SOUVERAINETÉ EUROPÉENNE DES PAIEMENTS (2026-2035)

De la dépendance structurelle à la construction d'une doctrine des paiements européenne

Camille BOULENGUER / Économiste, chercheuse à l'IRIS

Sami NAKIB / Assistant de recherche à l'IRIS

Juin 2026

PRÉSENTATION DES AUTEURS

Camille BOULENGUER / Économiste, chercheuse à l'IRIS

Camille Boulenguer est économiste, chercheuse à l'IRIS. Elle y dirige l'Observatoire géopolitique du numérique et des technologies émergentes.

Ses travaux se situent à la confluence entre l'économie industrielle et la fiscalité, et interrogent les imbrications entre économie légale et économie illégale. Elle est par ailleurs co-responsable pédagogique du parcours Risques géoéconomiques et intelligence stratégique d'IRIS Sup'.

Camille Boulenguer est doctorante en économie de l'Université Picardie Jules Verne.

Sami NAKIB / Assistant de recherche à l'IRIS

Sami Nakib est assistant de recherche à l'IRIS.

Étudiant en double diplôme Sciences Po Saint-Germain-en-Laye & CY Tech, il se spécialise dans l'analyse stratégique, par la combinaison de connaissances en sciences sociales et la maîtrise d'outils de traitement de données (statistiques, *machine learning*, NLP, *graph analysis*, cartographie).

Comment citer cette étude :

Camille Boulenguer et Sami Nakib, « Souveraineté européenne des paiements (2026-2035). De la dépendance structurelle à la construction d'une doctrine des paiements européens », Étude de l'IRIS, IRIS, juin 2026.

Cette étude a été réalisée dans le cadre d'une prestation pour un commanditaire privé. Les travaux de recherche et ses préconisations ont été menés en toute indépendance.

TABLE DES MATIÈRES

INTRODUCTION : L'ARCHITECTURE DES PAIEMENTS N'EST PAS *NEUTRE*

Les paiements constituent une infrastructure critique du fonctionnement économique dont la continuité conditionne la fluidité des échanges commerciaux et financiers mondiaux. Ils représentent à ce titre un point de vulnérabilité structurelle pour les économies qui en dépendent. Cette fragilité est aujourd'hui exacerbée par un double phénomène :

- D'une part, le marché des paiements de détail[1] par carte se caractérise par une forte concentration autour de deux acteurs états-uniens, Visa et MasterCard, qui représentent 90 % des paiements transfrontaliers en Europe[2] et près de 72 % de ceux de la zone euro[3]. Cette concentration confère à ces acteurs une position duopolistique, exposant en conséquence l'économie européenne à un risque de dépendance critique. Toute coupure, contrainte technique ou mesure coercitive unilatérale (notamment à caractère extraterritorial) affectant ces réseaux serait susceptible d'entraîner des répercussions immédiates et significatives sur l'ensemble des flux économiques européens.
- D'autre part, la numérisation massive de l'économie a profondément reconfiguré les chaînes de valeur, au prix d'une dépendance accrue de l'Union européenne (UE) à des infrastructures extra-européennes. Les fonctions essentielles de systèmes de paiement (*cloud*, interface de programmation - ou API -, dispositifs anti-fraudes, solution d'identité numérique) reposent désormais sur des acteurs numériques majoritairement états-uniens. À cet égard, près de 70 % du marché européen du *cloud* est détenu par trois hyperscalers[4] états-uniens (AWS, Microsoft et Google), contre seulement 15 % pour l'ensemble de leurs équivalents européens[5]. À moindre échelle, la Chine déploie également des centres de données en Europe[6]. Ces implantations s'inscrivent dans un cadre juridique permettant aux autorités chinoises d'exiger l'accès

[1] Les paiements de détail, hors usage de la monnaie fiduciaire, reposent sur un écosystème plus fragmenté et fortement ouvert à des acteurs privés internationaux. Ce segment, qui représente plus de 150 milliards de transactions annuelles dans la zone euro, constitue le principal point de vulnérabilité du système européen de paiement.

[2] Cour des comptes européenne, « Paiements numériques dans l'Union européenne », Rapport spécial n°01/2025, 2025, https://www.eca.europa.eu/fr/publications/SR-2025-01, citant Statista, Market Share of Visa, MasterCard, American Express, Diners Club (2022).

[3] François Villeroy de Galhau, « Lettre au président de la République : de la tétanie à la mobilisation générale, comment agir face au basculement américain », (Banque de France, 2026) : 13, https://www.banque-france.fr/fr/actualites/lettre-au-president-de-la-republique-de-la-tetanie-la-mobilisation-generale-comment-agir-face-au.

[4] Voir Glossaire.

[5] Cour des comptes, « Les enjeux de souveraineté des systèmes d'information civils de l'État », Rapport public, S2025-1479, délibéré le 11 septembre 2025, rendu public le 31 octobre 2025, p. 31. Les données de parts de marché du *cloud* sont issues de Synergy Research Group, cité par le rapport.

[6] Commission d'enquête TikTok (Protection des données aux États-Unis / Extraterritorialité du droit chinois), Sénat, 2019, https://www.senat.fr/lc/lc322/lc3221.html.

aux données y compris lorsqu'elles sont hébergées à l'étranger ou détenues par des entreprises soumises à leur juridiction[7].

Dans ce contexte, la double concentration, tant sur les paiements de détail par carte, que sur les systèmes numériques associés, conduit à placer des fonctions critiques du système financier européen sous dépendance d'infrastructures soumises à des législations extraterritoriales étrangères. L'évolution récente de l'environnement géopolitique renforce ces enjeux de dépendance qui deviennent de potentiels leviers de pression ou de déstabilisation. La nouvelle administration états-unienne a en effet ravivé la perspective d'un usage agressif de la puissance technologique contre l'UE, y compris la possibilité d'« un *switch* numérique » capable d'affecter massivement le fonctionnement des infrastructures européennes[8]. L'UE doit désormais intégrer un risque crédible de rupture, volontaire ou accidentelle, de chaînes technologiques essentielles[9] susceptibles d'affecter directement la continuité de ses fonctions économiques et régaliennes.

En matière de paiements de gros[10], l'UE bénéficie d'une maîtrise stratégique avérée. Les systèmes opérés par l'Eurosystème assurent le traitement sécurisé de ces flux critiques et constituent un socle robuste en matière de souveraineté et de résilience financière. S'agissant des paiements de détails, si la dépendance aux réseaux internationaux est importante, l'UE dispose de bases domestiques significatives dans plusieurs pays. Des schémas nationaux historiquement établis, tels que Cartes Bancaires (CB) en France, Girocard en Allemagne, Bancontact en Belgique, assurent une part substantielle des paiements du quotidien et témoignent d'une capacité européenne à développer et opérer des solutions performantes à grande échelle. Ces acquis restent toutefois fragmentés à l'échelle de l'Union et peinent à s'imposer comme alternatives intégrées aux schémas internationaux.

[7] À titre illustratif, Alibaba Cloud se déploie dans des régions en Allemagne, au Royaume-Uni et prochainement en France, tandis que ByteDance-TikTok investit plus d'un milliard d'euros dans la construction de *data centers* en Finlande dans le cadre du Projet Clover. Voir Emma Badaoui et Anne-Thida Norodom, « (Extra)territorialité des données : quelle souveraineté pour l'Europe ? », Études de l'IFRI, Centre géopolitique des technologies (Paris : IFRI, mars 2026).
[8] Mathieu Pollet, « Trump can pull the plug on the Internet, and Europe can't do anything about It », *Politico*, 23 juin 2025, https://www.politico.eu/article/donald-trump-eu-internet-europe-us-trade-war-data-cyber/
[9] Sébastian Seibt, « Digital Sovereignty: Have Trump Threats Spurred a European Awakening ? », France 24, 2 février 2026, https://www.france24.com/en/technology/20260202-digital-sovereignty-have-trump-threats-spurred-european-awakening.
[10] Paiements de gros : paiements correspondant aux règlements interbancaires de grande valeur.

Le marché des paiements par carte en Europe : volumes et influence internationale

États de la zone euro

Répartition de la valeur totale des transactions en 2024 par États, en milliards d'euros

856,7 (R-U)

500

inférieur à 100

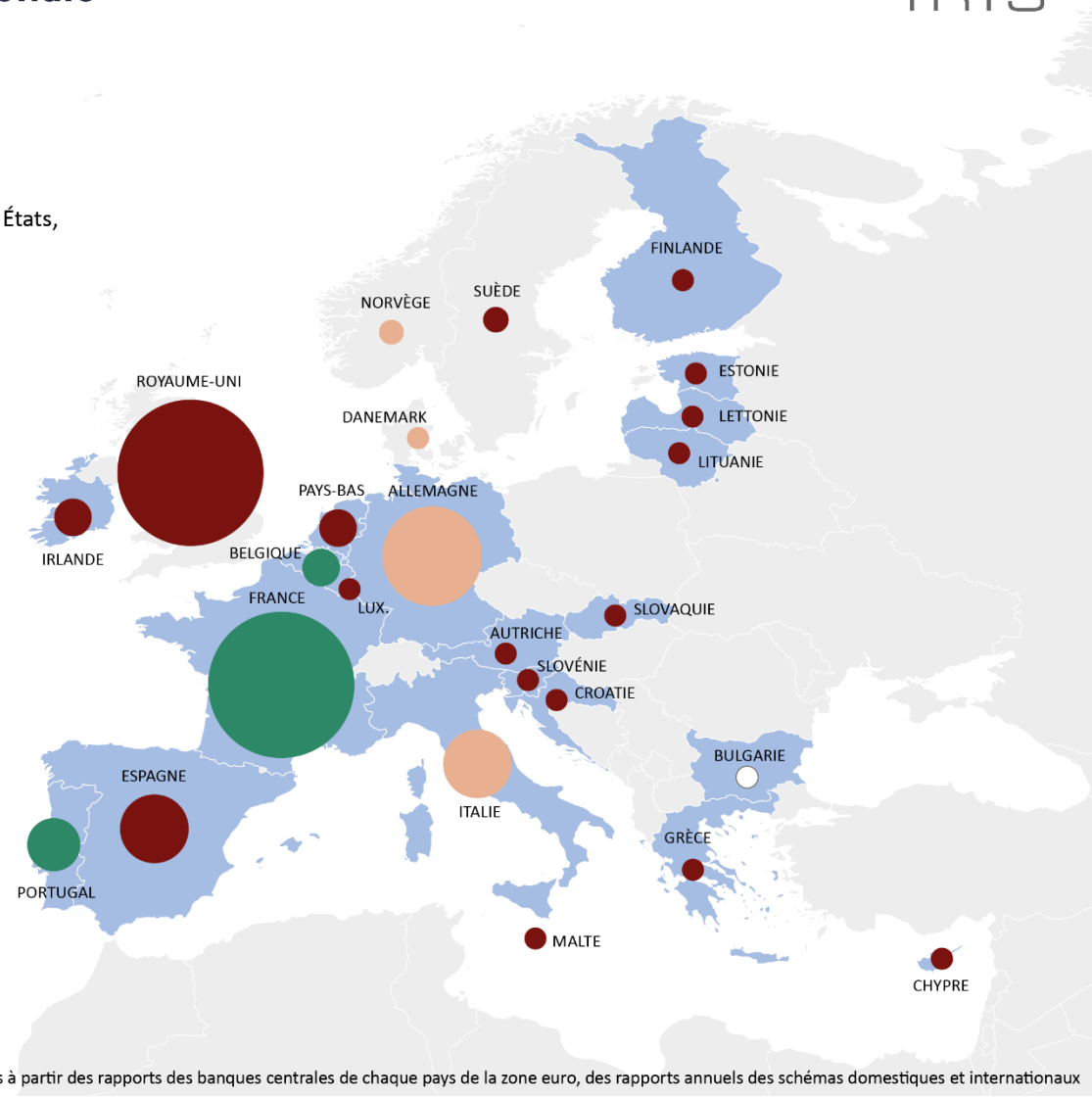
Absence de données

Niveau de dépendance à des réseaux internationaux, établi sur la part des réseaux internationaux empruntés par les paiements par carte

Faible (réseaux internationaux inférieur à 40 %)

Modéré (réseaux internationaux compris entre 40 et 75 %)

Total (100%)



Sources : données compilées à partir des rapports des banques centrales de chaque pays de la zone euro, des rapports annuels des schémas domestiques et internationaux

Pour les Européens, l'enjeu ne réside donc pas uniquement sur la réduction des dépendances, mais aussi sur la capacité à consolider et étendre ces acquis afin de rééquilibrer durablement la maîtrise des infrastructures de paiement et à tendre vers davantage de souveraineté. Cette dernière repose sur deux dimensions complémentaires :

- **D'une part, une capacité juridique et institutionnelle**[11] à réguler, attribuer et protéger les infrastructures de paiement, condition nécessaire à l'exercice de la souveraineté[12].
- **D'autre part, une forme d'autonomie stratégique**, entendue comme la capacité à choisir, orienter et gouverner les standards, les acteurs et les réseaux de paiement, sans dépendance subie[13].

En conséquence, la souveraineté repose sur la capacité effective à exercer un libre choix technologique et industriel, en garantissant la **maîtrise des solutions critiques** et la **faculté de recourir à des alternatives crédibles**. Elle repose également sur la **résilience des systèmes**, entendue comme leur aptitude à maintenir un niveau de fonctionnement acceptable en cas de défaillance technique ou d'attaque systémique. La souveraineté dans les paiements et les infrastructures numériques relève dans ce contexte, d'un triple enjeu pour l'économie nationale et européenne :

- ✓ **Un enjeu de sécurité économique et technologique** afin de garantir la continuité des paiements et des infrastructures critiques face à des acteurs capables de couper l'accès ou d'imposer des règles unilatérales ;
- ✓ **Un enjeu de stabilité macro-financière** afin d'éviter qu'un choc extérieur (sanctions, blocages, rupture du *cloud*) ne se propage à l'ensemble du système financier ;
- ✓ **Un enjeu d'attractivité économique** offrant aux entreprises un cadre stable sécurisé, prévisible (condition indispensable à l'investissement).

[11] Esther Noël, *La souveraineté de l'État à l'ère numérique*, thèse de doctorat (Université Paris Cité, 2025).
[12] BCE (Eurosystème), *The Eurosystem's Comprehensive Payments Strategy* (Francfort : BCE, mars 2026), https://www.ecb.europa.eu/press/pubbydate/2026/html/ecb.eurosystemcomprehensivepaymentsstrategy202603.en.html
[13] Françoise Drumetz et Christian Pfister, « La souveraineté monétaire à l'ère numérique », *Revue d'économie financière*, n°160 (2025).

PREMIÈRE PARTIE : DÉPENDANCES STRUCTURELLES ET RISQUES POUR LA SOUVERAINETÉ EUROPÉENNE

La dépendance structurelle de l'UE à l'égard d'acteurs non européens ne saurait être appréhendée comme un simple déficit de compétitivité industrielle ou un retard technologique à combler. Elle renvoie à des dépendances plus profondes (industrielles, technologiques et juridiques) qui se déclinent en trois dimensions complémentaires du risque et appellent une réponse stratégique à la hauteur de leurs implications :

- **Un risque de coercition technologique et juridique** : la concentration des infrastructures et des services critiques entre les mains d'acteurs extra-européens expose l'UE à des décisions unilatérales (interruption de service, restrictions d'accès, application de législations extraterritoriales), susceptibles d'affecter directement le fonctionnement des systèmes de paiement ;
- **Un risque systémique en matière de cybersécurité et de résilience opérationnelle** : la centralisation des flux et des infrastructures accroît la surface d'exposition aux cyberattaques et aux défaillances techniques majeures, avec un potentiel effet de contagion rapide à l'ensemble du système financier ;
- **Un risque d'atteinte à la souveraineté monétaire et financière** : la dépendance aux infrastructures et aux standards contrôlés par des acteurs étrangers limite la capacité des États membres à piloter de manière autonome leurs politiques monétaires, à garantir l'intégrité des circuits de paiement et, plus largement, à préserver leur souveraineté économique.

1.1 La coercition économique et technologique : quand l'infrastructure de paiement devient levier géopolitique

Le caractère extraterritorial du droit états-unien constitue l'un des principaux vecteurs de pression structurelle sur l'écosystème européen des paiements. Le fondement de cette asymétrie juridique se structure sur la capacité effective des États-Unis à transformer l'accès aux infrastructures financières et technologiques en levier de coercition. Sur le fondement extraterritorial de certaines lois, les États-Unis en particulier disposent d'une capacité à intervenir sur des États ou acteurs privés opérant en dehors de leur territoire, dès lors que ceux-ci utilisent des instruments, des infrastructures ou des technologies soumis au droit états-unien. Cette coercition peut s'exercer :

- **À l'échelle de l'entreprise** à travers des menaces juridiques ou des amendes ;
- **À l'échelle des États** par le truchement de sanctions économiques visant un pays tiers ou, de manière plus indirecte, de restrictions d'accès à des infrastructures critiques financières ou technologiques, dont dépendent les économies concernées.

Le secteur des paiements apparaît particulièrement ciblé par ces extensions de la juridiction au-delà du territoire, qui reposent sur plusieurs mécanismes cumulatifs :

- **D'une part, l'utilisation du dollar**, qui implique le recours aux systèmes de compensation états-uniens, place *de facto* les transactions sous la juridiction des États-Unis.
- **D'autre part, le recours à des infrastructures technologiques** opérées par des entreprises relevant du droit états-unien (*cloud*, services de paiement, traitement des données) étend cette juridiction aux couches numériques du système financier.

1.1.1 Une coercition à l'échelle de l'entreprise : l'extraterritorialité des sanctions états-uniennes : un levier de transformation des pratiques de marché

Une série de sanctions significatives prononcées à partir de 2010 à l'encontre d'établissements bancaires européens (BNP Paribas[14], Standard, Chartered, HSBC, Commerzbank, Crédit Agricole ou UniCredit), pour avoir réalisé des transactions en dollars[15] avec des pays sous embargo (Cuba, Iran, Soudan), constitue un cas d'école. Ces décisions ont conduit à une internationalisation progressive des contraintes du droit états-unien dans les dispositifs de conformité et leur opération afin d'anticiper le risque de sanctions. Depuis lors, les actions de l'*Office of Foreign Assets Control*[16] se sont à la fois élargies et intensifiées[17] : l'année 2023 illustre cette dynamique avec un niveau record d'application des sanctions, avec

[14] La BNP a été condamnée en 2014 à verser une amende de près de 9 milliards de dollars U.S. Voir : Department of Justice – U.S. Attorney's Office, Southern District of New York, « BNP Paribas Agrees to Plead Guilty to Conspiring to Process Transactions Through the U.S. Financial System for Sudanese, Iranian, and Cuban Entities Subject to U.S. Economic Sanctions », Communiqué de presse, 30 juin 2014, https://www.justice.gov/archive/usao/nys/pressreleases/June14/BNPParibasPlea.phph.

[15] Le recours à des infrastructures opérées par des entreprises de droit états-unien expose les acteurs européens à des obligations juridiques extraterritoriales, notamment en matière d'accès aux données ou de continuité de service. Les précédents montrent que l'accès aux infrastructures de paiement peut être conditionné, restreint ou suspendu, transformant des outils techniques en instruments opérationnels de coercition.

[16] Le régime de sanctions administré par l'Office of Foreign Assets Control (OFAC), fondé notamment sur l'International Emergency Economic Powers Act, permet de restreindre ou de conditionner l'accès aux circuits financiers internationaux, pour des acteurs non états-uniens.

[17] Camille Boulenguer et Julia Tomasso, « La lame et l'ombre : impacts des sanctions et chemins de contournement », *La Revue internationale et stratégique,* n°139 (2025/3), https://www.iris-france.org/ris/la-lame-et-lombre-impacts-des-sanctions-et-chemins-de-contournement/.

plus de 1,5 milliard de dollars de pénalités infligées[18]. Ces dernières ont concerné non seulement des banques, mais aussi des entreprises technologiques et des acteurs des nouveaux systèmes de paiement, traduisant une extension du périmètre de contrôle à l'ensemble de la chaîne de valeur des transactions du paiement.

1.1.2 Des États sous tensions : les infrastructures critiques comme levier de coercition

Les sanctions et dispositifs juridiques extraterritoriaux peuvent également s'inscrire dans une logique plus large d'instrumentalisation des infrastructures numériques et financières à des fins géopolitiques. Le retour de Donald Trump à la Maison-Blanche (2025) a en effet ravivé la perspective d'un usage plus affirmé de ces leviers dans les relations transatlantiques[19], notamment dans les différends relatifs à la régulation des grandes plateformes numériques[20] ou à certains dossiers plus stratégiques comme celui du rachat du Groenland[21]. Les précédents récents (Iran 2015, 2018 ; Russie 2014, 2022) confirment le caractère opérationnel de ces instruments[22] conduisant un certain nombre d'États à accélérer la mise en place de solutions alternatives (SPFS en Russie, systèmes domestiques de cartes en Iran, Pix au Brésil). Cette évolution s'inscrit dans une dynamique globale de fragmentation et de *re-souverainisation* des systèmes de paiements à l'échelle mondiale, recouvrant toutefois des configurations de souveraineté géographiquement différenciées :

- **La Russie**, bien que dotée d'infrastructures domestiques alternatives (*Encadré 1*), ne dispose ni de réseaux véritablement internationaux, ni de législation à portée extraterritoriale lui permettant de projeter son influence au-delà de son territoire. Ses solutions demeurent ainsi principalement limitées à un usage national ou à des partenariats restreints.

[18] John E. Smith, Brandon L. Van Grack, Rachel Miras Fiorill, Elyse Beth Martin et Nathanael Kurcab, « U.S. Sanctions Enforcement: 2023 Trends and Lessons Learned », Morrison Foerster Client Alert, 4 mars 2024, https://www.mofo.com/resources/insights/240304-us-sanctions-enforcement-2023-trends.

[19] Dominique Plihon, « La dédollarisation : une stratégie de vaccination contre les sanctions ? », *La Revue internationale et stratégique,* n° 139 (2025/3) : p.126, https://www.iris-france.org/ris/la-dedollarisation-une-strategie-de-vaccination-contre-les-sanctions/. Le premier mandat de Donald Trump (2017-2021) avait déjà marqué « un changement de philosophie : les sanctions ne sont plus seulement un outil de dissuasion, elles deviennent un instrument central de la politique étrangère états-unienne intégré à une stratégie offensive de domination économique ».

[20] Eulalia Rubio, « L'UE doit manier avec précaution la menace d'une taxe numérique européenne », Institut Jacques Delors, 23 avril 2024, https://institutdelors.eu/publications/lue-doit-manier-avec-precaution-la-menace-d-une-taxe-numerique-europeenne/.

[21] Emmanuel Hache et al., « Donald Trump et le Groenland : une ambition géopolitique au-delà des ressources », Observatoire des États-Unis de l'IRIS, IRIS, janvier 2025, https://www.iris-france.org/wp-content/uploads/2025/01/ObsEtatsUnis_2025_01_20_Groenland_Note_FR.pdf.

[22] L'exclusion de l'Iran du système SWIFT (2012, 2018) ainsi que le blocage des opérations Visa/MasterCard en Russie à la suite de l'invasion de l'Ukraine en 2022 démontrent que l'infrastructure de paiement internationale peut être mobilisée comme instrument de pression géopolitique.

- **Les États-Unis et, dans une moindre mesure la Chine**, cumulent deux leviers structurants : la maîtrise d'infrastructures critiques à portée internationale (*Encadré 2*) et l'existence de cadres juridiques permettant de projeter leur pouvoir de régulation au-delà de leur territoire national.

Le **risque de sanctions économiques ciblé sur des entreprises** stratégiques contribue à **orienter durablement les pratiques de marché** et à **structurer les conditions de la concurrence**, en **conférant un avantage aux acteurs opérant sous juridiction états-unienne**. Les sanctions extraterritoriales s'inscrivent désormais dans une stratégie plus large d'**instrumentalisation des infrastructures financières et numériques**. Les États-Unis, et dans une moindre mesure la Chine, combinent maîtrise d'infrastructures globales et capacité juridique extraterritoriale, contrairement à des acteurs comme la Russie à l'influence plus limitée. Cette dynamique alimente une **fragmentation croissante des systèmes de paiement au sein de l'UE**.

1.2 Une surface d'attaque continentale : concentration des infrastructures, vulnérabilité cyber et captation de données à haute valeur ajoutée

À la coercition de nature juridique ou politique s'ajoute un risque de nature distincte, tenant à la fragilité intrinsèque de systèmes numériques fortement connectés. **La concentration et l'imbrication croissantes des infrastructures économiques**, numériques et financières confèrent aux systèmes de paiement une **dimension systémique accrue qui renforce leur exposition aux défaillances techniques et aux attaques cyber**[23] dont les effets peuvent se propager rapidement à l'ensemble du système financier. Dès lors, l'enjeu ne se limite plus à la maîtrise juridique ou capitalistique des infrastructures, mais porte également sur leur **résilience opérationnelle**, entendue comme la capacité à prévenir, absorber et contenir des perturbations d'origine technique ou malveillante.

[23] ANSSI, « Panorama de la cybermenace 2025 », CERTFR-2026-CTI-002 (mars 2026).

Encadré n°1 - LE SYSTÈME DE MESSAGERIE BANCAIRE SPFS ET LE RÉSEAU DOMESTIQUE DE CARTES MIR EN RUSSIE

À la suite des premières sanctions économiques occidentales en 2014, la Russie a engagé le développement d'un écosystème de paiement et de messagerie bancaire alternatif, visant à réduire sa dépendance aux infrastructures internationales. Deux instruments ont été mis en place : le système de messagerie bancaire SPFS (équivalent domestique de SWIFT) et le réseau national de cartes Mir (équivalent domestique de Cartes Bancaires). Le système SPFS offre ainsi une solution de secours pour la transmission des messages financiers entre établissements russes, tandis que le réseau Mir garantit le fonctionnement des paiements par carte sur le territoire national.

Ces infrastructures ont permis d'assurer une continuité partielle des opérations domestiques en 2022 à la suite de l'invasion de l'Ukraine et de la suspension des opérations de Visa et MasterCard sur le sol russe. Parallèlement, la Russie a cherché à renforcer ses échanges avec des partenaires non occidentaux (la Chine en particulier) afin de réduire son exposition aux infrastructures dominées par le dollar.

1.2.1 La concentration comme point de défaillance unique

En cas de risque systémique, la défaillance d'un acteur central, qu'elle soit technique, opérationnelle ou malveillante, peut se propager rapidement à l'ensemble du système. **La vulnérabilité** ne tient alors pas uniquement à l'intensité de la menace, mais à **l'architecture même des interdépendances**, **qui transforme toute perturbation localisée en risque à l'échelle continentale**. En 2023, une panne majeure chez le fournisseur de solutions de paiements européen pour entreprises Worldline a entraîné des interruptions de paiement dans plusieurs pays. Ces perturbations ont affecté de nombreux commerçants majeurs tels que Carrefour, Auchan, Monoprix ou Fnac Darty pendant plusieurs heures, illustrant la dépendance de l'économie réelle à un nombre limité d'infrastructures critiques[24]. Cet exemple met en évidence un point essentiel : une défaillance localisée peut avoir des effets immédiats et étendus à l'échelle de plusieurs marchés nationaux. Cette logique vaut également pour les infrastructures technologiques sous-jacentes. L'indisponibilité temporaire d'un grand fournisseur *cloud* (AWS, Microsoft Azure, Google Cloud) serait susceptible

[24] Marion Heilmann, « Pannes de paiement : les grandes enseignes examinent des recours contre Worldline », *Les Echos*, 16 novembre 2023, https://www.lesechos.fr/finance-marches/banque-assurances/pannes-de-paiement-les-grandes-enseignes-examinent-des-recours-contre-worldline-2029466.

d'affecter simultanément les systèmes bancaires européens, les applications de paiement et les services de validation des transactions. En raison de leur concentration et de leur rôle transversal dans le fonctionnement des infrastructures financières, ces acteurs constituent des points de convergence critiques dont la défaillance pourrait entraîner des effets en chaîne sur l'ensemble de l'écosystème.

La dépendance de l'écosystème européen des paiements à un nombre limité d'acteurs extra-européens ne se traduit pas uniquement par une vulnérabilité opérationnelle, elle concentre également un risque cyber et un risque de captation des données.

1.2.2 Le risque d'attaque cyber par un tiers hostile *via* les infrastructures états-uniennes.

La concentration des traitements auprès de fournisseurs dominants crée des cibles privilégiées pour des acteurs malveillants, qu'il s'agisse de cybercriminels (« loups solitaires » ou groupes criminels organisés) ou de puissances étatiques étrangères, en particulier la Russie, la Corée du Nord ou la Chine[25]. Cette menace s'inscrit dans un contexte de conflictualité élargie[26], marqué par le développement de stratégies de *guerre hybride*[27], dans lesquelles les attaques cyber constituent un levier privilégié de déstabilisation économique et politique. Une attaque réussie contre un acteur systémique pourrait ainsi entraîner des effets en cascade sur l'ensemble du système, en perturbant simultanément les capacités de traitement, de validation et de règlement des transactions à l'échelle de l'UE. L'augmentation des incidents montre qu'une défaillance, même non malveillante, peut produire des effets similaires. En octobre 2025, une panne majeure d'Amazon Web Service a affecté de nombreuses plateformes de services financier entraînant l'indisponibilité de services bancaires et l'impossibilité d'effectuer certains paiements pour des millions d'utilisateurs[28]. Si un incident technique peut produire de tels effets, une attaque ciblée, en particulier dans un contexte de tensions géopolitiques accrues, serait susceptible d'avoir des conséquences plus profondes.

---

[25] ENISA, « ENISA Threat Landscape 2024 » (2024), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Le secteur bancaire et les infrastructures numériques figurent parmi les trois secteurs les plus ciblés en Europe. Les acteurs russo-affiliés (LockBit, NoName057, Cyber Army of Russia) dominent le premier, tandis que des groupes liés à la Chine (Cyber Dragon) ciblent spécifiquement les infrastructures numériques critiques.

[26] ANSSI, Panorama de la cybermenace 2024, 3–5 ; ANSSI, CTI-002, 2026.

[27] La guerre hybride désigne la combinaison de moyens militaires et non-militaires, opérations conventionnelles, tactiques irrégulières, cyberattaques et désinformation, visant à déstabiliser un adversaire sans franchir le seuil du conflit ouvert. OTAN, « Lutte contre les menaces hybrides » (2026), https://www.nato.int/fr/what-we-do/deterrence-and-defence/countering-hybrid-threats.

[28] « AWS, le service cloud d'Amazon, annonce avoir résolu la panne qui a touché des applications dans le monde entier », *Le Monde*, 21 octobre 2025.

1.2.3 Un risque de fuite de données sensibles vers des acteurs étrangers

En vertu de dispositifs juridiques tels que le *Cloud Act* (2018)[29] ou les programmes de surveillance encadrés par le *Foreign Intelligence Surveillance Act* (FISA)[30], les autorités états-uniennes peuvent, sous certaines conditions, accéder à des données détenues par des entreprises soumises à leur juridiction. Appliqué aux paiements, ce risque concerne des données particulièrement sensibles, portant sur les comportements économiques des agents, les flux commerciaux, les chaînes d'approvisionnement ou encore les activités d'acteurs stratégiques.

Ainsi, une entreprise européenne utilisant les services *cloud* fournis par une société états-unienne peut être amenée à héberger des données de transactions sur des infrastructures situées en Europe, mais juridiquement accessibles à la maison-mère états-unienne. Dans ce cadre, les autorités états-uniennes peuvent adresser directement une demande au fournisseur de service, sans nécessairement passer par les mécanismes classiques de coopération judiciaire internationale, ce qui soulève des enjeux de souveraineté juridique[31]. Ce dispositif crée une tension directe avec le cadre européen de protection des données, en particulier le Règlement général sur la protection des données (RGPD), qui encadre strictement le transfert de données personnelles hors de l'UE et impose des garanties élevées en matière de traitement. Cette divergence de normes juridiques place les acteurs européens dans une situation de potentielle contradiction réglementaire, entre obligations de conformité au droit états-unien et respect du droit européen. Cette problématique a notamment été mise en évidence dans les arrêts Schrems I et Schrems II de la Cour de justice de l'Union européenne (CJUE)[32], qui ont invalidé successivement les dispositifs Safe Harbor[33], puis Privacy Shield[34], au motif que le droit états-unien ne garantissait pas un niveau de protection substantiellement équivalent à celui assuré au sein de l'UE. Toutefois, si ces décisions constituent un progrès juridique important, leur portée demeure en pratique

[29] Le Clarifying Lawful Overseas Use of Data Act (Cloud Act, 23 mars 2018), oblige les prestataires états-uniens à fournir les données qu'ils contrôlent, indépendamment de leur lieu de stockage.
[30] Sous l'autorité de la Section 702 du FISA, la NSA collecte les communications *via* deux dispositifs : (1) PRISM, par lequel elle obtient directement les données auprès des opérateurs numériques, et (2) UPSTREAM, par lequel elle intercepte les flux sur les câbles de l'internet. NSA, « NSA Stops Certain Section 702 Upstream Activities », communiqué de presse, 28 avril 2017.
[31] Le Cloud Act prévoit la possibilité pour les États-Unis de conclure des *Executive Agreements* – accords bilatéraux limitant l'accès aux données de ressortissants étrangers ; or, à la date de rédaction, aucun accord de ce type n'a été signé entre les États-Unis et l'UE, laissant les données des acteurs européens sans protection spécifique dans ce cadre. Eurojust, *The Cloud Act* (décembre 2022).
[32] CJUE, arrêts Schrems I (C-362/14, 6 octobre 2015) et Schrems II (C-311/18, 16 juillet 2020), présentation sur CNIL https://www.cnil.fr/fr/presentation-de-larret-schrems-ii-de-la-cjue.
[33] Décision 2000/520/CE de la Commission européenne (Safe Harbor), invalidée par Schrems I. Parlement européen, Service de recherche, The US Safe Harbour Agreement, PE 595.892 (EPRS, 2017), https://www.europarl.europa.eu/thinktank/fr/document/EPRS_IDA(2017)595892.
[34] Décision 2016/1250/UE (Privacy Shield), invalidée par Schrems II. CNIL, « Invalidation du Privacy Shield : les suites de l'arrêt de la CJUE », https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-suites-de-larret-de-la-cjue.

limitée. En effet, les données restent majoritairement traitées et détenues par des acteurs étrangers, qui conservent la maîtrise effective des infrastructures et des services.

Les infrastructures de paiement apparaissent comme des points d'entrée privilégiés pour l'exercice de pressions graduées susceptibles de déstabiliser à terme le fonctionnement des systèmes économiques à grande échelle.

Les infrastructures de paiement, **fortement concentrées et interconnectées**, constituent une vulnérabilité systémique majeure, où une **défaillance technique ou cyber peut avoir des effets en cascade à l'échelle européenne**. Cette dépendance à des acteurs dominants, souvent extra-européens, accroît à la fois le **risque d'attaques cyber et celui de captation de données sensibles**. Elle s'inscrit enfin dans une **logique de conflictualité stratégique**, où les paiements deviennent un levier de puissance et de pression dans un contexte de recomposition des équilibres internationaux.

1.3 – La « guerre des systèmes » fragmentation européenne et risque de double dépendance envers les États-Unis et la Chine

1.3.1 Une Union fragmentée et fragilisée

Pleinement intégrées à la stratégie de puissance des États, les technologies numériques sont désormais considérées comme un pilier central de la dissuasion, au même titre que les instruments militaires traditionnels[35]. Cette évolution ne signifie pas que les nouvelles technologies soient systématiquement utilisées à des fins coercitives, mais qu'elles constituent à ce jour, un levier crédible et activable de pression dans les rapports de force internationaux contemporains. C'est dans ce cadre que les infrastructures de paiement prennent une dimension stratégique particulière, que l'on doit intégrer plus largement dans une logique de **«** guerre des systèmes » [36]. Plusieurs scénarios peuvent être envisagés :

[35] The White House, « National Security Strategy of the United States of America », Washington D.C. (5 décembre 2025 : 4 : « Le maintien de la suprématie économique et technologique des États-Unis est le moyen le plus sûr de dissuader et de prévenir les conflits militaires à grande échelle ».

[36] Julia Tasse, « Introduction à la guerre des systèmes », *La Revue internationale et stratégique*, n° 141, (2026/1), https://doi.org/10.3917/ris.141.0033.

- **Mesure de coercition ciblée, pouvant cibler des individus ou des entités** à l'instar de Nicolas Guillou, juge de la CPI. Dans cette perspective, on peut aisément imaginer la mise sous sanctions de personnalités politiques de premier plan[37] ;
- **Altération du fonctionnement des infrastructures numériques et de paiement**, selon une gradation d'intensité[38] :
    - ✓ Restriction ou limitation ciblée de certains services (paiement, *cloud*) ;
    - ✓ Interruption brutale d'infrastructures critiques susceptibles d'affecter rapidement la capacité à réaliser des transactions.

Ainsi, sans relever nécessairement d'une logique de rupture frontale, ces mécanismes peuvent progressivement altérer la capacité d'un État ou d'une union économique à assurer la continuité de ses échanges, à protéger ses données et à exercer pleinement sa souveraineté.

Encadré n°2 – LA DOCTRINE CHINOISE DES PAIEMENTS

Le 15e Plan quinquennal (2026-2030), adopté par le Congrès national du peuple le 12 mars 2026, prescrit la construction d'un « *système de paiement transfrontalier en renminbi indépendant et maîtrisable* »[39]. Cette orientation, également retenue pour des secteurs critiques tels que l'intelligence artificielle et les semi-conducteurs[40], inscrit les paiements au cœur d'une doctrine de sécurité économique intégrée, articulant étroitement infrastructures financières et technologiques.

La stratégie chinoise des paiements repose sur quatre piliers :

1. Un modèle domestique dominé par des paiements mobiles (Alipay et WeChat Pay)[41] ;

[37] Audition de Nicolas Guillou devant la Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France, Assemblée nationale, compte rendu n° 21, 29 avril 2026.
[38] On pense ici à la multiplication des menaces de sanctions contre l'UE : Von Thun, Riekeles et Kuzev, Doubling Down, Not Backing Down, EPC, 2025.
[39] Texte officiel du 15e Plan quinquennal (2026-2030), Congrès national du peuple, 12 mars 2026, publié par *Xinhua*, https://www.qualenergia.it/wp-content/uploads/2026/03/China_15th_Five-Year_Plan_English.pdf, chapitre 21, section 1 (Actively Expanding Independent Opening-up).
[40] Ibid., chapitre 4 (« Enhancing the Self-Reliance and Controllability of the Industrial Chain ») ; chapitre 12 (« Strengthening Computing Infrastructure Support : 'Accelerate the cultivation of an independent, controllable, and collaboratively operating software and hardware ecosystem' »).
[41] Le monopole détenait en 2020 près de 93 % des paiements mobiles en Chine Xin Ni Jiang. Voir « Analysis of WeChat Pay Based on Technology Acceptance Model », dans *Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development* (ICSSED 2022), *Atlantis Press*, 29 avril 2022, 668–675, https://doi.org/10.2991/aebmr.k.220405.110.

2. Le développement d'une monnaie numérique de banque centrale (e-CNY) depuis 2014 ;
3. Le système *China International Payment System* (CIPS) pour les paiements internationaux[42, 43] ;
4. Des initiatives multilatérales comme *mBridge* qui visent à faciliter les échanges internationaux pour les paiements de gros en monnaies numériques.

Ces avancées doivent toutefois être relativisées par des contraintes structurelles. Le renminbi demeure marginal dans les paiements internationaux[44], son internationalisation étant freinée par :

- Les nombreux contrôles de capitaux ;
- Sa faible convertibilité ;
- L'absence de mécanismes institutionnels comparables à deux des grandes monnaies internationales[45].

Paradoxalement, le modèle de contrôle interne mis en œuvre par les autorités chinoises constitue lui-même un frein à son adoption à l'international[46].

C'est précisément dans ce contexte que la fragmentation du paysage européen des paiements constitue une vulnérabilité structurelle. L'UE apparaît en effet affaiblie par l'hétérogénéité des situations au sein des différents pays membres, rendant plus difficile l'émergence d'une position commune et cohérente. Toutefois, si les incitations économiques restent hétérogènes, les incitations stratégiques convergent néanmoins progressivement dans le contexte actuel. Cette convergence demeure toutefois incomplète, ce qui continue de limiter la capacité de l'Union à définir une position pleinement unifiée. Les grands schémas internationaux et les plateformes technologiques globales sont précisément en mesure d'exploiter ces divergences de perception et de stratégie entre États membres, en adaptant

[42] The Clearing House Interbank Payments System.
[43] Le CIPS a traité 175,79 trillions de yuans en 2024, soit une hausse de 43 % sur un an représentant 8,2 millions de transactions, et relie 1 683 institutions financières, dont 17 % d'établissements européens. Voir : Cross-border Interbank Payment and Settlement Co., Ltd. (CIPS), *Rapport annuel sur les statistiques du système CIPS 2024* (Shanghai, 2025).
[44] En octobre 2025, le renminbi ne représente que 2,47 % des paiements SWIFT globaux (6e rang), contre 46,71 % pour le dollar.
[45] Dominique Plihon, « La dédollarisation : une stratégie de vaccination contre les sanctions ? », *La Revue internationale et stratégique*, n° 139 (2025/3) : 126, https://www.iris-france.org/ris/la-dedollarisation-une-strategie-de-vaccination-contre-les-sanctions/
[46] Dominique Plihon, *op. cit.* : 126.

leurs conditions commerciales et techniques à l'échelon national, pour prévenir l'émergence d'une solution européenne commune.

I.3.2 L'UE face à un risque de double dépendance

La situation de l'UE révèle un risque plus profond de « double dépendance » : dépendance aux systèmes états-uniens dominés par le dollar, sans pour autant qu'elle soit intégrée aux architectures émergentes portées par la Chine[47]. La stratégie de Pékin, plus discrète dans sa communication que celle de la Maison-Blanche, s'inscrit cependant dans une logique de domination fondée sur le contrôle des standards, des réseaux et des dépendances, avec l'ambition clairement affichée de renforcer sa position dominante à l'horizon 2049. Si la présence chinoise dans les paiements en Europe reste très peu marquée, elle génère néanmoins deux types de risques :

- **À court terme, le risque d'une pénétration progressive par les usages.** Des solutions telles que WeChat ou Alipay adossées à des écosystèmes complets (e-commerce, exploitation des données, services financiers, IA agentique), pourraient s'imposer de manière progressive et invisible, auprès de certains segments d'utilisateurs européens, les plus jeunes en particulier, sensibles au soft power chinois. Ce scénario est particulièrement plausible dans le secteur du commerce électronique transfrontalier[48] et dans les écosystèmes économiques intégrés à l'Asie.
- **À moyen et long terme, le risque d'exclusion du système chinois.** Le développement d'un écosystème de paiement international adossé au Yuan (*Encadré 2*) pourrait conduire à l'émergence de circuits financiers dédollarisés sino-centrés. Dans ce scénario, l'UE pourrait se trouver progressivement marginalisée au sein d'un système où les règles, les infrastructures et les instruments monétaires seraient structurés en dehors de son cadre économique et juridique. La vulnérabilité européenne ne réside pas uniquement dans sa dépendance actuelle aux infrastructures dominées par les États-Unis, elle tient également au risque de se trouver, à horizon 2050-60, exclue de systèmes de paiement alternatifs, actuellement en construction, à l'instar du Yuan.

[47] Massimo Ferrari Minesso et Olga Triay Bagur, « Geopolitics and Global Interlinking of Fast Payment Systems? », dans BCE, The International Role of the Euro (Francfort : BCE, juin 2025), https://www.ecb.europa.eu/press/other-publications/ire/focus/html/ecb.irebox202506_03~17c27de367.en.html.

[48] Visa Inc., *Fiscal Year 2025 Annual Report* (Form 10-K) (San Jose : Visa Inc., 2025) : 27, https://s29.q4cdn.com/385744025/files/doc_downloads/2025/Visa-Fiscal-2025-Annual-Report.pdf. « Des prestataires de services de paiement alternatifs tels qu'Alipay et WeChat Pay se sont rapidement développés dans les domaines du commerce électronique, des paiements hors ligne et des paiements transfrontaliers ».

La vulnérabilité européenne ne réside donc plus uniquement dans sa dépendance actuelle, mais dans le risque d'une marginalisation progressive d'un système financier international en recomposition.

L'Union européenne apparaît fragilisée par la **fragmentation structurelle** liée à la **concentration d'acteurs extra-européens sur ses marchés critiques**, ce qui limite sa capacité à répondre efficacement aux pressions extérieures. Elle est confrontée à un **risque de double dépendance** : à court terme vis-à-vis des systèmes états-uniens dominés par le dollar pouvant se traduire par **une exposition aux sanctions exterritoriales**, et à plus long terme face à **l'émergence de systèmes alternatifs sino-centrés**, susceptibles de la marginaliser dans l'ordre financier international.

DEUXIÈME PARTIE — UNE ARCHITECTURE FRAGMENTÉE, UNE VALEUR CAPTÉE : LE DOUBLE COÛT DE LA NON-SOUVERAINETÉ

La dépendance structurelle de l'UE aux technologies états-uniennes a pour conséquence un coût économique réel, quotidien, et largement sous-évalué. Ce coût prend deux formes distinctes, mais articulées.

- **La première est endogène :** la fragmentation du marché européen agit comme une **barrière douanière intra-européenne** générant des surcoûts et des inefficiences supportées par les acteurs économiques (consommateurs finaux et commerçants). Une partie de ces surcoûts se matérialise sous forme de **marges captées par les réseaux internationaux (Visa, MasterCard)**, auxquels les acteurs recourent faute d'alternatives intégrées à l'échelle européenne.
- **La seconde est exogène :** il s'agit d'une **rente d'infrastructure au profit d'acteurs extra-européens**, qui captent une part croissante de la valeur (flux financiers, données), tout en créant des **coûts d'inertie** freinant l'émergence d'alternatives européennes.

Ces deux dynamiques se renforcent mutuellement et forment ce qu'on pourrait appeler l'économie politique de la dépendance : le mécanisme par lequel la *non-souveraineté* se traduit en pertes financières concrètes. Comprendre cette architecture, ses acteurs, ses rails, ses logiques économiques est le préalable indispensable à toute stratégie de rattrapage économique et industriel.

2.1 Une souveraineté en trompe-l'œil sur l'ensemble de la chaîne de valeur des paiements

La situation européenne se caractérise par une situation profondément hétérogène selon la situation de chacun des États membres :

- **Les paiements de gros reposent sur des infrastructures opérées par l'Eurosystème** qui assurent un contrôle direct des flux critiques et garantissent un niveau élevé de sécurité et de résilience.
- **Les paiements de détail[49] sont marqués par des dépendances significatives** à des acteurs et des infrastructures extra-européennes, en particulier Visa et MasterCard,

[49] Si le cadre SEPA constitue une infrastructure paneuropéenne essentielle pour les virements et prélèvements, il ne couvre pas l'ensemble des usages, notamment les paiements par carte et les paiements du quotidien.

qui occupent une position systémique dans une majorité d'États membres de la zone euro ne disposant pas de schémas domestiques propres[50]. La cession de Visa Europe à sa maison-mère en 2016 a consacré l'intégration complète des capacités européennes au sein d'un groupe soumis au droit états-unien [51].

À cette dépendance structurelle s'ajoute une évolution des usages marquée par la montée en puissance des nouvelles interfaces de paiement. Les portefeuilles numériques intégrés aux systèmes d'exploitation (Apple Pay ou Google Pay) ainsi que les plateformes de paiements comme PayPal tendant à s'interposer dans la relation avec l'utilisateur final[52] et d'orienter les choix de paiements (sélection des instruments, parcours client, gestion du risque). Sans se substituer aux réseaux existants sous-jacents, ces interfaces s'imposent comme une couche d'accès privilégiée par l'utilisateur, captant la relation client et reléguant les infrastructures traditionnelles à un rôle d'exécution invisible - en particulier le paiement mobile et le commerce en ligne.

À un second niveau, plus structurel, les infrastructures technologiques sous-jacentes (services *cloud*, traitement de données, solutions antifraude ou d'identification) sont elles aussi, largement dominées par des acteurs extra-européens.

Ces briques critiques, invisibles pour l'utilisateur final, conditionnent pourtant le traitement, la sécurisation et l'analyse des transactions.

[50] Neuf schémas nationaux subsistent dans l'UE, soit dans à peine un tiers des États membres : Belgique (Bancontact), Bulgarie (Borica), Danemark (Dankort), Allemagne (Girocard), France (Cartes Bancaires - CB), Italie (PagoBancomat), Malte, Portugal (MultiBanco). Parmi ces neuf schémas nationaux, la Cour des comptes européenne considère que seuls six disposent d'une part de marché significative — Bancontact, CB, Girocard, PagoBancomat, MultiBanco et Dankort — et souligne que seul PagoBancomat ne domine pas son marché national. Cour des comptes européenne, *Rapport spécial 01/2025 : Paiements numériques dans l'Union européenne* (janvier 2025).

[51] Visa Inc., « Visa Inc. To Acquire Visa Europe » (2 novembre, 2015), https://www.visa.fr/visa/newsroom/press-releases.1245287.html.

[52] Les portefeuilles intégrés revendiquent plus de 430 millions d'utilisateurs dans le monde. La société déclare 439 millions de comptes actifs en 2025. PayPal Holdings, Inc., *2025 Annual Report* (2026) : 3.

Alternatives souveraines aux dépendances étrangères au sein des chaînes de paiement européennes

LE CLOUD

Amazon Web Services (AWS) Microsoft Azure Google Cloud	**65 à 70 %**	du cloud européen concentré chez trois acteurs américains	*Hébergent les systèmes des banques, des acquéreurs et des réseaux de cartes européens.*
Outscale, OVHcloud, Cloud Temple S3NS, CEGEDIM, Orange	**6**	fournisseurs européens qualifiés SecNumCloud	*Le label SecNumCloud impose l'immunité aux lois extraterritoriales états-uniennes (CLOUD Act, FISA)*

PAIEMENT

Apple Pay / Google Pay

15 %

des paiements par carte de proximité en France réalisés par portefeuille mobile en 2024

Contrôlent l'interface de paiement sur smartphone

Visa / Mastercard

72 %

des paiements par carte en zone euro transitent par des schémas états-uniens

Définissent les règles du réseau et autorisent chaque transaction par carte en Europe

WERO

53 millions

d'utilisateurs en 2026, par virement SEPA instantané

Non souverain pour les données stockées sur le cloud états-unien

Déjà opérationnel entre particuliers

CB, Multibanco, Girocard, Bancontact

Jusqu'à **10 x** moins chers

Jusqu'à **3 x** moins fraudés

Frais de réseaux inférieurs et données traitées et conservées en Europe

LES BANQUES COMMUNIQUENT

SWIFT arsenalisé par section 311 du PATRIOT Act

3e activation de SWIFT

comme outil de sanction en dix ans : Iran (2012), Corée du Nord (2017), Russie (2022)

Réseau belge de messagerie financière entre banques exposé à des pressions extraterritoriales américaines

LE RÈGLEMENT EST EFFECTUÉ

CHIPS (The Clearing House)

8,9 milliards de dollars

Amende infligée à BNP Paribas pour des transactions en dollars réalisées hors du territoire américain

Toute transaction en dollars est soumise à la juridiction états-unienne

T2 / TIPS

2 200 milliards

réglés par jour en euro, en monnaie de banque centrale, en instantané 24h/24

Un paiement en euro ne dépend jamais de CHIPS

QUI EST CONCERNÉ ?

Opérateurs d'importance vitale

(hôpitaux, énergie, télécommunications, PME, citoyens)

2.2 Le coût économique de la dépendance : barrière douanière invisible, rente d'infrastructure et coût de la dépendance

La dépendance étrangère dans le secteur des paiements possède un coût économique réel supporté quotidiennement par les entreprises et les consommateurs européens, sous deux formes, pourtant invisibles dans le débat public.

2.2.1 Une barrière douanière intra-européenne invisible : le coût de la fragmentation européenne

En dépit de l'existence du marché unique, de l'existence d'une monnaie unique pour la zone euro et de l'espace de paiement en euro SEPA (*Single Euro Payments Area*)[53], les paiements transfrontaliers intra-européens sont coûteux, ce qui constitue une anomalie structurelle au regard des objectifs d'intégration du marché unique. Ces surcoûts se manifestent à plusieurs niveaux :

- **Au niveau des commerçants** qui supportent des frais spécifiques intégrés dans les commissions d'interchanges au sein du montant global des commissions commerçants (*Merchant Service Charge* - MSC)[54] ;
- **Au niveau des transactions transfrontières**, qui donnent lieu à des commissions additionnelles liées au recours aux schémas internationaux ;
- **Au niveau opérationnel**, avec des coûts significatifs associés à la gestion multi-pays (multiplicité des contrats d'acquisition, hétérogénéité des systèmes d'acceptation, exigences techniques différenciées selon les juridictions, etc.).

Si cette situation ne constitue pas, au sens strict, une taxe juridique, elle s'apparente néanmoins à une barrière douanière subie et invisible. Cette friction agit en effet comme un coût implicite sur les échanges intra-européens, créant une double distorsion de concurrence :

- D'une part, **entre les schémas de paiement domestiques européens** (Cartes Bancaires, Bancontact, Girocard, etc.) limités à leur marché national, et **les réseaux internationaux** (Visa, MasterCard), qui bénéficient d'un effet d'échelle et d'une acceptation transfrontalière ;

[53] Banque centrale européenne, *Single Euro Payments Area (SEPA)*, BCE, 2024, https://www.ecb.europa.eu/paym/retail/sepa. L'espace SEPA regroupe 41 États et couvre virements (SCT/SCT Inst) et prélèvements (SDD).
[54] Voir Glossaire.

- D'autre part, **entre les acteurs opérant à l'échelle domestique** (commerçants locaux) **et ceux déployant leurs activités à l'échelle européenne**, en particulier dans les secteurs fortement intégrés comme le commerce électronique (Amazon, Zalando, Temu, Shein).

Dans ce contexte, la notion de « taxe invisible » peut être mobilisée avec prudence pour qualifier une friction subie sans contrepartie productive identifiable, et révélant les limites de l'intégration du marché européen des paiements. **Appliquée au volume total des paiements par carte dans la zone euro, estimé à environ 3 278 milliards d'euros en 2024, et à un niveau moyen de frais d'acceptation de l'ordre de 0,4 % à 0,6% cette friction représente un volume de coûts annuels de l'ordre de 13,1 à 19,7 milliards d'euros soit environ 0,09-0,13[55].** Celui-ci se traduit, *in fine*, par un coût implicite supporté par l'ensemble des agents économiques, principalement répercuté sur les consommateurs finaux *via* les prix. Cette charge se découpe en plusieurs composantes. Les effets de cette « taxe douanière invisible » sont particulièrement marqués pour les PME, pour qui les coûts de paiement constituent des frictions proportionnellement plus élevées affectant directement leur capacité à opérer à l'international.

Cas 1 – LES COÛTS TRANSFRONTALIERS INTRA-ZONE EURO : LE CAS DE LA FRANCE ET DE LA BELGIQUE

Pour un commerçant, ou une plateforme, opérant entre la France et la Belgique, les paiements par carte transfrontaliers peuvent engendrer des coûts plus élevés que les paiements domestiques, malgré l'utilisation de la même monnaie et un cadre réglementaire harmonisé.

Concrètement, pour un acteur présent dans les deux pays :

- Un paiement domestique par carte en France affiche généralement un MSC compris entre 0,30 % et 0,40 % (selon le secteur d'activité et la taille du commerçant) ;
- Un paiement transfrontalier entre la France et la Belgique peut atteindre un MSC total de 0,45 % à 0,60 %, soit un surcoût typique de 15 à 30 points de base[56].

[55] Voir Annexe « Estimation du coût agrégé d'acceptation en zone euro », pour 2024 (*Merchant service charge*).

[56] Les schémas domestiques CB et Bancontact n'étant pas interopérables au-delà de leur marché national, un paiement transfrontalier France-Belgique est nécessairement acheminé par Visa ou MasterCard et en supporte les commissions de schéma, supérieures aux niveaux domestiques. Voir Worldline, « *Scheme Fees* France 2024 », grille tarifaire acquéreur. Sur la

Ce différentiel s'explique principalement par :

- Le recours quasi systématique aux schémas internationaux pour les paiements transfrontaliers ;
- L'absence de concurrence des schémas nationaux en dehors de leur marché domestique ;
- La persistance d'une segmentation de *l'acquiring*, qui s'accompagne de grilles tarifaires spécifiques pour les transactions *cross-border*.

Ainsi, malgré l'intégration monétaire de la zone euro, des frictions subsistent dans l'acceptation des paiements par carte à l'échelle transfrontalière.

CAS 2 - LES COÛTS TRANSFRONTALIERS ENTRE LA FRANCE MÉTROPOLITAINE ET LA POLYNÉSIE FRANÇAISE

Bien qu'ils relèvent d'un même espace juridique national, les paiements entre la métropole et certains territoires ultramarins peuvent présenter des niveaux de coûts proches de ceux observés pour des flux internationaux, pouvant atteindre 0,60 % à 0,80 % pour certains paiements à distance ou e-commerce[57]. Ce surcoût s'explique notamment par :

- L'utilisation du franc Pacifique (XPF), qui implique des opérations de conversion monétaire ;
- Le recours à des routes de paiement externes s'appuyant sur des infrastructures non domestiques ;
- L'absence, pour certains usages, d'un rail de paiement entièrement unifié au niveau national.

Ainsi, ce différentiel de coût ne tient pas uniquement à une frontière territoriale au sens strict, mais aussi aux choix de moyens de paiements et à la gouvernance des infrastructures utilisées (les « rails »).

hausse documentée des commissions de schéma sur les flux internationaux, voir Payment Systems Regulator, « Market Review of Card Scheme and Processing Fees: Final Report » (Londres : PSR, 2025), MR22/1.10. https://www.psr.org.uk/publications/market-reviews/mr22110-market-review-of-card-scheme-and-processing-fees-final-report/ .

[57] Institut d'émission d'outre-mer (IEOM), « Rapport annuel 2023, Banque de France » (2024). Données sur les coûts d'acceptation des paiements dans les collectivités du Pacifique. Le différentiel par rapport aux transactions métropolitaines est structurel et lié aux conditions de clearing spécifiques aux zones XPF.

2.2.2 La taxe externe : rente d'infrastructure et coûts indirects de la dépendance

La dépendance aux infrastructures de paiement extra-européennes se traduit, en outre, par un phénomène de captation durable de valeur s'apparentant à une rente d'infrastructure au détriment des acteurs européens. Cette rente se manifeste à plusieurs niveaux.

- **Une rente financière visible**. Les commissions associées aux paiements par carte (frais de schéma et de *processing*, etc.) organisent un transfert continu de valeur depuis les commerçants et les consommateurs, vers des acteurs extra-européens. Cette dimension constitue la manifestation la plus immédiate et la plus identifiable de la dépendance.
- **Une rente informationnelle moins visible**. Les grands réseaux de paiement internationaux et les plateformes numériques disposent d'une vision consolidée, continue et extrêmement granulaire des comportements de consommation à l'échelle européenne. Cette asymétrie informationnelle renforce leur avantage concurrentiel en matière de ciblage commercial.
- **Une rente stratégique invisible, mais structurante : les coûts indirects de la dépendance.** En effet, la dépendance aux infrastructures européennes engendre des coûts indirects significatifs : exposition aux risques cyber, contraintes juridiques extraterritoriales, affaiblissement du pouvoir de négociation), et limite la capacité de l'Union à orienter la valeur générée par ses concitoyens sur ses propres systèmes de paiements.

Ce double diagnostic (fragmentation interne coûteuse, extraction externe organisée, nouveaux rails encore ouverts - euro numérique, paiements instantanés et A2A, *open banking*, tokenisation, IA agentique, etc.) dessine les contours d'une fenêtre d'action étroite, mais réelle. L'Union européenne dispose d'actifs sous-exploités, d'une infrastructure de gros souveraine, d'un cadre réglementaire avancé, et de plusieurs initiatives industrielles en cours de consolidation. La question n'est plus de savoir si une stratégie de souveraineté des paiements est nécessaire : le diagnostic de l'axe I et l'analyse économique de cet axe II en établissent la nécessité. La question est de savoir **quelle forme cette stratégie doit prendre, à quelle échelle, avec quels instruments, et selon quelle gouvernance**. C'est l'objet des recommandations.

TROISIÈME PARTIE — FORMALISER UNE DOCTRINE EUROPÉENNE DES PAIEMENTS FONDÉE SUR UNE GOUVERNANCE INDUSTRIELLE HYBRIDE ET UNE AUTONOMIE STRATÉGIQUE AFFIRMÉE

L'architecture des paiements, dominés jusqu'à présent par la carte, est en cours de reconfiguration. Des rails alternatifs émergent (paiements instantanés et A2A, *open banking*, tokenisation, IA agentique) qui ne sont pas encore verrouillés. **Les choix opérés dans les deux à trois prochaines années renforceront ou aggraveront la dépendance européenne**. L'enjeu dépasse la seule dimension économique : il s'agit de **garantir la continuité des échanges**, la **maîtrise des données** transactionnelles et la capacité des autorités européennes à **conserver un pouvoir de décision autonome** dans un environnement géopolitique et technologique en recomposition rapide. Pour cela, la stratégie européenne doit reposer sur une double approche :

- ✓ D'une part, une **réorientation des instruments politiques et réglementaires** permettant de structurer une véritable filière industrielle des paiements ;
- ✓ D'autre part, une action opérationnelle visant à sécuriser les infrastructures existantes, à maîtriser les couches critiques et à anticiper les mutations technologiques à venir (quantique).

3.1 Recommandation politique : doter l'Union européenne d'une véritable filière des paiements souveraine

L'objectif de ce premier ensemble de recommandations est de définir un cadre stratégique cohérent, permettant de corriger les asymétries concurrentielles et d'organiser un rapport de force plus équilibré au profit des acteurs européens. En somme, il s'agit de **réorienter les incitations économiques et sécuriser le cadre juridique.**

❖ Formaliser une doctrine européenne de souveraineté des paiements

Il apparaît indispensable de formaliser une doctrine explicite, reconnaissant l'ensemble de la filière des paiements comme composant critique de souveraineté. Si ses fonctions font déjà l'objet d'un encadrement au titre des Opérateurs d'importance vitale (OIV) ou systémique (OIS) au niveau national, cette approche demeure fragmentée et centrée sur les acteurs bancaires traditionnels sans intégrer les rails de paiement ou les nouvelles dépendances liées aux infrastructures numériques.

Il s'agit dès lors d'**élargir le périmètre et la portée à l'échelle européenne du caractère critique de l'ensemble de la chaîne de valeur des paiements** ainsi que les risques de dépendances technologiques et juridiques associés.

❖ Introduire une préférence stratégique

Le cadre réglementaire européen actuel repose historiquement sur un principe d'égalité de traitement entre acteurs et une approche centrée sur la protection du consommateur. Si ce double principe constitue un fondement du marché intérieur, il produit, dans un contexte de concurrence asymétrique, des effets contre-productifs :

- **D'une part, les acteurs extra-européens bénéficient d'économies d'échelles, d'effets de réseaux et d'un environnement réglementaire domestique plus favorable**. Cela recouvre :
    - ✓ L'existence d'un marché intérieur natif États-Unis) homogène et intégré permettant une diffusion rapide et massive des solutions ;
    - ✓ Un accès facilité à des infrastructures technologiques critiques, en particulier dans le *cloud* ;
    - ✓ Des cadres réglementaires plus centralisés et souvent plus prévisibles, ainsi que des dispositifs publics de soutien ou de projection extraterritoriaux.

Ces avantages permettent aux entreprises extra-européennes d'absorber les contraintes réglementaires de l'UE sans remise en cause de leur modèle économique, voire de les transformer en barrières à l'entrée pour leurs concurrents.

- **D'autre part, les acteurs européens supportent proportionnellement des coûts de conformité** pour plusieurs raisons :
    - ✓ La fragmentation du marché européen qui impose des adaptations nationales multiples (juridiques, techniques, commerciales) ;
    - ✓ La complexité et la superposition du cadre réglementaire européen (RGPD, DORA, DSP2/3, etc.), générant des coûts fixes importants ;
    - ✓ Une moindre capacité d'amortissement de ces coûts compte tenu de l'absence d'effets d'échelles comparables.

Ces éléments freinent le développement des entreprises européennes, *a fortiori* les acteurs émergents, et limitent leur capacité à concurrencer des acteurs globaux déjà installés.

Par ailleurs, cette **approche centrée sur le consommateur** tend à **minorer les enjeux économiques pesant sur les commerçants français et européens ainsi que sur l'ensemble du tissu productif, qui supportent pourtant une part significative des coûts du système de paiements** (commissions, intégration technique, dépendance aux schémas internationaux).

De surcroit, elle ne prend pas en compte les **stratégies de désintermédiation progressives des acteurs traditionnels**. Le modèle des grandes plateformes numériques repose en effet sur la **captation de la relation client et sur le contournement des intermédiaires existants** (banques, commerçants, schémas de paiements) qui se trouvent alors relégués à un rôle d'infrastructures ou d'exécution (voir 3.2.2). **Les coûts et les dépenses pèsent donc prioritairement sur les acteurs économiques qui assurent le fonctionnement du système de paiement, fragilisant des acteurs domestiques historiques** (Cartes Bancaires, Bancontact, Girocard).

L'introduction de mécanismes de préférence stratégique apparaît nécessaire pour rééquilibrer les incitations économiques et créer un véritable marché domestique européen :

- **Le conditionnement des financements publics à des critères de souveraineté** (juridiction applicable, localisation du traitement, contrôle des infrastructures) ;
- Une mobilisation plus volontariste de la commande publique au bénéfice d'acteurs européens ;
- **Une orientation des investissements** vers des infrastructures et solutions répondant à des exigences de maîtrise technologique et juridique.

❖ Construire une filière européenne intégrée

La réduction des dépendances structurelles suppose la construction d'une véritable filière européenne des paiements, couvrant l'ensemble de la chaîne de valeur. À cet égard, l'approche de l'opération militaire Aspides de l'Union européenne est riche en enseignements**.** Fondée sur une **approche pragmatique** reposant sur **une coalition d'États volontaires** et un **partage des investissements et des capacités**, elle illustre un modèle d'intégration flexible reposant sur des « nœuds » opérationnels. Transposée au domaine des paiements, cette logique permettrait de structurer un écosystème autour d'un noyau d'acteurs moteurs, **sans nécessiter une participation immédiate des 27 États membres**, et en

autorisant des points d'ancrage pouvant **inclure, le cas échéant, des partenaires ou infrastructures situés hors de l'Union**. Une telle approche offrirait ainsi **une voie réaliste** pour surmonter la fragmentation actuelle, en privilégiant une **montée en puissance progressive par cercles concentriques**.

3.2 Recommandations techniques : auditer et sécuriser les dépendances, construire une alternative européenne crédible et maîtriser les nouveaux points de rupture

Les orientations politiques présentées appellent à une traduction opérationnelle visant à reprendre un contrôle effectif sur les infrastructures et les fonctions critiques des systèmes de paiement.

❖ Mettre en place une cartographie opérationnelle des dépendances critiques

La priorité consiste à établir une cartographie exhaustive et partagée des dépendances critiques des systèmes de paiement européens. Celle-ci doit couvrir l'ensemble des couches du système afin d'identifier les points de concentration et de dépendance critique ainsi que la nature juridique des prestataires impliqués (droit applicable, accès potentiels aux données, localisation effective des opérations). Cette démarche pourrait être structurée sous la forme de tests de résilience technologique à l'échelle de l'UE, analogues aux stress test bancaires permettant d'évaluer la capacité du système à fonctionner en cas de dégradation ou d'indisponibilité critiques.

❖ Consolider les infrastructures SEPA et les solutions A2A dans une logique de souveraineté complète

Le virement instantané SEPA constitue une infrastructure de paiement intégralement européenne. Opéré par l'Eurosystème et reposant sur des infrastructures souveraines, il couvre l'ensemble de la zone euro et constitue, à ce titre, un actif stratégique majeur dont le potentiel est largement sous-exploité. Le règlement sur les virements instantanés (2024) impose désormais la généralisation de l'offre à parité tarifaire avec les virements classiques : une avancée réglementaire significative qui crée les conditions d'une montée en puissance des paiements A2A. Cependant, l'infrastructure de règlement ne suffit pas : la couche d'expérience utilisateur, d'initiation de paiement et de gestion du risque reste dominée par des acteurs privés dont l'ancrage européen n'est pas garanti.

Encadré n°4 – LES SOLUTIONS PANEUROPÉENNES A2A, UN ANGLE MORT DE LA SOUVERAINETÉ EUROPÉENNE DES PAIEMENTS

Les solutions paneuropéennes *account-to-account* (A2A), telles que Wero ou l'alliance EuroPA, constituent un levier pertinent pour réduire les frictions de paiement intra-européennes. Fondées sur SEPA Instant et réglées en monnaie de banque centrale *via* TIPS, elles offrent des gains potentiels en matière de coûts, de rapidité et d'intégration du marché intérieur. Toutefois, si le rail de règlement est pleinement européen, les couches technologiques critiques (*cloud*, logiciels d'orchestration, traitement et analyse des données, services antifraude) peuvent relever de fournisseurs soumis à des juridictions extra-européennes. Un avis juridique commandé par le ministère fédéral allemand de l'Intérieur et réalisé par l'Université de Cologne en mars 2025[58] confirme que, en application du CLOUD Act, du Stored Communications Act et de la section 702 du FISA, les autorités états-uniennes peuvent exiger l'accès à des données indépendamment de leur localisation géographique, dès lors qu'un prestataire soumis au droit états-unien exerce un contrôle juridique sur les services concernés[59]. Le rapport souligne par ailleurs que les mesures techniques, y compris le chiffrement, ne permettent pas d'exclure de manière certaine une telle obligation de transmission. Ces éléments n'invalident pas l'intérêt économique des solutions A2A, mais conduisent à considérer qu'elles ne constituent pas, à ce stade, des substituts complets aux schémas cartes existants du point de vue de la souveraineté. Elles doivent être intégrées dans une approche complémentaire et progressive, assorties d'exigences renforcées en matière de gouvernance technologique et de maîtrise des dépendances juridiques.

Il résulte de cette configuration l'émergence d'une solution que l'on pourrait qualifier de « semi-souveraine », caractérisée par une dualité entre, d'une part, des infrastructures de règlements maîtrisées au niveau européen et, d'autre part, des dépendances persistantes sur les couches technologiques, applicatives ou de gouvernance. Cette hybridation crée une illusion d'autonomie, dans laquelle la souveraineté apparente des infrastructures ne se traduit pas nécessairement par une maîtrise opérationnelle des fonctions critiques du système. En pratique, certaines briques essentielles (*cloud*, interface d'orchestration ou gouvernance

[58] « US Zugriffsbefugnisse auf Daten in der Cloud : Gutachten Uni Köln vom März 2025 », rapport pour le ministère fédéral de l'Intérieur allemand (Cologne : Université de Cologne, mars 2025), cité par Datenrecht.ch, https://datenrecht.ch/en/us-zugriffsbefugnisse-auf-daten-in-der-cloud-gutachten-uni-koeln-vom-maerz-2025/.

[59] « Point de vue : les autorités états-uniennes disposent d'un accès étendu aux données stockées dans le cloud européen », *Heise Online*, 10 décembre 2025.

technique) demeurent sous influence ou dépendance d'acteurs extra-européens, limitant la capacité à exercer un contrôle réel sur le fonctionnement des paiements.

Au-delà de cette dépendance technique, ces architectures hybrides présentent également un risque structurel de fragmentation et de faible passage à l'échelle. En l'absence de standardisation et de gouvernance intégrée, les initiatives européennes tendent à se développer de manière segmentée, ciblant des usages spécifiques sans parvenir à constituer des alternatives complètes et compétitives face aux acteurs globaux. Cette dispersion limite les effets de réseau, affaiblit la proposition de valeur et freine l'adoption à grande échelle. À cet égard, **des initiatives comme Wero ne pourront constituer une alternative crédible que si elles s'inscrivent dans une logique de souveraineté intégrale, couvrant l'ensemble des couches critiques** (*cloud*, traitement de données, orchestrations des paiements et gouvernance).

❖ Déployer une architecture européenne de paiement multi-rails : création d'un *switch* européen de paiement

La première condition d'une autonomie effective réside dans le fait que l'Union européenne ne soit plus à la merci d'un « *kill switch* » états-unien. La mise en place d'un « *switch* européen » vise donc à assurer l'interconnexion des principaux schémas domestiques européens Cartes Bancaires (France), Girocard (Allemagne) et Bancontact (Belgique) afin de dépasser leur fragmentation et permettre le fonctionnement comme un ensemble cohérent à l'échelle du marché intérieur.

Au-delà de l'interconnexion, ce switch aurait pour fonction d'introduire une **capacité de routage interne, permettant d'orienter les flux de paiement vers les solutions les plus pertinentes** selon des critères prédéfinis, notamment le coût, la localisation du paiement, la sécurité ou encore les exigences de souveraineté.

❖ Construire une souveraineté européenne sur les données et les dispositifs antifraude

La captation et l'exploitation des données transactionnelles constituent aujourd'hui un levier central de pouvoir économique et technologique. Dans ce domaine, les acteurs extra-européens bénéficient d'un avantage cumulatif, fondé sur la concentration des données et sur leur capacité à développer et entraîner des modèles performants.

Cette asymétrie ne se limite pas à une dimension concurrentielle : elle s'étend également au champ de la conformité réglementaire. Les grands réseaux internationaux de paiement jouent en effet un rôle structurant dans la mise en œuvre des obligations de lutte contre le

blanchiment de capitaux et le financement du terrorisme (LCB-FT), en s'inscrivant dans les référentiels internationaux, notamment ceux du GAFI. À ce titre, ils disposent d'une **capacité d'influence significative sur les conditions d'accès aux flux et sur les standards de conformité**, ce qui peut conduire, en pratique, à des situations de dépendance fonctionnelle.

Afin de corriger cette double asymétrie (informationnelle et réglementaire), il apparaît nécessaire de structurer une stratégie européenne articulée autour de plusieurs mesures :

- **La constitution de pools européens de données transactionnelles**, dans le respect des exigences en matière de protection des données, permettant de mutualiser les ressources, de renforcer les capacités d'analyse et de soutenir le développement de modèles performants à l'échelle européenne ;
- **Le développement de solutions antifraude européennes**, mutualisées et interopérables, intégrant pleinement les exigences en matière de LCB-FT, afin de réduire la dépendance à des prestataires extra-européens et de renforcer la capacité de supervision des autorités européennes ;
- **L'introduction d'exigences en matière de portabilité et d'audibilité des modèles**, garantissant la transparence, la réversibilité et le contrôle des dispositifs utilisés, en particulier lorsque ceux-ci contribuent à la prise de décision sur les flux de paiement.

Cette stratégie vise à limiter l'avantage cumulatif des acteurs dominants, à renforcer l'autonomie des acteurs européens dans la gestion des risques et de la conformité, et à restaurer des conditions de concurrence plus équilibrées au sein du marché des paiements.

❖ Accélérer le développement d'un *cloud* de confiance adapté aux paiements

La maîtrise des infrastructures de paiement repose de manière croissante sur celle des environnements de traitement et de stockage des données. Dans ce contexte, le développement d'une offre *cloud* de confiance, spécifiquement adaptée aux besoins des paiements, constitue une condition indispensable à toute stratégie de souveraineté. À cet égard, il apparaît pertinent de s'appuyer sur la certification SecNumCloud de l'ANSSI, en étendant le périmètre et les exigences au niveau européen. Une telle approche permettrait de définir un standard opérationnel applicable aux infrastructures critiques de paiement, fondé sur des garanties renforcées en matière de sécurité, de contrôle et de protection des données.

Dans cette perspective, il pourrait être envisagé de :

- Rendre obligatoire, pour certaines fonctions critiques des systèmes de paiement (traitement des données transactionnelles, antifraude, orchestration), le recours à des infrastructures certifiées selon des standards de type SecNumCloud ;
- Adapter ce référentiel aux spécificités du secteur des paiements, en intégrant des exigences relatives à la continuité d'activité, à la résilience et au contrôle opérationnel ;
- Promouvoir, à l'échelle européenne, un cadre de certification harmonisé, permettant d'assurer une indépendance juridique effective vis-à-vis des législations extraterritoriales.

Cette approche permettrait d'éviter le développement de solutions de « *cloud* de confiance de façade », reposant sur des dépendances juridiques persistantes, et de garantir un contrôle effectif des données et des traitements associés aux paiements. Ces exigences devraient s'appliquer prioritairement aux infrastructures critiques et aux prestataires de services de paiement, compte tenu de leur rôle central dans le fonctionnement du système.

❖ Positionner l'euro numérique comme infrastructure publique de dernier recours

Le positionnement de l'euro numérique comme infrastructure publique de **dernier recours** appelle à une réflexion sur ses modalités d'intégration au sein des système existants. Une option consisterait à s'appuyer sur les réseaux domestiques européens tels que Cartes Bancaires en France ou Girocard en Allemagne afin d'en **assurer la diffusion selon une logique de *co-badging*.** Ce modèle permettrait d'intégrer l'euro numérique dans les instruments de paiement déjà largement utilisés, en capitalisant sur leurs réseaux d'acceptation et leurs relations avec les commerçants. À l'échelle européenne, il supposerait toutefois une **interconnexion renforcée de ce système afin de dépasser leur fragmentation actuelle** et de constituer une véritable infrastructure paneuropéenne. Dans cette architecture, l'euro numérique occupe une fonction de socle public, tandis que les réseaux cartes et les solutions A2A assureraient la distribution et l'acceptation. Cette logique multi-rails permettrait de concilier continuité des usages, efficacité économique et souveraineté. Toutefois, la réussite de cette approche dépend de la maîtrise de la couche numérique, qui constitue désormais le principal point de contrôle du système. À ce titre, des solutions applicatives comme Wero pourraient jouer un rôle structurant, à condition de répondre à des exigences renforcées en matière de souveraineté technologique et juridique, telles qu'évoquées *supra*.

Encadré n°5 – LE *CO-BADGING* : UN MODÈLE D'INTÉGRATION DES RAILS

Le modèle de *co-badging* (ou co-marque), historiquement utilisé dans les réseaux de cartes, illustre une forme d'architecture permettant de concilier innovation et continuité. Il consiste à associer, sur un même instrument de paiement, plusieurs réseaux ou schémas distincts, généralement un réseau domestique et un réseau international, afin de combiner leurs avantages respectifs. Ce modèle a permis, par le passé, d'assurer une coexistence entre des infrastructures nationales, telles que Cartes Bancaires en France, et des réseaux globaux comme Visa ou Mastercard, tout en garantissant l'interopérabilité internationale. Il repose sur une logique de partage du routage et des fonctions, selon des règles définies *ex ante*.

Transposé aux évolutions actuelles, ce principe offre une grille de lecture utile pour penser l'articulation entre anciens et nouveaux rails. L'intégration de l'euro numérique, des solutions A2A ou des couches d'intelligence artificielle pourrait ainsi s'inscrire dans une logique de co-existence structurée, plutôt que de substitution.

La gouvernance de ces solutions devrait être assurée à l'échelle européenne en lien étroit avec les institutions publiques, en premier lieu, la Banque centrale européenne, afin de garantir l'alignement avec les objectifs de souveraineté. Sous l'impulsion de la BCE, un consortium européen associant public et privé pourrait permettre de coordonner ces différents niveaux et d'assurer la cohérence de leur ensemble. À défaut d'un tel encadrement, le risque est celui d'une architecture fragmentée dans laquelle la superposition des solutions publiques et privées ne se traduirait pas par une autonomie stratégique réelle, mais par une dépendance recomposée en particulier sur les couches numériques critiques.

❖ Encadrer et anticiper le développement de l'IA appliqué aux paiements

L'émergence des agents d'intelligence artificielle[60] constitue une transformation structurelle dont les implications pour la souveraineté des paiements sont encore sous-évaluées. Depuis 2025, plusieurs acteurs états-uniens (Visa, Mastercard, Stripe, Google, OpenAI) développent des **protocoles automatisant le parcours d'achat du début à la fin, intégrant le paiement dans une chaîne décisionnelle pilotée par des algorithmes**. Dans ce modèle, **le choix du**

[60] Sonja Davidovic et Hervé Tourpe, « How Agentic AI Will Reshape Payments », IMF Notes, n° 2026/004. (Washington, D.C. : Fonds monétaire international, 2026), https://doi.org/10.5089/9781513533308.068. On désigne par « IA agentique » des systèmes capables d'interpréter des objectifs, de les décomposer en tâches et d'interagir avec des services numériques avec une intervention humaine limitée.

moyen de paiement n'est plus effectué par l'utilisateur ni même par un établissement financier, mais par un agent d'intelligence artificielle, souvent **opéré par une plateforme à l'instar d'OpenIA** (ChatGPT), Antropic (Claude), Deepseek (Deepseek) ou Google (Gemini[61]). Le développement de ces architectures demeure encore incertain en raison d'une adoption commerçante limitée, de difficultés d'interopérabilité ainsi que d'importants enjeux de sécurité, de responsabilité juridique et de gouvernance des standards. Ces schémas sont cependant amenés à voir le jour d'ici quelques années.

À terme, ce mode de fonctionnement devrait redéfinir en profondeur la gouvernance effective des paiements de détail[62]. Selon un rapport publié par McKinsey (2025), ces modèles pourraient médiatiser entre 3 000 et 5 000 milliards de dollars de commerce mondial d'ici 2030, redéfinissant profondément la gouvernance effective des paiements de détail[63]. En effet, la position de ces agents dans la chaîne de valeur numérique leur permettra de **contrôler non seulement les interfaces utilisateur, mais également les modèles d'intelligence artificielle et les infrastructures de traitement associées.** Ce déplacement du pouvoir décisionnel confère à ces acteurs majoritairement extra-européens, un **rôle central dans le routage des transactions** leur permettant **d'orienter les flux selon leurs propres critères – économiques, techniques ou stratégiques.** Cette situation introduira à terme, une nouvelle couche de dépendance qui se superposera aux dépendances existantes (*cloud*, données, infrastructures de paiement), tout en les renforçant.

Cette dépendance présente une particularité : elle s'inscrit directement dans les usages et les comportements des utilisateurs. Contrairement aux infrastructures techniques potentiellement substituables, les systèmes agentiques créent un **effet de verrouillage** plus profond qui pourrait **structurer durablement les choix de paiement pour les consommateurs**, tout en les rendant invisibles pour l'utilisateur final. Dans ces conditions, les choix technologiques effectués aujourd'hui en matière de développement de modèles, de règles de routage ou d'intégration dans les plateformes numériques sont susceptibles de déterminer la structure de pouvoir dans les paiements pour la décennie à venir. Face à ce risque, le développement de capacités européennes en matière d'IA appliquée aux paiements apparait comme un levier stratégique. Plutôt que de concurrencer les modèles généralistes dominants,

---

[61] Tobin South et al., « Identity Management for Agentic AI » (Stanford Loyal Agents Initiative / OpenID Foundation, 2025) : 14–20. Le document identifie l'absence de cadre unifié de délégation, les lacunes en matière d'enregistrement dynamique de clients et les risques liés à la traçabilité des agents comme obstacles structurels au déploiement à grande échelle.

[62] Ryan McInerney, « A Message from the CEO », dans Visa Inc., *2025 Annual Report* (San Jose : Visa Inc., 2025), https://annualreport.visa.com/chairman-and-ceo-message/default.aspx.

[63] McKinsey & Company, « Europe's Agentic Commerce Moment: Decision Influence Is Here, Execution Is Coming » (2026), https://www.mckinsey.com/capabilities/quantumblack/our-insights/europes-agentic-commerce-moment-decision-influence-is-here-execution-is-coming. « McKinsey research estimates that by 2030, agentic commerce could orchestrate $3 trillion to $5 trillion globally ».

il s'agirait **de développer des modèles spécialisés de type *Small Language Model* (SLM)**, **adaptés aux usages de paiement, notamment en matière de détection de fraude, ou d'optimisation des transaction**s. Toutefois, le développement de telles capacités ne saurait à lui seul garantir une autonomie stratégique s'il n'est pas accompagné d'exigences relatives **à leur déploiement et à leur gouvernance**. Dans les fonctions les plus critiques, en particulier celles relatives à la prise de décision, au traitement des données transactionnelles et au routage des paiements, il apparaît nécessaire que les systèmes d'IA reposent sur des infrastructures compatibles avec les exigences de l'UE en matière de souveraineté. Cela implique de garantir que ces systèmes soient opérés dans un cadre assurant un contrôle effectif des données et des décisions : notamment à travers leur hébergement dans des environnements conformes aux standards européens, leur soumission au droit de l'Union, ainsi qu'une transparence suffisante de leur fonctionnement. Dans cette perspective, une **exigence de nationalité, de localisation et de traitement des données sensibles au sein de l'Union** pourrait être envisagée pour certaines fonctions critiques, en particulier celles liées à l'analyse et à l'exploitation des données transactionnelles. Cette approche permettrait de limiter l'exposition aux mécanismes d'extraterritorialité et de renforcer la capacité de supervision des autorités européennes.

CONCLUSION

Le retour de Donald Trump à la Maison-Blanche, ne marque pas tant une rupture qu'une inflexion dans l'usage des instruments de puissance économiques états-uniens. Le système juridique, financier et technologique de la première puissance mondiale a en effet été conçu de longue date pour protéger leur souveraineté et leurs intérêts stratégiques. Toutefois, là où ces leviers s'inscrivaient jusqu'alors dans une logique de compétition économique, leur mobilisation s'opère désormais au service d'un projet de coercition ouvert et assumé au service de la puissance états-unienne. Cette évolution s'inscrit dans un contexte de rivalité accrue avec la Chine de plus en plus structuré, dans lequel les infrastructures de paiement, au cœur des flux économiques mondiaux, deviennent des outils centraux de la compétition stratégique mondiale.

Dans ce cadre, le premier enseignement tient à l'**existence d'un risque systémique lié à la dépendance européenne aux infrastructures de paiements détenues par des acteurs états-uniens**. Cette situation expose l'Union à des mécanismes de coercitions, notamment sous la forme de sanctions extraterritoriales. Parallèlement, l'émergence progressive d'un système de paiement sino-centré, adossé au renminbi et à des infrastructures dédiées fait peser un **risque de marginalisation à plus long terme, en structurant des circuits alternatifs dont l'UE pourrait être partiellement exclue**.

Le deuxième enseignement réside dans **l'existence d'une fenêtre d'intervention étroite, mais réelle**. Les rails de paiement de nouvelles générations (paiement A2A, tokenisation des actifs, commerce agentique) demeurent en cours de structuration. Les choix opérés aujourd'hui en matière d'infrastructures, de gouvernance et de standard seront déterminants pour façonner les équilibres futurs avant que ces architectures ne se stabilisent autour de modèles dominants.

Enfin, le troisième enseignement tient à la nécessité d'une approche fondée sur **l'hybridation, l'agilité et la résilience.** Face à la fragmentation européenne, une réponse efficace ne peut reposer sur une intégration uniforme à 27, mais doit s'appuyer sur **des coalitions d'États volontaires**, capables de structurer rapidement des « nœuds » opérationnels et évolutifs, y compris en lien avec des partenaires extérieurs. Cette logique permettrait de concilier montée en puissance progressive, mutualisation des capacités et adaptation à un environnement technologique et géopolitique en rapide transformation.

À défaut d'une telle stratégie, l'Union européenne s'expose à **un risque de marginalisation progressif, mais certain**, dans un système financier international en recomposition, au sein duquel elle ne maîtriserait ni les infrastructures, ni les standards, ni les règles du jeu.

ANNEXE - ESTIMATION DU COÛT AGRÉGÉ D'ACCEPTATION EN ZONE EURO, POUR 2024 (*MERCHANT SERVICE CHARGE*)

L'ordre de grandeur avancé résulte de l'application d'un taux moyen de frais d'acceptation au volume total des paiements par carte de la zone euro.

Le volume total des paiements par carte de la zone euro s'élève à 3 277,62 Md€[64]. Le taux moyen de frais d'acceptation (MSC), c'est-à-dire le coût total prélevé sur chaque transaction acceptée, qui agrège l'interchange, les commissions de schéma et la marge de l'acquéreur, est évalué dans une fourchette de 0,40 % à 0,60 %.

Cette fourchette est encadrée par deux mesures indépendantes et convergentes :

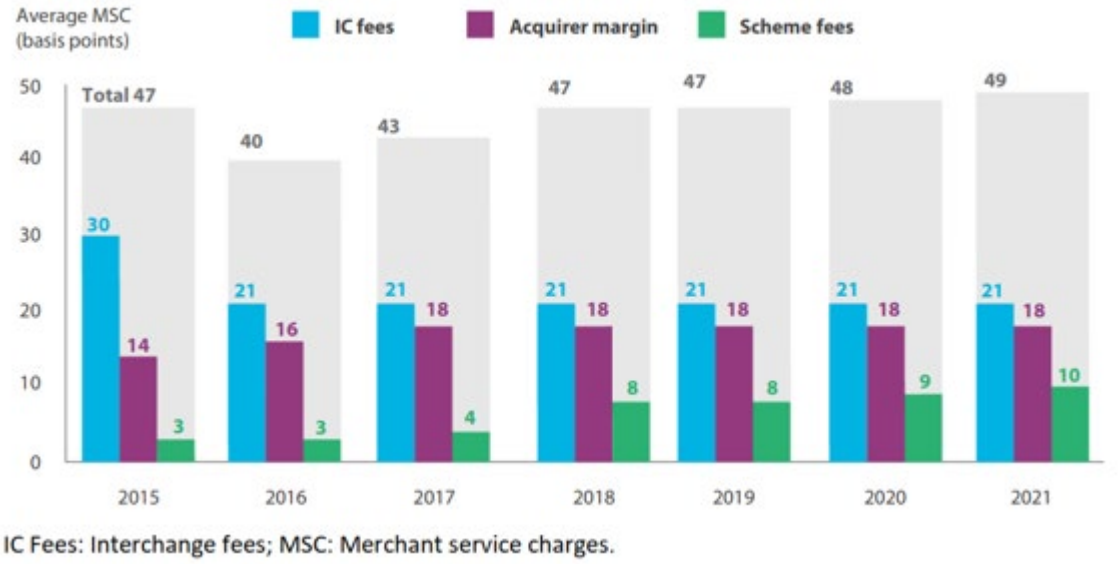
- L'étude réalisée par CMSPI et Zephyre pour EuroCommerce estime le MSC moyen tous postes (débit et crédit, transactions domestiques et intra-européennes) à 0,48 % de la valeur de transaction pour l'Union à vingt-huit en 2020 (CMSPI & Zephyre, Scheme Fee Study, 2021).
- L'étude commanditée par la Commission européenne sur les développements récents des marchés de cartes établit le MSC net moyen des cartes de débit à 0,44 % en 2022 pour un échantillon de douze États membres, en hausse depuis 0,27 % en 2018 (Commission européenne DG Concurrence, VVA Brussels & GDCC, *Study on New Developments in Card-Based Payment Markets*, 2024, p.95).
- La borne haute de 0,60 % reflète l'exposition aux paiements en ligne et aux cartes commerciales, non couverts par le plafonnement de l'interchange et supportant des coûts sensiblement supérieurs chaque année.

Ainsi, sur 3 277,62 milliards d'euros, de paiement par carte le coût se situe entre 13,1 milliards d'euros ($3\,277{,}62 * 0{,}40$) et, 19,7 milliards d'euros ($3\,277{,}62 * 0{,}60$).

Rapporté au produit intérieur brut de la zone euro, estimé à environ 15 200 milliards d'euros en prix courants pour 2024[65], ce montant représente entre 0,09 % et 0,13 % du PIB.

[64] Payments transactions (Key indicators) – PAY, BCE, PAY. Disponible sur : https://data.ecb.europa.eu/data/datasets/PAY.
[65] Produit intérieur brut (PIB) et principales composantes (production, dépenses et revenu) - données annuelles Eurostat, juin 2026. Disponible sur : https://ec.europa.eu/eurostat/databrowser/view/nama_10_gdp/default/table?lang=fr.

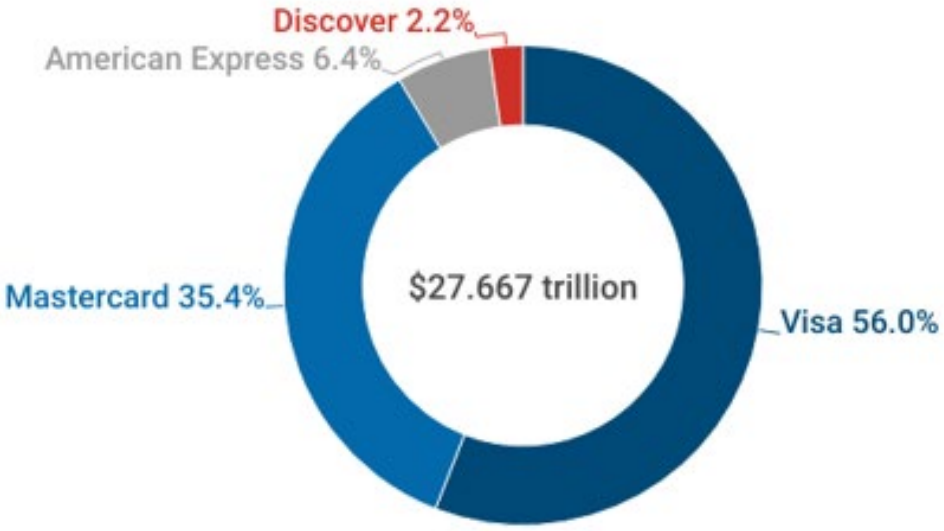
Composition of merchant services charges 2015-2021



IC Fees: Interchange fees; MSC: Merchant service charges.

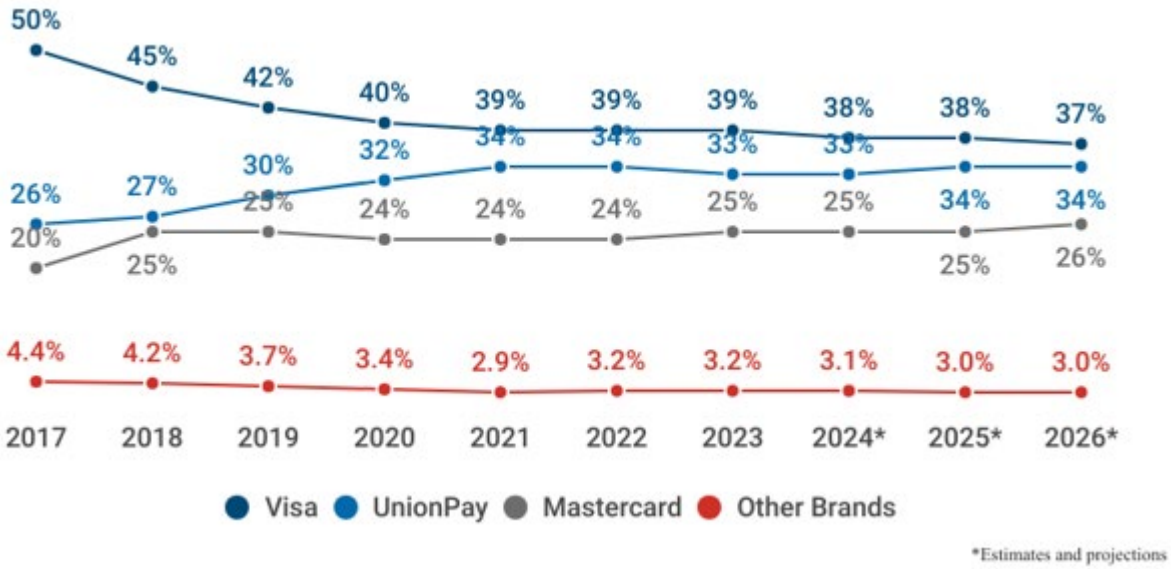
Source : CMSPI & Zephyre Scheme Fee Study (2021).

U.S. Card Processor's Purchase Volume Share



Source : U.S. Securities and Exchange Commission

Credit Card Brand Share of Global Transactions



Source : Nilson Report

GLOSSAIRE ET ACRONYMES

- **A2A (*Account-to-Account*)** : Paiement par virement interbancaire, transférant directement la monnaie d'un compte à un autre.
- **CBDC - MNBC (Central Bank Digital Currency - Monnaie numérique de banque centrale) :** Forme numérique de la monnaie émise par une banque centrale, une version numérique de l'espèce. Contrairement aux dépôts bancaires classiques, elle est une créance directe sur la banque centrale, sans risque de crédit. On distingue la CBDC de gros (entre banques) et la CBDC de détail (grand public).
- **CIPS (*Cross-border Interbank Payment System*)** : Système chinois de paiement et de compensation internationaux en renminbi (Yuan), lancé en 2015, destiné à réduire la dépendance de la Chine aux infrastructures dominées par le dollar.
- **Co-badging (co-marque)** : Présence de deux logos de réseaux sur un même instrument, comme CB et Visa. Permet actuellement d'utiliser un réseau domestique en France et un réseau international à l'étranger.
- **Clarifying Lawful Overseas Use of Data Act (CLOUD Act, 2018)** : Loi fédérale états-unienne autorisant les autorités judiciaires des États-Unis à contraindre des entreprises technologiques soumises à leur juridiction à fournir des données numériques hébergées à l'étranger.
- **Extraterritorialité du droit** : Application par les États-Unis de leur législation à des personnes ou entités étrangères, pour des actes réalisés hors du territoire états-unien, dès lors que ces actes impliquent un lien avec les États-Unis : usage du dollar, recours à des entreprises états-uniennes, etc.
- **Groupe d'action financière (GAFI)** : Organisme intergouvernemental fondé en 1989 par le G7, chargé de définir les normes internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme.
- **Hyperscalers** : Fournisseurs de services d'infrastructure *cloud* à très grande échelle, caractérisés par leur capacité à déployer et opérer des centres de données massifs au niveau mondial. Les trois principaux hyperscalers états-uniens sont Amazon Web Services (AWS), Microsoft Azure et Google Cloud.
- **IA agentique** : Système d'intelligence artificielle capable d'effectuer de manière autonome des séquences d'actions orientées vers un objectif, sans intervention humaine active. Dans les paiements, il désigne des agents capables d'initier et d'exécuter des transactions à la place de l'utilisateur.

- **Interchange** : Frais versés par la banque du commerçant à la banque du porteur de carte à chaque transaction par carte. Plafonnés en Europe à 0,2 % pour les cartes de débit et 0,3 % pour les cartes de crédit, par le règlement IFR en 2015.
- **Office of Foreign Assets Control (OFAC)** : Bureau du Trésor états-unien chargé d'administrer et de faire appliquer les sanctions économiques et financières, y compris hors du territoire des États-Unis.
- **Merchant Service Charge (MSC)** : Coût total supporté par le commerçant pour accepter un paiement par carte, intégrant les frais d'interchange, frais de schéma et marge d'acquisition.
- **Paiement de détail (*retail*)** : Paiements entre les particuliers et les entreprises. Ils se caractérisent par le traitement d'opérations de montants peu élevés, mais en grande quantité, jouant un rôle essentiel dans la sphère économique.
- **Paiement de Gros** : Systèmes de paiement, essentiellement utilisés par les banques pour transférer ou recevoir de l'argent, permettant ainsi de faire circuler la monnaie dans l'économie. Ils sont essentiels pour alimenter les marchés financiers et les acteurs économiques en liquidités, assurer les paiements et la bonne fin des échanges.
- **Rail de paiement** : Infrastructure technique et organisationnelle sur laquelle transitent les transactions d'un payeur à un bénéficiaire. Plusieurs rails coexistent : réseaux de cartes (Visa, MasterCard), virements (SEPA), paiements instantanés (SCT Inst / TIPS), messagerie interbancaire (SWIFT). Le choix du rail détermine le coût, la vitesse et le niveau de souveraineté de l'opération.
- **Registre distribué (Distributed Ledger Technology – DLT)** : Base de données dont les enregistrements sont partagés et validés par plusieurs participants simultanément, sans administrateur central. La *blockchain* en est la forme la plus connue.
- **Résilience** : Capacité d'un système, à absorber un choc, à s'adapter en réorganisant ses flux, puis à se transformer structurellement pour réduire les vulnérabilités identifiées.
- **Risque systémique** : Risque qui résulte de la structure même du système, et en particulier de la dépendance à un nombre limité d'acteurs ou de nœuds critiques.
- **Risque cyber classique** : Risque qui renvoie à la probabilité qu'un système soit compromis à la suite d'une attaque malveillante (intrusion, rançon-logiciel, sabotage).
- **Single Euro Payments Area (SEPA)** : Espace harmonisé des paiements en euros, le virement instantané SEPA (SCT Inst) en constitue le rail intégralement européen.

- **Society for Worldwide Interbank Financial Telecommunication (SWIFT)** : Réseau de messagerie interbancaire transfrontalière transmettant les ordres de paiement entre banques, reliant plus de 11 000 institutions dans près de 200 pays. Bien que son siège social soit à Bruxelles, en Belgique, SWIFT a un centre de données aux États-Unis, ce qui soumet ces données au droit états-unien, indépendamment de la nationalité de l'émetteur du message.
- **Stablecoin** : Monnaie numérique, émise par une entreprise privée, conçue pour maintenir une valeur stable, généralement adossée à une monnaie fiat (dollar, euro), à un panier de devises ou à des actifs réels.
- **T2 (anciennement TARGET2) :** Système de règlement brut en temps réel (RTGS) opéré par l'Eurosystème pour les paiements de gros en euros.
- **TIPS (TARGET Instant Payment Settlement)** : Service de règlement des paiements instantanés en monnaie de banque centrale opéré par l'Eurosystème, socle de règlement des solutions A2A paneuropéennes.
- **Tokenisation** : Représentation numérique d'un actif (monnaie, titre), sous forme de jeton (*token*), enregistré sur un registre distribué. Ce registre fusionne en une seule opération des fonctions normalement séparées dans le circuit classique : émission, règlements, transfert de propriété.

BIBLIOGRAPHIE

- Agence de l'Union européenne pour la cybersécurité (ENISA), *ENISA Threat Landscape 2024*. 12e éd. (Athènes: ENISA, 2024). https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.
- Agence nationale de la sécurité des systèmes d'information (ANSSI). *Panorama de la cybermenace 2024* (Paris : ANSSI, 2024). https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2024/
- *Panorama de la cybermenace 2025*, Rapport CERTFR-2026-CTI-002. (Paris : ANSSI, 2026). https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2025/
- Gregory C. Allen et Isaac Goldston, « Understanding U.S. Allies' Current Legal Authority to Implement AI and Semiconductor Export Controls », Center for Strategic and International Studies (mars 2025). https://www.csis.org/analysis/understanding-us-allies-current-legal-authority-implement-ai-and-semiconductor-export.
- Assemblée nationale (France), Audition de Nicolas Guillou devant la Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique, Compte rendu n° 21, 29 avril 2026.
- Emma Badaoui et Anne-Thida Norodom, « (Extra)territorialité des données : quelle souveraineté pour l'Europe ? », *Études de l'Ifri* (Paris : IFRI, mars 2026). https://www.ifri.org/fr/etudes/extraterritorialite-des-donnees-quelle-souverainete-pour-leurope
- Banque centrale de Russie, *National Payment System: Results of 2024* (Moscou : Banque centrale de Russie, 2025). https://www.cbr.ru/collection/collection/file/59323/results_2024_e.pdf
- Banque centrale européenne, « Payment Statistics » (Francfort : BCE, 2026). https://data.ecb.europa.eu/data/datasets/PAY.
- « Payments Statistics: Second Half of 2024 » (Francfort : BCE, 2025).
- « Single Euro Payments Area (SEPA) » (Francfort : BCE, 2024). https://www.ecb.europa.eu/paym/retail/sepa.
- « Survey on the Access to Finance of Enterprises in the Euro Area (SAFE) » (Francfort : BCE, 2024). https://www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.space2024~19d46f0f17.en.html.
- Banque centrale européenne (Eurosystème), *The Eurosystem's Comprehensive Payments Strategy* (Francfort : BCE, 2026). https://www.ecb.europa.eu/press/pubbydate/2026/html/ecb.eurosystemcomprehensivepaymentsstrategy202603.en.html.

- Banque de France, *Paiements et infrastructures de marché à l'ère digitale* (Paris : Banque de France, 2022). https://publications.banque-france.fr/publications-economiques-et-financieres/livre-paiements-et-infrastructures-de-marche-lere-digitale
- *Stratégie nationale des moyens de paiement 2025-2030* (Paris : Banque de France, Comité National des Moyens de Paiements (CNMP), 2025). https://www.banque-france.fr/fr/strategie-monetaire/moyens-de-paiement/cnmp/strategie-nationale
- Camille Boulenguer et Julia Tomasso, « La lame et l'ombre : impacts des sanctions et chemins de contournement », *La Revue internationale et stratégique,* n°139 (2025/3). https://www.iris-france.org/ris/la-lame-et-lombre-impacts-des-sanctions-et-chemins-de-contournement/
- Frances Burwell et Kenneth Propp, *Digital Sovereignty: Europe's Declaration of Independence* (Washington, D.C. : Atlantic Council, 2025). https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/.
- Chine (République populaire de Chine), *Loi sur la cybersécurité* (Pékin, 2017).
    . Loi sur la protection des informations personnelles (Pékin, 2021).
    . Loi sur la sécurité des données (Pékin, 2021).
- CMSPI et Zephyre, *Scheme Fee Study*, Étude commanditée par EuroCommerce (2021). https://www.bargeldlosblog.de/wp-content/uploads/CMSPI-Zephyre-Scheme-Fee-Study-V3-1.pdf
- Commission européenne, « Communication sur la définition du marché en cause aux fins du droit communautaire de la concurrence », Journal officiel de l'Union européenne C 372 (9 décembre 1997).
    . « Décision 2000/520/CE du Parlement européen et du Conseil (Safe Harbor) ». *Journal officiel de l'Union européenne* (2000).
    . « Décision 2016/1250/UE du Parlement européen et du Conseil (Privacy Shield) », *Journal officiel de l'Union européenne* (2016).
- Commission européenne, *Study on New Developments in Card-Based Payment Markets, Including as Regards Relevant Aspects of the Application of the Interchange Fee Regulation* (Luxembourg : Office des publications de l'Union européenne, 2024). https://op.europa.eu/en/publication-detail/-/publication/ed0da3f4-c57a-11ee-95d9-01aa75ed71a1.
- Congrès national du peuple (Chine), *Texte officiel du 15ᵉ Plan quinquennal (2026-2030)* (Pékin : *Xinhua*, 12 mars 2026). https://www.qualenergia.it/wp-content/uploads/2026/03/China_15th_Five-Year_Plan_English.pdf.
- Copenhagen Economics et EY, S*tudy on the Application of the Interchange Fee Regulation*, Commandé par la Commission européenne (Copenhague : Copenhagen Economics, mars 2020). https://copenhageneconomics.com/wp-content/uploads/2021/12/copenhagen-economics_march_ifr-report.pdf.

- Cour de justice de l'Union européenne, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II). Affaire C-311/18, 16 juillet 2020. Maximillian Schrems v. Data Protection Commissioner (Schrems I). Affaire C-362/14, 6 octobre 2015.
- Cour de justice des Communautés européennes. AKZO Chemie BV c. Commission des Communautés européennes. Affaire C-62/86. 3 juillet 1991. Recueil de jurisprudence I-3359. https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:61986CJ0062.
- Cour des comptes (France), *Les enjeux de souveraineté des systèmes d'information civils de l'État*, Rapport public S2025-1479 (Paris : Cour des comptes, 2025).
- Cour des comptes européenne. *Rapport spécial 01/2025 : Paiements numériques dans l'Union européenne* (Luxembourg : Cour des comptes européenne, 2025). https://www.eca.europa.eu/fr/publications/SR-2025-01.
- Cross-border Interbank Payment and Settlement Co., Ltd. (CIPS). *Rapport annuel sur les statistiques du système CIPS 2024* (Shanghai : CIPS, 2025).
- Sonja Davidovic et Hervé Tourpe, « How Agentic AI Will Reshape Payments ». *IMF Notes*, n° 2026/004 (Washington, D.C. : Fonds monétaire international, 2026). https://doi.org/10.5089/9781513533308.068
- Nicolas De Sèze, « Monnaies numériques de banque centrale : une mise en perspective des travaux à travers le monde », *Revue d'économie financière*, n° 149 (2023) : 91–105. https://doi.org/10.3917/ecofi.149.0091
- Hubert De Vauplane, « Stablecoins : la nouvelle bataille des monnaies », *Études*, n°4332 (2025) : 39–50. https://doi.org/10.3917/etu.4332.0041
- Deutsche Bundesbank, « The Payments Ecosystem in Transition: Current Developments in the German Card Market », *Monthly Report* (décembre 2025). https://publikationen.bundesbank.de/publikationen-en/reports-studies/monthly-reports/monthly-report-december-2025-972374.
- Chris Dinga, « Mir Breaks Visa-Mastercard Duopoly in Russia », *Finextra Research*, 2021, https://www.finextra.com/newsarticle/38166/mir-breaks-visa-mastercard-duopoly-in-russia
- Françoise Drumetz et Christian Pfister. « La souveraineté monétaire à l'ère numérique », *Revue d'économie financière*, n° 160 (2025), https://doi.org/10.3917/e.ecofi.160.0153
- Eurojust, *The CLOUD Act* (La Haye: Eurojust, 2022).
- Union européenne, « Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on Interchange Fees for Card-Based Payment Transactions », *Official Journal of the European Union* (2015). https://eur-lex.europa.eu/eli/reg/2015/751/oj/eng
- « Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data (General Data Protection Regulation) », *Official Journal of the European Union*, (2016).

- Eurostat, « GDP and Main Aggregates » (2024).
- Henry Farrell et Abraham L. Newman, « Weaponized Interdependence: How Global Economic Networks Shape State Coercion ». *International Security* 44, n° 1 (2019): 42–79.
- Foo Yun Chee, « Visa, Mastercard Fees Probe Widens as EU Antitrust Regulators Look into Market Power », *Reuters*, 23 mai 2025. https://www.reuters.com/sustainability/boards-policy-regulation/visa-mastercard-fees-probe-widens-eu-antitrust-regulators-look-into-market-power-2025-05-23/
- FOTI – Future of Technology Institute, *Cloud Defence: An Exposed European Flank*, Note stratégique, avril 2026. https://futureinstitute.tech/assets/doc/FOTICloudDefenceReport26.pdf
- Emmanuel Hache et Candice Roche, « Rapport Draghi : reflet d'une Europe sans puissance », *La Revue internationale et stratégique*, n°137 (2025/1) : 19–31. https://doi.org/10.3917/ris.137.0019.
- Emmanuel Hache et al., « Donald Trump et le Groenland : une ambition géopolitique au-delà des ressources », Observatoire des États-Unis de l'IRIS, IRIS, janvier 2025. https://www.iris-france.org/wp-content/uploads/2025/01/ObsEtatsUnis_2025_01_20_Groenland_Note_FR.pdf
- Marion Heilmann, « Pannes de paiement : les grandes enseignes examinent des recours contre Worldline, *Les Échos*, 16 novembre 2023. https://www.lesechos.fr/finance-marches/banque-assurances/pannes-de-paiement-les-grandes-enseignes-examinent-des-recours-contre-worldline-2029466
- Rémy Hernu, « Le principe d'égalité et le principe de non-discrimination dans la jurisprudence de la CJUE », *Titre VII*, n° 4 (2020). DOI 10.3917/tvii.004.0044
- Institut d'émission d'outre-mer (IEOM), *Rapport annuel 2023* (Paris : Banque de France, 2024). https://www.ieom.fr/IMG/pdf/241191_ieom_ra_23_bd_web_pap.pdf
- Xin Ni Jiang, « Analysis of WeChat Pay Based on Technology Acceptance Model », dans *Proceedings of the 2022 7th International Conference on Social Sciences and Economic Development (IOSSED 2022)* (Amsterdam: Atlantis Press, 2022) : 668-675. https://doi.org/10.2991/aebmr.k.220405.110.
- Ryan McInerney « A Message from the CEO ». Dans *Visa Inc. 2025 Annual Report* (San Jose, CA : Visa Inc., 2025). https://annualreport.visa.com/chairman-and-ceo-message/default.aspx.
- New York State Department of Financial Services, « Superintendent Harris and Five Other State Regulators Secure $4.2 Million Settlement from Wise US, Inc., for Inadequate Anti-Money Laundering Program », Communiqué de presse, 9 juillet 2025. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250709.
- Esther Noël, *La souveraineté numérique en droit international*, Thèse de doctorat en droit public, Université Paris 1 Panthéon-Sorbonne, 2024. https://theses.fr/2025UNIP7139

- Anne-Thida Norodom, « Numérique, entreprises et États : l'usurpation diplomatique », *Revue du droit public et de la science politique en France et à l'étranger*, n° 2025/3 : 17–23. https://www.ifri.org/fr/etudes/extraterritorialite-des-donnees-quelle-souverainete-pour-leurope
- National Security Agency (NSA), « NSA Stops Certain Section 702 Upstream Activities », Communiqué de presse, 28 avril 2017.
- Observatoire de la sécurité des moyens de paiement, *Rapport annuel 2024* (Paris : Banque de France, 2024).
- OCDE, *Concurrence dans l'offre de services d'informatique en nuage* (Paris : Éditions de l'OCDE, 2025). https://www.oecd.org/fr/publications/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad.html
- OTAN, « Lutte contre les menaces hybrides » (Bruxelles : Secrétariat général de l'OTAN, 2026). https://www.nato.int/fr/what-we-do/deterrence-and-defence/countering-hybrid-threats
- *The US Safe Harbour Agreement*. EPRS, PE 595.892 (Bruxelles : Parlement européen, 2017).
- Payment Systems Regulator (PSR). Market Review of Card Scheme and Processing Fees: Final Report. MR22/1.10. Londres : Payment Systems Regulator, mars 2025. https://www.psr.org.uk/publications/market-reviews/mr22110-market-review-of-card-scheme-and-processing-fees-final-report/.
- PayPal Holdings, Inc. *2025 Annual Report*. San Jose, CA : PayPal, 2026.
- Dominique Plihon, « La dédollarisation : une stratégie de vaccination contre les sanctions ? », *La Revue internationale et stratégique,* n° 139 (2025/3) : p.126. https://www.iris-france.org/ris/la-dedollarisation-une-strategie-de-vaccination-contre-les-sanctions/.
- Mathieu Pollet, « Trump Can Pull the Plug on the Internet, and Europe Can't Do Anything about It », *Politico Europe*, 23 juin 2025. https://www.politico.eu/article/donald-trump-eu-internet-europe-us-trade-war-data-cyber/.
- Redbridge DTA, *The Impact of Brexit on Card Acceptance Costs*, Rapport sectoriel, 2021. https://www.redbridgedta.com/market-intelligence/brexit-card-acceptance-costs/
- Eulalia Rubio, « L'UE doit manier avec précaution la menace d'une taxe numérique européenne » (Paris : Institut Jacques Delors, 23 avril 2024). https://institutdelors.eu/publications/lue-doit-manier-avec-precaution-la-menace-d-une-taxe-numerique-europeenne/.
- Sébastian Seibt, « Digital Sovereignty: Have Trump Threats Spurred a European Awakening? », *France 24*, 2 février 2026. https://www.france24.com/en/technology/20260202-digital-sovereignty-have-trump-threats-spurred-european-awakening

- John E. Smith, Brandon L. Van Grack, Rachel Miras Fiorill, Elyse Beth Martin, et Nathanael Kurcab, « U.S. Sanctions Enforcement: 2023 Trends and Lessons Learned », *Morrison Foerster Client Alert*, 4 mars 2024. https://www.mofo.com/resources/insights/240304-us-sanctions-enforcement-2023-trends.
- Tobin South et al., *Identity Management for Agentic AI*. OpenID Foundation, 2026.
- Stripe Inc., « European Cross-Border Fees Update Due to Network Cost Changes ». Communiqué de tarification sectorielle, 2023.
- Julia Tasse, « Introduction à la guerre des systèmes », *La Revue internationale et stratégique*, n° 141 (2026/1). https://doi.org/10.3917/ris.141.0033.
- Max von Thun, Georg Riekeles et Pencho Kuzev, *Doubling Down, Not Backing Down: Defending the EU's Digital Sovereignty*, EPC Discussion Paper (Bruxelles: European Policy Centre, 2025). https://www.epc.eu/publication/Doubling-down-not-backing-down-defending-the-EUs-digital-sovereignt-626768/.
- United States, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*. H.R. 4943, 115ᵉ Congrès (Washington, D.C., 2018).
- Foreign Intelligence Surveillance Act (FISA), Section 702. 50 U.S.C. § 1881a (Washington D.C., 1978).
- United States, Department of Justice (U.S. Attorney's Office, Southern District of New York), « BNP Paribas Agrees to Plead Guilty to Conspiring to Process Transactions Through the U.S. Financial System for Sudanese, Iranian, and Cuban Entities Subject to U.S. Economic Sanctions », Communiqué de presse, 30 juin 2014. https://www.justice.gov/archive/usao/nys/pressreleases/June14/BNP%20Paribas%20Plea.php.
- United States, Department of the Treasury (Office of Foreign Assets Control), « OFAC Settles with Swedbank AS (Latvia) for Apparent Violations of the Ukraine-Related Sanctions Regulations », Rapport d'exécution, 20 juin 2023. https://ofac.treasury.gov/recent-actions/20230620_33.
- Université de Cologne (Universität zu Köln), *US-Zugriffsbefugnisse auf Daten in der Cloud: Gutachten Uni Köln vom März 2025* (Cologne : Université de Cologne, 2025). https://datenrecht.ch/en/us-zugriffsbefugnisse-auf-daten-in-der-cloud-gutachten-uni-koeln-vom-maerz-2025/.
- Visa Inc, *2025 Annual Report* (San Jose, CA : Visa Inc., 2025). https://s29.q4cdn.com/385744025/files/doc_downloads/2025/Visa-Fiscal-2025-Annual-Report.pdf
- The White House, *Executive Order on Imposing Sanctions on the International Criminal Court* (Washington, D.C. : Bureau de la présidence des États-Unis, 6 février 2025). https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.
- *National Security Strategy of the United States of America* (Washington, D.C. : Bureau de la présidence des États-Unis, 5 décembre 2025).

https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

- Worldline, Indicative Card Scheme Fee Rates as of January 2026: France, (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-france.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Belgium (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-belgium.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Spain (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-spain.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Portugal (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-portugal.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Germany (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-germany.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Italy (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-italy.pdf.
    - Indicative Card Scheme Fee Rates as of January 2026: Ireland (Bruxelles: Worldline, 2026). https://worldline.com/content/dam/worldline/global/documents/brochures/scheme-fees-ireland.pdf.
- « AWS, le service cloud d'Amazon, annonce avoir résolu la panne qui a touché des applications dans le monde entier », *Le Monde*, 21 octobre 2025.
- « China to Enhance Digital Yuan Management with Deposit Features Starting 2026 ». english.www.gov.cn, *Xinhua*, 29 décembre 2025. https://english.www.gov.cn/news/202512/29/content_WS69526d4ec6d00ca5f9a08511.html.
- « China's Digital RMB Transactions Top 14.2 Trillion Yuan ». english.www.gov.cn, 29 octobre 2025. https://english.www.gov.cn/archive/statistics/202510/29/content_WS6901a9c9c6d00ca5f9a0726a.html.

L'expertise stratégique en toute indépendance

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.