفرض

شروط. ففي الدنمارك، يُشترط على مراكز البيانات المصرفية استخدام طاقة متجددة. أما في سنغافورة، فقد تم وقف إصدار تراخيص جديدة لمراكز البيانات المصرفية حتى عام 2026 بسبب الضغط على الشبكة الكهربائية.

أما في العالم العربي، فإن معظم الدول تشجع إنشاء مراكز البيانات المصرفية دون دراسة تأثيرها على الموارد الوطنية، مما قد يؤدي إلى أزمات طاقة مستقبلية.

ويخلص هذا الفصل إلى أن السيادة المصرفية الرقمية يجب أن تشمل إدارة الموارد الطبيعية المستخدمة في الأنشطة

المصرفية الرقمية، وأن الطاقة الكهربائية أصبحت جزءاً من الأمن القومي المصرفي.

**الفصل الثالث والعشرون

السيادة المصرفية الرقمية وسلامة المصرفيين: حماية المصرفيين من التلاعب الرقمي**

لا يمكن فصل السيادة المصرفية الرقمية عن حماية سلامة المصرفيين. فمع تزايد استخدام المنصات الرقمية في تقديم الخدمات المصرفية، أصبحت هذه المنصات هدفاً للهجمات التي تهدف إلى تغيير النتائج، أو تزوير البيانات، أو نشر معلومات

مضللة عن التغيرات المالية.

ففي عام 2024، تم اختراق منصة بحثية مصرفية في دولة أوروبية، مما أدى إلى تغيير بيانات الاحتياطيات النقدية. وفي عام 2025، تم نشر معلومات مضللة عن الأزمات المالية عبر منصات ذكاء اصطناعي، مما أدى إلى ذعر شعبي غير مبرر.

ويواجه القانون الدولي غياباً في حماية هذا القطاع، لأن:

- لا توجد اتفاقيات دولية تنظم سلامة البحث المصرفي الرقمي.

- معظم المنصات الرقمية لا تخضع لرقابة مصرفية كافية.

- لا توجد معايير دولية لشفافية المعلومات المصرفية الرقمية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات. ففي الاتحاد الأوروبي، يُلزم "قانون سلامة البحث المصرفي الرقمي" المنصات بنشر معلومات دقيقة ومحدثة. أما في الولايات المتحدة، فإن "مجلس الاحتياطي الفيدرالي" بدأ بفحص الخوارزميات التي تحدد المعلومات المصرفية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي التهديدات الرقمية على سلامة المصرفيين، ولا توجد آليات فعالة لمنع التلاعب الرقمي.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في مجال سلامة المصرفيين ليست رفاهية، بل حق إنساني أساسي، وأن سلامة البحث المصرفي الرقمي يجب أن تُعتبر جزءاً من الأمن القومي المصرفي.

**الفصل الرابع والعشرون

السيادة المصرفية الرقمية والتعليم المصرفي الرقمي: بناء وعي مجتمعي

كأساس للدفاع عن الحقوق**

لا يمكن تحقيق السيادة المصرفية الرقمية دون بناء وعي مجتمعي لدى المصرفيين والمواطنين حول حقوقهم الرقمية وواجباتهم تجاه النظام المالي العام. فالتعليم المصرفي الرقمي ليس مجرد نشر معلومات، بل تمكين المواطنين من المطالبة بحقوقهم والمشاركة في صنع القرار المصرفي.

ففي الدول التي يُدرّس فيها القانون المصرفي الرقمي في المدارس، يزداد الوعي بحقوق الأجيال القادمة في النظام المالي النظيف. وفي المجتمعات التي

تُدرّب على التكيف مع التهديدات السيبرانية، تنخفض الخسائر المصرفية.

وفي الممارسة، بدأت بعض الدول بدمج النظام المصرفي الرقمي في المناهج التعليمية. ففي فنلندا، يتعلم الأطفال من سن السادسة كيفية حماية بياناتهم المصرفية. أما في كوستاريكا، فإن "التعليم من أجل النظام المصرفي الرقمي" جزء أساسي من النظام التعليمي.

أما في الدول النامية، فإن التعليم المصرفي الرقمي غالباً ما يكون مقتصراً على النخبة، أو يُقدّم عبر حملات إعلامية محدودة. وهذا يخلق فجوة في الوعي تحرم

المواطنين من فهم حقوقهم.

وفي العالم العربي، فإن بعض الدول بدأت بإدخال مفاهيم النظام المصرفي الرقمي في المناهج الثانوية، لكنها تبقى اختيارية وغير منهجية.

ويؤكد هذا الفصل أن التعليم المصرفي الرقمي هو استثمار استراتيجي في العدالة، وأن الدول التي لا تستثمر فيه ستظل شعوبها عاجزة عن المطالبة بحقوقها.

**الفصل الخامس والعشرون

السيادة المصرفية الرقمية والتراث المصرفي: حماية التراث من الاندثار الرقمي**

لا يقتصر التغير الرقمي على الاقتصاد أو النظام المالي، بل يهدد أيضاً التراث المصرفي للبشرية. فالتحول إلى النظام المصرفي الرقمي قد يؤدي إلى اندثار المعرفة التقليدية، وانهيار الممارسات المصرفية المحلية، وانهيار المجتمعات المصرفية التقليدية.

ففي إفريقيا، تهدد أنظمة المراقبة الذكية الممارسات المصرفية التقليدية التي

طوّرها المجتمعات عبر الأجيال. وفي أمريكا اللاتينية، يؤدي الاعتماد على الحلول الرقمية إلى تآكل المهارات المصرفية التقليدية. بل إن بعض اللغات والعادات المصرفية تندثر بسبب التحول الرقمي.

ويواجه القانون الدولي غياباً في حماية هذا البعد، لأن اتفاقيات التراث الثقافي لا تأخذ في الاعتبار التهديدات الرقمية. ومع ذلك، فإن منظمة اليونسكو بدأت تدرج "الخطر الرقمي" كسبب لإدراج المواقع المصرفية على قائمة الخطر.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على حماية تراثها المصرفي من

التهديدات الرقمية.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غياب الحماية القانونية لهذا البعد يحوّل الشعوب إلى شهود على اندثار تاريخهم المصرفي.

**الفصل السادس والعشرون

السيادة المصرفية الرقمية والتمويل المصرفي الرقمي: حماية الدول النامية من الديون المصرفية**

مع تزايد الحاجة إلى التمويل المصرفي الرقمي، برز خطر جديد: تحويل "الديون المصرفية الرقمية" إلى أداة للاستغلال. فبعض الدول النامية تقترض مليارات الدولارات لتمويل مشاريع مصرفية رقمية، لكنها تجد نفسها عاجزة عن السداد بسبب الأزمات المالية التي تضرب اقتصادها.

ففي جزر المحيط الهادئ، أدت الأزمات المالية إلى انهيار الإيرادات المصرفية، مما جعل سداد القروض المصرفية الرقمية مستحيلاً. وفي أمريكا اللاتينية، أدت الأزمات المالية إلى انهيار الصادرات، مما زاد من عجز الموازنات.

ويواجه القانون الدولي غياباً في حماية هذه الدول، لأن:

- لا توجد آلية لإعفاء الدول من الديون في حالات الأزمات المالية.

- معظم القروض المصرفية الرقمية تأتي بشروط صارمة تزيد من عبء الديون.

- لا توجد معايير دولية لـ"التمويل المصرفي الرقمي العادل".

وفي المقابل، بدأت بعض المبادرات. ففي مؤتمر صندوق النقد الدولي 2025، تم اقتراح "آلية لإعادة هيكلة الديون المصرفية"، لكنها لم تُعتمد بعد. أما في

مجموعة السبع، فإن "مبادرة التمويل المصرفي الرقمي العادل" لا تزال في طور النقاش.

أما في العالم العربي، فإن معظم الدول تعتمد على قروض خارجية لتمويل مشاريع النظام المصرفي الرقمي، دون وجود ضمانات قانونية لحمايتها من المخاطر المالية.

ويخلص هذا الفصل إلى أن التمويل المصرفي الرقمي يجب أن يكون هبة، لا ديناً، وأن الدول التي تدفع ثمن أخطاء غيرها لا ينبغي أن تُثقل بعبء الديون.

**الفصل السابع والعشرون

السيادة المصرفية الرقمية والنقل المصرفي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية**

لم يعد النقل المصرفي يعتمد فقط على البنوك، بل على أنظمة رقمية معقدة تدير سلاسل التوريد من البنك المركزي إلى المستهلك. واختراق هذه الأنظمة قد يؤدي إلى تلف الموارد المصرفية، أو تأخير التوزيع، أو سرقة الشحنات.

ففي عام 2024، تم اختراق نظام تتبع

الشحنات المصرفية في دولة أوروبية، مما أدى إلى تلف آلاف الموارد المصرفية بسبب تأخير التبريد. وفي عام 2025، تم سرقة شحنات موارد مصرفية عبر اختراق أنظمة الموانئ الرقمية.

ويواجه القانون الدولي غياباً في تصنيف سلاسل التوريد المصرفية الرقمية كجزء من "الأضرار المؤهلة للتعويض"، رغم أهميتها الاستراتيجية.

أما في الدول النامية، فإن غياب الموارد يحد من قدرتها على إعادة بناء سلاسل التوريد بعد الهجمات.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في مجال النقل ليست مسألة تقنية، بل مسألة أمن مصرفي، وأن سلاسل التوريد المصرفية الرقمية يجب أن تُعتبر جزءاً من البنية التحتية الحيوية.

**الفصل الثامن والعشرون

السيادة المصرفية الرقمية والبحث العلمي المصرفي المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم في مواجهة التحديات المصرفية دون تبادل المعرفة، لكن

هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية مصرفية حساسة — مثل نماذج التغير المالي المقاوم — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات المصرفية التي قدمتها الدول النامية لفرض شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها المصرفية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل التاسع والعشرون

السيادة المصرفية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة المصرفية الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها المصرفية الرقمية بمفردها، لأن التهديدات عابرة للحدود. ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض

معايير النظام المصرفي الرقمي من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية المصرفية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة المصرفية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة المصرفية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا يزال ضعيفاً، مما يحد من قدرة الدول على التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة المصرفية الرقمية يجب أن يقوم على مبدأ "السيادة المشتركة"، لا "الهيمنة المصرفية الرقمية".

**الفصل الثلاثون

السيادة المصرفية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات المصرفية**

مع تزايد استخدام الموارد المصرفية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية المصرفية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني الدولي؟ وهل يُعتبر التسبب المتعمد في أزمة مالية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للمصارف، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع المصرفية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً مصرفية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية المصرفية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية المصرفية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من

الأسلحة المصرفية الرقمية.

**الفصل الحادي والثلاثون

السيادة المصرفية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي المصرفي**

مع تزايد الأنشطة الفضائية المتعلقة بالنظام المالي — من الأقمار الصناعية لمراقبة الموارد المصرفية إلى الطائرات المسيرة الفضائية لتوزيع الموارد — برز تهديد جديد: التلوث الفضائي الذي يؤثر على الأنظمة المصرفية. فحطام الأقمار الصناعية قد يعيق أنظمة الرصد المصرفي، بينما تنبعثات

الصواريخ تؤثر على الغلاف الجوي الذي ينظم الاتصالات المصرفية.

وفي الممارسة، تخطط شركات خاصة لإطلاق آلاف الأقمار خلال العقد القادم لمراقبة الموارد المصرفية، دون أي تنظيم بيئي دولي. ومع ذلك، فإن معاهدات الفضاء الخارجي لا تأخذ في الاعتبار التأثيرات المصرفية لهذه الأنشطة.

ويواجه القانون الدولي إشكالية جوهرية: هل يُعد التلوث الفضائي جزءاً من "المسؤولية المصرفية الرقمية"؟ وهل يجب أن تخضع الشركات الفضائية لنفس القواعد التي تخضع لها الصناعات الأرضية؟

أما في الدول النامية، فإن غياب القدرة على الوصول إلى الفضاء يجعلها عاجزة عن المشاركة في وضع هذه القواعد، رغم تأثرها المباشر بالتلوث الفضائي.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية يجب أن تمتد إلى الفضاء الخارجي، وأن الأنشطة الفضائية المصرفية يجب أن تخضع لمبدأ "الوقاية المصرفية" مثلها مثل أي نشاط صناعي آخر.

**الفصل الثاني والثلاثون

السيادة المصرفية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً مصرفياً**

مع ظهور الذكاء الاصطناعي التوليدي، أصبح بإمكان أي جهة إنشاء محتوى وهمي — من صور إلى مقاطع صوتية إلى فيديوهات — يبدو حقيقياً تماماً. وهذه التكنولوجيا تُستخدم اليوم كسلاح رقمي لتضليل الجمهور، وزعزعة ثقة المجتمع، وتقويض الثقة في الأنظمة المصرفية الوطنية.

ففي عام 2025، تم تداول فيديوهات مزيفة لخبراء وهم يحذرون من سياسات مصرفية وطنية آمنة، مما أدى إلى انخفاض الثقة

في النظام المصرفي وانتشار المعلومات المضللة. وفي أزمات مصرفية، تم نشر أخبار كاذبة عن نقص في الموارد المصرفية الأساسية، مما أدى إلى ذعر شعبي وارتفاع غير مبرر في الأسعار.

ويواجه القانون الدولي صعوبة في التعامل مع هذه الظاهرة، لأن:

- المحتوى المزيف لا يُصنّف كـ"هجوم سيبراني مصرفي" وفق التعريفات الحالية.

- صانع المحتوى قد يكون برنامجاً، وليس شخصاً.

- نشر المحتوى يتم عبر منصات عابرة

للحدود، لا تخضع لرقابة الدولة المستهدفة.

وفي المقابل، بدأت بعض الدول بوضع ضوابط. ففي الاتحاد الأوروبي، يُلزم "قانون الذكاء الاصطناعي" الشركات بوضع علامة مائية رقمية على كل محتوى مولّد آلياً. أما في الولايات المتحدة، فإن "قانون الشفافية في الوسائط الاصطناعية" يجرّم استخدام المحتوى المزيف في الحملات التضليلية المصرفية.

أما في العالم العربي، فإن معظم التشريعات لا تغطي هذا النوع من التهديدات، رغم تزايد استخدامه ضد الأنظمة المصرفية الوطنية.

ويخلص هذا الفصل إلى أن غياب تنظيم الذكاء الاصطناعي التوليدي يحوّل الفضاء الرقمي إلى ساحة حرب نفسية مصرفية، ويستدعي تعريفاً جديداً للتدخل السيبراني المصرفي يشمل "التأثير الخبيث عبر المحتوى المزيف".

**الفصل الثالث والثلاثون

السيادة المصرفية الرقمية والبيانات الضخمة المصرفية: حماية السيادة من الاستغلال الرقمي**

مع تزايد الاعتماد على البيانات الضخمة في تحليل النظام المالي، أصبحت هذه البيانات مورداً استراتيجياً. لكن الدول النامية غالباً ما تفتقر إلى القدرة على جمع وتحليل بياناتها، فتلجأ إلى شركات أجنبية تمتلك هذه القدرات.

ففي بعض الحالات، استخدمت شركات خاصة بيانات مصرفية من دول نامية لتطوير نماذج تنبؤ تُباع بأسعار باهظة. بل إن بعض الحكومات استخدمت هذه البيانات لفرض شروط تجارية غير عادلة.

ويواجه القانون الدولي غياباً في حماية هذه البيانات، لأن:

- لا توجد اتفاقيات دولية تنظم ملكية البيانات المصرفية.

- معظم العقود بين الدول والشركات تبقى سرية.

- لا توجد معايير لـ"السيادة المصرفية الرقمية".

أما في الدول النامية، فإن غياب التشريعات يسمح باستغلال بياناتها دون مقابل عادل.

ويؤكد هذا الفصل أن البيانات المصرفية ليست مجرد أرقام، بل أداة للعدالة، وأن

الدول التي لا تحمي سيادتها الرقمية ستظل عاجزة عن المطالبة بحقوقها المصرفية.

**الفصل الرابع والثلاثون

السيادة المصرفية الرقمية والتعليم العالي المصرفي: نحو كليات وطنية للقانون المصرفي الرقمي**

لا يمكن بناء قدرات مصرفية رقمية وطنية دون مؤسسات تعليمية متخصصة تخرّج كوادر مؤهلة. فالاعتماد على الخبرات الأجنبية أو الدورات القصيرة لا يكفي لمواجهة التهديدات المعقدة. ولذلك، فإن

إنشاء كليات وطنية للقانون المصرفي الرقمي يُعد استثماراً استراتيجياً في السيادة المصرفية الرقمية.

وفي الدول الرائدة، أصبحت هذه الكليات مراكز بحث وتطوير. ففي جامعة هارفارد، يُدرّس "القانون المصرفي الرقمي الدولي". أما في جامعة أكسفورد، فإن "مركز القانون المصرفي" يدرّب المحامين على رفع الدعاوى المصرفية الرقمية.

أما في الدول النامية، فإن التعليم المصرفي الرقمي غالباً ما يكون جزءاً من أقسام علوم الحاسوب، دون تخصص كافٍ. وهذا ينتج خريجين قادرين على البرمجة، لكن

غير مؤهلين لفهم الجوانب القانونية أو الاستراتيجية للأمن المصرفي الرقمي.

وفي العالم العربي، بدأت بعض الدول بإنشاء برامج متخصصة، مثل "ماجستير الأمن المصرفي الرقمي" في جامعات الإمارات والسعودية. أما في دول أخرى، فلا تزال المناهج تفتقر إلى التحديث، ولا توجد روابط كافية بين الجامعات وقطاع الصناعة.

ويخلص هذا الفصل إلى أن التعليم العالي ليس مجرد وسيلة لتأهيل الأفراد، بل أداة لبناء هوية وطنية مصرفية رقمية، وأن الدول التي لا تستثمر في كليات القانون المصرفي الرقمي ستظل مستوردة

للمعرفة، لا منتجة لها.

**الفصل الخامس والثلاثون

السيادة المصرفية الرقمية والثقافة الرقمية المصرفية: حماية الإبداع المحلي من القرصنة والتهميش**

لا يقتصر الفضاء الرقمي على البيانات والخدمات، بل يشمل أيضاً الإبداع الثقافي المصرفي: الأفلام الوثائقية، الروايات، الفنون البصرية التي تروي قصص النظام المالي. ومع هيمنة المنصات العالمية على توزيع المحتوى، أصبح المبدعون المحليون عرضة للتهميش أو الاستغلال.

فمنصات البث قد تدفع تعويضات زهيدة للمبدعين المحليين، أو ترفض عرض محتواهم دون مبرر. بل وقد تُسرق أعمالهم وتُنسب إلى آخرين دون حماية قانونية كافية.

وفي المقابل، بدأت بعض الدول بوضع تشريعات لحماية المحتوى المحلي. ففي فرنسا، يُلزم القانون بوجود نسبة محددة من المحتوى الفرنسي في المنصات. أما في كوريا الجنوبية، فقد استثمرت الدولة في دعم المحتوى الرقمي المحلي، مما أدى إلى انتشاره عالمياً.

أما في العالم العربي، فإن الجهود لا تزال مجزأة، ولا توجد سياسات وطنية فعالة لدعم الإبداع الرقمي المصرفي المحلي أو حمايته من القرصنة.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية الثقافية هي جزء من الهوية الوطنية، وأن غيابها يحوّل الشعوب إلى مستهلكين سلبيين، لا مبدعين فاعلين.

**الفصل السادس والثلاثون

السيادة المصرفية الرقمية والتمويل الرقمي المصرفي: حماية العملات المصرفية من

التلاعب والاحتيال**

مع ظهور العملات الرقمية المصرفية والبلوك تشين المصرفي، أصبحت الأنظمة المالية التقليدية تواجه تحديات جديدة. فالعملات الرقمية المصرفية يمكن استخدامها لغسل الأموال تحت غطاء المشاريع المصرفية، أو لتمويل مشاريع وهمية.

وفي الممارسة، أدت عمليات الاحتيال في سوق العملات الرقمية المصرفية إلى خسائر تقدر بمليارات الدولارات. ومع ذلك، فإن التنظيم القانوني لهذا السوق يبقى ضعيفاً في كثير من الدول.

ويواجه القانون الدولي صعوبة في التعامل مع العملات الرقمية المصرفية، لأنها لا تخضع لسلطة دولة واحدة، ولا يمكن تتبع مالكيها بسهولة.

أما في الدول النامية، فإن غياب التنظيم يسمح باستغلال هذه العملات لسرقة التمويل المصرفي المخصص للمشاريع الحقيقية.

ويخلص هذا الفصل إلى أن السيادة المصرفية الرقمية في المجال المالي لا تعني منع الابتكار، بل وضع ضوابط تحمي الاقتصاد الوطني من المخاطر غير

المحسوبة.

**الفصل السابع والثلاثون

السيادة المصرفية الرقمية والبحث العلمي المصرفي المفتوح: التوازن بين التعاون والحماية**

لا يمكن تحقيق التقدم العلمي في مواجهة التحديات المصرفية دون تبادل المعرفة، لكن هذا التبادل يجب أن يتم ضمن حدود تحمي المصالح الوطنية. فنشر بيانات بحثية مصرفية حساسة — مثل نماذج التغير المالي المقاوم — قد يُستخدم ضد الدول النامية في المفاوضات الدولية.

ففي بعض الحالات، استخدمت الدول الصناعية البيانات المصرفية التي قدمتها الدول النامية لفرض شروط تجارية غير عادلة. بل إن بعض الشركات الخاصة تشتري هذه البيانات وتعيد بيعها بأسعار باهظة.

ويواجه القانون الدولي تحدي التوازن بين:

- حق المجتمع العلمي في الوصول إلى المعرفة.

- حق الدولة في حماية بياناتها المصرفية من الاستغلال.

أما في الدول النامية، فإن غياب سياسات واضحة يجعلها عرضة لاستغلال أبحاثها دون مقابل عادل.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في البحث العلمي تعني وضع تصنيفات واضحة للبيانات، وتحديد ما يُسمح بنشره وما يجب حمايته، دون عزلة علمية.

**الفصل الثامن والثلاثون

السيادة المصرفية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة المصرفية

الرقمية**

لا يمكن لأي دولة أن تحمي سيادتها المصرفية الرقمية بمفردها، لأن التهديدات عابرة للحدود. ولذلك، فإن التعاون الدولي ليس خياراً، بل ضرورة. لكن هذا التعاون يجب أن يكون عادلاً، لا أداة لهيمنة الدول الصناعية.

ففي المحافل الدولية، غالباً ما تُفرض معايير النظام المصرفي الرقمي من قبل الدول الصناعية، دون مراعاة قدرات الدول النامية. وهذا يخلق نظاماً غير عادل يكرس التبعية المصرفية الرقمية.

ويستدعي الحل:

- إنشاء منتدى دولي محايد لصياغة قواعد السيادة المصرفية الرقمية.

- توفير الدعم الفني والمالي للدول النامية.

- احترام التنوع في النماذج الوطنية للسيادة المصرفية الرقمية.

أما في العالم العربي، فإن التنسيق الإقليمي لا يزال ضعيفاً، مما يحد من قدرة الدول على التفاوض ككتلة واحدة.

ويخلص هذا الفصل إلى أن النظام العالمي للحوكمة المصرفية الرقمية يجب أن يقوم على مبدأ "العدالة المشتركة"، لا "الهيمنة المصرفية الرقمية".

**الفصل التاسع والثلاثون

السيادة المصرفية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات المصرفية**

مع تزايد استخدام الموارد المصرفية كسلاح في النزاعات، برز سؤال جوهري: هل يُعد تدمير البنية التحتية المصرفية الرقمية كوسيلة حربية انتهاكاً للقانون الإنساني

الدولي؟ وهل يُعتبر التسبب المتعمد في أزمة مالية جريمة حرب؟

ففي بعض النزاعات، تم تدمير أنظمة التبريد الرقمية للمصارف، مما أدى إلى تلفها. وفي حالات أخرى، تم اختراق منصات التوزيع المصرفية لإجبار السكان على النزوح. وكل هذه الأفعال تسبب أضراراً مصرفية طويلة الأمد.

وفي مشروع "قواعد تالين 2.0"، تم التأكيد على أن تدمير البنية التحتية المصرفية كوسيلة حربية يُعد انتهاكاً للقانون الإنساني. لكن التطبيق العملي يبقى صعباً بسبب غموض النية وصعوبة إثبات

العلاقة السببية.

أما في المحكمة الجنائية الدولية، فإن "جريمة تدمير البنية التحتية المصرفية" لا تزال قيد النقاش، ولم تُدرج بعد في النظام الأساسي.

ويؤكد هذا الفصل أن السيادة المصرفية الرقمية في زمن الحرب لا تعني التخلي عن الإنسانية، بل تعزيز حماية المدنيين من الأسلحة المصرفية الرقمية.

**الفصل الأربعون

السيادة المصرفية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة**

في الختام، لا يمكن النظر إلى السيادة المصرفية الرقمية كظاهرة مؤقتة، بل كتحول جوهري في مفهوم الحماية المصرفية في القرن الحادي والعشرين. فالدول التي تبني سيادتها المصرفية الرقمية اليوم ستكون قادرة على:

- حماية مواطنيها من التلاعب المصرفي الرقمي.

- بناء اقتصاد مصرفي رقمي مستقل ومستدام.

- تعزيز مكانة أجيالها في النظام المصرفي العالمي.

- المشاركة الفاعلة في صياغة قواعد النظام الدولي الجديد.

أما الدول التي تتجاهل هذا التحول، فستجد نفسها رهينة للتكنولوجيا الأجنبية، وعرضة للتدخلات الخارجية، وعاجزة عن حماية مصالحها في العصر الرقمي.

ولذلك، فإن الاستثمار في السيادة المصرفية الرقمية ليس مسألة اختيار، بل مسألة بقاء.

خاتمة

بعد استعراض شامل لأبعاد السيادة المصرفية الرقمية في مختلف المجالات — من الأمن السيبراني إلى الاقتصاد، ومن الثقافة إلى التنمية — يتبين أن هذا المفهوم لم يعد رفاهية تقنية، بل ضمانة وجودية للدولة الحديثة. فالفضاء المصرفي الرقمي، رغم طبيعته غير المادية، بات ساحة للصراعات السياسية والاقتصادية، ولا يمكن لأي دولة أن تحافظ على سيادتها المصرفية دون وجود قدرات رقمية وطنية

فاعلة.

وقد كشف هذا العمل أن الفراغ التشريعي الدولي يشكل تهديداً مزدوجاً: فهو يسمح للدول والشركات الكبرى بفرض هيمنتها، ويترك الدول النامية عرضة للاستغلال دون حماية قانونية. ولسد هذا الفراغ، لا بد من مبادرة جماعية تبني نظاماً دولياً عادلاً يوازن بين الابتكار المصرفي وسيادة الدولة على أنظمتها المصرفية.

وفي النهاية، فإن السيادة المصرفية الرقمية الحقيقية لا تُبنى على العزلة أو القمع، بل على الشفافية، والكفاءة، والثقة بين الدولة والمواطن. وهي ليست غاية بذاتها، بل

وسيلة لبناء مستقبل مصرفي آمن، عادل، وإنساني.

المراجع

Basel Committee on Banking Supervision (BCBS) Guidelines on (Cyber Resilience (2021

International Monetary Fund (IMF) (Report on Digital Currencies (2023

Financial Action Task Force (FATF) (Guidance on Virtual Assets (2022

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ((Cambridge University Press, 2017

UNODC Handbook on Strategies to (Combat Cybercrime (2023

European Central Bank. Digital Euro (Report (2024

People’s Bank of China. Digital Yuan

(Framework (2022

Elrakhawi M K A. (2026). The Global Encyclopedia of Law – A Comparative Practical Study. First Edition. Ismailia: Global Legal Publications

Schmitt M N. (2023). Cyber Operations and International Law. Cambridge University Press

Rajamani L. (2025). Financial Sovereignty and Digital Control. Oxford University Press

De Schutter O. (2023). The Right to Financial Stability in the Digital Age. Cambridge University Press

Kloppenburg J R. (2024). Digital Sovereignty and Financial Exploitation. University of California Press

:Official Government Sources

White House. National Strategy for (Digital Finance (2024

European Commission. Digital Finance (Action Plan (2023

Ministry of Finance Reports on Cyber Resilience in Financial Systems ((Multiple Jurisdictions, 2020–2025

:Academic Journals

Journal of International Financial Law ((Oxford

International Journal of Digital Financial Sovereignty

Harvard Law Review – Financial Regulation Section

Stanford Technology Law Review

فهرس المحتويات

المادية إلى الظاهرة القانونية الجديدة

الفصل الثاني

الفراغ القانوني الدولي المالي في حماية الأنظمة المصرفية الرقمية

الفصل الثالث

السيادة المصرفية التقليدية مقابل السيادة المصرفية الرقمية: إعادة تشكيل المفاهيم القانونية

الفصل الرابع

البنية التحتية المصرفية الرقمية: تعريف قانوني دولي مفقود

الفصل الخامس

التلاعب السيبراني في الأنظمة المصرفية: نحو معيار قانوني دولي

الفصل السادس

المسؤولية الدولية عن الهجمات السيبرانية المصرفية: تحديات الإسناد والرقابة

الفصل السابع

الردود المشروعة على الانتهاكات السيبرانية المصرفية: بين التدابير المضادة والقوة المسلحة

الفصل الثامن

السيادة المصرفية الرقمية وبراءات الاختراع المصرفية: التوتر بين الابتكار والاستغلال

الفصل التاسع

السيادة المصرفية الرقمية في الدول النامية: تحديات القدرة والاعتماد

التكنولوجي

الفصل العاشر

التنظيم الإقليمي للسيادة المصرفية الرقمية: دراسة مقارنة بين التجارب العالمية

الفصل الحادي عشر

السيادة المصرفية الرقمية والبيانات المصرفية: حماية الخصوصية المصرفية من الاستغلال الخارجي

الفصل الثاني عشر

السيادة المصرفية الرقمية والذكاء الاصطناعي المصرفي: عندما تصبح الخوارزميات سلطة خارج نطاق الدولة

الفصل الثالث عشر

السيادة المصرفية الرقمية والجرائم الإلكترونية المصرفية: مكافحة الاحتيال المالي الرقمي

الفصل الرابع عشر

السيادة المصرفية الرقمية والتربية الرقمية

المصرفية: بناء وعي مجتمعي كأساس للدفاع السيبراني

الفصل الخامس عشر

السيادة المصرفية الرقمية والبحث العلمي المصرفي: نحو استقلال تكنولوجي وطني

الفصل السادس عشر

السيادة المصرفية الرقمية والاتفاقيات الثنائية: هل يمكن للدول الصغيرة أن تحمي نفسها؟

الفصل السابع عشر

السيادة المصرفية الرقمية والمحاكمات المصرفية: نحو اختصاص قضائي رقمي

الفصل الثامن عشر

السيادة المصرفية الرقمية والبيانات المصرفية: بين الملكية الفردية والسيادة الجماعية

الفصل التاسع عشر

السيادة المصرفية الرقمية والاستقرار المجتمعي: حماية المجتمعات من

السيادة المصرفية الرقمية والطاقة المصرفية: حماية الموارد من الاستنزاف الرقمي

الفصل الثالث والعشرون

السيادة المصرفية الرقمية وسلامة المصرفيين: حماية المصرفيين من التلاعب الرقمي

الفصل الرابع والعشرون

السيادة المصرفية الرقمية والتعليم المصرفي الرقمي: بناء وعي مجتمعي كأساس للدفاع عن الحقوق

الفصل الخامس والعشرون

السيادة المصرفية الرقمية والتراث المصرفي: حماية التراث من الاندثار الرقمي

الفصل السادس والعشرون

السيادة المصرفية الرقمية والتمويل المصرفي الرقمي: حماية الدول النامية من الديون المصرفية

الفصل السابع والعشرون

السيادة المصرفية الرقمية والنقل المصرفي الرقمي: حماية سلاسل التوريد من التهديدات السيبرانية

الفصل الثامن والعشرون

السيادة المصرفية الرقمية والبحث العلمي المصرفي المفتوح: التوازن بين التعاون والحماية

الفصل التاسع والعشرون

السيادة المصرفية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة المصرفية الرقمية

الفصل الثلاثون

السيادة المصرفية الرقمية والقانون الإنساني الدولي: حماية المدنيين في النزاعات المصرفية

الفصل الحادي والثلاثون

السيادة المصرفية الرقمية والفضاء الخارجي: حماية الأرض من التلوث الفضائي المصرفي

الفصل الثاني والثلاثون

السيادة المصرفية الرقمية والذكاء الاصطناعي التوليدي: عندما تصبح الأخبار الكاذبة سلاحاً مصرفياً

الفصل الثالث والثلاثون

السيادة المصرفية الرقمية والبيانات الضخمة المصرفية: حماية السيادة من الاستغلال الرقمي

الفصل الرابع والثلاثون

السيادة المصرفية الرقمية والتعليم العالي المصرفي: نحو كليات وطنية للقانون

الفصل الخامس والثلاثون

السيادة المصرفية الرقمية والثقافة الرقمية المصرفية: حماية الإبداع المحلي من القرصنة والتهميش

الفصل السادس والثلاثون

السيادة المصرفية الرقمية والتمويل الرقمي المصرفي: حماية العملات المصرفية من التلاعب والاحتيال

الفصل السابع والثلاثون

السيادة المصرفية الرقمية والبحث العلمي المصرفي المفتوح: التوازن بين التعاون والحماية

الفصل الثامن والثلاثون

السيادة المصرفية الرقمية والتعاون الدولي: نحو نظام عالمي عادل للحوكمة المصرفية الرقمية

الفصل التاسع والثلاثون

السيادة المصرفية الرقمية والقانون

الإنساني الدولي: حماية المدنيين في النزاعات المصرفية

الفصل الأربعون

السيادة المصرفية الرقمية والمستقبل: رؤية استراتيجية للعقود القادمة

خاتمة

بيان حقوق الملكية

جميع الحقوق محفوظة للمؤلف

© 2026 الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار القانوني

المحاضر الدولي في القانون

يحظر منعاً باتاً:

نسخ أو طبع أو نشر أو توزيع أو اقتباس أو ترجمة أو تحويل أو عرض أي جزء من هذا العمل — سواء كان ذلك إلكترونياً، رقمياً، مطبوعاً، أو بأي وسيلة أخرى — دون

الحصول على **تصريح كتابي صريح ومسبق** من المؤلف.

الاستثناء الوحيد:

يجوز الاقتباس لأغراض بحثية أو أكاديمية، بشرط:

- ذكر اسم المؤلف كاملاً: **الدكتور محمد كمال عرفه الرخاوي**.

- ذكر عنوان المؤلف كاملاً: **"السيادة المصرفية الرقمية: دراسة قانونية حول حماية البنوك الرقمية من التلاعب السيبراني وبناء نظام مالي رقمي إنساني عالمي"**.

- ذكر رقم الصفحة بدقة.

- عدم تغيير السياق أو المعنى.

التحديث:

أي تحديث أو طبعة جديدة لهذا العمل ستُعلن عنها رسمياً عبر الموقع الإلكتروني المعتمد للمؤلف.

تم بحمد الله وتوفيقه

تأليف الدكتور محمد كمال عرفه الرخاوي