BANQUE DE FRANCE
EUROSYSTÈME

Paiements : Préserver la confiance dans un monde plus incertain

Discours d'introduction à la conférence de l'OSMP et du CNMP

Mardi 6 mai 2025

Denis Beau, Premier sous-gouverneur

Introduction

- C'est avec grand plaisir que j'ouvre cette conférence organisée conjointement par l'Observatoire de la sécurité des moyens de paiement (OSMP) et le Comité national des moyens de paiement (CNMP), que nous avons intitulée « *Préserver la confiance dans un monde plus incertain* ».
- En juin 2024, l'OSMP avait organisé une conférence centrée sur les perspectives de l'informatique quantique. Pour cette deuxième édition, je me réjouis d'y associer le CNMP, présidé par Erick Lacourrège. Il s'agit en effet de deux instances « sœur », qui ont pour caractéristique d'associer l'ensemble des acteurs de l'écosystème des paiements dans la définition des orientations stratégiques et de sécurité. Au regard de l'actualité récente comme des tendances de fond, cette caractéristique, tout à fait unique en Europe, est une force.
- En effet, notre monde n'a jamais été aussi interconnecté, mais également aussi incertain et imprévisible. Pour nous, Français et Européens, les évolutions technologiques, la montée des risques géopolitiques et les positions récentes prises par la nouvelle administration américaine en matière de dérégulation de leur système financier soulèvent de nouveaux défis en termes de sécurité, d'innovation et de souveraineté. Le secteur des paiements n'échappe pas à ces dynamiques et connaît des transformations d'ampleur.

- Dans ce contexte, il est primordial de maintenir des paiements sûrs, tout en veillant à promouvoir l'innovation grâce à l'exploitation des nouvelles technologies. L'alliance de la sécurité et de l'innovation constitue le socle fondamental de la confiance dans notre système de paiement et dans notre monnaie, l'euro.
- Ces objectifs sont au cœur du mandat de la Banque de France et de l'OSMP, et inspirent en particulier leur activité de veille technologique, dont les résultats en matière d'intelligence artificielle (IA) vont être présentés et discutés ce matin dans le cadre de deux table-rondes.
- Avant de leur laisser la place, je voudrais partager avec vous trois convictions, forgées par mon expérience à la Banque de France dans l'exercice de notre mandat de veiller à la sécurité des paiements et à notre travail commun au sein de l'OSMP. Elles contribuent à expliquer nos succès passés dans la lutte contre la fraude aux moyens de paiement, et peuvent, je le crois, continuer à guider nos actions pour préserver ces résultats et les renforcer à l'avenir dans le nouveau contexte que nous connaissons.

I. En premier lieu, l'innovation technologique peut être « la meilleure comme la pire des choses » en matière de sécurité des paiements et il faut donc tenir compte de son appropriation par les fraudeurs.

- **Notre action pour la sécurité des paiements évolue et s'améliore grâce à l'innovation technologique**. Face à la complexification des techniques de fraude, notamment, les nouvelles technologies nous permettent d'identifier plus efficacement et plus rapidement les schémas et stratagèmes des fraudeurs. L'intégration de l'IA dans les modèles de lutte contre la fraude, qui sera le thème de la première table-ronde ce matin, renforce d'ores et déjà la sécurité des moyens de paiement numériques proposés au public. L'OSMP a fourni un travail de veille approfondi sur ce sujet en 2024, montrant que ces techniques sont essentielles et matures pour mieux détecter les fraudes, surtout dans un monde où l'instantanéité des paiements se déploie. L'étude de l'OSMP qui sera publiée dans notre prochain rapport annuel, en septembre prochain, constitue un appel à l'ensemble des acteurs des paiements à s'en saisir avec volonté mais aussi avec méthode.
- **Cependant, l'innovation crée de nouveaux risques et des incertitudes, notamment dans son appropriation par les fraudeurs**. Parmi ces risques, l'intelligence artificielle est un facteur clair d'amplification des risques de fraude. Et, ainsi qu'il sera discuté dans la seconde table-ronde de la matinée, l'IA peut considérablement faciliter de nouvelles

formes d'escroqueries dans les paiements, par exemple au moyen de falsifications documentaires ou de *deepfakes*, formes d'hypertrucages qui peuvent aller jusqu'à imiter la voix de personnes de confiance pour perfectionner les schémas de manipulation.

- **La sécurité des paiements passe, en conséquence, par une veille permanente des nouveaux usages et technologies**, à la fois pour améliorer les techniques de sécurisation des paiements, mais aussi pour identifier les nouvelles vulnérabilités et y répondre.

II. En deuxième lieu, il me faut aussi rappeler que la sécurité des paiements doit impliquer et associer tous les acteurs de la chaîne et par conséquent que le cercle des parties prenantes doit être géré de façon dynamique

- **En effet, la technologie ne saurait suffire à assurer la pleine sécurité des moyens de paiement et il est primordial de rappeler l'importance du bon usage des moyens de paiement par les particuliers, les entreprises et les administrations.**
  - Pour s'assurer de cela, il faut **mettre en avant les bonnes pratiques en matière de paiement**, ce qui apparaît, chaque année, à la fois dans les recommandations portées par l'OSMP, ainsi que dans les campagnes de communication menées avec le soutien de l'Observatoire et de la Banque de France. Ces conseils de prudence, qui sont rédigés en collaboration avec les représentants des consommateurs, des commerçants et des émetteurs, sont essentiels mais ils doivent surtout être largement relayés et répétés par l'ensemble de l'écosystème, sous des formats diverses et innovants, y compris au travers des réseaux sociaux et des influenceurs, pour que ces conseils de prudence touchent leur public et deviennent des « réflexes naturels ».
  - Les manipulations par téléphone, avec un faux conseiller bancaire, sont désormais contenues mais elles n'ont malheureusement pas disparu. Nous avons donc encore des marges de progrès et c'est la raison pour laquelle **l'OSMP défend une approche exigeante mais équilibrée en matière de remboursement des fraudes.**
- **La sophistication et la « professionnalisation » des fraudeurs impose, en complément, d'élargir le cercle des parties associées à la lutte contre la fraude**.
  - L'expérience nous montre, en effet, la nécessité d'**installer une coopération rapprochée entre autorités et acteurs privés** pour contenir la fraude et comprendre ses transformations. C'est l'esprit de l'élargissement du tour de table de l'OSMP que nous avons mené ces dernières années, en associant les opérateurs téléphoniques,

leurs représentants et leur régulateur. Ceci a déjà permis de suivre le déploiement du dispositif d'authentification des appels, qui a été déployé avec succès fin 2024 et début 2025, et de promouvoir d'autres outils coopératifs de lutte contre la fraude entre les banques et les opérateurs téléphoniques.

- Nous devons travailler désormais, avec l'appui des autres régulateurs nationaux (ARCOM, CNIL, DGCCRF), à élargir cette coopération de l'OSMP aux **réseaux sociaux et aux grandes plateformes numériques**, car ceux-ci sont les nouveaux terrains d'action des fraudeurs, par le biais de communications et liens frauduleux.
- Enfin, alors que nous faisons la promotion de moyens de paiement européens et que les fraudeurs ne connaissent pas de frontières, nous devons **penser la lutte contre la fraude à l'échelle européenne.** Dans ce contexte, il faut se réjouir que les dernières évolutions du projet de Règlement européen sur les services de paiement (RSP), discutées au Conseil européen, évoquent l'installation d'un Forum pour la sécurité des paiements, qui serait le miroir européen de l'OSMP français, avec donc une participation large de tous les acteurs de marché : offre, demande et autorités publiques concernées. Plus qu'un simple forum d'échange, il lui faudra un mandat clair, des statistiques fiables et des pouvoirs d'action pour réussir ; et je souhaite que les banques centrales y prennent toute leur part.

III. Enfin, 3e conviction, au regard du contexte actuel, le lien entre la sécurité et la souveraineté des moyens de paiement est appelé à se renforcer.

- **Notre écosystème des paiements est résilient, mais on observe aujourd'hui une domination des acteurs non-européens dans la fourniture de services critiques, ce qui génère des risques dans la nouvelle donne géopolitique.**
  - Les **orientations politiques de la nouvelle administration américaine, qui donnent la priorité aux intérêts économiques et financiers américains et à l'usage des rapports de force pour l'imposer**, génèrent en effet des incertitudes en matière d'utilisation et de récupération des données, de continuité et de disponibilité de leurs services, ou encore sur les prix de ces services.
  - **L'utilisation de nouvelles technologies est hautement souhaitable pour la sécurité des paiements,** mais j'appelle aussi l'écosystème des paiements à tenir compte de l'origine de ces technologies et de leurs fournisseurs. Conscients de nos interdépendances, les enjeux de sécurité ne peuvent plus se détacher des enjeux de souveraineté et d'autonomie stratégique dans les paiements.

- **L’action menée sur les moyens de paiement doit donc être systématiquement pensée en conséquence de ces évolutions et du risque géopolitique sous-jacent, et ce sujet sera abordé plus longuement dans les table-rondes de cet après-midi.**
    - **Les cadres réglementaires doivent évidemment être adaptés** pour répondre à ces enjeux, qu’il s’agisse de la réglementation du secteur des crypto-actifs, sous forte domination d’acteurs américains, dans le cadre de MiCA, ou du cadre général des paiements, avec le Règlement sur les services de paiement (RSP), qui devrait remplacer la DSP2, en travaillant par exemple à une meilleure régulation des systèmes de paiement par carte, des portefeuilles électroniques ou des grands prestataires d’acceptation.
    - **Il faudra veiller également à ce que les moyens de paiement sûrs et innovants de demain soient européens.** Les initiatives privées visant à renforcer la souveraineté, dans un cadre de concurrence ouverte, comme celles portées par CB ou Wero, sont évidemment essentiels pour assurer des moyens de paiement européens, qui répondent aux besoins des concitoyens. Elles pourront et elles devront s’appuyer sur les initiatives publiques, dont bien évidemment le projet d'euro numérique, pour assurer conjointement la souveraineté des paiements et donc notre sécurité collective en ce domaine.

Conclusion

Pour nous éclairer sur ces différents enjeux et lancer cette conférence, j’ai le plaisir d’accueillir M. Renaud Labelle, sous-directeur de l’expertise à l’Agence Nationale de Sécurité des Systèmes d’information (ANSSI), laquelle est un membre actif de l’OSMP et qui va nous apporter son éclairage sur les enjeux actuels en matière de sécurité dans le monde numérique, dans ce contexte géopolitique plus risqué que nous connaissons.

Je vous remercie de votre attention et vous souhaite une excellente conférence.