



Conférence OSMP – CNMP

Jeudi 9 avril 2026

L'Europe des paiements face à ses défis

Discours d'introduction

Denis Beau, Premier sous-gouverneur

Introduction

- C'est avec grand plaisir que j'ouvre cette troisième édition de la conférence organisée par les deux instances « sœur » que sont l'Observatoire de la sécurité des moyens de paiement (OSMP) et le Comité national des moyens de paiement (CNMP), intitulée cette année « *L'Europe des paiements face à ses défis* ».
- Bienvenue à ce rendez-vous annuel qui témoigne à la fois de l'ancrage de ces deux instances dans leur écosystème, et de leur ouverture vers l'ensemble des personnes intéressées par les paiements, qu'ils soient professionnels, utilisateurs ou tout simplement citoyens.
- Pour cette édition, je voudrais plus spécialement saluer trois personnalités présentes aujourd'hui, en les remerciant par avance pour leurs interventions. Elles sont la manifestation de cet ancrage et de cette ouverture :
 - Tout d'abord, Mme la sénatrice Nathalie Goulet, qui participe activement aux sessions de l'Observatoire et est particulièrement mobilisée comme Parlementaire sur les sujets de lutte contre la fraude, comme l'a illustrée son action dans l'adoption de la loi du 6 novembre 2025 contre la fraude bancaire ;
 - Ensuite, Mme Constance Guisset, qui participe au jury pour le design de la troisième gamme de billets en euro, et qui partagera avec nous son regard d'artiste sur la monnaie ;
 - Et enfin M. Jean-Baptiste Djebbari, ancien ministre des Transports, qui pourra nous éclairer sur ce secteur, aussi critique que celui des paiements pour notre vie quotidienne, et qui est traversé, comme celui des paiements, par des enjeux d'autonomie européenne et de coopération entre les secteurs public et privé.

- Notre conférence de cette année s'ouvre dans un contexte où la numérisation des paiements se déploie résolument et suscite de nouveaux défis en matière de sécurité, de résilience et de souveraineté. Même s'ils sont parfois traités séparément, ces trois défis me semblent en réalité intimement liés et je voudrais partager avec vous deux réflexions liminaires, pour alimenter les débats qui se succéderont aujourd'hui.

I. La première réflexion porte sur la sécurité des paiements qui n'est jamais définitivement acquise et requiert une vigilance constante et appelle de nouveaux outils.

- **Même si l'on observe des tendances encourageantes –la dernière publication de l'OSMP sur les chiffres du premier semestre 2025 en atteste–, nous devons rester constamment vigilants et mobilisés, pour deux raisons principales.** Tout d'abord, parce que le niveau de menaces reste très élevé. La fraude se déplace en ciblant moins les failles technologiques mais en s'attaquant aux vulnérabilités humaines, avec un niveau toujours élevé de fraudes par manipulation et un usage de plus en plus répandu des outils d'intelligence artificielle par les fraudeurs. Ensuite, parce que de nouveaux produits se développent dans la sphère des paiements. C'est le cas des crypto-actifs, sujet qui sera exploré lors de notre 2^e table-ronde. Ceux-ci présentent à la fois des risques similaires aux moyens de paiement traditionnels, justifiant ainsi l'application du principe « *mêmes activités, mêmes risques, mêmes règles* », mais aussi des risques spécifiques, par exemple la sécurité de leurs propres infrastructures, les *blockchains*, rendant nécessaire l'application de règles propres. C'est également le cas des paiements dits « agentiques », c'est-à-dire des paiements réalisés tout ou partie par l'intermédiaire d'un agent d'IA. Ces paiements, encore en développement, devront évidemment s'articuler avec les exigences d'authentification forte des paiements.
- **Par conséquent, le développement de nouveaux outils apparaît indispensable pour concilier efficacement innovation et sécurité.** C'est ce qui a été fait avec la vérification du bénéficiaire en octobre 2025, qui permet de vérifier la cohérence des coordonnées bancaires, pour sécuriser le développement du virement instantané. C'est aussi ce que nous préparons avec le nouveau fichier national des comptes signalés pour risque de fraude (FNC-RF) qui entrera en service début mai et qui permettra aux acteurs bancaires de partager leurs signalements sur les comptes utilisés par les fraudeurs. Outre le fait que cette plateforme résulte d'une coopération particulièrement efficace entre parlementaires, administrations et profession bancaire, elle préfigurera aussi le partage de données prévu par la future réglementation européenne sur les paiements (DSP3-RSP), en cours de finalisation. Par-delà la réglementation, qui est souvent nécessaire mais jamais suffisante, la coopération entre les

différents acteurs de la chaîne reste absolument primordiale pour contrecarrer l'action des fraudeurs. À cet égard, la coopération qui existe déjà, notamment au sein de l'OSMP, avec les opérateurs téléphoniques, doit désormais se prolonger avec les grands acteurs du numérique. La présence de Google pour la première table-ronde dédiée à la lutte contre la fraude par manipulation en est la parfaite illustration.

- **De nouveaux outils restent à explorer et à construire avec les acteurs du numérique, mais il faudra nécessairement préserver un équilibre entre protection des utilisateurs et responsabilisation des acteurs.** Celui-ci repose, à mon sens, à la fois sur le cadre légal en matière de remboursement des fraudes, sur lequel nous nous aurons tout à l'heure l'éclairage déterminant de la Cour de cassation, et l'indispensable vigilance des utilisateurs. Les actions et campagnes de sensibilisation, à tous niveaux et par tous canaux, sont véritablement utiles et nécessaires et doivent s'inscrire dans la dynamique globale d'éducation financière.

II. Ma seconde réflexion est que la sécurité des paiements ne s'arrête pas à la lutte contre la fraude : elle doit désormais s'élargir aux enjeux de résilience et prendre en compte le besoin de souveraineté.

- Si le grand public perçoit les risques de fraude, il est moins naturellement conscient des enjeux de résilience et de souveraineté. Sans doute, parce que l'écosystème français a su démontrer sa robustesse et garantir son autonomie, probablement mieux que d'autres pays.
- Il s'agit pourtant d'une activité critique, au cœur de notre vie quotidienne, de l'activité de nos entreprises et de nos administrations, qui est essentielle à notre indépendance et à notre sécurité collective : il appartient donc à l'écosystème des paiements de répondre à cette triple exigence de sécurité, résilience et souveraineté.
- **L'objectif de résilience suppose tout d'abord de disposer d'un cadre de réponse aux incidents opérationnels et à la menace cyber.** En ce sens, le cadre réglementaire européen a rehaussé le niveau d'exigences sur l'ensemble de la chaîne, y compris vis-à-vis des prestataires critiques, notamment avec le règlement DORA, sur lequel reviendra plus en détails Marc Andriès au nom des autorités européennes de supervision cet après-midi. Mais notre capacité collective de réponse aux crises doit aussi continuer à se renforcer sous l'égide du Groupe de Place Robustesse (GPR) et de ses cellules de place dédiées aux moyens de paiement (CCP-S pour le scriptural, CCP-F pour le fiduciaire) pour réagir en cas d'incident ou d'attaque cyber, mobiliser les dispositifs de secours et conforter la communication auprès de l'ensemble des acteurs de la chaîne et du public.
- **Cette résilience passe aussi par une offre plurielle de moyens de paiement, de façon à transformer la « liberté de choix » des utilisateurs en situation nominale en « capacité de payer » en cas d'incident.** Les espèces sont, en ce sens, un excellent instrument de notre

résilience et nous nous engageons pleinement pour son avenir avec l'ensemble de la filière fiduciaire : que ce soit au niveau industriel, avec la construction d'une nouvelle imprimerie de billets en Auvergne, ou pour l'adhésion des citoyens, avec la future gamme de billets en euros, désignée dans notre jargon l'ES3. Cet impératif de résilience justifie aussi notre défense du principe de co-marquage des cartes avec le réseau national CB, qui est une force de l'écosystème français, dans un contexte où la carte reste prédominante sur tous les cas d'usage, y compris dans le paiement mobile. Les dernières annonces de grands établissements sur leur pleine adhésion au co-marquage ne peuvent qu'être très largement saluées dans cette optique. Ce principe de résilience justifie aussi notre soutien au projet Wero qui doit prochainement offrir une alternative supplémentaire aux consommateurs européens pour leurs paiements sur internet comme en magasin.

- **Les objectifs de sécurité et résilience doivent naturellement être associés à cette ambition stratégique de souveraineté, et nous croyons fermement à la Banque de France que celle-ci doit pouvoir fédérer les acteurs publics et privés.** La dépendance à des technologies et des acteurs extra-européens suscite en effet des risques de continuité dans la nouvelle donne géopolitique. C'est, en conséquence, la motivation de l'euro numérique que d'offrir un nouveau moyen de paiement complètement souverain sous la forme d'un « billet numérique ». Les différents projets publics et privés qui visent à répondre à cet objectif de souveraineté ne s'opposent pas. Ils se complètent au contraire et ce sera l'enjeu de la 4^e table-ronde que d'explorer les conditions de leur coexistence et les possibilités de coopération.

Conclusion

- Dans un marché des paiements de plus en plus intégré, ces enjeux de sécurité, de résilience et de souveraineté sont naturellement européens, et les réponses doivent idéalement être européennes.
- Ces défis européens n'interdisent toutefois pas l'action au niveau national, bien au contraire, car ces grands projets européens ont besoin d'instances nationales comme l'OSMP et le CNMP à même de déployer ces réponses européennes sur leur marché et d'explorer de nouveaux outils, dans un va-et-vient permanent entre l'échelon national et l'échelon européen.
- C'est exactement ce que nous avons démontré avec le nouveau fichier national des comptes signalés comme frauduleux. Je suis heureux d'accueillir maintenant Mme Nathalie Goulet, qui a participé à l'élaboration de cette loi, pour lancer cette conférence et partager avec nous ses réflexions sur les défis des paiements et les enjeux de lutte contre toutes les formes de fraude.