Haut Comité Juridique
de la Place financière de Paris

RAPPORT SUR LA RÉVISION DE LA DIRECTIVE SUR LES SERVICES DE PAIEMENT 2 (DSP2)

du Haut Comité Juridique
de la Place Financière de Paris

Septembre 2023

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

TABLE DES MATIÈRES

INTRODUCTION

Dans une période de croissance rapide et continue des technologies de paiements dématérialisés, telles que les technologies de paiement sans contact, les cartes de paiement « *tokenisées* » (les solutions *X-pay*, offertes notamment par Apple, Samsung, Google, etc.), les *stablecoins* et bientôt, la monnaie numérique de banque centrale,[1] la nécessité de revoir le cadre juridique actuel des services de paiement posé par la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (« **DSP2** »)[2] s'impose, malgré son entrée en vigueur voici à peine quatre ans.

En 2007, la première directive sur les services de paiement (« **DSP1** ») avait eu pour objectif de créer un espace unique de paiement au sein de l'Union européenne. Dix-sept ans plus tard, la mise en œuvre de cet objectif reste encore d'actualité. En effet, dans le cadre de son paquet digital, la Commission européenne a dévoilé le 24 septembre 2020 ses stratégies en matière de finance numérique[3] et de paiements de détail[4], prévoyant une étude complète de l'application de l'impact de la DSP2 à la lumière des évolutions du marchés et de la technologie. Cette initiative vise à résoudre des aspects différents, et notamment faire face aux nouveaux acteurs du marché (tels que les fintechs et les « *Big Techs* ») qui proposent des services de paiement en complément de leur activité ou d'autres entreprises qui adoptent des nouvelles technologies pour mettre en place des solutions de paiement telles que les portefeuilles numériques ou les paiements sans contact. Parallèlement, les habitudes des consommateurs ont également évolué, avec un recours accru au paiement en ligne et aux moyens de paiement alternatifs à la traditionnelle carte bancaire en particulier, notamment grâce au smartphone et la technologie NFC (*near field communication*). La Commission tient à s'assurer que le champ d'application, les exclusions et les définitions restent adéquats pour garantir la réglementation de ces acteurs, une concurrence équitable

[1] *Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/UE et 2009/110/CE et abrogeant la directive 2007/64/CE, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013PC0547.*

[2] *Il en va de même de la directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (« **DME2** »), https://eur-lex.europa.eu/eli/dir/2009/110/oj/fra.*

[3] *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions sur une stratégie en matière de finance numérique pour l'UE, 24 septembre 2020, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0591&from=FR.*

[4] *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions en matière de paiements de détails, 24 septembre 2020, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52020DC0592.*

et assurer une sécurité des utilisateurs de services de paiement[5], objectifs d'ores et déjà identifiés dans la proposition de la DSP2 en 2013.[6] La Commission entend également intensifier et rendre plus efficace la lutte contre la fraude aux paiements, en réexaminant les conditions d'authentification de l'utilisateur de services de paiement qui adresse un ordre de paiement à son prestataire de services de paiement (« **PSP** »).[7] Enfin, le réexamen de la DSP2 vise également à faire évoluer l'accès aux données relatives aux comptes de paiement et rendre les paiements internationaux rentables et transparents.[8]

En octobre 2021, l'Autorité bancaire européenne (« **ABE** ») a été invitée à donner son avis sur la révision de la DSP2, lequel a été rendu public le 23 juin 2022. Cet avis, encourageant la Commission à réviser la DSP2, présente plus de deux-cents propositions visant à contribuer au développement du marché unique des paiements de détail dans l'Union européenne (« **UE** ») et à garantir une application harmonisée et cohérente des exigences légales dans l'ensemble de l'UE. Plus particulièrement, les propositions de l'ABE cherchent à renforcer la concurrence, à faciliter l'innovation, à protéger les fonds et les données des consommateurs, à encourager le développement de services conviviaux et à prévenir l'exclusion des plus démunis de l'accès aux services de paiement, ainsi qu'à garantir une application harmonisée et cohérente des exigences légales dans toute l'UE.[9] En parallèle, la Direction générale de la stabilité financière, des services financiers et de l'union des marchés de capitaux (« **DG FISMA** ») de la Commission européenne[10] s'est également penchée sur les conditions de mise en œuvre de la DSP2 et des pistes d'amélioration de ce texte. Elle a publié un rapport début 2023[11], soulignant le développement des technologies et une demande croissante pour des solutions de paiement plus rapides, plus fiables et moins couteuses. En effet, la DSP2 a inclus deux nouveaux services dans la liste des services de paiement (services d'information sur les

---

[5] *Commission européenne, appel à contributions, 10 mai 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Services-de-paiement-reexamen-des-regles-de-lUE_fr.*

[6] *Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/UE et 2009/110/CE et abrogeant la directive 2007/64/CE, p. 2, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013PC0547.*

[7] *Ibid.*

[8] *Ibid.*

[9] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 June 2022, https://www.eba.europa.eu/eba-replies-european-commission%E2%80%99s-call-advice-%C2%A0-review-payment-services-directive.*

[10] *Financial Stability, Financial Services and Capital Markets Union Directorate - General (Direction générale de la stabilité financière, des services financiers et de l'union des marchés de capitaux).*

[11] *European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Bosch Chen, I., Fina, D., Hausemer, P., et al., A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2), Publications Office of the European Union, 2023, https://op.europa.eu/en/publication-detail/-/publication/f6f80336-a3aa-11ed-b508-01aa75ed71a1/language-en.*

comptes et d'initiation d'opérations de paiement), mais de nombreux autres prestataires de services dits techniques participent de manière plus étroite qu'auparavant à la chaine de valeur des services de paiement. Cela, alors qu'ils restent en dehors du champ d'application de la DSP2 à la faveur d'une définition de la notion de prestation de services techniques dont la frontière avec les services de paiement est particulièrement poreuse (comme cela est observé avec les « *géants de la Tech* » offrant de régler ses achats directement avec un smartphone, tels que Apple, Samsung ou Google, qui offrent des solutions de paiement de type « *X-pay* »).

La prise en compte de nouvelles technologies (*blockchain*, *cloud*, numérisation / « *tokenisation* », actifs et monnaies numériques, etc.) et des services et activités associés, par la législation européenne (tels que l'adoption récente des règlements DORA[12] et MiCA[13] par exemple) mettent à l'épreuve des textes plus anciens comme la DSP2 et la DME2.

Au surplus, la trajectoire des textes législatifs européens modernes (tendant vers plus de règlements et moins de directives)[14] préconisée par le Rapport de Larosière en réponse à la grande crise financière de 2008,[15] ainsi que les rapports précités plaident en faveur d'une harmonisation renforcée du cadre juridique des services de paiement dans les différents États membres. Ainsi, l'élévation de la DSP2 en un règlement[16] devrait constituer une solution cohérente avec cette évolution. De manière équivalente, il est également nécessaire d'harmoniser les approches des différentes autorités de supervision intervenant dans les services de paiement, afin de s'assurer une application identique de

[12] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) 600/2014, (UE) 909/2014 et (UE) 2016/1011, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R2554 (« **Règlement DORA** »).*

[13] *Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) 1093/2010 et (UE) 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023R1114 (« **Règlement MiCA** »).*

[14] *Initiée par le règlement CRA (Règlement (CE) 1060/2009 du Parlement européen et du Conseil du 16 septembre 2009 sur les agences de notation de crédit), puis MAR (Règlement (UE) 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché), Benchmark (Règlement (UE) 2016/1011 du Parlement européen et du Conseil du 8 juin 2016 concernant les indices utilisés comme indices de référence dans le cadre d'instruments et de contrats financiers ou pour mesurer la performance de fonds d'investissement), Prospectus (Règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus); plus récemment, MiCA, Régime Pilote (règlement (UE) 2022/858 du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (DLT)).*

[15] *« Report of the High Level Group on Financial Supervision in the EU », présidé par J. de Larosière, 25 février 2009, spéc. §109 et Recommandation 10.*

[16] *Ou, à défaut, d'une partie de ses dispositions, comme en matière bancaire avec le paquet CRD/CRR (Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 et Règlement (UE) 575/2013 du Parlement européen et du Conseil du 26 juin 2013).*

ses dispositions aux quatre coins de l'Union. Il a été observé que, bien trop souvent, les approches entre les autorités compétentes des États membres divergent et mènent à des pratiques de supervision différentes préjudiciables à la sécurité juridique et conditions de concurrence équitable entre les États membres. Les analyses multi-juridictionnelles qui ont été menées dans le cadre du présent rapport en donnent quelques illustrations qui complètent celles de l'ABE et de la Commission européenne/DG FISMA.[17]

Dans ce contexte, le Haut Comité Juridique de la Place de Paris (HCJP) a constitué en mai 2022 un groupe de travail pour réfléchir, en vue d'une imminente proposition législative de la Commission, aux changements souhaités pour la DSP2 et formuler des propositions concrètes. La composition de ce groupe de travail a recherché une représentation aussi large que possible des acteurs du marché des services de paiement en France. Ainsi, des représentants d'établissements de crédit, de paiement, de monnaie électronique, d'organisations professionnelles et de l'Autorité de contrôle prudentiel et de résolution (« **ACPR** »), ainsi que des universitaires, des avocats spécialisés et des autorités financières ont été invités à contribuer aux travaux du groupe et en faire bénéficier de leur expertise.[18]

Face à la variété des thèmes et au risque de se disperser, le groupe de travail a décidé de se concentrer sur un nombre limité de sujets, à savoir :

- l'élévation de la DSP2 en un règlement ;

- la fusion de la DSP2 avec la directive sur la monnaie électronique (DME2) ;

- le champ d'application territorial de la DSP2 ;

- la question de la soumission de l'activité d'encaissement de fonds pour le compte de tiers à la DSP2 ;

- certains régimes d'exclusion du champ d'application matériel de la DSP2 (notamment, les prestataires de services techniques, l'exclusion intragroupe, etc.) ;

- la notion du compte de paiement ;

- le régime de responsabilité des PSP ; et

- l'accès accordé aux prestataires de services d'information sur les comptes (« **PSIC** ») et les prestataires de service d'initiation de paiement (« **PSIP** ») aux données détenues par les PSP gestionnaires de comptes de paiement.

---

[17] *Voir notes de bas de page n° 9 et 10 ci-dessus.*

[18] *La composition du groupe de travail figure en Annexe II.*

Compte tenu de la diversité des membres composant le groupe de travail, certains sujets ont donné lieu à des débats qui n'ont parfois pas abouti à un consensus permettant de formuler des recommandations. Le présent rapport fait état de ces antagonismes. Le rapport parvient toutefois à formuler vingt et une recommandations.

Afin de mettre en lumière les différences de transposition de la DSP2 ou de pratiques de supervision dans les États membres des analyses multi-juridictionnelles synthétiques ont été menées sur certains sujets.[19] Ces analyses ont permis de comparer les différentes approches réglementaires et législatives et de tenir compte des approches adoptées par d'autres États membres pour enrichir les réflexions du groupe de travail.

Entre temps, le 28 juin 2023, la Commission a dévoilé son projet de réforme de la DSP2 sous la forme d'un « *paquet* » lequel comprend une proposition de directive relative aux services de paiement et aux services de monnaie électronique (la « **Proposition de DSP3** »)[20] et une proposition de règlement relatif aux services de paiement (la « **Proposition de Règlement RSP** »)[21], à l'instar notamment du paquet CRD/CRR (le « **Paquet DSP3/RSP** »). Tandis que le règlement renferme les règles relatives à la fourniture de services de paiement, la directive concentre pour sa part celles qui gouvernent l'accès à la profession et la surveillance des établissements. Au passage, le Paquet DSP3/RSP fusionne les anciens textes (DSP2 et DME2) régissant les services de paiement et la monnaie électronique. On notera que, le même jour la Commission a également dévoilé sa proposition sur l'euro numérique.[22] À cet égard, il est intéressant à noter que ces différents textes sont liés puisque, d'une part, la définition de « *fonds* » contenue dans la DSP2 est modifiée en vue d'y inclure une référence à la monnaie de banque centrale émise à des fins de paiement de détail,[23] ce qui inclut l'euro numérique,[24] étant également précisé que, étant assimilés à la monnaie électronique par le Règlement MICA,[25] les jetons de monnaie électronique (ou *electronic money tokens*) entrent

[19] *Les analyses multi juridictionnelles figurent en Annexe III.*

[20] *Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement et les services de monnaie électronique dans le marché intérieur modifiant la directive 98/26/CE et abrogeant les directives 2015/2366/UE et 2009/110/CE, la directive 98/26/CE et abrogeant les directives 2015/2366/UE et 2009/110/CE, COM(2023) 366 final.*

[21] *Proposition de Règlement du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) n° 1093/2010, COM(2023) 367 final.*

[22] *Proposition de Règlement du Parlement européen et du Conseil sur l'établissement de l'euro numérique, COM(2023) 369 final (https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-regulation_en.pdf), complétée par un proposition de Règlement du Parlement européen et du Conseil sur la fourniture de services d'euros numériques par les prestataires de services de paiement immatriculés dans les États membres dont la devise n'est pas l'euro, COM(2023) 368 final (https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-services-regulation_en.pdf).*

[23] *Voir article 2(23) de la Proposition de DSP3 et 3(30) de la Proposition de Règlement RSP.*

[24] *Considérant n° 15 de la Proposition de DSP3.*

[25] *Article 48(2) du Règlement MiCA.*

nécessairement dans la définition de fonds ;[26] et, d'autre part, la distribution de l'euro numérique sera effectuée par les PSP auprès desquels les comptes de paiement d'euro numériques (*digital euro payment accounts*) devront être ouverts.[27]

La synthèse des recommandations du HCJP, qui figurent après l'introduction du présent rapport, indique si le Paquet DSP3/RSP rejoint ou non ces recommandations.

Enfin, afin de faciliter la lecture du présent rapport, un glossaire des termes définis, abréviations et acronymes qui y sont utilisés figure en Annexe I du présent rapport.

[26] *Considérant n° 16 de la Proposition de DSP3.*

[27] *Article 2(5) de la proposition de règlement sur la création de l'euro numérique.*

SYNTHÈSE DES RECOMMANDATIONS

Élévation de la directive en règlement

Recommandation n° 1 : le HCJP recommande le remplacement de la directive par un règlement.

Paquet DSP2/RSP : la proposition de la Commission est partiellement en ligne avec cette recommandation puisqu'une partie de la DSP2 est contenue dans la Proposition de Règlement RSP, sur le modèle du paquet CRD/CRR.

Fusion DSP2 et DME2

Recommandation n° 2 : le HCJP recommande que la notion de monnaie électronique soit reconsidérée, non seulement parce que la définition actuelle demeure absconse, mais encore pour qu'elle puisse servir aux innovations en cours, notamment concernant les crypto-actifs, mais plus largement les nouvelles « *chaînes de valeur du paiement* ».

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Recommandation n° 3 : le HCJP recommande : (i) d'abord que la fusion permette de réunir, en un seul corps de règles figurant dans un texte unique, l'ensemble du régime commun à la monnaie électronique et aux services de paiement (droit des opérations de paiement et des contrats de services de paiement) ; et (ii) ensuite qu'une seule et même catégorie de prestataires de services de paiement soit créée (les « *établissements de paiement et de monnaie électronique* » ou « **EPME** ») soumise à des dispositions prudentielles, de protection de la clientèle, etc., communes, sous réserve de quelques exceptions (capital minimum, remboursement de la monnaie électronique, etc.).

Paquet DSP3/RSP : la proposition de la Commission est en ligne avec cette recommandation car elle fusionne la DSP2 et la DME2, en créant un statut unique d'établissement de paiement et de monnaie électronique, tout en préservant certaines spécificités relatives aux conditions d'agrément, en particulier en termes de capital initial et de fonds propres, ainsi que certains concepts fondamentaux régissant les activités de monnaie électronique, tels que l'émission de monnaie électronique, la distribution de monnaie électronique et sa remboursabilité.[28]

[28] *Proposition de Règlement RSP, considérant n° 5.*

Recommandation n° 4 : le HCJP recommande qu'une clarification soit faite entre le modèle ouvert de paiement universel ou de système de paiement exclusivement entre affiliés, sous peine sinon de maintenir le flou entre services de paiement et monnaie électronique ou de se heurter à des difficultés pratiques (exemple : remboursement) insurmontables.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Recommandation n° 5 : le HCJP recommande que le futur texte contienne une définition du support de la monnaie électronique, pour deux raisons au moins : (i) la première concerne le fait que la monnaie électronique est souvent confondue avec le support (carte de paiement, compte de paiement) qui la stocke, nuisant par-là à son identification et à sa qualification ; et (ii) la seconde est tournée vers l'avenir et suggère une définition du support de monnaie électronique propre à embrasser les futurs jetons de monnaie électronique (*e-money tokens*) du Règlement MiCA.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Champ application territorial de la DSP

Recommandation n° 6 : le HCJP recommande de retenir la sollicitation du client dans l'Union européenne comme critère de rattachement territorial pour la révision de la DSP2.

Paquet DSP2/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Champ application matériel de la DSP - Encaissement de fonds pour compte de tiers

Recommandation n° 7 : le HCJP recommande de : (i) clarifier le fait que l'activité d'encaissement de fonds pour le compte de tiers implique la fourniture de services de paiement identifiés, que la qualification soit claire pour les acteurs ; et (ii) donner compétence à l'ABE d'élaborer des normes techniques de réglementation afin de définir dans quelles conditions les services identifiés s'appliquent.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Recommandation n° 8 : le HCJP recommande d'indiquer que les États membres peuvent prévoir des exceptions concernant des professions ou des activités identifiées.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Exclusions du champ de la DSP - Prestataires techniques (« PST »)

Recommandation n° 9 : le HCJP recommande de clarifier les notions d'« *initiation d'opération de paiement* » et d'« *instrument de paiement* », en vue de préciser les conditions dans lesquelles : (i) s'agissant des paiements par carte ; et (ii) plus généralement les solutions technologiques apportées par les prestataires de services techniques peuvent se distinguer des services de paiement fournis par les PSP.

Paquet DSP3/RSP : la proposition de la Commission est partiellement en ligne avec cette recommandation : (i) en incluant une nouvelle définition d' « *initiation d'opération de paiement* » ; [29] (ii) en précisant que les « *pass-through wallets* », impliquant la tokenisation d'un instrument de paiement tel une carte de paiement doivent être considérés comme des services techniques et exclus de la définition d'instrument de paiement et considérés comme une application de paiement au sens du Règlement Interchange. Toutefois, certaines autres catégories de portefeuilles numériques comme les portefeuilles prépayés ou les utilisateurs peuvent stocker de l'argent en vue de futures transactions en ligne devraient être considérées comme un instrument de paiement au sens de la RSP ;[30] et (iii) en prévoyant qu'il est nécessaire que, dans le futur réexamen de la présente directive, la Commission prenne particulièrement en considération les évolutions technologiques et évalue si le champ d'application de la directive doit être élargi pour couvrir de nouveaux services et de nouveaux risques.[31]

Recommandation n° 10 : le HCJP recommande de clarifier l'articulation de la réglementation applicable en matière de sous-traitance à des PST, particulièrement entre DORA et la DSP.

Paquet DSP3/RSP : la proposition de la Commission est en ligne avec cette recommandation.[32]

---

[29] *« Initiation of a payment transaction means the steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process » (article 3(6) de la Proposition de Règlement RSP).*

[30] *Considérant n° 24 de la Proposition de Règlement RSP.*

[31] *Considérant n° 68 in fine de la Proposition de DSP3.*

[32] *Article 81 de la Proposition de Règlement RSP.*

Recommandation n° 11 : le HCJP recommande de clarifier la définition de système ou schéma de paiement, afin de lier l'exclusion correspondante à la soumission du système ou schéma de paiement au cadre de supervision des systèmes et schémas de paiement de l'Union (PISA).

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation. Toutefois, elle exclut, dans un considérant, les systèmes, schémas ou dispositifs de paiement du champ du texte, en précisant vouloir éviter toute duplication notamment avec le cadre PISA.[33]

Exclusions du champ de la DSP - Exclusion Intragroupe

Recommandation n° 12 : le HCJP recommande de modifier la DSP2 afin de préciser dans le texte de l'Exclusion Intragroupe que cette exclusion s'applique à la centralisation des paiements reçus de tiers ainsi qu'au bénéfice des tiers, pour le compte d'entités appartenant au même groupe.

Paquet DSP3/RSP : la proposition de la Commission est partiellement en ligne avec cette recommandation, car elle ne vise pas l'encaissement de fonds reçus d'un tiers et dû à une société du groupe. .[34]

Compte de paiement

Recommandation n° 13 : le HCJP recommande de ne retenir qu'une seule et unique définition de compte de paiement qui serait contenue dans la DSP, les autres textes pertinents (en particulier, la Directive PAD, le Règlement SEPA et le Règlement Interchange) devant y faire référence.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation.

Recommandation n° 14 : le HCJP recommande :

- de modifier la DSP2 (soit dans les considérants, soit dans la définition de compte de paiement) afin de préciser qu'un compte à partir duquel des opérations de paiement ne peuvent être effectuées directement, mais nécessitent le recours à un compte intermédiaire n'est pas un compte de paiement ; et

- au législateur européen et à l'ABE d'évaluer de manière plus approfondie si la notion de tiers est pertinente au regard de la définition de compte de paiement, et de prendre expressément parti aux fins de sécurité juridique.

[33] *Considérant n° 68 de la Proposition de DSP3.*
[34] *Article 2.2(m) de la Proposition de Règlement RSP.*

Paquet DSP3/RSP : la proposition de la Commission va au-delà de la recommandation en incluant une référence expresse aux paiements reçus de tiers et au profit de tiers.[35]

Responsabilité des PSP

Recommandation n° 15 :

- le HCJP recommande de compléter l'article 97 de DSP2 par un 6e paragraphe : (i) permettant aux PSP gestionnaires de comptes (PSPGC) et aux prestataires d'initiation de services de paiement (PSIP) de pouvoir convenir que la procédure d'authentification forte incombera, non à le PSPGC mais au prestataire de services d'initiation de paiement ; (ii) précisant que, dans ce cadre, le PSIP est responsable vis-à-vis de l'utilisateur dans les termes de l'article 73(1) de la DSP2 ; et (iii) que le PSIP doit préalablement en informer l'utilisateur conformément à l'article 52 de la DSP2 ;

- en conséquence il s'agira également de compléter l'article 73(2) de la DSP2 par un 3e paragraphe prévoyant en substance que c'est le PSIP qui supporte l'obligation de rembourser au payeur le montant de l'opération de paiement non autorisée.

Paquet DSP3/RSP : la proposition de la Commission ne contient pas de disposition reflétant cette recommandation. En revanche, la proposition ajoute de nouvelles dispositions sur l'authentification forte dans le cadre de l'initiation de paiement, prévoyant que l'authentification forte s'applique également dans le cas où les paiements sont initiés par un PSIP et que le PSPGC doit autoriser les PSIP de s'appuyer sur ses procédures d'authentification forte.[36]

Recommandation n° 16 : le HCJP recommande de modifier l'article 73 de la DSP2 afin d'allonger le délai de remboursement en cas d'opération de paiement non autorisée à cinq (si l'utilisateur du service de paiement est un consommateur) ou quinze (dans le cas contraire) jours ouvrables au lieu de un jour ouvrable comme c'est le cas actuellement.

Paquet DSP3/RSP : la Proposition du RSP ne prévoit pas de modifier l'article en ce sens.[37]

---

[35] *Article 2(13) de la Proposition de DSP3 et 3(15) de la Proposition de Règlement RSP : « payment account means an account held by a payment service provider in the name of one or more payment service users which is used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties ». Voir également considérant n° 20 de la Proposition de Règlement RSP.*

[36] *Article 86 de la Proposition de Règlement RSP.*

[37] *Voir article 56(1) de la Proposition de Règlement RSP, inchangé sur ce point.*

Recommandation n° 17 : le HCJP recommande la modification de l'article 72 de la DSP2 afin de prévoir que, lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée ou affirme que l'opération de paiement n'a pas été exécutée correctement, le PSP peut apporter la preuve « *qu'il n'a pas détecté une déficience technique ou autre en relation avec le service fourni qui aurait pu affecter l'opération* », et non pas la preuve que l'opération en question « *n'a pas été affectée par une déficience technique ou autre du service fourni par le PSP* ».

Paquet DSP3/RSP : la Proposition du RSP ne prévoit pas de modifier l'article en ce sens.[38]

Recommandation n° 18 : le HCJP recommande de compléter l'article 26 de la DSP2 par un nouveau paragraphe (3) visant à permettre, sans que cela ne constitue une obligation, l'échange d'information entre PSP dans la seule finalité de lutte contre la fraude et sans que le secret professionnel ne constitue un obstacle ou ne soit opposable.

Paquet DSP3/RSP : la proposition de la Commission est partiellement en ligne avec cette recommandation, en ce qu'elle prévoit : (i) la possibilité d'échange d'informations entre PSP pour les besoins de la lutte contre la fraude[39] ; et (ii) une obligation de coopération avec les PSP mise à la charge des opérateurs de télécommunication.[40] En contrepartie, les PSP sont soumis à une obligation de surveillance des opérations de paiement (*transaction monitoring*) selon l'article 83(1) de la Proposition de Règlement RSP.

Accès aux données

Recommandation n° 19 : le HCJP recommande la suppression de l'article 94(2) de la DSP2 (qui prévoit que les PSP n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement qu'avec le consentement explicite de l'utilisateur de services de paiement), comme ne se justifiant pas eu égard aux dispositions du RGPD.

Paquet DSP3/RSP : la proposition de la Commission est en ligne avec cette recommandation en ce qu'elle a réécrit l'article en renvoyant aux dispositions du RGPD.[41]

[38] *Voir article 55(1) de la Proposition de Règlement RSP, inchangé sur ce point.*

[39] *Article 83(3) de la Proposition de Règlement RSP.*

[40] *Article 58(5) de la Proposition de Règlement RSP.*

[41] *Article 80 de la Proposition de Règlement RSP.*

Recommandation n° 20 : le HCJP recommande de remplacer le concept de « *donnée de paiement sensible* » définie à l'article 4(32) de la DSP2 par celui de « *donnée de paiement protégée* » et ayant la définition suivante : « *des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude et qui nécessitent un niveau de protection adapté* ».

Paquet DSP3/RSP : la proposition de la Commission ne prévoit pas de modifier le terme défini, mais modifie toutefois la substance de la définition.[42]

Recommandation n° 21 : le HCJP recommande :

- concernant l'authentification forte de l'utilisateur (« **SCA** ») et les *digital identity wallets* (« **DIW** ») : considérant que le PSPGC ne peut pas être responsable d'une solution technique d'identification et de SCA dont il n'a pas le contrôle et qui lui est imposée par la réglementation, la révision de DSP2 pourrait prévoir qu'en cas de recours à une solution tierce telle que le DIW, le consentement de l'utilisateur à l'exécution des opérations de paiement ne pourra pas être contesté par ce dernier auprès du PSPGC. Au mieux, en cas de contestation, le PSPGC ne pourra être tenu qu'à une obligation d'assistance dans la récupération des fonds auprès du PSP du bénéficiaire ;

- l'exigence d'authentification forte dynamique requise par la DSP2 lors de l'initiation de l'opération de paiement devra être compatible avec la solution d'authentification proposée par le DIW et s'imposant aux PSPGC ; et

- en ce qui concerne l'articulation entre les révisions respectives de la DSP2 et du Règlement eIDAS, compte tenu des impacts du projet de révision du Règlement eIDAS sur les paiements, il semble indispensable que la cohérence entre la révision de ce texte et celle de la DSP2 soit assurée. En conséquence, il devrait être recommandé que la révision de DSP2, qui devra prendre en compte la révision du Règlement eIDAS, n'intervienne que lorsque la révision de ce dernier texte sera complétement stabilisée.

Paquet DSP3/RSP : la Proposition de Règlement RSP ne contient pas de modification en ce sens, mais prévoit que le PSP conserve la responsabilité de la mise en œuvre de la SCA lorsque celle-ci est externalisée auprès d'un prestataire de services techniques.[43]

---

[42] *Article 3(38) de la Proposition de Règlement RSP : « sensitive payment data' means data which can be used to carry out fraud, including personalised security credentials ».*

[43] *Article 87 de la Proposition de Règlement RSP.*

I. Élévation de la directive en règlement

1.1 - Enjeux liés à la question

La révision de la DSP2 implique de s'interroger, de façon liminaire, sur le choix de l'acte juridique de droit de l'Union européenne. Trois options sont envisageables :

(a) la première est que la DSP2 soit remplacée dans son intégralité par une nouvelle directive ;

(b) la deuxième est que la DSP2 soit remplacée dans son intégralité par un règlement, à l'instar de ce qui a été fait pour le règlement MAR qui a abrogé et remplacé la directive « *abus de marché* » ou encore le règlement « *Prospectus* » qui a abrogé et remplacé la directive du même nom[45] ; et

(c) la troisième option reviendrait à adopter deux actes complémentaires, d'un côté, une directive, de l'autre côté, un règlement, à l'instar de ce qui a été fait en matière bancaire avec le paquet CRD/CRR.[46]

Le choix est tributaire du degré recherché d'uniformité du droit applicable aux services de paiements prestés dans les États membres. Il s'agit dès lors d'apprécier la mesure dans laquelle des exigences nationales divergentes peuvent subsister ou dans laquelle est recherchée l'application des mêmes règles dans l'ensemble des États membres.

Sur la base des analyses juridictionnelles figurant dans le présent rapport, ainsi que dans les documents de l'ABE et de la DG FISMA précités, il est loisible d'identifier quelques dispositions de la DSP2 qui, en l'état actuel du droit, donnent lieu à une application et une interprétation différente entre les États membres. On peut citer comme exemples :

(i) la notion de compte de paiement et sa confrontation à d'autres types de comptes, tels que les comptes techniques ;

---

[44] *Règlement (UE) 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014R0596.*

[45] *Règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32017R1129#:~:text=R%C3%A8glement%20(UE)%202017%2F1129,pr%C3%A9sentant%20de%20l'int%C3%A9r%C3%AAt%20pour.*

[46] *Composé de la directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32013L0036) et du Règlement (UE) 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32013R0575).*

(ii) la définition des fonds propres des établissements de paiement, notamment en ce qui concerne le calcul des volumes de paiement (notamment, pour les activités traversantes, la question de savoir si seul les flux de paiement entrant (*payment in*) ou sortant (*payment out*) ou si le cumul des deux flux est pris en compte dans le calcul – *payments one leg* ou *two legs*) donne lieu à des interprétations divergentes expliquant par exemple des pratiques différentes des régulateurs en Allemagne et France ;

(iii) certains régimes d'exclusion, comme ceux des agents commerciaux ou des opérations de paiement intragroupe ;

(iv) pour les réserves (la technique dite de « *pied de compte* »), on relève une différence d'interprétation sur l'exigence d'encadrer ou de ne pas encadrer la mise à disposition des fonds collectés par un service de paiement. Alors que certains régulateurs autorisent cet encadrement pour réserver des fonds à l'exercice d'opérations futures sur les comptes de clients agissant dans un cadre professionnel (*chargeback/ refund*, notamment), d'autres l'interdisent.

En tout état de cause, la sécurité juridique, principe général du droit de l'Union européenne, devra être garantie.

1.2 - Quel est le régime juridique actuel ?

La directive DSP2 constitue une directive au sens de l'article 288, alinéa 3, TFUE. Celui-ci dispose que « *[l]a directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens* ».

Lors des travaux préparatoires de la DSP2, le choix de l'acte juridique n'a pas été discuté. En revanche, la Commission a proposé, sans le justifier, que la directive soit d'« *harmonisation totale* ».

L'article 107 de la DSP2 est ainsi intitulé «harmonisation totale». Il dispose :

« *1. Sans préjudice de l'article 2, de l'article 8, paragraphe 3, de l'article 32, de l'article 38, paragraphe 2, de l'article 42, paragraphe 2, de l'article 55, paragraphe 6, de l'article 57, paragraphe 3, de l'article 58, paragraphe 3, de l'article 61, paragraphes 2 et 3, de l'article 62, paragraphe 5, de l'article 63, paragraphes 2 et 3, de l'article 74, paragraphe 1, deuxième alinéa, et de l'article 86,* ***dans la mesure où la présente directive contient des dispositions harmonisées, les États membres ne peuvent maintenir en vigueur ni introduire des dispositions différentes de celles contenues dans la présente directive*** ».[47]

[47] *Gras ajouté.*

Toutefois, le législateur a fait le choix de ne pas retenir l'harmonisation totale pour certaines dispositions (voir Annexe IV).

La notion d'harmonisation totale a été explicitée par la jurisprudence. La CJUE a précisé qu'une directive peut, sur les points qu'elle règlemente, poursuivre une « *harmonisation totale* » des dispositions législatives, réglementaires et administratives des États membres, sans pour autant avoir vocation à harmoniser de manière « *exhaustive* » le domaine couvert par la directive, en dehors desdits points.[48] L'harmonisation totale porte ainsi sur « *la marge de manœuvre laissée aux États membres et donc sur le niveau de discrétion dont ils disposent pour transposer dans leur droit interne les points visés par la directive (…), tandis que les termes « harmonisation exhaustive » concernent le champ d'application rationae materiae de cette directive* ».[49]

Lorsque l'harmonisation est totale, les États membres ne disposent pas d'une marge de manœuvre dans la transposition des dispositions de la directive : ils ne peuvent pas introduire de dispositions différentes de celles contenues à ces articles. Ainsi, selon l'article 107 de la directive DSP2, « *dans la mesure où la présente directive contient des dispositions harmonisées, les États membres ne peuvent maintenir en vigueur ni introduire des dispositions différentes de celles contenues dans la présente directive* ».

L'harmonisation n'est cependant pas exhaustive dans la mesure où elle est limitée aux seules dispositions de la directive et, qu'en dehors de celles-ci, « *les États membres restent libres de légiférer dès lors qu'ils ne portent pas atteinte à l'effet utile de cette même directive* ».[50] L'harmonisation totale signifie que les États membres doivent transposer les règles sans pouvoir ajouter ou retirer des conditions ou des effets.[51]

En conséquence, sur le principe, la DSP2 n'a pas entendu dessaisir les États membres de tout pouvoir normatif dans le domaine des paiements. En revanche, ces derniers peuvent toujours légiférer ou réglementer les questions relatives aux paiements qui ne font pas l'objet d'une disposition de la directive. En revanche, ils ne disposent pas, en principe, d'une marge de manœuvre dans la transposition de ses dispositions.

---

[48] *CJUE, 4 juin 2009, Moteurs Leroy Somer, C-285/08, EU:C:2009:351, point 25.*

[49] *CJUE, 8 juillet 2021, DM et LR contre Caisse régionale de Crédit agricole mutuel (CRCAM) Alpes-Provence, C-337/20, ECLI:EU:C:2021:564, point 69.*

[50] *Ibid., point 70.*

[51] *J. Rochfeld, « Les ambiguïtés des directives d'harmonisation totale : la nouvelle répartition des compétences communautaire et interne », Dalloz actualité, 14 septembre 2009, § 4.*

L'autonomie normative des États membres est en théorie réduite par l'harmonisation totale. D'une part, lorsque l'État transpose la directive, il doit veiller à en respecter les dispositions, lesquelles peuvent néanmoins viser des notions imprécises ou présenter des ambiguïtés. D'autre part, en dehors de l'opération de transposition, les États membres doivent également édicter leurs règles dans le respect des dispositions de la directive. En conséquence, l'harmonisation totale s'avère d'une telle intensité normative qu'elle « *impose des règles qui se substituent entièrement aux règles nationales existantes en la matière* ».[52] Cela induit que les États membres n'ont plus la possibilité de prendre pour les questions régies par les dispositions de la directive des règles nationales.[53] Cependant, cette substitution est purement substantielle en ce que les États membres sont formellement tenus d'adopter des mesures de transposition qui reprennent les dispositions de la directive. Il demeure que les autorités nationales et les établissements appliquent des règles édictées par des dispositions de droit national.

Si elle se distingue de l'harmonisation exhaustive, l'harmonisation totale se rapproche de l'harmonisation complète. Aussi est-elle tributaire de l'intensité normative produite par les dispositions de la directive. En effet, par harmonisation complète, on entend la caractéristique des dispositions des directives dont le contenu s'avère suffisamment complet qu'il n'appelle aucune intervention complémentaire par l'État membre sur le plan substantiel. La disposition de la directive d'harmonisation complète ou totale épuise la compétence de l'État membre en ce qu'il ne peut ajouter aucune exigence supplémentaire.

En conséquence, la directive d'harmonisation totale se rapproche du règlement. L'article 288, alinéa 2, TFUE prévoit en effet que les règlements ont une portée générale, sont obligatoires dans tous leurs éléments et sont directement applicables dans tous les États membres. Les dispositions des règlements n'appellent en principe aucune mesure de réception dans l'ordre juridique national. Il existe toutefois une différence essentielle entre règlement et directive d'harmonisation totale. Dans tous les cas, les dispositions des directives doivent faire l'objet d'une transposition dans l'ordre juridique interne, conformément à l'article 288, alinéa 3, TFUE. Si la transposition prend généralement la forme d'une disposition législative ou réglementaire, elle n'est pas nécessaire lorsque le droit national est déjà compatible avec les dispositions de la directive. Toutefois, même lorsque l'harmonisation est totale, les États membres adoptent des mesures de transposition qui reprennent formellement en droit national, le contenu substantiel de la directive. L'État membre peut ainsi se cantonner à recopier les exigences prévues par les dispositions de la directive. Cependant, en pratique, peuvent subsister des divergences dans la transposition nationale soit parce que les dispositions de la directive peuvent s'avérer imprécises

[52] *A. Mattera, « Le marché unique européen », Jupiter, 1990, 2e édition, p. 180.*

[53] *CJCE, 25 avril 2002, Commission c/ République française, C-52/00, ECLI:EU:C:2002:252 ; CJCE, 25 avril 2002, Commission c/ Grèce, C-154/00, ECLI:EU:C:2002:254.*

et conduire à des interprétations qui diffèrent d'un État à l'autre, d'autant que les concepts employés sont généralement complexes et ne recouvrent pas toujours des objets juridiques qui existent dans les ordres juridiques nationaux. En conséquence, par essence, quand bien même serait-elle d'harmonisation totale, une directive peut présenter un risque de divergences normatives dans sa transposition et son application dans les États membres. À l'inverse, un règlement garantit une application uniforme dans tous les États membres.

1.3 - Options disponibles

1.3.1 - La base juridique

De façon liminaire, il convient de préciser que l'article 114 TFUE constitue la base juridique de la DSP2.

Sur le fondement de cette disposition, le législateur de l'Union peut adopter aussi bien des règlements que des directives. Il est encore en droit de remplacer une directive par un règlement. Des précédents existent, à l'instar du règlement relatif aux abus de marché qui a abrogé la directive 2003/6/CE du Parlement européen et du Conseil et trois autres directives de la Commission[54] ou encore le règlement « *Prospectus* » qui a abrogé et remplacé la directive du même nom.[55]

Le choix entre règlement et directive est politique qu'il revient à la Commission dans l'exercice de son pouvoir d'initiative et au Parlement européen et au Conseil dans l'exercice de leur fonction législative, d'effectuer. Dans l'esprit du traité, la différence entre règlement et directive s'explique par deux visions des rapports normatifs dans l'ordre juridique de l'Union européenne.

1.3.2 - Règlement et directive

Ainsi que cela a été anticipé, selon l'article 288 TFUE, règlement et directive ne présentent pas les mêmes caractéristiques.

Une fois qu'il est entré en vigueur, le règlement produit des effets juridiques complets sans nécessiter une quelconque mesure de réception. Il est donc directement et immédiatement applicable dans

[54] *Règlement (UE) 596/2014, précité.*

[55] *Règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé.*

l'ordre juridique des États membres tant dans les rapports verticaux c'est-à-dire entre l'État *lato sensu* – les autorités nationales – et les particuliers que dans les rapports horizontaux c'est-à-dire entre particuliers. Cela signifie que les dispositions d'un règlement sont invocables et applicables tant dans des rapports entre les autorités publiques et les établissements que dans des rapports entre particuliers (établissements entre eux ou avec des clients). Le règlement postule une uniformisation du droit dans les ordres juridiques nationaux : il s'applique en effet par lui-même dans tous les États membres. Ainsi, pour justifier que le règlement MAR « *abus de marché* » a remplacé la directive, le législateur a indiqué la nécessité de « *garantir l'uniformité des règles et la clarté des principaux concepts employés* ».[56]

En revanche, la directive nécessite des mesures nationales de transposition. L'article 288, alinéa 3, TFUE fait peser l'obligation sur l'État membre de mettre son ordre juridique en compatibilité avec les objectifs de la directive. Celle-ci prévoit un délai de transposition – de plusieurs mois à quelques années – au terme duquel des mesures nationales doivent avoir été adoptées. Au cours de ce délai, l'État doit s'abstenir de prendre des dispositions de nature à compromettre sérieusement la réalisation du résultat prescrit par la directive. À l'expiration du délai de transposition, le droit national doit être compatible avec les objectifs de la directive. Dans le cas contraire, les dispositions de la directive sont invocables par les particuliers, à la condition d'être claires, précises et inconditionnelles, mais uniquement dans des rapports verticaux ascendants ; autrement dit, un particulier peut invoquer lesdites dispositions de la directive à l'encontre des seules autorités nationales. En revanche, un particulier ne peut invoquer la directive directement à l'encontre d'un autre particulier. En tout état de cause, le droit national doit toujours être interprété de façon conforme à la directive. Celle-ci est donc invocable dans tous les rapports verticaux et horizontaux aux fins de l'interprétation conforme.

Dès lors, la distinction entre règlement et directive est déterminante à deux titres.

Sur le plan temporel, alors que l'entrée en vigueur du règlement est immédiate, la directive ne produit pleinement ses effets dans l'ordre juridique national, par le truchement du droit national, que lorsque le délai de transposition de la directive a expiré. Cela signifie qu'entre la date d'entrée en vigueur de la directive et la date d'expiration du délai de transposition, subsiste une période au cours de laquelle des divergences persistent entre droits nationaux.

Sur le plan normatif, le règlement produit ses effets par lui-même dans l'ordre juridique national ce qui conduit à une uniformisation des règles substantielles du domaine qu'il régit. Ses dispositions

[56] *Règlement (UE) 596/2014, précité, considérant n° 3.*

s'appliquent en effet dans tous les États membres. En revanche, quand bien même serait-elle d'harmonisation totale, la directive ne s'applique pas par elle-même ; si elle a été correctement transposée, ce sont les dispositions du droit national qui sont appliquées ce qui induit la coexistence formelle de vingt-sept droits nationaux dont la substance est, en théorie uniquement, convergente. Est ainsi maintenue une diversité des droits nationaux puisque, dans chaque État membre, s'appliquent les dispositions nationales de transposition, interprétées le cas échéant conformément à la directive ; celle-ci a vocation à permettre uniquement un rapprochement des dispositions législatives et réglementaires nationales. Certes, la directive présente un intérêt lorsque des dispositions nationales en cause relèvent de domaines de compétence nationale. Tel est le cas lorsqu'il s'agit de se saisir de notions de droit civil ou de droit commercial, typiquement nationales. Toutefois, l'argument de la compétence n'est aucunement dirimant. Si l'Union ne dispose pas d'une compétence générale pour harmoniser le droit civil ou le droit commercial des États membres, l'article 114 TFUE constitue la base juridique adaptée pour harmoniser celles des dispositions nationales qui sont de nature à entraver la libre circulation des services et des paiements.

1.3.3 - Le choix du règlement

Le groupe de travail est parvenu à la conclusion qu'il est nécessaire de remplacer la directive par un règlement. En effet, ce dernier s'avère bien plus adapté lorsqu'il s'agit d'avoir une règle uniforme dans tous les États membres alors que la directive comporte le risque de persistances de divergences nationales.

En tout état de cause, il n'est guère opportun de remplacer la directive par deux instruments que seraient un règlement et une directive. Comme on le voit en matière bancaire avec l'articulation entre la CRD et le règlement CRR, la coexistence d'un règlement et d'une directive complexifie le corpus normatif du fait de renvois non seulement entre règlement et directive, mais également entre mesures nationales de transposition et règlement.

Le choix d'un règlement s'explique par la nécessité de garantir la sécurité juridique qui constitue un principe général de droit de l'Union dont le respect s'impose au législateur européen.

Ensuite, deux séries de considérations permettent de justifier le recours au règlement. À cet égard, est éclairant le considérant n° 5 du Règlement MAR qui explicite les arguments ayant justifié le remplacement de la directive par le règlement.[57] Sur un plan économique,

[57] *« Afin de lever les obstacles aux échanges qui subsistent et l**es distorsions de concurrence importantes dues aux divergences entre les législations nationales**, et de prévenir l'apparition d'éventuels nouveaux obstacles aux échanges et de distorsions*

le règlement promeut une uniformité des règles qui permet d'éviter le risque de fragmentation du marché intérieur des services de paiements. En effet, la transposition de la directive laisse persister des risques de divergences de régimes applicables au gré des États membres. Cela conduit à maintenir des distorsions de concurrence aiguisées par le *forum shopping* que les États membres pourraient pratiquer en exploitant les options et les imprécisions que comporterait la directive. En effet, la divergence des cadres juridiques nationaux peut constituer un facteur de compétitivité et d'attractivité que certains États membres recherchent en exploitant les marges de manœuvre laissées par la directive.

Sur un plan juridique, l'uniformité promue par le règlement permet de favoriser la liberté de circulation des opérateurs de paiements qui entendent exercer leur activité sur une base transfrontalière. Avec un droit uniforme, on évite aux opérateurs de supporter des coûts de mise en conformité avec chaque droit national, coûts dont l'effet dissuasif peut être important de sorte que la liberté de circulation s'en trouve entravée.

Un membre du sous-groupe attire néanmoins l'attention sur les importants travaux de transposition au sein du CMF de la première directive sur les services de paiement.[58] [59] La transformation de la directive en règlement devrait conduire nécessairement à un « *détricotage* » des dispositions de la directive incorporées de façon cohérente dans notre corpus législatif, ce que nous pourrions regretter, compte tenu de la qualité de la transposition à l'époque, au-delà de la transposition purement « *littérale* ».

1.3.4 - Renvoi à des actes de niveau 2

Dans le choix entre règlement et directive, entre uniformité du droit et harmonisation des droits nationaux, un argument en faveur de la directive pourrait être le renvoi à des actes juridiques de niveau 2. Il s'agirait, en substance, pour la future directive, de renvoyer à des actes délégués de

---

de concurrence importantes, il est nécessaire d'adopter ***un règlement établissant une interprétation plus uniforme du cadre de l'Union*** *relatif aux abus de marché, qui définisse plus clairement des règles applicables dans tous les États membres. Le recours à un règlement pour mettre en place des exigences en matière d'abus de marché garantira le caractère directement applicable de ces exigences. Cela permettrait de garantir des* ***conditions homogènes en évitant des exigences nationales divergentes découlant de la transposition d'une directive****. Le présent règlement exigera l'application des mêmes règles par tout un chacun dans toute l'Union. Il rendra également la réglementation moins complexe et réduira les coûts de mise en conformité pour les entreprises, en particulier celles qui mènent des activités sur une base transfrontalière, et contribuera à éliminer les distorsions de concurrence ». Gras ajoutés. Considérant n° 5 du règlement (UE) n° 596/2014, précité.*

[58] *Cf. ordonnance n° 2009-866 du 15 juillet 2009 relative aux conditions régissant la fourniture de service de paiement et portant création des établissements de paiement transposant la directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.*

[59] *Emmanuel Jouffin, Olivia Laplagne et Catherine L'hostis, « La pratique du droit bancaire – Transposition de la directive 2007/64/CE sur les services de paiement – Les nouvelles règles régissant la relation banque-client », Revue Banque, hors-série décembre 2009.*

l'article 290 TFUE ou des actes d'exécution de l'article 291 TFUE, le soin d'établir, le cas échéant, des dispositions uniformes dans l'Union. Une directive peut en effet charger la Commission d'adopter des règlements délégués ou d'exécution qui présentent l'intérêt d'uniformiser le droit lorsque cela se révèle par la suite nécessaire.

Toutefois, le renvoi à des actes de niveau 2 est loin de constituer la panacée.

D'une part, sur le plan temporel, un délai parfois de dix-huit à vingt-quatre mois peut s'écouler entre l'entrée en vigueur de l'acte législatif et l'adoption de l'acté délégué ou d'exécution. Cela risque d'alimenter l'insécurité juridique d'autant que l'adoptions des actes d'exécution implique le recours à la comitologie qui peut complexifier inutilement le droit applicable.

D'autre part, le choix de renvoyer à un acte délégué ou à un acte d'exécution doit prendre en compte la volonté d'impliquer les autorités européennes de surveillance (notamment, l'ABE) dans l'établissement de la réglementation.

1.3.5 - Sanctions

Dans le choix entre règlement et directive, la question des sanctions se pose également. Dans l'état actuel du droit, l'article 103 de la DSP2 prévoit que : « *Les États membres déterminent le régime de sanctions applicables en cas d'infraction aux dispositions de droit national visant à transposer la présente directive et prennent toutes les mesures nécessaires pour en assurer l'application. Ces sanctions sont effectives, proportionnées et dissuasives.* ».

La solution est classique. Pour garantir l'effectivité de la directive, le pouvoir de sanction est exercé par les autorités nationales dans le respect du principe d'autonomie institutionnelle et procédurale. Il revient à chaque État membre de désigner l'autorité ou la juridiction compétente pour sanctionner les violations des règles découlant de la directive (ou du règlement).

Dans l'hypothèse où il serait envisagé d'européaniser les sanctions, un règlement s'avère en revanche nécessaire. Il s'agirait d'habiliter une institution de l'Union – par exemple la Commission ou la BCE – ou un organisme de l'Union – par exemple une autorité européenne de surveillance – à exercer un pouvoir de sanction directement à l'encontre des particuliers. Sur le fondement de l'article 114 TFUE, il est possible de consacrer un pouvoir de sanction. Toutefois, cela implique l'adoption d'un règlement qui, de surcroît, doit prévoir précisément les conditions d'exercice d'un tel pouvoir.

1.4 - Recommandations du HCJP

Le groupe de travail estime qu'un règlement est de nature à garantir une application uniforme des règles relatives aux services de paiements et que le précédent que constitue le paquet CRD/CRR peut être mis en balance par les règlements Benchmark et MiCA qui encadrent tant l'accès à la profession auprès des autorités nationales des États membres et leur supervision par ces autorités, que la fourniture des services réglementés selon des règles uniformes qui s'imposent directement dans la législation des États membres. Une telle uniformité est requise pour garantir la liberté de circulation des services de paiements et donc pour favoriser l'achèvement du marché intérieur de ces services.

Recommandation n° 1 : le HCJP recommande le remplacement de la directive par un règlement.

II. Fusion de la DSP2 et de la DME2

La question d'une fusion de la DSP2 et de la DME2 renvoie à cette autre interrogation : celle de l'autonomie de la monnaie électronique, de sa notion, de son régime et, plus largement, de sa réglementation, par rapport à la catégorie des services de paiement et du droit bâti par les DSP1 et 2.

La question d'une fusion entre services de paiement et monnaie électronique n'est toutefois pas nouvelle. Elle s'est posée dès les travaux de révision de la DME1.[60] Quant à la DME2, le rapport d'évaluation qui devait être remis au plus tard le 1er novembre 2012, et l'a finalement été le 25 janvier 2018, soulignait que « *l'un des principaux défis mis en évidence par l'étude économique concerne la classification de produits et de services comme monnaie électronique ou comme services de paiement, comme comptes de monnaie électronique ou comptes de paiement, et donc l'application du cadre juridique approprié* ».[61]

2.1 - Enjeux liés à la question

Rappelons, au préalable, les définitions légales de la monnaie électronique :

Texte	Dispositions concernées	Disposition
DME2	Article 2(2)	(2) "monnaie électronique" : une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.
CMF	Article L. 315-1	I. – La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique. II. – Les unités de monnaie électronique sont dites unités de valeur, chacune constituant une créance incorporée dans un titre.

[60] *« From a purely legislative perspective, the ideal objective should be to incorporate the E-money Directive into the Payment Services Directive », Commission staff working document on the review of the e-money directive (2000/46/EC), 19 juillet 2006, SEC(2006) 1049, p. 15.*

[61] *Commission européenne, « Rapport de la Commission au Parlement européen et au Conseil sur la mise en œuvre et l'incidence de la directive 2009/110/CE, notamment en ce qui concerne l'application des exigences prudentielles aux établissements de monnaie électronique », COM(2018) 41 final, 25 janvier 2018, p. 9.*

On se remémorera par ailleurs une ancienne définition donnée par la Banque centrale européenne (« BCE »), qui conserve toute sa pertinence : « *Electronic money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument* ».[62]

Du côté, cette fois, de la DSP2, on peut lire dans l'exposé des motifs de la proposition de DSP2 : « *À l'heure où la distinction entre établissements de paiement (relevant de la DSP) et établissements de monnaie électronique (relevant de la directive 2009/110/CE du Parlement européen et du Conseil, dite « seconde directive sur la monnaie électronique » ou « DME ») tend de plus en plus à se brouiller sous l'effet de la convergence des technologies et des modèles d'entreprise, l'idéal serait de moderniser totalement le cadre régissant les paiements électroniques, de manière à aboutir à une fusion de ces deux catégories d'acteurs ainsi que des législations qui leur sont respectivement applicables* ».[63] L'idée est reprise dans la communication de la Commission de 2020 sur une stratégie en matière de paiements de détail pour l'UE.[64]

Autrement dit, l'émission et la gestion de monnaie électronique sont-elles un service de paiement comme un autre ? La communication précitée de la Commission le laisserait entendre : « *(…) dans le cadre du processus d'évaluation de la DSP2, [elle] harmonisera les cadres de la DSP2 et de la directive sur la monnaie électronique (DME2) en reconnaissant l'émission de monnaie électronique comme service de paiement dans la DSP2* ».[65]

Mais ce serait, peu ou prou, nier l'autonomie de la monnaie électronique, au risque de la rendre inutile.

2.2 - Quel est le régime juridique actuel ?

Deux textes coexistent aujourd'hui, mais dont la coexistence est marquée par un décalage dans le temps : la première DME1 date de 2000[66], alors qu'il a fallu attendre 2007 pour

[62] *« Report on electronic money », August 1998, p. 9.*

[63] *OM(2013) 547 final, 24 juillet 2013, p. 3.*

[64] *« Si la DSP2 n'en est qu'au début de sa mise en œuvre, la directive sur la monnaie électronique (DME2) est quant à elle en vigueur depuis plus de dix ans, soit une durée suffisante pour tirer des enseignements de cette expérience. Après l'adoption de la DSP2, les deux régimes ont convergé, tout en demeurant séparés. Les différences entre les services fournis par les établissements de paiement et les établissements de monnaie électronique ne semblent plus justifier des régimes d'autorisation et de surveillance distincts. Les deux types d'établissements pourraient donc être regroupés dans un cadre unique », COM(2020) 592 final, 24 sept. 2020, p. 21.*

[65] *COM(2020) 592 final, précit., p. 23.*

[66] *Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000, concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.*

la DSP1.[67] Partant, la DME2[68] a logiquement précédé la DSP2.[69]

À ce décalage dans le temps s'ajoutent de multiples références croisées entre la DME2 et la DSP1 (puis 2), ce qui ne facilite pas la lisibilité du régime de la monnaie électronique. Cela est sans doute un facteur de confusion.

2.2.1 - La monnaie électronique dans la DME2

Comme son intitulé l'indique, la DME2 n'est pas directement relative à la monnaie électronique (comme la DSP2 avec les services de paiement), mais concerne l'accès à l'activité des établissements de monnaie électronique (EME), son exercice et sa surveillance (à l'exemple de la CRD). Ce qui plaiderait en faveur d'un objet « *monnaie électronique* » qui ne serait pas directement assimilable à un « *service* » mais caractériserait, en amont, un « *moyen de paiement* », voire un « *véritable « système de paiement », composé d'un émetteur, de porteurs-consommateurs et d'un réseau de commerçants* ».[70]

2.2.1.1 - Les considérants de la DME2

La DME2, à l'évidence, ne se suffit pas à elle-même et, dès son considérant n° 3, évoque ce qui, à l'époque, était la DSP1, qui « *a établi un cadre juridique moderne et cohérent pour les services de paiement* ».

Cette dépendance du droit de la monnaie électronique par rapport à celui des services de paiement est parfaitement illustrée au considérant n° 9 de la DME2.[71]

---

[67] *Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007, concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE.*

[68] *Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE.*

[69] *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.*

[70] *S. Lanskoy, « La nature juridique de la monnaie électronique », Bulletin Banque de France n° 70, octobre 1999.*

[71] *« Il y a lieu de réexaminer le régime de surveillance prudentielle des établissements de monnaie électronique et de mieux l'adapter aux risques propres à ces établissements. Il convient également de le rendre cohérent avec le régime de surveillance prudentielle applicable aux établissements de paiement régis par la directive 2007/64/CE. À cet égard, les*

Il est encore précisé, au considérant 19 (et repris à l'article 13 de la DME2), que « *le titre IV, chapitre 5, de la directive 2007/64/CE devrait donc s'appliquer mutatis mutandis dans le cadre de la présente directive, sans préjudice des dispositions de la présente directive* » ; qu'« *une référence à un « prestataire de services de paiements » dans la directive 2007/64/CE doit donc se comprendre comme une référence à un émetteur de monnaie électronique* » ; qu'« *une référence à un « utilisateur de services de paiement » doit se comprendre comme une référence à un détenteur de monnaie électronique* », et qu'« *une référence aux titres III et IV de la directive 2007/64/CE doit se comprendre comme une référence au titre III de la présente directive* ».

Au considérant 24 de la DME2, enfin, il est dit que « *la présente directive établit une nouvelle définition de la monnaie électronique, dont l'émission peut bénéficier des dérogations prévues aux articles 34 et 53 de la directive 2007/64/CE* ».

2.2.1.2 - Les dispositions de la DME2

La dépendance du régime de la monnaie électronique vis-à-vis du droit des services de paiement est manifeste dès l'article 1er de la DME2 relatif à son objet et à son champ d'application, dans la mesure où les paragraphes (4) et (5) excluent de celui-ci la valeur monétaire elle-même exclue en vertu de l'article 3(k) et (l) de la DSP1.

La définition de la monnaie électronique fait également référence à la DSP1 :

« *monnaie électronique : une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de*

[71 (suite)] *dispositions pertinentes de la directive 2007/64/CE devraient s'appliquer mutatis mutandis aux établissements de monnaie électronique, sans préjudice des dispositions de la présente directive. Ainsi, une référence à un « établissement de paiement » dans la directive 2007/64/CE doit se comprendre comme une référence à un établissement de monnaie électronique ; une référence à des « services de paiement » doit se comprendre comme une référence à l'activité de services de paiement et d'émission de monnaie électronique ; une référence à un « utilisateur de services de paiement » doit se comprendre comme une référence à un utilisateur de services de paiement et à un détenteur de monnaie électronique ; une référence à la présente directive doit se comprendre comme une référence à la fois à la directive 2007/64/CE et à la présente directive ; une référence au titre II de la directive 2007/64/CE doit se comprendre comme une référence à la fois au titre II de la directive 2007/64/CE et au titre II de la présente directive ; une référence à l'article 6 de la directive 2007/64/CE doit se comprendre comme une référence à l'article 4 de la présente directive ; une référence à l'article 7, paragraphe 1, de la directive 2007/64/CE doit se comprendre comme une référence à l'article 5, paragraphe 1, de la présente directive ; une référence à l'article 7, paragraphe 2, de la directive 2007/64/CE doit se comprendre comme une référence à l'article 5, paragraphe 6, de la présente directive ; une référence à l'article 8 de la directive 2007/64/CE doit se comprendre comme une référence à l'article 5, paragraphes 2 à 5, de la présente directive ; une référence à l'article 9 de la directive 2007/64/CE doit se comprendre comme une référence à l'article 7 de la présente directive ; une référence à l'article 16, paragraphe 1, de la directive 2007/64/CE doit se comprendre comme une référence à l'article 6, paragraphe 1, points c) à e), de la présente directive ; une référence à l'article 26 de la directive 2007/64/CE doit se comprendre comme une référence à l'article 9 de la présente directive* ».

fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5), de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique »[72].

Le régime prudentiel des EME emprunte encore largement à celui des EP[73], de même que le calcul des fonds propres en ce qui concerne les activités non liées à l'émission de monnaie électronique (la question sera au centre de l'arrêt *Paysera*, que l'on verra plus loin).[74]

S'agissant, précisément, des activités des EME, l'article 6 de la DME2 les habilite à fournir des services de paiement (et services connexes) au sens de la DSP1, de même qu'il les oblige à protéger les fonds reçus en échange de la monnaie électronique émise conformément à l'article 9(1) et 2, de la DSP1.[75]

Sur le terrain, enfin, des exemptions optionnelles, DME2 et DSP1 semblent former un seul texte :

« *Les États membres peuvent exempter ou autoriser leurs autorités compétentes à exempter de l'application de tout ou partie des procédures et conditions fixées aux articles 3, 4, 5 et 7 de la présente directive, à l'exception des articles 20, 22, 23 et 24 de la directive 2007/64/CE, et autoriser des personnes morales à être inscrites dans le registre des établissements de monnaie électronique, si les deux conditions suivantes sont respectées (…)* ».[76]

2.2.2 - La monnaie électronique dans la DSP2

À l'inverse, la DSP2 (qui, au demeurant, à modifier en quelques endroits la DME2)[77] affirme à plusieurs occasions son emprise sur la monnaie électronique, au-delà de son régime prudentiel propre.

Le considérant n° 25 de la DSP2 est emblématique de cet empire :

« *La présente directive fixe les règles relatives à l'exécution des opérations de paiement lorsque les fonds sont constitués de monnaie électronique, au sens de la directive 2009/110/CE. Cependant, la*

[72] *Article 2(2) de la DME2.*

[73] *Article 3(1), (4) et (5) de la DME2.*

[74] *Article 5(2) de la DME2.*

[75] *Article 7(1) de la DME2.*

[76] *Article 9(1) de la DME2.*

[77] *Article 111 de la DSP2.*

présente directive ne régit pas l'émission de monnaie électronique prévue par la directive 2009/110/CE. Dès lors, les établissements de paiement ne devraient pas être autorisés à émettre de la monnaie électronique ».

Car les « *fonds* » objets des opérations de paiement sont tout aussi bien, et indifféremment, constitués par « *les billets de banques et les pièces, la monnaie scripturale ou la monnaie électronique au sens de l'article 2, point 2), de la directive 2009/110/CE* »[78] (à ne pas confondre avec les fonds reçus par les EP de la part d'utilisateurs de services de paiement, qui ne constituent ni des dépôts, ni de la monnaie électronique).[79]

Notons encore que des règles communes aux instruments de paiement relatifs à des montants de faible valeur et à la monnaie électronique sont posées aux articles 42 et 63 de la DSP2.

2.2.3 - La monnaie électronique en droit français

Pour mémoire, dans le CMF, le droit de l'exécution des opérations de paiement est expressément déclaré applicable à l'émission et la gestion de monnaie électronique.[80]

En sens inverse, l'article L. 315-5 du CMF fait du droit des contrats de services de paiement la norme concernant les activités d'émission et de gestion de la monnaie électronique. [81]

2.2.4 - Autres textes visant la monnaie électronique

2.2.4.1 - Cartes prépayées

Les cartes prépayées sont très généralement analysées comme des instruments de paiement en monnaie électronique, la plupart du temps « *anonymes* », d'où l'expression, un peu galvaudée de « *monnaie électronique anonyme* ».[82]

---

[78] *Article 4(25) de la DSP2.*

[79] *Article 18(3) de la DSP2.*

[80] *Cf. article L. 133-1-VII du CMF : « Sans préjudice de l'application de la section 12 [Les modalités de remboursement de la monnaie électronique], le présent chapitre [Les règles applicables aux autres instruments de paiement et à l'accès aux comptes] s'applique à l'émission et la gestion de monnaie électronique ».*

[81] *Cf. article L. 315-5 du CMF : « Le chapitre IV [Les services de paiement] du présent titre [Les opérations de banque, les services de paiement et l'émission et la gestion de monnaie électronique] s'applique aux activités d'émission et de gestion de monnaie électronique, sans préjudice des exigences supplémentaires prévues à la présente section ».*

[82] *Par exemple, cf. Banque de France, « La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers », Rapport 2017, pp. 37 et s. Voir aussi M. Perdrix, « La problématique des paiements par cartes prépayées », Bulletin Banque de France 1994, p. 93.*

Les cartes prépayées sont par exemple visées dans le Règlement CMI, où elles sont définies comme « *une catégorie d'instrument de paiement permettant de stocker de la monnaie électronique au sens de l'article 2, point 2, de la directive 2009/110/CE* ».[83]

Elles apparaissent également dans le règlement (UE) 2018/1672 du Parlement européen et du Conseil du 23 octobre 2018 relatif aux contrôles de l'argent liquide entrant dans l'Union ou sortant de l'Union et abrogeant le règlement (CE) n° 1889/2005, où elles composent, avec les espèces, les instruments négociables au porteur et les marchandises servant de valeur très liquide, la catégorie « *argent liquide* » :

« *carte prépayée : une carte non nominative, telle qu'elle figure à l'annexe I, point 2, sur laquelle sont déposés une valeur monétaire ou des fonds qui peuvent servir pour des opérations de paiement, pour l'acquisition de biens ou de services ou pour le remboursement d'espèces, ou qui donne accès à un telle valeur ou de tels fonds, et qui n'est pas liée à un compte bancaire* »[84] (article 2, f).

Par ailleurs, leur anonymat a nécessairement fait l'objet d'un encadrement en termes de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT). Il a ainsi justifié, en partie (l'anonymat des « *monnaie virtuelles* » était également visé), la révision de la 4e directive anti-blanchiment[85] par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018.

2.2.4.2 - Moyens d'échange numérique

Même plus anecdotique, on n'oubliera pas la catégorie des « *moyens d'échange numérique* », que la directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil définit ainsi : « *toute monnaie électronique telle que définie à l'article 2, point 2, de la directive 2009/110/CE du Parlement européen et du Conseil ou monnaie virtuelle* » (article 2, c).

---

[83] *Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, article 2(35).*

[84] *Il convient de remarquer que le règlement fait référence à la notion de « compte bancaire », laquelle n'est pas définie en dans le droit européen des services de paiement. Il conviendrait probablement de lire « compte de paiement ». Voir la discussion à ce sujet au paragraphe 7.1.1 ci-dessous.*

[85] *Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.*

2.2.4.3 - Crypto-actifs

La Commission européenne a annoncé que, « *dans la proposition de règlement concernant les marchés de crypto-actifs, [elle] soumettr[a] les émetteurs de jetons de monnaie électronique à des dispositions supplémentaires complétant la DME2* » [86]

La monnaie électronique est en effet omniprésente dans le Règlement MiCA. S'y distingue en particulier la catégorie (et même la première catégorie de crypto-actifs) des jetons de monnaie électronique (ou *e-money tokens* ou EMT), ainsi présentés au considérant 18 du règlement : « *(…) des crypto-actifs qui visent à stabiliser leur valeur en se référant à une seule monnaie officielle. La fonction de ces crypto-actifs est très semblable à celle de la monnaie électronique, telle qu'elle est définie dans la directive 2009/110/CE. À l'instar de la monnaie électronique, ces crypto-actifs constituent des substituts électroniques des pièces et des billets de banque et sont susceptibles d'être utilisés pour effectuer des paiements. Ces crypto-actifs devraient être définis dans le présent règlement comme des « jetons de monnaie électronique »* ».

On peut noter que les *e-money tokens* sont très présents dans l'étude de la DG FISMA publiée le 2 février 2023, qui suggère en particulier d'établir une consolidation législative entre MiCA et la DSP2 (cf. ci-après).

2.2.4.4 - LCB-FT

La 4e directive anti-blanchiment modifiée, après avoir donné une définition de la monnaie électronique par renvoi à l'article 2(2), de la DME2[87], prévoit un régime de vigilance allégée pour un usage très limité de la monnaie électronique.[88]

À l'article 45(9), elle ménage aux États membres l'option d'exiger des EME (et des EP) européens établis sur leur territoire sous une forme autre que celle de la succursale qu'ils nomment un point de contact central.

---

[86] *COM(2020) 592 final, précit., p. 23.*

[87] *4e Directive LCB-FT, article 3(16). Voir encore Annexe II qui liste, parmi les facteurs et types d'éléments à risque potentiellement moins élevé, les « produits pour lesquels les risques de blanchiment de capitaux et de financement du terrorisme sont contrôlés par d'autres facteurs tels que l'imposition de limites de chargement ou la transparence en matière de propriété (par exemple pour certains types de monnaie électronique). »*

[88] *4e Directive LCB-FT, article 12.*

Quant au règlement qui accompagne la directive (4e règlement anti-blanchiment[89]), il présente l'intérêt de viser à quelques reprises les transferts de fonds « *en espèces ou sous forme de monnaie électronique anonyme* » .[90]

2.2.5 - Jurisprudence relative à la monnaie électronique

2.2.5.1 - Arrêt « Paysera »

On se réfère ici au premier arrêt important en matière de monnaie électronique : l'arrêt *Paysera*, rendu par la CJUE le 16 janvier 2019.[91]

Non seulement s'est-il prononcé sur la notion de « *services de paiement liés à l'émission de monnaie électronique* », afin de résoudre une question de calcul des fonds propres à cheval entre la DME2 et la DSP1 (en l'espèce), mais encore a-t-il affirmé la « *remboursabilité* » de nature de la monnaie électronique : « *(…) l'émission de monnaie électronique implique inconditionnellement et automatiquement un droit au remboursement (…)* » (point 28).

Partant, une future DSP3 intégrant le droit de la monnaie électronique devrait prévoir cette nouvelle dimension de la remboursabilité de la monnaie électronique, qui est une notion typique de la nature et du régime de la monnaie électronique, que son détenteur peut exercer à tout moment en vertu de son droit de créance sur l'émetteur. Remarquons que ce droit de créance contre l'émetteur de la monnaie électronique est un élément qui différencie notablement la monnaie scripturale de la monnaie électronique, en ce sens que la banque n'est pas débitrice de la monnaie émise par l'institut d'émission (pour l'euro, la BCE), mais est débitrice d'une créance de restitution du dépôt réalisé auprès d'elle par le déposant. Lors d'un transfert de monnaie électronique, le bénéficiaire qui reçoit de la monnaie électronique se voit donc transférer un droit contre l'émetteur de la monnaie électronique.

2.2.5.2 - Décision du Conseil d'État

Doit encore être mentionnée ce qui serait la première décision du Conseil d'État sur la qualification de monnaie électronique,[92] encore que d'une portée très limitée :

---

[89] *Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006.*

[90] *4e Règlement LCB-FT, article 5(3), a), article 6(2)(b) et article 7(4)(a).*

[91] *CJUE, 16 janvier 2019, Paysera LT UAB, C-389/17, ECLI:EU:C:2019:25, concl. avocat général M. Wathelet.*

[92] *En ce sens, E. Rogey et M. Pachebat, « Le Conseil d'État confirme l'interdiction temporaire d'activité d'un établissement de monnaie électronique pour défaut de protection des fonds des clients », RDBF n° 1, janvier-février 2023, étude 4, n° 8.*

« (…) la société, qui dispose d'un agrément en qualité d'établissement de monnaie électronique, propose à ses clients d'acquérir, par tout moyen habituel, dans un point de vente de son réseau, essentiellement composé de buralistes, un ticket qui comporte un code électronique PIN qu'elle émet et auquel est associée une ligne de valeur monétaire qui peut être soit consommée en ligne auprès des sites marchands, notamment de jeux et de paris en ligne, acceptant ce mode de paiement, soit remboursée sous conditions à hauteur de la créance détenue sur la société. Il suit de là que le produit « Ticket Premium » commercialisé par la société Wari Pay constitue une monnaie électronique au sens du I de l'article L. 315-1 du Code monétaire et financier ».[93]

2.3 - Options disponibles

2.3.1 - Travaux

2.3.1.1 - Rapport de la Commission au Parlement européen et au Conseil

Le rapport précité de la Commission de 2018 demeure très prudent quant à la perspective d'une fusion entre DSP2 et DME2 :

« Un futur réexamen de la directive et sa fusion avec la directive révisée sur les services de paiement nécessiteraient une analyse plus approfondie. Il semble opportun de n'envisager de telles mesures qu'après que les États membres et les acteurs concernés auront pu accumuler de l'expérience avec le cadre adapté à la suite de l'adoption de la DSP2, qui aura également une incidence sur les établissements de monnaie électronique ».[94]

2.3.1.2 - Réponse de l'ABE au call for advice de la Commission[95]

Dans sa réponse du 23 juin 2022, l'ABE exprime son plein soutien à l'idée d'une fusion entre DSP2 et DME2 et propose en outre :

(i) que les services de monnaie électroniques soient couverts par les services de paiement existants en raison de leur nature similaire et des risques attachés ;

(ii) d'appliquer les mêmes exigences juridiques aux EP et EME, en particulier concernant la procédure d'agrément, et les exigences de sauvegarde des fonds de la clientèle, de capital initial et de fonds propres ; et

---

[93] *CE, 9e et 10 ch. Réunies, 9 décembre 2022, société WariPay, n° 4565582, concl. C. Guibe.*

[94] *COM(2018) 41 final, 25 janvier 2018, p. 10.*

[95] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 juin 2022.*

(iii) de clarifier la nature et le statut de distributeur de monnaie électronique afin d'appliquer un régime cohérent entre les agents de PSP et les distributeurs.

Incidemment, on notera que l'ABE[96] avance curieusement qu'elle a identifié deux voies potentielles pour réaliser l'unification entre services de paiement et monnaie électronique :

(A) la première consisterait à considérer que tous les services liés à la monnaie électronique sont couverts par les services de paiement existants de l'annexe I de la DSP2, supprimant par-là même la nécessité de distinguer entre monnaie scripturale et monnaie électronique, réunies sous le même vocable de « *fonds* » ; et

(B) la seconde reviendrait à enrichir la liste des services de paiement des seuls « *hardware-based electronic money services, which are stored on pre-paid cards that are not linked to accounts* ».

2.3.1.3 - Rapport de l'ABE sur la revue des autorisations dans le cadre de la DSP2

Publié le 11 janvier 2023, le rapport de l'ABE appelle la Commission européenne, « *afin d'assurer plus de cohérence et d'harmonisation dans l'ensemble de l'UE et de créer des conditions équitables* », à « *fournir des critères clairs pour délimiter les différentes catégories de services de paiement ainsi que l'émission de monnaie électronique* ».[97]

2.3.1.4 - Étude de la DG FISMA[98]

L'étude de la DG FISMA,[99] en date du 2 février 2023, est censée préparer directement la révision de la DSP2.

Au titre du pilier 1 (champ d'application de la DSP2 et exclusions), il est recommandé « *d'unifier la DSP2 et l'EMD2 pour remédier à l'incertitude juridique et à l'application divergente des règles d'un pays à l'autre et pour les différents acteurs du marché. Pour ce faire, une consolidation législative entre les deux textes est proposée :*

- 1. en ajoutant un chapitre sur les exigences en matière d'agrément et de surveillance des établissements de monnaie électronique dans le titre de la DSP2 sur les prestataires de services de paiement ;

---

[96] *ABE, op. cit., n° 109, 110 et 111.*

[97] *EBA/REP/2023/01, paragraphe 187.*

[98] *DG FISMA, « A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) », FISMA/2021/OP/0002.*

[99] *Laquelle fait 188 pages et 172 pages d'annexes.*

- 2. en étendant l'application des titres III et IV de la DSP2 aux opérations de paiement en monnaie électronique ;

- 3. en supprimant le paragraphe (6) préambule de la DME2 ; et

- 4. en établissant un corpus unique de définitions fondamentales applicables à la fois à la monnaie électronique et aux services de paiement. »

Le rapport poursuit, en préconisant « *d'adopter des définitions plus cohérentes des principales questions suivantes : accès aux comptes (dans le cadre de la PSD2+EMD2) ; accès aux systèmes de paiement (mieux dans le cadre de la FSD) ; agents/externalisation (dans le cadre de la PSD2+EMD2). Il existe des approches divergentes au niveau national en ce qui concerne l'exemption relative aux « agents » ; des pratiques d'application divergentes pour l'accès direct et indirect des EME et des PSIP aux systèmes de paiement, ce qui crée une incertitude juridique, ralentit le développement des paiements transfrontaliers et constitue un obstacle au marché. Pour y remédier, les recommandations suivantes sont proposées :*

- 1. l'ABE devrait publier régulièrement des lignes directrices sur l'exemption relative aux «agents» ;

- 2. des lignes directrices de l'ABE sur l'accès indirect des EME et des PSIP aux systèmes de paiement ; et

- 3. consolider les lignes directrices, les dispositions de la PSD2 et les questions-réponses sur « l'accès aux comptes » dans la relation PSPGC-TTP».

La DG FISMA propose également de « *renforcer la coopération entre les autorités nationales de surveillance des plateformes de paiement et des plateformes numériques fournissant des services de paiement afin d'éviter une application divergente de la DSP2 et des pratiques de surveillance divergentes. Cela réduira l'incertitude juridique concernant les règles de la DSP2 et les coûts pour les entreprises. Pour ce faire, les recommandations suivantes sont proposées :*

- 1. donner un cadre juridique aux plateformes numériques fournissant des services de paiement (par exemple : Amazon ; Apple Pay, etc.) comme le prévoit le DMA ; et

- 2. mettre en place un comité de surveillance des plateformes sur une base transfrontalière, coordonné par l'ABE. »[100]

[100] *DG FISMA, op. cit., p. 17 et 18.*

L'étude de la DG FISMA s'attache par ailleurs de manière significative au thème de la monnaie électronique et des portefeuilles numériques (*digital wallets*), qui l'amène à s'intéresser aux « *Big Techs* » qui, en majorité constate-t-elle (mais sans en tirer de conclusions significatives), ont choisi le statut d'EME, comme l'illustre ce tableau reproduit ci-après :

Table 5 BigTech Payment Licence in Europe

BigTech Firm	Year of Licence	Type of Licence	EEA National Competent Authority
PayPal	2007	Banking Licence	CSSF- Luxembourg
Amazon Payments Europe	2010	E-money Licence	CSSF- Luxembourg
eBay	2014	Payment Institutions Licence	CSSF- Luxembourg
Rakuten Europe Bank	2016	Banking Licence	CSSF- Luxembourg
Facebook Payment Intl Ltd	2018	Payment Institutions Licence	Central Bank of Ireland
Alipay Limited	2018	E-money Licence	CSSF- Luxembourg
Airbnb Payment	2018	E-money Licence	FCA-UK
Google Payment Lithuania	2018	E-money Licence	Lietuvos Banka-Lithuania
Google Payment Ireland	2019	E-money Licence	Central Bank of Ireland
Uber Payment	2019	E-money Licence	De Nederlandsche Bank-Netherlands
Takeaway.com	2019	Payment Institutions	De Nederlandsche Bank-Netherlands
Zalando Payment Solution	2019	E-money	BaFin – Germany

Sur l'opportunité de fusionner DME2 et DSP2, enfin, on renvoie à la page 108 de l'étude (qui offre l'intérêt de présenter les arguments contre), ainsi qu'aux pages 113 à 115 consacrées au concept de monnaie électronique (*the concept of « e-money »*). Il en ressort en particulier : « *La grande majorité des parties prenantes consultées ont fait remarquer que, puisque les EME semblent en fait fournir les mêmes services de paiement, elles approuvent les propositions visant à fusionner la directive DME2 et la PSD2 en un seul texte et à ajouter la monnaie électronique dans les définitions des services de paiement* ».[101]

2.3.2 - Vers la fusion entre DSP2 et DME2

Selon toute vraisemblance, on s'acheminerait vers un texte unique : la DSP3 (ou son équivalent sous la forme d'un règlement), qui fusionnerait droit des services de paiement et droit de la monnaie électronique.

[101] *DG FISMA, op. cit., p. 113.*

Un consensus se dégagerait en faveur de cette fusion, ne serait-ce que pour clarifier un cadre juridique jusque-là jugé complexe, peu lisible, mal pratique, etc.

Il n'en demeure pas moins que l'on ne sait pas, à ce jour, si la DSP3 procéderait à une fusion « *technique* » (c'est-à-dire incorporer à « *droit constant* » les dispositions de la DME2) ou, au contraire, en profiterait pour recomposer, en partie, le droit des paiements, en particulier le volet « *institutionnel* » avec la création d'un seul « *EPME* » au régime prudentiel unifié.

On peut raisonnablement penser que cette fusion annoncée créerait l'opportunité de corriger et enrichir le régime de la monnaie électronique qui, soit dit en passant, a sans doute vieilli depuis 2009. À cet égard, la numérisation du paiement à laquelle on assiste ne devrait pas laisser intacts la notion ni le régime de la monnaie électronique.

Il ne faudrait pas, toutefois, qu'une telle incorporation du droit de la monnaie électronique dans celui des services de paiement soit au prix d'un « *affadissement* », voire d'une « *dilution* », de la notion comme de l'intérêt de la monnaie électronique.

2.3.2.1 - Ce qui est souhaitable

Il apparaît d'abord souhaitable de réunir dans un texte unique (la DSP3) les règles disséminées auparavant dans la DME2 et la DSP2 et qui s'appliquent pareillement aux EP et EME (agrément, dispositions prudentielles, protection des fonds, etc.) et à leur supervision, aux contrats qu'ils passent (information contractuelle, contrats-cadres de services de paiement), au contrôle interne (dont externalisation), au passeport européen ou aux obligations de LCB-FT.

De même, les EME étant avant tout des PSP, il serait de bonne législation qu'un corps de règles communes à la fourniture des services de paiement indifféremment par les EP et EME figure dans la future DSP3. Au demeurant, comme cela a déjà été souligné, les règles relatives aux opérations de paiement (autorisation, exécution, contestation) sont indifférentes à la qualité du PSP. Que les fonds soient constitués de monnaie fiduciaire, de monnaie scripturale ou de monnaie électronique (et, bientôt, de crypto-actifs, quand le règlement sur les informations accompagnant les transferts de fonds et de certains crypto-actifs s'appliquera), un même droit de l'exécution des opérations de paiement devrait s'appliquer.

Enfin, on assistera sans doute à la fusion entre agents (de PSP) et distributeurs (de monnaie électronique), dont la distinction et la différence de régime (enregistrement dans un cas, simple information du superviseur dans l'autre) ne se justifient pas ou plus.

De manière générale, un texte unique viendrait remédier à ce qui pouvait apparaître comme une fragmentation inutile et préjudiciable des règles applicables aux paiements (en monnaie scripturale comme en monnaie électronique).

2.3.2.2 - Ce qui ne l'est pas (ou serait dangereux)

Il nous semble en revanche qu'il serait préjudiciable à l'autonomie, sinon à l'existence, de la monnaie électronique d'en faire un service de paiement comme les autres ; d'ériger par exemple l'émission (et la gestion) de monnaie électronique en service 9° (en l'état de l'annexe de la DSP2 et du II de l'article L. 314-1 du CMF).

Nous croyons en effet que la monnaie électronique se situe en amont de la qualification de service de paiement, en ce sens qu'elle est un véritable « *moyen de paiement* » (encore que la notion soit peu pratiquée en droit européen, et qu'elle l'est improprement dans le CMF), voire un schéma ou un système de paiement à part entière.

Que la monnaie électronique soit davantage qu'un service de paiement, c'est le point 25 de l'article 4 qui le commande, dans la mesure où il définit les « *fonds* » comme « *les billets de banque et les pièces, la monnaie scripturale ou la monnaie électronique au sens de l'article 2, point 2, de la directive 2009/110/CE* ».

Que la monnaie électronique soit autre chose qu'un service de paiement, le Règlement MiCA en témoigne parfaitement lorsqu'il établit une parenté de « *fonction* » (la stabilisation de leur valeur) entre les crypto-actifs se référant à une monnaie officielle afin de conserver une valeur stable, et la monnaie électronique ; et lorsqu'il permet aux détenteurs d'*e-money tokens* d'en demander le remboursement, à l'instar de la monnaie électronique.[102]

Il n'en demeure pas moins que la tendance semble être à l'« *alignement* » des concepts, moyens ou instruments. Prenons par exemple le nouveau cadre PISA de surveillance des paiements électroniques : aux différents corps de règles relatifs à la carte, au virement, au prélèvement ainsi qu'à la monnaie électronique, succède désormais un cadre unique (*the PISA framework*) au sein duquel les instruments de paiement électronique sont aussi bien les « *payment cards, credit transfers, direct debits, e-money transfers and digital payment tokens* ».[103]

2.3.2.3 - Ce qu'il reste à éclaircir

Il y a d'abord la notion même de monnaie électronique qui demeure à trouver, sans quoi l'on continuera à parler d'un objet mal défini.

---

[102] *À tel point qu'on peut se demander ce qui diffère de la monnaie électronique de l'établissement de monnaie électronique du point de vue de la définition juridique qui est au fond différent car elle dispose du caractère libératoire obligatoire, Règlement MiCA.*

[103] *« Eurosystem oversight framework for electronic payment instruments, schemes and arrangements », novembre 2021, p.3.*

On continue, en effet, malgré le temps écoulé depuis la DME2, à ne pas parvenir à qualifier correctement tel produit ou service se situant à la frontière entre services de paiement et monnaie électronique.

Est-ce le « *pré-paiement* » qui caractérise fondamentalement la monnaie électronique ? La réserve de valeur monétaire ou de pouvoir d'achat[104] ? Est-ce plutôt son réseau (conventionnel) d'acceptation en paiement ? D'autres éléments caractéristiques existent-ils et, si oui, lesquels ?

Le débat persiste et, surtout, continue de nourrir l'impression, à vrai dire un peu lassante, selon laquelle la monnaie électronique se laisse difficilement appréhender faute d'une notion clairement et solidement définie.

Cette difficulté n'est pas que conceptuelle, comme la DG FISMA l'a relevé :

« *Plusieurs parties prenantes ont noté que les utilisateurs ne perçoivent pas de différence entre un compte de monnaie électronique et un compte bancaire, que les EP et les EME émettent tous deux des cartes de paiement et que les entités de monnaie électronique agissent de plus en plus en tant que prestataires de services de paiement* ».[105]

L'intention de la DME2 était pourtant manifeste :

« *Il y a lieu de veiller à ce que la définition de la monnaie électronique soit claire afin qu'elle soit neutre sur le plan technique. Cette définition devrait couvrir toutes les situations dans lesquelles un prestataire de services de paiement émet en contrepartie de fonds une valeur stockée prépayée, qui peut être utilisée à des fins de paiement car elle est acceptée par des tiers en tant que paiement* ».[106]

À défaut, peut-être, de toujours bien savoir ce qu'elle est, la monnaie électronique sert-elle cependant à quelque chose ? Si oui, à quoi ? etc.

Se pose ici la question des « *utilités* » (pratiques, concrètes, modèles de marché à l'appui) de la monnaie électronique : à quoi peut-elle bien servir que la qualification de services de paiement, notamment, ne peut satisfaire ?

---

[104] *Comp., G. Blanluet, « La monnaie électronique, valeur monétaire », Revue de droit bancaire et financier n° 2, mars 2001, dossier 100018 ; Adde J. Rochfeld, « Monnaie électronique », RTD civ. 2003, p. 361.*

[105] *DG FISMA, op. cit., p. 113.*

[106] *Considérant n° 7 de la DME2.*

Manifestement, le Règlement MiCA offre un formidable démenti à ceux qui seraient tentés de répondre que la monnaie électronique ne sert somme toute à pas grand-chose, sinon à embuer les esprits. Elle présente ainsi l'utilité de pouvoir catégoriser toute une variété de crypto-actifs qui seront « *réputés être de la « monnaie électronique »* »[107] et seront soumis à son régime (émission, remboursement, etc.).

Cela illustre l'idée que, dès son origine, la monnaie électronique fut conçue comme une représentation monétaire propre à un usage en ligne ; propre à payer de manière sécurisée sur internet. Cette utilité d'une « *monnaie de réseau* » (*network money*) a été parfaitement démontrée par PayPal, qui outre sa solution en tant que telle, a développé un véritable schéma de paiement, reconnu comme tel par le cadre PISA, au même titre que les schémas SCT ou SDD.[108]

Dans cette veine, on peut remarquer que la Banque de France, de manière significative, voit dans la monnaie électronique, « *une forme spécifique de monnaie dédiée aux transactions* ».[109]

Se révèle également cette originalité que le paiement en monnaie électronique n'a pas besoin de compte bancaire (ou plus exactement compte de paiement) pour prospérer, ce qu'avait très bien vu à l'origine la Banque centrale européenne : « *A distinguishing feature of transactions carried out with electronic money is that they do not necessarily involve a bank account. This is a fundamental difference between electronic money and access products. With access products, such as debit cards, payments are settled by means of transfers between bank accounts* ».[110]

Quoi qu'il en soit, ces « *utilités positives* » doivent être mises en valeur pour contrebalancer ce qui, trop souvent, justifie le recours à la monnaie électronique : son anonymat. Lorsque l'on mesure combien l'anonymat est sans cesse pourchassé par la réglementation LCB-FT, on s'aperçoit sans peine que le temps d'une « *monnaie électronique anonyme* » est derrière-nous. Or si le choix de la monnaie électronique n'était justifié que par la recherche de l'anonymat, elle n'aurait d'ores et déjà plus d'intérêt.

Se pose également, et de manière récurrente, la question de la distinction entre compte de paiement et compte de monnaie électronique.

[107] *Considérant n° 66 du Règlement MiCA.*

[108] *Cf. , « List of overseen schemes under the PISA framework », 4 octobre 2022.*

[109] *Banque de France, « Paiements et infrastructures de marché à l'ère digitale », chapitre 1, mai 2022, p. 12.*

[110] *« Issues arising from the emergence of electronic money », ECB Monthly Bulletin, novembre 2000, p.49.*

Sans entrer ici dans la discussion, qui fait l'objet de développements à part entière dans le présent rapport,[111] un compte de monnaie électronique (dont on sait aujourd'hui qu'il peut être « *ibanisé* ») est-il toujours un compte de paiement ? L'étude précitée de la DG FISMA fait état d'une incertitude et de divergences dans l'Union européenne concernant la possibilité de combiner compte de monnaie électronique et compte de paiement.[112] Un compte de monnaie électronique serait-il un compte de paiement seulement lorsqu'il permet d'exécuter et de recevoir des opérations de paiement ? Peut-il servir à « *stocker* » là où le compte de paiement ne peut servir qu'à exécuter ? etc.[113] Un compte de monnaie électronique serait-il plus « *technique* » qu'un compte de paiement ? Pourrait-il, à cet égard, demeurer anonyme ? etc.

Comment interpréter la règle, postulée par le Règlement SEPA, que celui-ci ne s'applique pas « *aux opérations de paiement de monnaie électronique, telle que définie à l'article 2, point 2 [de la DME 2], sauf si ces opérations entraînent un virement ou un prélèvement vers et depuis un compte identifié par un numéro BBAN ou IBAN* »[114] ?

On relèvera qu'une opinion s'est fait entendre, dans le groupe de travail, selon laquelle la difficulté récurrente d'appréhender la monnaie électronique viendrait du fait que coexisteraient, en réalité, deux modèles bien différents de monnaie électronique :

(i) dans l'un, plutôt anglo-saxon, la monnaie électronique se distingue difficilement de la monnaie scripturale car, comme elle, elle est utilisée en circuit ouvert dans un réseau ouvert d'accepteurs (paiement par carte universelle) ; l'utilité de la qualification de monnaie électronique serait qu'elle permettrait au compte qui la recueille de conserver les fonds, au contraire du compte de paiement qui, par définition, ne sert qu'à exécuter des opérations de paiement. Jusqu'à une réponse récente de l'ABE dans les Q&A, il existait une incertitude concernant la possibilité de conserver des fonds sur un compte de paiement sous forme de solde en l'absence d'ordre de paiement prédéfini.[115] Selon ce modèle, la monnaie électronique ainsi stockée sur un compte offrant des fonctionnalités

[111] *Voir paragraphe 7.1.2 ci-dessous.*

[112] *« There is for example uncertainty about whether an account combined with a prepaid card with an IBAN number can be defined as an electronic money account or a payment account », DG FISMA, « A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) », FISMA/2021/OP/0002. p. 115.*

[113] *Sur la distinction entre compte de paiement et compte de monnaie électronique, cf. , « Avis du 5 décembre 2008 sur une proposition de directive concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements » (CON/2008/84).*

[114] *Règlement (UE) 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) 924/2009, article 1(2)(f), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32012R0260.*

[115] *Voir ABE, Q&A n° 2018_4221.*

comparables à celles d'un compte de paiement au sens de la Directive PAD serait de nature à impliquer l'existence d'un compte de paiement ;

(ii) l'autre modèle, en circuit fermé, s'apparenterait à celui du compte PayPal, ou closed-loop (staged) digital wallet, qui ne permet des transactions en monnaie électronique que si le payeur et l'accepteur sont tous deux titulaires d'un compte ouvert auprès de PayPal.[116] C'est l'hypothèse où la réception de la monnaie électronique implique un système de comptabilité centralisée auprès de l'émetteur de la monnaie électronique. Cette approche, bien que limitante, reflète pourtant les exigences caractéristiques intrinsèques de la monnaie électronique, notamment la nécessité que tout détenteur de monnaie électronique, payeur ou bénéficiaire, soit lié par contrat à l'émetteur de monnaie électronique et que la monnaie électronique circule entre les supports de monnaie électronique conformément aux règles définies par l'émetteur. Le support de monnaie électronique, physique ou dématérialisé, n'aurait pas les fonctionnalités caractéristiques d'un compte de paiement.

2.4 - Recommandations du HCJP

Fusion, ou non, la priorité serait de redéfinir la monnaie électronique, pour que l'on sache enfin de quoi l'on parle et ce que l'on veut en faire.

Recommandation n° 2 : le HCJP recommande que la notion de monnaie électronique soit reconsidérée, non seulement parce que la définition actuelle demeure absconse, mais encore pour qu'elle puisse servir aux innovations en cours, notamment concernant les crypto-actifs, mais plus largement les nouvelles « *chaînes de valeur du paiement* ».

Dès lors qu'un consensus en faveur d'une fusion entre DME2 et DSP2 semble se dégager, encore importe-t-il de s'entendre sur le champ (tout ou partie du droit de la monnaie électronique) ainsi que la nature de cette fusion (seulement technique ou recomposant le droit des services de paiement et de la monnaie électronique).

Cette opportunité permettrait également de fusionner les agréments des EP et des EME, corrigeant par-là les trop nombreux arbitrages règlementaires qui aboutissent, à l'heure actuelle, à ce que certains pays (exemples : Lituanie, Malte, etc.) soient les champions de la monnaie électronique, sans autre raison apparente que d'être très accueillants aux EME.

[116] *Voir infra paragraphe 7.1.2. (Compte spécifique de monnaie électronique et compte de paiement).*

Recommandation n° 3 : le HCJP recommande : (i) d'abord que la fusion permette de réunir, en un seul corps de règles figurant dans un texte unique, l'ensemble du régime commun à la monnaie électronique et aux services de paiement (droit des opérations de paiement et des contrats de services de paiement) ; et (ii) ensuite qu'une seule et même catégorie de prestataires de services de paiement soit créée (les « *établissements de paiement et de monnaie électronique* » ou « EPME ») soumise à des dispositions prudentielles, de protection de la clientèle, etc., communes, sous réserve de quelques éventuelles exceptions (capital minimum, remboursement de la monnaie électronique, etc.).

Il s'avère que les modèles économique et juridique de la monnaie électronique oscillent entre moyen de paiement universel (*prepaid cards*) ou, au contraire, système fermé de paiement entre affiliés. Est-il concevable de conserver ces deux usages avec un régime commun indifférencié ? Faut-il au contraire les distinguer clairement et leur destiner des règles particulières (par exemple, un régime d'anonymat limité à la monnaie électronique en circuit fermé) ? À quoi s'ajoute une problématique de fond, dès lors que la jurisprudence *Paysera* a consacré la remboursabilité de la monnaie électronique comme caractère substantiel : comment assurer-celle-ci au sein d'un réseau d'acceptation universel ?

Recommandation n° 4 : le HCJP recommande qu'une clarification soit faite entre le modèle ouvert de monnaie électronique universelle et entre le modèle de monnaie électronique fermée fonctionnant en système de paiement exclusivement entre affiliés, sous peine sinon de maintenir le flou entre services de paiement et monnaie électronique ou de se heurter à des difficultés pratiques (par exemple : remboursement) insurmontables.

Le « *support* », la « *forme* » dans laquelle la valeur monétaire constituée par la monnaie électronique est stockée mérite qu'elle soit éclaircie, ce que n'ont pas fait la DME1 ni la DME2.

Recommandation n° 5 : le HCJP recommande que le futur texte contienne une définition du support de la monnaie électronique, pour deux raisons au moins : (i) la première concerne le fait que la monnaie électronique est souvent confondue avec le support (carte ou compte de paiement) qui la stocke, nuisant par-là à son identification et à sa qualification ; et (ii) la seconde est tournée vers l'avenir et suggère une définition du support de monnaie électronique propre à embrasser les futurs jetons de monnaie électronique (e-money tokens) du Règlement MiCA.

III. Champ d'application territorial de la DSP2

3.1 - Enjeux liés à la question

L'identification de la localisation du service de paiement (et, en particulier, la question de savoir à partir de quel moment on doit considérer qu'un service de paiement est fourni ou non sur le territoire d'un État membre de l'Union européenne donné) soulève un certain nombre de difficultés en raison du fait qu'un tel service correspond la plupart du temps à des prestations immatérielles, délocalisées et/ou fournies à distance. La situation est d'autant plus critique qu'elle s'accompagne d'une digitalisation croissante des services financiers.

Les enjeux de la localisation des services de paiement sont pour autant réels et se posent à deux niveaux :

(i) dans le contexte de services intra-communautaires : en relation avec les passeports européens, la question de savoir si un service de paiement est fourni sur une base transfrontalière au sein d'un État membre est cruciale afin de déterminer si un tel service requiert le passeport libre établissement, le cas échéant, ou libre prestation de services ;

(ii) dans le contexte de services fournis par un prestataire de pays tiers : la question se pose de savoir si un service de paiement fourni par un prestataire de pays tiers à un utilisateur (autrement dit, un client) domicilié dans un État membre est soumis aux règles de la DSP2 et, partant, déclenche l'obligation pour ce prestataire d'obtenir un agrément[117]. Formulée autrement, la question se pose de savoir si le simple fait que le client soit domicilié dans le territoire de l'Union suffit à considérer que, en l'absence de tout autre lien de rattachement géographique, de tels services sont fournis sur le territoire de l'Union européenne et sont justiciables des dispositions de la DSP2. L'enjeu de cette détermination est particulièrement important du fait que, dans certains États membres comme la France, des sanctions pénales résultant de la violation des monopoles, dont celui relatif aux services de paiement.[118] Il convient également de noter que, dans ce cas de figure, l'application ou non du cadre posé par la DSP2 à un prestataire donné engendre des conséquences allant au-delà de la question de l'agrément, puisque c'est l'applicabilité des règles matérielles de la DSP2 elles-mêmes (et donc la protection de l'utilisateur des services de paiement) qui est en jeu. Or une telle hypothèse n'est pas théorique. On peut par exemple évoquer le cas d'un expatrié ayant

[117] *En qualité d'établissement de paiement, de crédit, voire de monnaie électronique.*

[118] *Voir article L. 521-2 du CMF.*

ouvert un compte à l'étranger qui, une fois revenu dans son pays d'origine n'a pas clôturé son compte et continue de l'utiliser (par exemple, pour continuer de rembourser un emprunt immobilier sur place, payer les charges afférentes à son appartement, etc.). Au-delà de cette situation anecdotique, de nombreuses entreprises ayant des activités à l'étranger ouvrent généralement des comptes à l'étranger pour les besoins de leurs activités internationales, afin d'accéder à des liquidités et devises (par exemple, en dollars) auprès de banques étrangères n'ayant pas d'établissement réglementés au sein de l'Union. Parfois également les banques situées dans l'Union peuvent avoir recours à des banques correspondantes, établies dans des pays tiers pour le compte de leur client. Dans tous ces cas, la banque de pays tiers est susceptible de fournir un ou plusieurs services de paiement au client domicilié dans un État membre. Pour autant doit-on considérer que la banque étrangère se met en infraction avec la DSP notamment en termes d'obligation d'agrément en tant que PSP ? La problématique de la détermination de la localisation de la fourniture des services de paiement au sein de l'Union européenne a, par exemple, été mise en exergue récemment avec le Brexit s'agissant des contrats de prestation de services de paiement conclus avant le Brexit mais se poursuivant après celui-ci. Si la validité de ces contrats, appréciée au moment de leur conclusion intervenue avant le Brexit n'avait pas été remise en question, leur exécution intervenant après le Brexit (et donc, la perte du passeport européen) a pu soulever des difficultés.[119] Les situations pratiques européennes ci-dessus ont fait l'objet d'analyses de la part du HCJP. En particulier dans les cas des comptes bancaires/comptes de paiement et des banques correspondantes, le HCJP a considéré que les services règlementés (réception des dépôts, services de paiement, etc.) n'étaient pas fournis sur le territoire de l'État membre dans lequel le client est domicilié.[120]

3.2 - Quel est le régime juridique actuel ?

La revue des règles de droit positif applicables en matière de services de paiement, que ce soit au niveau européen (ou des États membres) conclut à une absence de critères clairs permettant de localiser la fourniture d'un service de paiement. Les pratiques de supervision, quant à elles, varient d'un État membre à un autre, conduisant alors à une application disparate des règles découlant de la DSP2.

[119] *Avis de l'Autorité bancaire européenne sur les questions liées au départ du Royaume-Uni de l'Union européenne, 12 octobre 2017, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1756362/81e612c6-dcab-4c4b-87e9-32784cb44de1/EBA%20Opinion%20on%20Brexit%20Issues%20%28EBA-Op-2017-12%29.pdf?retry=1 ; L'ABE appelle les institutions financières à finaliser les préparatifs en vue de la fin des dispositions transitoires entre l'UE et le Royaume-Uni, 29 juillet 2020, https://www.eba.europa.eu/eba-calls-financial-institutions-finalise-preparations-end-transitional-arrangements-between-eu-and.*

[120] *HCJP, Rapport sur le Brexit, activités bancaires et de services d'investissement, 15 octobre 2018, https://www.banque-france.fr/sites/default/files/rapport_20_f.pdf.*

3.2.1 - Dans la DSP2

Si la DSP2 précise expressément son application territoriale, pour autant, elle ne fixe aucun critère permettant de déterminer précisément à quel moment un service de paiement doit être considéré comme étant fourni au sein de l'Union européenne ou sur le territoire d'un État membre donné.

C'est ainsi que l'article 2.1 de la DSP2 fixant son champ d'application se contente d'indiquer ce qui suit : « *La présente directive s'applique aux services de paiement fournis au sein de l'Union* ».

Les articles 2.2 à 2.4 de la DSP2 envisagent indirectement l'hypothèse de la fourniture d'un service de paiement par un prestataire de service de paiement hors de l'Union européenne, mais uniquement par référence à la situation où l'autre prestataire est situé au sein de l'Union européenne dans le but de déterminer le champ d'application de certaines règles. Par exemple, lorsqu'un consommateur résident de l'Union règle ses achats à un marchand établi dans un pays tiers à l'Union, le prestataire de service de paiement du marchand, généralement lui-même établi dans le pays du marchand (le PSP accepteur), fournit le service de paiement au marchand de pays tiers (transaction « *one leg out* »). Inversement, lorsqu'un consommateur résident de pays tiers règle ses achats auprès d'un marchand établi sur le territoire de l'Union, le prestataire de service de paiement du consommateur (PSP payeur) de pays tiers fournit le service de paiement au consommateur hors de l'Union. Dans les deux cas de figure, le prestataire de service de paiement du résident de l'Union dans le premier exemple et le prestataire de service de paiement du marchand établi dans l'Union dans le second exemple, fournissent le service de paiement dans l'Union. L'élément transfrontalier dans ces deux exemples est le flux de paiement qui transite d'un compte de paiement envers l'autre (et non pas la fourniture du service de paiement, qui reste de nature domestique).[121] Pour autant, le texte ne règle pas la question de savoir à partir de quel moment un service de paiement doit être considéré comme étant fourni par un prestataire de pays tiers à un utilisateur de services de paiement sur le territoire d'un État membre de l'Union européenne.

3.2.2 - Dans la législation des États membres

Dans les législations des État-membres consultés, il apparaît qu'il n'existe aucune disposition de nature normative (loi, règlement, arrêté, etc.) posant des règles de rattachement au territoire concerné. On peut cependant constater que dans plusieurs États membres (Italie, Espagne et France),

[121] *Voir ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 juin 2022.*

la règle de la sollicitation est retenue par les autorités de supervision. D'autres pays, tels que l'Espagne et le Luxembourg, est également pris en compte le lieu de la localisation de la prestation caractéristique ou encore la localisation du compte de paiement (Allemagne).

Comme cela a été démontré dans le rapport précité du HCJP relatif au Brexit, la question du champ d'application territorial des règles de monopole n'intéresse pas uniquement la DSP. D'autres règlementations sectorielles sont concernées. Il est donc intéressant de comparer ces textes afin de vérifier si une telle question y reçoit une réponse adaptée.

3.2.3 - Comparaison avec d'autres textes sectoriels européens

Concernant les autres services financiers, la question semble se poser en des termes similaires. En effet, alors que la localisation des autres services financiers soulève les mêmes enjeux (relatifs au passeport et à l'agrément), les autorités de supervision européennes notent elles-mêmes qu'aucune définition de la fourniture de services transfrontalière n'est retenue dans aucun des textes de niveau 1 revus.[122] Elles soulignent sur ce point une absence de critères clairs permettant de déterminer le lieu où le service est fourni, alors que la question est clé.[123]

S'il faut mentionner la directive 2002/65/CE du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs qui couvre la fourniture transfrontalière des services financiers, ce texte ne permet pas pour autant de déterminer le moment à partir duquel il conviendrait de considérer qu'un service financier est fourni sur le territoire de l'Union ou d'un État membre donné.

Cela étant dit, il apparait utile de considérer le régime de pays tiers qui est prévu par le paquet MiFID/MiFIR. Ce régime élude la question de la territorialité analysée sous l'angle de critères matériels objectifs de rattachements géographiques (analyse multicritère reposant principalement sur les prestations caractéristiques du service afin de déterminer le lieu où cette prestation est exécutée), qui a pu être considéré comme étant non pertinent dans le contexte de la fourniture de services d'investissement transfrontaliers,[124] en prévoyant un mécanisme juridique alternatif

[122] *Joint Committee of the European Supervisory Authorities, « Report on the cross-border provision of financial services », 9 juillet 2019, JC/2019-22, par. 66 : « there is no definition of cross-border provision of financial services in any of the Level 1 texts reviewed. »*

[123] *Joint Committee of the European Supervisory Authorities, op. cit., par. 66.*

[124] *Comité des établissements de crédit et des entreprises d'investissement (CECEI), « The freedom to provide services in the area of investment services », 20 novembre 1998, spéc. p. 3. Certes dans, le contexte de la fourniture de services transfrontaliers au titre du passeport (mais le raisonnement s'applique aussi bien dans le cadre de services fournis depuis un pays tiers).*

reposant sur la sollicitation inversée (voir Annexe V). D'autres textes récents contiennent des dispositions relatives aux services fournis par des entreprises de pays tiers.

De l'analyse d'autres textes sectoriels européens mentionnés dans le tableau ci-dessus, on notera avec intérêt que les textes récents (ou projets de textes) suivent la voie ouverte par le paquet MiFID/MiFIR en appliquant le régime de la sollicitation inversée (Règlement MiCA et CRD6). En revanche, les solutions retenues pour EMIR, CSDR et AIFMD sont spécifiques aux services réglementés par ces textes et leurs solutions ne semblent pas transposables au cas des services de paiement.

3.3 - Options disponibles

Si l'on souhaite que la DSP incorpore des dispositions spécifiques permettant de déterminer selon quels critères la fourniture d'un service de paiement frontalier déclenche l'obligation d'agrément, plusieurs options sont disponibles.

3.3.1 - Lieu d'exécution de la prestation caractéristique

Applications	Description	Avantages	Inconvénients
Services bancaires. Le lieu d'exécution de la prestation caractéristique a été retenu en matière bancaire par la jurisprudence et préconisé par le HCJP dans le contexte spécifique du Brexit pour ce qui concerne les services de paiement (plus particulièrement, s'agissant de l'ouverture et du fonctionnement des comptes de paiement).[125]	Cette approche consiste à retenir le lieu de l'exécution de la prestation caractéristique (*characteristic performance*) comme critère déterminant de la localisation géographique d'un service. En application d'une analyse multicritères de localisation géographique de l'exécution de la prestation caractéristique, un service de paiement	Sécurité juridique reposant sur l'identification de critères objectifs. Approche adaptée à une clientèle professionnelle ou institutionnelle disposant d'implantations à l'étranger ou ayant une activité tournée vers l'étranger.	Approche potentiellement inadaptée à des services dématérialisés. En matière de services de paiement, cette approche pourrait conduire à considérer que, lorsque le service de paiement est fourni à partir d'un compte de paiement et que le compte de paiement est tenu au siège du prestataire de pays tiers, alors le service serait systématiquement

[125] *HCJP, « Rapport sur le Brexit, activités bancaires et de services d'investissement », 15 octobre 2018, p. 22. Dans ce rapport, le groupe de travail a considéré que, s'agissant des contrats de « correspondent banking » les prestations accomplies par l'entité située au Royaume-Uni ne devraient pas tomber dans le champ d'application géographique des monopoles bancaire et de la prestation de services de paiement, permettant ainsi la continuité de l'exécution de ce contrat post-Brexit et qu'en l'absence de jurisprudence, la même approche devrait s'appliquer s'agissant de l'ouverture et du fonctionnement d'un compte de paiement.*

	donné ne devrait ainsi pas être considéré comme fourni sur le territoire de l'Union européenne ou d'un Etat membre donné si la prestation caractéristique du service est localisée en dehors de ce territoire. La détermination de ce lieu d'exécution de la prestation caractéristique pourrait tenir compte d'un certain nombre de critères en fonction du service de paiement concerné (tels que la localisation du compte de paiement, le lieu où les moyens de paiement sont émis et mis à disposition, etc.), lesquels devraient en principe pointer vers le lieu d'établissement du prestataire de services de paiement.[126]		fourni hors du territoire de l'UE[127] Par ailleurs, dans le cas de services de paiement qui ne sont pas fournis en relation avec un autre service de paiement (c'est à dire service n° 6, 7 et 8), l'approche reposant sur la prestation caractéristique ne parait pas adaptée, car les seuls critères objectifs seront limités au pays de résidence du prestaire et de son client (les autres critères, tels que le lieu de conclusion de contrat, ne conviennent pas vraiment à des contrats conclus en ligne[128]

[126] *Voir sur ce point, notamment HCJP, « Rapport relatif à l'accessibilité du marché français par les établissements bancaires et financiers britanniques dans un environnement post-Brexit », 7 novembre 2017, p. 13.*

[127] *Ici le même reproche a été fait en matière de services d'investissement c.f. supra.*

[128] *Peut également donner lieu à des stratégies de contournement en localisant artificiellement les caractéristiques du service ou de l'opération hors du territoire de l'UE Cela dit, si le rattachement à un territoire donné apparait comme artificiel, il est probable que le juge rejette un tel rattachement.*

3.3.2 - Sollicitation du client

Applications	Description	Avantages	Inconvénients
Approche retenue par MiFID/MiFIR, MiCA et CRD 6 par application inversée de l'exception dite de « sollicitation inversée ».	Cette approche consiste à mettre l'accent sur le lieu où le client a été sollicité. Ainsi, dès lors qu'un prestataire de services de paiement sollicite un client sur le territoire de l'Union, que ce soit directement ou par l'intermédiaire d'un tiers agissant pour son compte, le service de paiement devrait être considéré comme étant fourni sur ce territoire, et cela indépendamment du fait que la prestation caractéristique du contrat ait lieu en dehors de l'Union. À l'inverse, dans l'hypothèse où la relation d'affaires avec le prestataire de services de paiement de pays tiers et la fourniture de services de paiement en découlant par la suite serait nouée à	Critère objectif et prévisible, et conforme à l'idée que le régime de protection du client ne vise pas à lui interdire d'accéder à des services fournis depuis l'étranger. Critère adapté à une clientèle professionnelle ou institutionnelle qui recherche la fourniture de services de paiement par des prestataires de pays tiers dans le cadre de ses activités internationale (accès aux systèmes de paiement/changes étrangers, solutions de gestion de trésorerie internationale, etc.) Cette approche aurait l'avantage de contribuer à un régime de pays tiers harmonisé trans-sectoriel, notamment par l'élaboration d'une	Risque de contournement par l'usage de clauses contractuelles standard (risque toutefois atténué par la doctrine de l'AEMF dans le cadre de MiFID/MiFIR). Solution peu adaptée à une clientèle de détail. Difficulté d'apporter la preuve de l'initiative exclusive du client.

	l'initiative exclusive du client (*reverse solicitation*), sans aucune sollicitation préalable par le prestataire sur le territoire concerné, ces services de paiement seraient considérés comme étant fournis en dehors de l'Union quand bien même la prestation caractéristique du contrat aurait, elle, lieu au sein de l'Union.	doctrine par le comité conjoint des ESA.	

3.3.3 - Domicile du client

Applications	Description	Avantages	Inconvénients
Approche retenue par EMIR, conformément à l'interprétation retenue par la Commission européenne. Position implicitement retenue par l'ABE dans son communiqué de presse sur les conséquences du Brexit concernant la fourniture de services de paiement et de services de monnaie électronique.[129]	Le simple fait que le client soit domicilié dans l'Union suffit à déclencher l'obligation d'agrément de la part du prestataire de pays tiers fournissant un service transfrontalier depuis son siège.	Critère *a priori* simple à mettre en œuvre et prévisible. Très protecteur et adapté à une clientèle de détail.	Critère inadapté à une clientèle professionnelle ou institutionnelle qui recherche la fourniture de services de paiement par des prestataires de pays tiers dans le cadre de ses activités internationales. Une telle approche aurait surtout pour conséquence pour une

[129] *Communiqué de presse de l'ABE, « L'ABE appelle les institutions financières à finaliser les préparatifs en vue de la fin des dispositions transitoires entre l'UE et le Royaume-Uni », 29 juillet 2020.*

Applications	Description	Avantages	Inconvénients
Approche retenue par MiFID/MiFIR, MiCA et CRD 6 par application inversée de l'exception dite de « sollicitation inversée ».	Cette approche consiste à mettre l'accent sur le lieu où le client a été sollicité. Ainsi, dès lors qu'un prestataire de services de paiement sollicite un client sur le territoire de l'Union, que ce soit directement ou par l'intermédiaire d'un tiers agissant pour son compte, le service de paiement devrait être considéré comme étant fourni sur ce territoire, et cela indépendamment du fait que la prestation caractéristique du contrat ait lieu en dehors de l'Union. À l'inverse, dans l'hypothèse où la relation d'affaires avec le prestataire de services de paiement de pays tiers et la fourniture de services de paiement en découlant par la suite serait nouée à	Critère objectif et prévisible, et conforme à l'idée que le régime de protection du client ne vise pas à lui interdire d'accéder à des services fournis depuis l'étranger. Critère adapté à une clientèle professionnelle ou institutionnelle qui recherche la fourniture de services de paiement par des prestataires de pays tiers dans le cadre de ses activités internationale (accès aux systèmes de paiement/changes étrangers, solutions de gestion de trésorerie internationale, etc.) Cette approche aurait l'avantage de contribuer à un régime de pays tiers harmonisé trans-sectoriel, notamment par l'élaboration d'une	Risque de contournement par l'usage de clauses contractuelles standard (risque toutefois atténué par la doctrine de l'AEMF dans le cadre de MiFID/MiFIR). Solution peu adaptée à une clientèle de détail. Difficulté d'apporter la preuve de l'initiative exclusive du client.

3.4 - Recommandations du HCJP

Le critère de la sollicitation du client domicilié dans un État membre de l'Union est un critère simple à mettre en œuvre et il est protecteur de la clientèle, notamment non professionnelle. Ce critère est également cohérent avec les régimes de pays tiers des textes sectoriels récents. Ce sont les raisons pour lesquelles le HCJP recommande de retenir la sollicitation du client domicilié dans l'Union comme critère de rattachement territorial pour la révision de DSP2.

Recommandation n° 6 : le HCJP recommande de retenir la sollicitation du client dans l'Union européenne comme critère de rattachement territorial pour la révision de DSP2.

IV. Chambre d'application matériel de la DSP2 - Encaissement de fonds pour le compte de tiers

4.1 - Enjeux liés à l'inclusion de l'encaissement de fonds pour le compte de tiers dans le champ de la DSP

Traditionnellement, on connaissait l'activité de recouvrement amiable de créances pour compte d'autrui, encadrée par quelques règles depuis 1996[130]. Avec l'essor du commerce en ligne (les *marketplaces*), des plateformes de financement participatif et celles d'échange d'actifs numériques, cette activité est sortie de son terrain naturel pour être poursuivie de façon informelle par ces plateformes internet qui encaissent ou collectent des fonds pour le compte de leurs utilisateurs (par exemple, pour un achat de biens réalisé sur une plateforme de commerce en ligne, le consommateur verse le prix entre les mains de cette dernière, laquelle le reversera au marchand).

Or, dans la foulée de l'entrée en vigueur de la DSP en 2009 la question s'est posée de savoir si cette activité pouvait être justiciable de cette directive.[131] Question à laquelle l'ACPR[132] et la jurisprudence[133] y ont répondu positivement.

En effet, bien qu'elle ne constitue pas, en tant que telle, un service de paiement au sens de la DSP, ni ne fait l'objet de dispositions spécifiques dans cette directive (ni dans le CMF), l'activité d'encaissement pour le compte de tiers peut, selon l'ACPR, impliquer la fourniture d'un ou plusieurs des services de paiement mentionnés à l'article L. 314-1 du CMF. Elle a précisé, à propos des *marketplaces*, qui encaissent auprès des acheteurs dans un premier temps des sommes pour le compte des marchands, qu'elles reversent dans un second temps auxdits marchands, le cas échéant

---

*[130] Décret n° 96-1112 du 18 décembre 1996 portant réglementation de l'activité des personnes procédant au recouvrement amiable des créances pour le compte d'autrui. À présent codifié dans le Code des procédures civiles d'exécution (« **CPCE** »), aux articles L.124-1 et R. 124-1 à R. 124-7.*

[131] P. Storrer, « L'encaissement de fonds pour le compte de tiers vaut-il fourniture de services de paiement ? », Revue Banque n° 777, novembre 2014, p. 86.

[132] « La régulation des nouveaux intervenants du marché des services de paiement », Revue de l'ACPR n° 21, janvier-février 2015, p.6. Voir également, site internet de l'ACPR : « Qualifier mon activité », question 5 : « Dès lors que j'encaisse des fonds, quel statut dois-je adopter ? », et ACPR et AMF, « S'informer sur le nouveau cadre applicable au financement participatif (crowdfunding) », 30 septembre 2014 et mises à jour les 26 août 2016 et 9 mai 2017 (les entreprises opérant une plateforme de financement participatif doivent, lorsqu'elles encaissent des fonds, être agréées en qualité d'établissement de paiement ou être enregistrées en tant qu'agent de prestataire de services de paiement).

[133] À propos d'une plateforme d'échange de Bitcoins : CA Paris 26 septembre 2013, n° 12/00161, SAS Macaraja c/ SA Crédit Industriel et Commercial.

déduction faite de leur commission, que leur activité pouvait relever de la fourniture de deux services de paiement : d'une part, l'acquisition d'ordre de paiement[134] et, d'autre part, l'exécution d'opération de virement associée à la gestion d'un compte de paiement,[135] voire le service de transmission de fonds (en l'absence de compte de paiement ouvert au nom du payeur ou du bénéficiaire dans les livres de la plateforme)[136]. Par conséquent, selon l'ACPR, des services de paiement sont fournis par le prestataire si les fonds sont, d'une part, collectés ou réceptionnés sur un compte de paiement appartenant au prestataire et, d'autre part, encaissés par le prestataire pour le compte d'un tiers (en d'autres termes, le prestataire ne reçoit pas des fonds pour lui-même, mais en qualité d'intermédiaire dans le but de les reverser à leur véritable destinataire). Dès lors, *a contrario*, si l'une des conditions vient à manquer, alors aucune fourniture de paiement ne devrait être caractérisée.[137]

Dès lors, seuls un texte législatif spécial prévalant sur les dispositions de la DSP transposées dans le CMF ou une dérogation expressément prévue par la DSP[138] peuvent permettre d'écarter l'application de la réglementation des services de paiement.[139] Ou encore, alternativement, le prestataire peut conclure un partenariat avec un PSP et se faire enregistrer comme agent de ce PSP (APSP).[140]

Cette approche a été vivement critiquée en doctrine,[141] d'autant qu'à l'époque, ni l'ABE, ni aucune autre autorité nationale compétente en matière de services de paiement dans un autre État membre

---

[134] Service n° 5 de l'Annexe I de la DSP2 et article L. 314-1, I, 5° du CMF.

[135] Service n° 3(c) de l'Annexe I de la DSP2 et article L. 314-1, I, 3°(c) du CMF. On notera la différence subtile de rédaction entre le texte de transposition français et celui de la version française de la directive, qui n'existe pas dans les transpositions francophones de la DSP2 (en Belgique et au Luxembourg). La transposition française semble pouvoir donner un champ d'application beaucoup plus large à ce service de paiement.

[136] Article L. 314-1, II, 6° du CMF. Voir également, « La régulation des nouveaux intervenants du marché des services de paiement », Revue de l'ACPR, ibid.

[137] « La régulation des nouveaux intervenants du marché des services de paiement », Revue de l'ACPR, ibid.

[138] Il s'agit de l'exclusion relative à l'agent commercial (article 3(b) de la DSP, transposée à l'article 314-1, III, 3° du CMF) et de l'exemption relative au réseau limité d'accepteurs ou à l'éventail limité de biens ou services (article 3(k) de la DSP2, complété par des « Orientations sur l'exclusion relative aux « réseaux limités » au titre de la DSP2 » publiée par l'ABE le 24 février 2022 (EBA/GL/2022/02) et Position 2022-P-01 ayant été publiée par l'ACPR le 20 juillet 2022 concomitamment à sa notice de conformité aux Orientations de l'ABE, en remplacement de la Position 2017-P-01).

[139] Ainsi, selon l'ACPR, il s'agit de certains textes législatifs qui donnent à des professions particulières comme les avocats, les notaires, les agents immobiliers ou encore les agents de voyage un cadre juridique ad hoc pour encaisser des fonds pour le compte de tiers. En l'absence d'un texte spécifique, seule une exclusion ou une exemption d'agrément prévue par la DSP permet la poursuite de l'activité sans agrément : l'exclusion relative aux agents commerciaux, ou l'exemption relative aux réseaux limités ou à l'éventail limité de biens et services.

[140] Spéc. article 19 de la DSP2, transposé aux articles L. 523-1 et s. du CMF.

[141] M. Roussille, « Marketplaces et services de paiement : jusqu'où ira l'impérialisme de l'ACPR ? », Revue de droit bancaire et financier, novembre-décembre 2014, focus 23 et T. Bonneau, « Une société qui utilise un compte bancaire sur lequel transitent des bitcoins est-elle un prestataire de service de paiement ? », JCP E n° 8, 20 février 2014, 1091.

ne s'étaient officiellement prononcées sur cette question.[142]

Au surplus, comme l'ACPR l'indique elle-même, cette approche dépasse le seul cadre des plateformes internet et a ainsi vocation à englober toute situation dans laquelle une personne poursuit une activité d'encaissement pour compte de tiers[143]. Ce sera le cas par exemple d'une société de financement[144] qui, dans le cadre de la syndication de ses financements, agirait comme agent du crédit pour le compte du syndicat. Le cas de l'agent des sûretés, agissant pour le compte des créanciers qui l'ont désigné pour prendre, inscrire, gérer et réaliser des sûretés garantissant leurs créances, et amené à encaisser pour leur compte le produit de l'exécution des sûretés, pose certainement question. Les dispositions des articles 2488-6 et suivants du Code civil,[145] qui n'imposent aucune condition tenant au statut – règlementé ou non – de l'agent, constituent-elles un texte législatif spécial prévalant sur la DSP ? Ou alors le fait que l'agent des sûretés agit en son propre nom (et non au nom des créanciers) pour les besoins de la réalisation des sûretés – et donc de l'encaissement de fonds qui s'ensuit –,[146] suffit-il à considérer qu'il n'agit pas comme simple intermédiaire et échappe donc aux prévisions de la DSP ?

De manière moins anecdotique, la question du statut des sociétés de recouvrement de créances devrait également se poser. En effet, leur profession n'est pas, en tant que telle, règlementée, seule l'activité de recouvrement de créance pour compte d'autrui l'étant par le CPCE.[147] Mais le cadre posé par ce code est ouvert à toute personne, y compris agissant à des fins non professionnelles, occasionnelles ou accessoires : « *L'activité des personnes physiques ou morales non soumises à un statut professionnel qui, d'une manière habituelle ou occasionnelle, même à titre accessoire,*

---

[142] *Voir ci-après, paragraphe 4.2.2.*

[143] *« La régulation des nouveaux intervenants du marché des services de paiement », Revue de l'ACPR, ibid.*

[144] *Agréée par l'ACPR (article L. 511-1-II du CMF) pour la réalisation d'opérations de crédit à titre habituel et pour compte propre (article L. 511-10-II du CMF). Pour fournir des services de paiement, une société de financement doit obtenir, en complément, un agrément en qualité d'établissement de crédit, ou être agréée en complément comme établissement de paiement.*

[145] *L'hypothèse de l'encaissement pour compte de tiers n'est pas expressément prévue par ces dispositions, mais découle nécessairement de l'autorité donnée à l'agent de réaliser les sûretés pour le compte des créanciers (voir Fédération nationale de l'information d'entreprise, de la Gestion des créances et de l'enquête civile, « Activité de recouvrement de créances » : aucune mention n'est faite à la DSP2). Également : https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/recouvrement-creances.*

[146] *Étant précisé que les fonds ainsi encaissés forment un patrimoine affecté à la mission de l'agent, distinct de son patrimoine propre (article 2488-6 du Code civil) et doivent être reversés par l'agent aux créanciers l'ayant désigné.*

[147] *Cf. supra, note de bas de page n° 130. D'ailleurs, c'est bien comme cela que les professionnels du recouvrement de créances comprennent leurs obligations réglementaires (FIGEC, « Le recouvrement de créances, enjeux et perspectives », Livre Blanc, novembre 2014, spéc. p. 19). V également, DGCCRF, « Recouvrement amiable, les règles à connaître » (https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/recouvrement-creances).*

procèdent au recouvrement amiable des créances pour le compte d'autrui, s'exerce dans des conditions fixées par décret en Conseil d'État. » L'articulation entre ce texte et la DSP est incertaine car le CPCE ne constitue à l'évidence pas un texte législatif spécial prévalant sur les dispositions de la DSP puisqu'il pose un cadre général auxiliaire applicable à défaut de tout statut professionnel. Dès lors, les dispositions du CPCE et celles de la DSP semblent avoir le même objet, à savoir encadrer l'activité d'encaissement de fonds pour le compte de tiers lorsqu'elle ne relève pas d'un statut professionnel réglementé.[148]

Au surplus, l'application des règles de la DSP2 à l'activité d'encaissement pour le compte de tiers devra s'articuler avec celles découlant de la directive gestionnaire de crédit, dont la transposition en France est attendue pour le 29 décembre 2023.[149] Cette directive encadre en effet les activités de gestion de crédits, qui incluent, notamment, « la perception ou le recouvrement auprès de l'emprunteur, conformément au droit national, des paiements dus liés aux droits d'un créancier au titre d'un contrat de crédit ou au contrat de crédit lui-même »[150] et soumet les gestionnaires de crédit à une obligation d'agrément.[151]

Les enjeux liés à la soumission de l'activité d'encaissement de fonds pour le compte de tiers sont nombreux et importants au regard des conséquences qui découlent de l'application de la DSP2. On peut mentionner :

(i) l'obligation d'agrément (en qualité d'établissement de paiement, de crédit, ou éventuellement, de monnaie électronique) ; et

(ii) lorsque le prestataire est considéré comme tenant un compte de paiement au nom du créancier (lorsque le service n° 3 de l'Annexe I de la DSP2 est identifié), l'obligation d'appliquer l'authentification forte (SCA) du titulaire du compte,[152] ainsi que la facilitation de la fourniture des services d'informations sur les comptes et d'initiation de paiement sur les comptes[153], (l'*open*

[148] *On remarquera au passage que l'ACPR ne cite pas ces dispositions parmi celles qui pourraient prévaloir sur celles de la DSP (voir supra note de bas de page n° 132).*

[149] *Directive (UE) 2021/2167 du Parlement européen et du Conseil du 24 novembre 2021 sur les gestionnaires de crédits et les acheteurs de crédits, et modifiant les directives 2008/48/CE et 2014/17/UE.*

[150] *Article 3(9).*

[151] *Article 4(1).*

[152] *Article 97(1)(a) de la DSP2.*

[153] *Respectivement, services n° 8 et 7 de l'Annexe I de la DSP2.*

banking)[154] et le respect des contraintes techniques qui en découlent.[155]

4.2 - Quel est le régime juridique actuel ?

4.2.1 - Dans la DSP2

Comme indiqué auparavant, l'encaissement de fonds pour le compte de tiers ne constitue pas une activité tombant de manière manifeste dans les prévisions de la DSP2. Elle ne constitue en tout état de cause pas un service de paiement figurant dans l'Annexe I de cette directive. Tout au plus est-elle envisagée de manière indirecte par son considérant n° 9, principalement sous l'angle de la transmission de fonds : « *La transmission de fonds est un service de paiement simple généralement basé sur des espèces fournies par un payeur à un prestataire de services de paiement, qui transmet le montant correspondant, par exemple par le biais d'un réseau de communication, à un bénéficiaire ou à un autre prestataire de services de paiement agissant pour le compte d'un bénéficiaire. Dans certains États membres, les supermarchés, les commerçants et autres détaillants fournissent au public un service équivalent leur permettant de régler des factures de services d'utilité publique et d'autres factures régulières du ménage. Ces services de règlement des factures devraient être traités comme une transmission de fonds, à moins que les autorités compétentes ne considèrent que cette activité correspond à un autre service de paiement* ».

Toutefois, postérieurement à la publication de l'ACPR de 2015,[156] l'ABE a, entre 2021 et janvier 2023, publié trois Q&A qui entérinent la position française,[157] et aux termes desquels elle considère que l'encaissement pour le compte de tiers doit être qualifié de service de paiement en vertu de l'article 4(3) de la DSP2 et de son annexe I, sauf application de l'exclusion de l'article 3 de la DSP2 relative à l'agent commercial. L'ABE rappelle que l'activité d'encaissement pour le compte de tiers peut constituer, selon les schémas contractuels et les flux analysés, l'activité de transmission de fonds (article 4(22) de la DSP2, service de paiement n° 6 de l'annexe I de la DSP2), ou tout autre service de paiement, tel que l'acquisition d'opérations de paiement (article 4(44) de la DSP2, service de paiement n° 5 de l'annexe I de la DSP2).[158] Il est donc certain que l'encaissement de

[154] *Articles 66 et 67 de la DSP2.*

[155] *Prévues dans le règlement délégué 2018/349.*

[156] *Voir supra note de bas de page n° 132.*

[157] *ABE, Q&A n° 2020_5216, n° 2020_5355 et n° 2020_5099 (publiées le 6 janvier 2023).*

[158] *On notera avec intérêt que l'ABE ne mentionne pas (mais n'exclut pas) le service n° 3 de l'Annexe I de la DSP2. A notre connaissance, seule l'ACPR identifie en premier lieu ce service (avec le service n° 5 de l'Annexe I de la DSP2) dans le contexte de l'encaissement pour le compte de tiers.*

fonds pour le compte de tiers est un service de paiement selon l'ABE, qui relèvera d'un ou plusieurs des cas prévus par l'annexe I en fonction des circonstances de l'espèce et du type d'activité. Elle retient par ailleurs une interprétation littérale de l'exclusion de l'agent commercial. Cette exclusion ne peut en effet jouer que si l'agent est autorisé par le bénéficiaire à négocier ou conclure la vente de biens ou de services et s'il n'agit pas, aussi, pour le compte du payeur.[159] L'exclusion ne joue donc que dans des cas limités.

Le règlement (UE) du 7 octobre 2020[160] qui pose un cadre juridique harmonisé du financement participatif (*crowdfunding*) dans l'Union, précise pour sa part qu'un prestataire de services de financement participatif qui fournit des services de paiement en lien avec ses services de financement participatif doit également disposer d'un agrément en qualité de PSP.[161]

4.2.2 - Dans la législation des États membres

Une analyse multi juridictionnelle a été conduite dans quatre pays afin de savoir si les États membres en question considèrent que l'activité d'encaissement de fonds pour le compte de tiers relève du champ d'application de la DSP2[162]. *Premier constat* : dans aucun de ces États membres, l'autorité compétente n'a pris officiellement position et aucune jurisprudence n'a été identifiée. *Deuxième constat*, les praticiens semblent considérer que cette activité d'encaissement est susceptible de tomber dans le champ de la DSP2, notamment en raison des Q&A de l'ABE que les autorités nationales compétentes suivront probablement. *Troisième constat*, l'identification précise des services de paiement concernés est très incertaine, quoique le service de transmission de fonds (service n° 6 de l'Annexe I de la DSP2) semble être celui qui s'impose de prime abord.

Le détail de l'analyse multi juridictionnelle se trouve en annexe du présent document.

4.3 - Recommandations du HCJP

En conclusion, il apparait aux membres de travail que, dans le silence des dispositions de DSP et compte tenu de la position exprimée par l'ABE et certaines autorités nationales compétentes telles que l'ACPR, l'activité d'encaissement de fonds pour le compte de tiers devrait être considérée

[159] *ABE, Q&A n° 2020_5355.*

[160] *Règlement n° 2020/1503 du 7 octobre 2020 relatif aux prestataires européens de services de financement participatif pour les entrepreneurs et modifiant le règlement 2017/1129 et la directive 2019/1937.*

[161] *Considérant n° 29 du règlement.*

[162] *Allemagne, Espagne, Italie, Luxembourg et Pologne.*

comme relevant de la prestation de services de paiement selon les prévisions de la DSP. Toutefois le groupe de travail note également le fait que, *d'une part*, cette position reste généralement méconnue des acteurs pratiquant habituellement cette activité ; *d'autre part*, il existe un certain flou quant à la question de déterminer quel(s) services de paiement sont pertinents,[163] en l'absence d'indications suffisamment précises de la part des autorités,[164] notamment au regard des conséquences attachées à la qualification de certains services (en particulier, en termes d'obligations liées à l'*open banking*) qui peuvent paraître disproportionnées eu égard aux objectifs de la DSP2 ; et, enfin, la portée de la position de l'ABE au regard d'activités liées au recouvrement de créance ou à des activités économiques impliquant celle d'encaissement de fonds pour le compte de tiers mais qui n'ont pas vocation à tomber dans le champ de la réglementation sur les services de paiement (le besoin de régulation des intermédiaires poursuivant à ce titre une activité d'encaissement pour le compte de tiers pouvant être assouvi par la mise en place d'un cadre juridique spécifique).

Recommandation n° 7 : le HCJP recommande de (i) clarifier le fait que l'activité d'encaissement de fonds pour le compte de tiers implique la fourniture de services de paiement identifiés, que la qualification soit claire pour les acteurs ; et (ii) donner compétence à l'ABE d'élaborer des normes techniques de réglementation afin de définir dans quelles conditions les services identifiés s'appliquent, incluant des exemples non limitatifs le cas échéant.

Recommandation n° 8 : le HCJP recommande d'indiquer que les États membres peuvent prévoir des exceptions concernant des professions ou des activités identifiées, ce qui supposera, dans le cas de la France, de clarifier la situation notamment de certaines activités professionnelles s'inscrivant dans le cadre du CPCE.

[163] On relèvera à cet égard que, comme le remarque l'ABE, il existe un débat sur la distinction entre deux services de paiement qui paraissent difficile de distinguer l'un de l'autre : le virement associé à un compte de paiement (relevant du service n° 3(c) de l'Annexe I de la DSP2) et la transmission de fonds (service n° 6 de l'Annexe I de la DSP2)(ABE, op. cit., § 5 à 9, pp. 8 et 9.), alors que le premier nécessite l'ouverture d'un compte de paiement, l'autre en fait abstraction, étant entendu que la plasticité de la notion de compte de paiement rend cette distinction plus difficile à appréhender.

[164] On notera les efforts récents de l'ACPR de rendre ses positions plus didactiques notamment au travers de son site internet de l'ACPR : « Qualifier mon activité », question 5 : « Dès lors que j'encaisse des fonds, quel statut dois-je adopter ? ». L'ACPR effectue au demeurant une analyse au cas par cas des modèles présentés.

V. Exclusions du champ de la DSP - Prestataires techniques (PST)

5.1 - Enjeux liés à l'exclusion de la fourniture de prestations techniques du champ de la DSP2

Dans le cadre des services de paiement qu'ils fournissent à leurs clients, de nombreux PSP, ont recours à des prestataires de services techniques (« **PST** ») qui sont souvent des entités non réglementées évoluant dans l'écosystème des services de paiement. La Commission européenne relève que les prestations techniques comprennent, notamment, la maintenance informatique, la mise en place de services d'authentification forte (SCA) ou de passerelles API unifiées et de hubs.[165]

Ces PST peuvent intervenir de manière visible (intervention en « *front-end* ») entre les utilisateurs de services de paiement et le PSP en offrant des solutions technologiques permettant à l'USP de procéder à des paiements en ligne ou sur le lieu de vente (POS) via des terminaux de paiement électroniques. D'autres peuvent également intervenir comme sous-traitants d'un PSP et ne sont pas nécessairement visibles des USP (intervention en « *back-end* »).[166] Quelle que soit la formule, leurs activités sont souvent intrinsèquement liées à la fourniture de services de paiement par les PSP aux utilisateurs de services de paiement et peuvent soulever de nombreux risques liés à leur intervention dans la chaine de paiement. Des risques liés à la protection de la vie privée et des données, à la concurrence et à la cybersécurité peuvent se réaliser du point de vue « *front-end* », tandis que la stabilité financière des acteurs peut être affectée du point de vue « *back-end* ».[167] Un risque d'effet de contagion existe ainsi entre les entités non réglementées (les PST) et les PSP. Par exemple, les problèmes opérationnels et/ou financiers d'un PST pourraient entraîner une suspension de la fourniture des services d'un PSP.[168]

L'introduction de l'*open banking* par la DSP2, au travers de deux nouveaux services de paiement, le service d'initiation de paiement (service n° 7, Annexe 1 de la DSP2)[169] et le service d'information sur les comptes (le service n° 8, Annexe 1 de la DSP2)[170], a encouragé un nombre croissant d'acteurs à intervenir auprès des PSP afin d'offrir des prestations techniques. De fait, bien que les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'information sur les

[165] *DG FISMA, « A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) », FISMA/2021/OP/0002, février 2023, p. 36.*

[166] *DG FISMA, op. cit., p. 104.*

[167] *Ibid.*

[168] *DG FISMA, op. cit., p. 37.*

[169] *En France, article L. 314-1 II n° 7 du CMF.*

[170] *Ibid, article L. 314-1 II n° 8 du CMF.*

comptes (PSIC) entrent désormais dans le champ d'application de la DSP2, de nombreux autres prestataires techniques restent en dehors du champ de la DSP2, alors que, en raison de l'évolution technologique, la frontière entre prestation technique et services de paiement est devenue plus ténue. Cela est d'autant plus vrai que la frontière traditionnelle fixée par la manipulation ou l'entrée en possession de fonds des utilisateurs de services de paiement par les PSP au titre des services de paiement traditionnels sous l'empire de la DSP1 n'est plus pertinente avec les nouveaux services introduits par la DSP2, qui n'impliquent aucune manipulation ou entrée en possession des fonds des utilisateurs de ces services.[171]

L'ABE et la Commission européenne[172] ont identifié un certain nombre de PST dont l'inclusion ou non dans le champ d'application de la DSP2 interroge.[173]

Parmi eux, on peut relever, en particulier, les grandes entreprises de services de technologie telles qu'Apple, Google, Samsung, ou encore Tencent, qui fournissent un service (qualifié d'« *X-Pay* »)[174] consistant à répliquer virtuellement, pour le compte du PSP émetteur, la carte de paiement émise par ce PSP dans le smartphone du client de l'émetteur de la carte.[175] D'autres prestataires de services techniques peuvent également intervenir dans la chaîne de paiement, notamment en fournissant des solutions techniques liées à l'initiation, l'acquisition ou au traitement des ordres de paiement. La frontière entre prestation technique et service de paiement (dont, en particulier, celui de l'initiation de paiement) est devenue poreuse, notamment dans les cas où l'entreprise fournissant la prestation technologique contrôle le processus technique d'initiation de l'ordre de paiement et d'authentification de l'utilisateur du service de paiement.[176] Cette frontière est même rendue plus théorique encore avec la définition d'instrument de paiement telle qu'interprétée par la CJUE.[177] Or, bien que certaines d'entre elles disposent d'entités réglementées autorisées à fournir

---

[171] Au contraire, interdiction est ainsi faite au PSIC de détenir les fonds du payeur en liaison avec la fourniture du service d'initiation de paiement (article 66(3)(a) de la DSP2).

[172] ABE, « EBA's response to the Call for advice on the review of PSD2… », DG FISMA, op. cit.

[173] Payment gateways, digital wallet providers, card payment schemes, processing entities, etc.

[174] Par exemple : ApplePay (https://www.apple.com/fr/apple-pay/), GooglePay (https://pay.google.com/intl/fr_fr/about/), SamsungPay (https://www.samsung.com/fr/apps/samsung-pay/), ou encore WeChatPay (https://pay.weixin.qq.com/index.php/public/wechatpay) qui est limité à une clientèle chinoise.

[175] On parle de tokenisation de la carte, ou encore, de création d'une version numérique de la carte de paiement. Voir DG FISMA, op. cit, p. 104 : « More and more (technical) service providers are engaging in the payment transaction value chain, but are not regulated under PSD2. Card wallets in the form of mobile applications (most often applications supported by Google, Apple, or Samsung) provide an interface for initiating card payment transactions at POI. These services are based on the tokenised card. »

[176] DG FISMA, op. cit., loc. cit.

[177] Voir ci-après.

des services de paiement dans l'Union,[178] ces entreprises fournissent ces services technologiques à partir d'entités ne disposant pas d'un agrément adéquat.

On peut également relever l'existence des systèmes ou schémas de paiement, notamment par carte, tels que Visa ou Mastercard, qui ne semblent pas se limiter à la seule fourniture de services techniques, notamment de communication. En effet, traditionnellement, les schémas de paiement par carte, par exemple, se limitent à faciliter l'échange d'informations entre le PSP accepteur (c'est-à-dire le PSP du client du marchand) et le PSP émetteur de la carte (c'est-à-dire le PSP de l'USP). Or, ces dernières années, de nouveaux services se sont développés[179] lesquels impliquent la fourniture de certains services de paiement.

Ces prestataires ne fournissent-ils pas des services de paiement sous couvert de fourniture de simples services techniques ?

5.2 - Quel est le régime juridique actuel ?

5.2.1 - Prestataires « *front-end* »

Tout d'abord, la DSP2 exclut expressément de son champ les « *services fournis par des prestataires de services techniques à l'appui de la fourniture de services de paiement, sans qu'ils entrent, à aucun moment, en possession des fonds à transférer et consistant notamment dans le traitement et l'enregistrement des données, les services de protection de la confiance de la vie privée, l'authentification des données et des entités, les technologies de l'information et la fourniture de réseaux de communication, ainsi que la fourniture et la maintenance des terminaux et dispositifs utilisés aux fins des services de paiement, à l'exception des services d'initiation de paiement et des services d'information sur les comptes*. »[180] Cette exclusion est rédigée en substance de la même manière[181] que sous l'empire de la DSP1, sous réserve de l'ajout des nouveaux services n° 7 et n° 8 qui viennent restreindre son champ d'application. D'ailleurs, on notera que cette exclusion était prévue substantiellement dans les termes de la DSP1 depuis son origine.[182]

---

[178] *DG FISMA, op. cit., p. 108. On y trouve par exemple Google Payments (deux EME agréés respectivement en Lituanie et en Irlande).*

[179] *Voir par exemple Visa B2B Connect, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16401.html.*

[180] *Article 3(j) de la DSP2, transposé à l'article L. 314-1 III, n° 7 du CMF.*

[181] *Sous réserve de quelques modifications rédactionnelles.*

[182] *Commission européenne, « Proposition de directive du Parlement européen et du Conseil concernant les services dans le marché intérieur, (…) », COM(2005) 603 final, article 3(h).*

Dans le cadre de révision de la DSP1, un problème de frontière avait déjà été soulevé entre, d'une part, certaines prestations techniques consistant à traiter et stocker des données de paiement et à authentifier les données et les entités et, d'autre part, l'acquisition d'opérations de paiement, qui constitue un service de paiement (service n° 5, Annexe 1 de la DSP2).[183] Or, un tel service n'était pas défini dans la DSP1, ni d'ailleurs dans la proposition de DSP2 de la Commission européenne.[184] Dans son avis, la BCE avait donc recommandé l'ajout d'une définition englobant « *la fourniture, au bénéficiaire, de services d'authentification, d'autorisation et d'autres services liés à la gestion des flux financiers, que le prestataire de services de paiement détienne ou non les fonds pour le compte du bénéficiaire* »[185] et donc excluant notamment les services d'authentification du champ de la prestation technique. La définition a été partiellement reprise dans la DSP2 sans les précisions apportées par la BCE.[186] Au contraire même, le considérant n° 10 de cette directive précise « *que le simple fait de traiter et de stocker des données ou la gestion des terminaux* » ne constitue pas le service d'acquisition d'une opération de paiement.

Pour autant, pour bénéficier actuellement de cette exclusion, il ne suffit plus, pour un PST, de se contenter de ne pas entrer en possession des fonds de l'USP, encore faut-il également qu'il ne fournisse pas des services qui pourraient s'apparenter, ou participer, à l'initiation de paiement ou l'information sur les comptes, services qui ne nécessitent pas l'entrée en possession des fonds des USP.

Deux cas méritent d'être analysés.

5.2.1.1 - Cas des entreprises gérant des portefeuilles numériques

Comme indiqué plus haut, des grandes entreprises de services technologiques, telles qu'Apple, Google, Samsung, etc., fournissent des services facilitant les paiements par l'utilisation des téléphones portables par le biais de la numérisation des cartes de paiement (services de type

[183] *On notera au passage un glissement terminologique important entre la DSP1 qui parle d'acquisition d'instrument de paiement, et la DSP2 qui évoque l'acquisition d'opération de paiement.*

[184] *Commission européenne, « Proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, (…) », COM(2013) 547 final.*

[185] *« Avis de la Banque Centrale Européenne du 5 février 2014 sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur (…)», (2014/C 224/01), Modification 12, p. 11. La définition proposée était la suivante : « un service de paiement fourni par un prestataire de services de paiement lié par un contrat à un bénéficiaire afin d'accepter et de traiter les opérations de paiement de ce dernier initiées par un instrument de paiement du payeur ; le service pourrait comprendre la fourniture, au bénéficiaire, de services d'authentification, d'autorisation et d'autres services liés à la gestion des flux financiers, que le prestataire de services de paiement détienne ou non les fonds pour le compte du bénéficiaire ».*

[186] *Article 4(44) de la DSP2 : « acquisition d'opérations de paiement : un service de paiement fourni par un prestataire de services de paiement convenant par contrat avec un bénéficiaire d'accepter et de traiter des opérations de paiement, de telle sorte que les fonds soient transférés au bénéficiaire ».*

« *X-Pay* », tels que Apple Pay, Google Pay, Samsung Pay, etc.), au travers de portefeuilles numériques[187] (*digital wallets*), dont l'utilisation a bondi ces dernières années.[188] Les portefeuilles numériques sont utilisés pour procéder à des paiements par carte de paiement (de crédit ou de débit) en ligne et en magasin. Ces portefeuilles numériques stockent des copies virtuelles des cartes de paiement et permettent au titulaire d'une carte de paiement d'initier un paiement et ainsi de réaliser des achats grâce à la technologie sans fil permettant le paiement sans contact par téléphone mobile (communication en champ proche ou *near field communication*).[189] Lorsque l'utilisateur souhaite mettre en place son portefeuille numérique, il doit lier sa carte de paiement audit portefeuille. Ce lien passe par la création d'une version numérisée de la carte de paiement (un jeton ou *token*). Or, pour la plupart, les entreprises technologiques qui fournissent ce service de portefeuille électronique ne disposent pas d'agrément adéquat[190] et considèrent bénéficier de l'exemption relative à la fourniture de services techniques.

Comme le remarque la Commission européenne, les fournisseurs de ce type de solutions technologiques « *front-end* », telles que celles de type « *X-Pay* » par exemple, fournissent pourtant des services qui sont très proches des services d'initiation de paiement, en ce qu'ils contrôlent effectivement l'étape d'initiation de la transaction et l'authentification de l'utilisateur de services de paiement, alors même que les PSP disposent d'un contrôle limité de la sécurité et de l'exécution de ces solutions techniques,[191] même si, en bout de chaîne, ils sont responsables de la sécurité des données.[192] La difficulté est encore renforcée par la jurisprudence de la CJUE concernant la définition d'instrument de paiement, pour qui la fonction technologique permettant le paiement sans contact

[187] *Ou portefeuilles électroniques. L'ensemble des expressions digital wallets, e-wallets, portefeuilles numériques et portefeuilles électroniques étant tenues pour équivalentes.*

[188] *Le nombre de portefeuilles mobiles utilisés va atteindre 4.8 milliards en 2025, 2.8 milliards étaient utilisés en 2020. Voir Global Newswire, « Study : More than half of the world's population will use mobile wallets by 2025 », 2021, https://www.globenewswire.com/en/news-release/2021/07/08/2259605/0/en/Study-More-than-half-of-the-world-s-population-will-use-mobile-wallets-by-2025.html.*

[189] *S. Chaptal « Apple Pay : le paiement NFC à la sauce Apple », Revue Banque, Septembre 2014, https://www.revue-banque.fr/archive/apple-pay-paiement-nfc-sauce-apple-BORB13254.*

[190] *On notera que Paypal dispose d'une entité agréée en qualité d'établissement de crédit au Luxembourg, PayPal (Europe) S.à r.l. et Cie, S.C.A. et fournit ses services de monnaie électronique et de paiement à partir de cette entité. Ce n'est pas le cas d'Apple qui, bien que disposant d'un véhicule agréé dans l'Union ne l'utilise pas aux fins du service Apple Pay.*

[191] *DG FISMA, op. cit., p. 104.*

[192] *Voir ABE, « EBA clarifies the application of strong customer authentication requirements to digital wallet », 31 January 2023 : « the Q&As, overall, clarify that issuers may outsource the provision and verification of the elements of SCA to a third party (e.g. by concluding contractual arrangements with the third party), such as a digital wallet provider, in compliance with the general requirements on outsourcing, including the requirements of the EBA Guidelines on Outsourcing arrangements. However, the responsibility for compliance with the SCA requirements cannot be outsourced and issuers remain fully responsible for the compliance with the requirements in PSD2 and the Regulatory Technical Standards (RTS) on SCA&CSC. »*

(communication en champ proche, *near field* communication ou NFC), sans devoir faire usage des données de sécurité personnalisées, constitue en tant que telle un instrument de paiement distinct de la carte de paiement (Arrêt « *DenizBank* »).[193] Cette interprétation de la CJUE est contestable car elle élargit la définition d'instruments de paiement donnée par la DSP2.[194] La CJUE dissocie le paiement sans contact de la carte de paiement et y voit un instrument de paiement distinct. Effectivement, il peut être affirmé qu'il s'agit uniquement d'un moyen de communication différent entre le terminal et la carte, la carte étant liée à un seul utilisateur de services de paiement et les transactions imputées au compte bancaire de cet utilisateur. Par ailleurs, la transaction n'est soumise à l'obligation de SCA qu'à partir d'un certain montant, en dessous duquel l'opération est exemptée d'une telle sécurité. Cette interprétation a conduit à un manque de clarté et à une confusion entre les acteurs du marché.[195] Au regard de cette jurisprudence, logiquement, la représentation numérique de la carte de paiement, associée à l'utilisation de la technologie NFC devrait correspondre à la fourniture de services de paiement (notamment le service n° 5 de l'Annexe 1 de la DSP2 consistant en l'émission d'instruments de paiement). C'est en effet l'avis de l'ABE pour qui l'émission d'un jeton qui est lié à un instrument de paiement sous-jacent ou le compte de paiement d'un utilisateur de services de paiements, constitue en elle-même l'émission d'un instrument de paiement et tombe dans le champ d'application de la DSP2.[196] La question que l'on peut se poser est de savoir pour le compte de qui le jeton/*token* est créé. S'il est confirmé, par les autorités ou les tribunaux, qu'il est créé pour le compte du PSP émetteur, ceci pourrait conduire à considérer que c'est le PSP émetteur qui émet l'instrument de paiement dans ce cas. Ceci repose la question de la qualification du rôle des « *X-Pay* » par rapport aux PSP émetteurs. L'ABE précise en revanche que d'autres services fournis par le prestataire de portefeuille numérique, tels que la gestion d'un portefeuille numérique, n'entrent pas dans le champ d'application de ladite directive en raison de leur nature technique.[197]

Un autre sujet, connexe, est relatif à la responsabilité juridique attachée à la mise en œuvre de l'authentification forte de l'utilisateur de services de paiement. L'opération de paiement effectuée par le biais d'un portefeuille numérique a également un impact dans la SCA. La DSP2 exige des PSP d'appliquer la SCA lorsque l'utilisateur de services de paiement initie des opérations de paiement

[193] *CJUE, DenizBank AG c/ Verein für Konsumenteninformation, Affaire C-287/19, 11 novembre 2020, considérants n° 79 et §2.*

[194] *Article 4(14) de la DSP2 : « tout dispositif personnalisé et/ou ensemble de procédures convenues entre l'utilisateur de services de paiement et le prestataire de services de paiement et utilisé pour initier un ordre de paiement ».*

[195] *DG FISMA, op. cit., p. 112.*

[196] *ABE, « EBA's response to the Call for advice on the review of PSD2… », n° 85. Voir également, DG FISMA, op. cit., p. 68, appelant à un encadrement plus holistique des prestataires fournissant des services de paiement.*

[197] *Ibid.*

électronique.[198] L'ABE a indiqué qu'un PSP peut recourir à la technologie fournie par un prestataire tiers (telle que celle permettant de déverrouiller un téléphone mobile, par reconnaissance faciale ou empreinte digitale), tout en restant responsable de la sécurité.[199] Il s'agit ici des cas où des applications mobiles sont installées sur le téléphone et où le PSP interagit pour les besoins de la SCA avec lui. Dans cette hypothèse, aucune relation contractuelle n'est généralement établie entre le PSP et le fabricant de smartphone.[200] Ceci pose des difficultés, en particulier lorsque le PSP n'effectue aucun contrôle des mesures de sécurité.[201] L'ABE a précisé que le PSP peut choisir de sous-traiter l'authentification forte du client à un prestataire technique, à condition que le PSP et le prestataire technique concluent un contrat de sous-traitance obéissant aux règles relatives à l'externalisation de fonctions critiques ou importantes régissant ces contrats. Néanmoins, il a été observé qu'il est souvent difficile de mettre en place de tels contrats, notamment avec les « *Big Techs* », qui considèrent qu'ils mettent uniquement une technologie tierce à la disposition du PSP. La DSP2 manque de précisions sur la conclusion de ces contrats de sous-traitance.[202]

5.2.1.2 - Cas d'autres prestataires dont les services sont proches de l'initiation de paiement

Le service d'initiation de paiement reçoit, dans la lettre du texte, une définition très large dans la DSP2 : « *un service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement* ».[203] Les règles à respecter pour la fourniture de ces services sont également décrites de manière très large dans l'article 66 de la DSP2 et dans les normes techniques de réglementation mettant en œuvre DSP2. Tandis que, dans son esprit, tel que reflété dans les considérants de la DSP2, ces services semblent être d'une portée plus limitée : « *ces services de paiement interviennent dans les paiements dans le cadre du commerce électronique en établissant une passerelle logicielle entre le site internet du commerçant et la plate-forme de banque en ligne du prestataire de services de paiement gestionnaire de compte du payeur en vue d'initier des paiements par l'internet sur la base d'un virement* ».[204]

On observe donc une discordance entre l'intention initiale du législateur et la définition qu'il a finalement retenue du service d'initiation de paiement, ainsi que des règles à respecter pour fournir ce service, d'une portée plus large.

---

[198] *Article 97(1) de la DSP2, transposée à l'article L. 133-44 du CMF.*

[199] *ABE, Q&A 4047, https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047.*

[200] *ABE, « EBA's response to the Call for advice on the review of PSD2… », n° 313.*

[201] *ABE, op. cit., n° 309 et s.*

[202] *ABE, op. cit., n° 315 et s.*

[203] *Article 4(15) de la DSP2, transposé à l'article D. 314-2 du CMF.*

[204] *Considérant n° 27 de la DSP2.*

Au surplus, la DSP2 n'aborde l'initiation de paiement que de manière monolithique sans envisager le cas de figure dans lequel plusieurs acteurs distincts interviendraient à des étapes différentes de la phase d'initiation de paiement. Or, ce manque de précision pose question en pratique. Par exemple, de manière récurrente, une entreprise peut confier à un prestataire fournissant des services de gestion de trésorerie, la tâche d'effectuer, en son nom et pour son compte, certaines opérations tenant à la gestion de son compte de paiement ouvert auprès de son PSP. Il est fréquent en pratique que ce prestataire ne soit pas agréé aux fins de réalisation de service d'initiation de paiement.

Le type d'opérations effectuées par de tels prestataires varie en fonction de l'USP et de ses besoins : certains prestataires n'interviendront que pour préparer le fichier de paiement (c'est-à-dire le créer sur la base des instructions reçues de l'utilisateur de services de paiement et le mettre en forme), d'autres assureront également la validation et/ou l'envoi de l'ordre de paiement au PSP pour le compte de l'utilisateur. Certains encore peuvent effectuer l'intégralité de ces opérations. Ainsi, la qualification des services rendus et du rôle de ces prestataires peut faire débat tant le texte de la DSP2 est large par rapport à son objectif initial.

Deux approches peuvent être adoptées selon que l'interprétation est effectuée à la lumière des considérants de la DSP2 ou au regard de la lettre du texte de la directive.

En l'absence de précisions, lignes directrices, doctrine ou jurisprudence en la matière, il semble possible d'interpréter la définition de l'initiation de paiement à la lumière des considérants de la DSP2 qui l'inscrivent dans le cadre du commerce électronique. Le considérant n° 27 cible précisément « *ces services de paiement [qui] interviennent dans les paiements dans le cadre du commerce électronique en établissant une passerelle logicielle entre le site internet du commerçant et la plate-forme de banque en ligne du prestataire de services de paiement gestionnaire de compte du payeur en vue d'initier des paiements par l'internet sur la base d'un virement* ».

Plusieurs éléments vont dans le sens de cette interprétation, notamment le rapport de la Commission des finances de l'Assemblée nationale sur le projet de loi portant transposition française de la DSP2, dans lequel le service d'initiation de paiement est entendu dans le cadre du commerce électronique : « *Le premier axe est la consécration juridique au niveau européen de deux nouveaux types d'acteurs : les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes. Les premiers, également appelés initiateurs de paiements, passent des ordres de paiement à la demande du consommateur, à partir d'un compte de paiement détenu auprès d'une banque. Ils permettent aux consommateurs de payer leurs achats en ligne par simple virement, en donnant aux commerçants l'assurance que le paiement a bien été initié* ».[205]

[205] *Rapport de l'Assemblée nationale fait au nom de la Commission des finances, de l'économie générale et du contrôle budgétaire, en nouvelle lecture, sur le projet de loi, modifié par le sénat, ratifiant l'ordonnance n° 2017 1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (n° 812) en date du 27 juin 2018, https://www.assemblee-nationale.fr/dyn/15/rapports/cion_fin/l15b1105_rapport-fond#.*

Cette interprétation est renforcée par la description de l'initiation de paiement que l'ACPR donne : « *le service d'initiation de paiement (défini en Annexe I) qui permet de proposer à des commerçants en ligne d'accepter des paiements par virements initiés pour le compte des acheteurs* ».[206] Enfin, cette interprétation est cohérente avec les objectifs du législateur lors de la création de la notion d'initiation de paiement tels que la protection des données d'utilisateurs de service de paiement et le développement de l'e-commerce. Partant de cette lecture, l'initiation de paiement vise uniquement les opérations réalisées dans le cadre du commerce électronique, de sorte que les différentes situations décrites ci-dessous n'entrent pas dans le champ des services d'initiation de paiement.

Néanmoins, la définition retenue par le texte de la DSP2 et les règles édictées pour encadrer ce service sont suffisamment larges pour dépasser le périmètre de services que le législateur a souhaité encadrer, et englobe des relations hors commerce en ligne. D'autres cas d'usage ont ainsi pu se développer, comme par exemple le cas selon lequel un PSP offre un service d'initiation de paiement à des clients multibancarisés pour leur permettre de gérer leurs comptes. Au regard du développement de ces multiples cas d'usage, la qualification du PSIP a pu interroger dans certaines hypothèses.

En particulier :

(i) Cas n° 1 : le PST exécute chacune des étapes de l'initiation de paiement : préparation, validation et envoi de l'ordre. L'utilisateur n'intervient qu'en amont pour donner ses instructions au PST. L'intervention du PST au stade de l'envoi de l'ordre relèverait bien de l'activité d'initiation de paiement et ce mode de fonctionnement nécessiterait donc que le PST dispose d'un agrément.

À titre d'illustration, l'utilisateur confie à un prestataire l'intégralité de la gestion de la paie. À la demande de l'utilisateur, le prestataire prépare chaque mois les fichiers, les valide et les envoie directement au PSP gestionnaire de compte pour paiement à bonne date des salaires.

(ii) Cas n° 2 : l'intervention du PST comprend la préparation du fichier de paiement et l'envoi de l'ordre de paiement au PSP. L'envoi de l'ordre de paiement par le PST déclenche l'exécution de l'opération de paiement par le PSPGC qui tient le compte de paiement de l'utilisateur, de telle sorte que le PST – et non l'utilisateur – devrait être considéré comme ayant initié l'opération de paiement. Il en résulte que le PST devrait donc disposer d'un agrément.

En matière de gestion comptable ou d'externalisation de trésorerie, il existe des logiciels qui permettent de prévoir des opérations à réaliser au sein d'un groupe de sociétés, afin de planifier

[206] *ACPR, « Panorama des nouveaux acteurs de paiement », mars 2022, p. 13, https://acpr.banque-france.fr/sites/default/files/medias/documents/20220315_etude_acpr_panorama_paiement.pdf.*

les paiements, par exemple, aux fournisseurs. En effet, sur la base de l'analyse de l'historique des opérations passées et des informations communiquées par l'USP, le prestataire prépare des fichiers d'opérations à venir. L'utilisateur de services de paiement valide le fichier et le prestataire envoie l'ordre de paiement au PSPGC. Le prestataire agit ainsi en tant que PSIP.

(iii) Cas n° 3 : le PST prépare, valide et envoie les ordres de paiement à chaque instruction de l'utilisateur. La partie de cette activité relative à l'envoi de l'ordre de paiement relève du service d'initiation de paiement et requiert donc également un agrément.

Il s'agit ici de l'hypothèse, par exemple, de l'avance demandée par des salariés directement sur la plateforme du PST. Lorsque l'employeur en convient, ce dernier valide chaque demande, une par une, et le PST envoie directement l'ordre de paiement au PSP de l'employeur. Le PST agit ainsi en tant que PSP.

(iv) Cas n° 4 : l'intervention du PST est limitée à la seule préparation du fichier de paiement au nom et pour le compte de l'utilisateur sans envoi de l'ordre de paiement. Elle ne devrait pas relever de l'activité de PSIP, y compris au regard du texte de la DSP2.

Dans ce contexte, il existe une incertitude quant aux conséquences réglementaires attachées aux droits accordés au PST par l'utilisateur de services de paiement. Il apparait ainsi que deux lectures soient possibles :

- le fait de conférer un mandat spécial limitant les pouvoirs du mandataire aux seules opérations, notamment de paiement, définies par l'utilisateur mandant et de permettre au mandataire d'accéder au compte à l'aide de ses propres identifiants écarteraient la qualification de PSIP. Ainsi, disposant de ses propres codes d'accès, il n'y aurait plus de difficultés liées au *web scrapping* ; ou

- un mandat donné au prestataire ne l'exonère pas d'un agrément de PSIP. Le mandat ne permet pas d'exonérer le prestataire (mandataire) de la nécessité d'être agréé en tant que PSIP, dès lors que les paiements ainsi initiés le sont dans le cadre d'une activité réglementée exercée à titre professionnel. Ainsi, il est donc tout à fait possible d'être à la fois mandataire et PSIP. Les qualifications sont cumulatives. Les partisans de cette lecture défendent le fait que l'activité de PSIP étant réglementée, le caractère exclusif du mandat/de l'activité de PSIP reviendrait à contourner les obligations notamment d'agrément, alors que toute l'activité de certains prestataires consiste à gérer et à envoyer des ordres de paiement.

Bien que ni la DSP2, ni la jurisprudence, ni la doctrine n'apportent de précision à ce sujet, il pourrait toutefois être considéré selon cette lecture que l'envoi de l'ordre de paiement par le PST au PSPGC constitue l'élément déclencheur de l'opération de paiement et que cette action relève donc du service d'initiation de paiement. Dès lors, l'activité du prestataire qui se contenterait d'envoyer

à la banque des ordres de paiement préparés et validés par l'USP lui-même, relèveraient également de cette qualification.

Cette interprétation permet au PSPGC de déceler en pratique toutes les hypothèses d'intervention d'un tiers dans une initiation de paiement, que l'utilisateur soit une personne morale ou une personne physique, consommateur ou non, et permet d'éviter ainsi le recours à la pratique de *web scrapping*. Ainsi, elle va dans le sens d'un des objectifs poursuivis par la DSP2 consistant à éviter le partage des identifiants de l'USP avec un tiers non réglementé et de limiter les risques de fraudes et pertes de données.

5.2.2 - Prestataires « *back-end* »

Par ailleurs, les PST interviennent également et le plus souvent en « *back-end* », pour reprendre la terminologie de la Commission européenne, c'est-à-dire, en fournissant une prestation de nature technique permettant au PSP de fournir les services de paiement, sans que le PST ne soit visible de l'utilisateur de services de paiement, ni assure une quelconque responsabilité directe à son égard, n'ayant pas de lien contractuel avec ce dernier. Dans ce cas les règles en matière de sous-traitance ont vocation à s'appliquer, notamment celles spécifiques à la DSP2.[207] Dans le domaine des technologies de l'information et de la communication, le nouveau règlement européen sur la résilience opérationnelle numérique du secteur financier, aussi connu sous le nom de « DORA »[208], reprend ces règles et les précise pour en faire un corpus de règles destinées à encadrer de manière spécifique « *la gestion, par les entités financières, du risque lié aux prestataires tiers de services TIC [technologies de l'information et de la communication], qui revêtent une importance particulière lorsque les entités financières ont recours à des prestataires tiers de services TIC pour soutenir leurs fonctions critiques ou importantes*. »[209] DORA fait ainsi entrer dans son champ d'application les PST en rappelant le fait que « *compte tenu de l'évolution du marché des services de paiement, qui dépend de plus en plus de solutions techniques complexes, et des types émergents de services de paiement et de solutions liées au paiement, les participants à l'écosystème des services de paiement, qui exercent des activités de traitement du paiement ou exploitent des infrastructures de paiement, devraient également être considérés comme des prestataires tiers de services TIC au titre du présent règlement, à l'exception des banques centrales lorsqu'elles exploitent des systèmes*

[207] *Article 19(6) de la DSP2. Pour un rappel des textes applicables en matière de sous-traitance informatique dans le domaine bancaire qui s'applique également au secteur des paiements, voir le rapport du HCJP sur le Cloud bancaire : états des lieux et propositions, https://www.banque-france.fr/sites/default/files/rapport_42_f.pdf.*

[208] *Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011.*

[209] *Considérant n° 29 de DORA.*

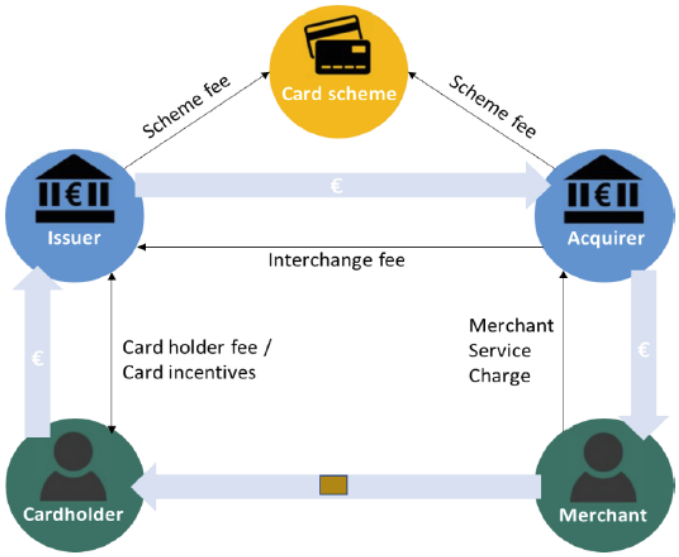
de paiement ou de règlement des opérations sur titres et des autorités publiques lorsqu'elles fournissent des services liés aux TIC dans le contexte de l'exercice de fonctions de l'État. »[210] Comme le fait remarquer DORA, il serait donc judicieux d'aligner ces deux textes afin d'assurer une complémentarité entre eux.[211]

5.2.3 - Cas particulier des schémas de paiement

Le cas des schémas de paiement (*payment schemes*) comme Visa ou Mastercard apparaît ambigu. Ils semblent être, de prime abord, appréhendés comme des services de communication et, partant, exclus du champ de la DSP2 au titre de l'exclusion des prestations techniques.[212] De fait, certains opérateurs de ces systèmes ne sont pas agréés comme PSP au sein de l'Union.[213]

Visa et Mastercard sont identifiés dans l'EEE comme les deux systèmes de paiement les plus importants et interviennent dans la facilitation de communication entre l'établissement acquéreur et l'établissement émetteur (voir schéma ci-dessous).[214]

Schéma simplifié d'un schéma de paiement[215]



[210] *Considérant n° 63 de DORA.*

[211] *Considérant n° 104 de DORA.*

[212] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 June 2022, n° 83 : « This is mainly due to the fact that they provide communication protocols used by PSPs for the application of SCA and other security requirements. »*

[213] *Visa est un schéma de paiement américain, qui est opéré en Europe par Visa Europe Limited (VEL), une entreprise établie au Royaume-Uni agréée en tant qu'établissement de paiement auprès de la FCA (https://register.fca.org.uk/s/firm?id=001b000000NMaIFAAT), mais qui, depuis le Brexit, ne dispose plus d'un statut réglementé dans l'Union. MasterCard est un schéma de paiement américain également, qui est opéré en Europe par Mastercard Transaction Services (Europe) une entreprise belge agréée en qualité d'établissement de paiement en Belgique pour les services n° 3 et n° 4 de la DSP2 et est passeportée dans toute l'Union.*

[214] *DG FISMA, op. cit., p. 35.*

[215] *DG FISMA, op. cit., p. 36.*

À titre d'exemple, d'un côté, Mastercard indique acheminer grâce à son réseau central une transaction vers l'émetteur pour approbation de la transaction. L'objectif est de faciliter l'échange d'informations sur les transactions entre les émetteurs et les acquéreurs et le règlement de la transaction en facilitant l'échange de fonds entre les parties par l'intermédiaire de banques de règlement choisies par eux et les clients.[216] De l'autre côté, Visa indique que dans le cadre d'une transaction de paiement Visa C2B typique, lors de laquelle le consommateur achète des biens ou des services à un commerçant au moyen d'une carte Visa, le commerçant présente les données de la transaction à un acquéreur, généralement une banque ou une société de traitement tierce qui accepte les cartes ou les produits de paiement Visa, pour vérification et traitement. Par l'intermédiaire de VisaNet, l'acquéreur présente les données de la transaction à Visa qui, à son tour, contacte l'émetteur pour vérifier le compte ou la ligne de crédit du titulaire du compte en vue d'une autorisation. Une fois la transaction autorisée, l'émetteur paie effectivement à l'acquéreur un montant égal à la valeur de la transaction, moins la commission de remboursement de l'interchange, puis inscrit la transaction sur le compte du consommateur.[217]

Néanmoins, les services fournis par les *payment schemes* ne se limitent pas à la fourniture de réseaux de communication, et comprennent des services de paiement. Visa opère par exemple un service de virements transfrontaliers appelé Visa B2B Connect,[218] reposant sur la *tokenisation* des informations bancaires sensibles des participants (les numéros de compte) en leur donnant un identifiant unique qui peut être utilisé pour faciliter les transactions dans le réseau. L'ACPR a d'ailleurs noté l'accroissement de la « *dépendance de l'ensemble de la chaine du paiement aux (payment schemes) internationaux* » lié à « *l'essor de la tokenisation* ».

Dans ce cas, l'exception liée à la fourniture de services techniques ne suffit plus.

Il convient de relever que la DSP2 prévoit une autre exception, relative aux « *opérations de paiement effectuées au sein d'un système de paiement ou de règlement des opérations sur titres entre des agents de règlement, des contreparties centrales, des chambres de compensation et/ou des banques centrales et d'autres participants au système, et des prestataires de services de paiement, (…)* ».[220]

---

[216] *Rapport annuel de Mastercard Inc., 2021, p. 9 à 10, https://s25.q4cdn.com/479285134/files/doc_financials/2021/ar/2021-Annual-Report-NO-EMAIL-ALERTS.pdf.*

[217] *Rapport annuel de Visa, 2022, p. 5, https://s29.q4cdn.com/385744025/files/doc_downloads/2022/Visa-Inc-Fiscal-2022-Annual-Report.pdf.*

[218] *https://www.businesswire.com/news/home/20190611005296/en/.*

[219] *Rapport, ACPR, « La surveillance des moyens de paiement scripturaux et des infrastructures des marchés financiers », 2020, https://publications.banque-france.fr/sites/default/files/medias/documents/smpsimf_2020-2.pdf.*

[220] *Article 3(h) de la DSP2. À noter que cette exclusion n'a pas été transposée en droit français, ce qui crée une certaine incertitude juridique lorsque le système ou schéma de paiement fournit des services de paiement sur le territoire français.*

Un système de paiement est par ailleurs défini comme « *un système permettant de transférer des fonds régi par des procédures formelles standardisées et des règles communes pour le traitement, la compensation et/ou le règlement d'opérations de paiement* »[221]. On peut s'interroger sur la question de savoir si cette notion de système de paiement est limitée aux systèmes notifiés à la Commission européenne en application de la directive finalité des règlements (ce qui aurait pour effet d'exclure des schémas de paiement comme Visa), ou si elle englobe tout système répondant factuellement à la définition fonctionnelle prévue par la DSP2. C'est cette deuxième acception qui est pertinente. En effet, dans ses considérants, la DSP2 vise précisément les schémas de carte faisant intervenir quatre parties, ainsi que les principaux systèmes permettant de traiter des virements et des prélèvements.[223] En pratique, on comprend que sont, notamment, ciblés les schémas de paiement par carte (*payment schemes*), qui peuvent être domestiques, comme en France GIE Cartes Bancaires, ou internationaux, tels que Visa et Mastercard.[224]

Pour autant, même s'ils sont exclus du champ d'application de la DSP2,[225] certains systèmes ou schémas de paiement, notamment systémiques, relèvent du cadre de surveillance de l'Eurosystème pour les instruments, systèmes et dispositifs de paiement électronique (« **PISA** »)[226]. Cela dit, la soumission au cadre de surveillance PISA s'applique autant aux acteurs agrées comme établissement de paiement[227], que non agrées sous l'empire de la DSP2[228], par conséquent cette soumission ne devra pas à elle seule constituer une raison d'exclure *ipso facto* les schémas de paiement du champ de la DSP2.

---

[221] *Article 4(7) de la DSP2.*

[222] *Directive 98/26/CE du Parlement européen et du Conseil du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titre.*

[223] *Considérant n° 49 de la DSP2.*

[224] *On relèvera que, dans son avis sur la proposition de DSP1 du 26 avril 2006 (/2006/21), la BCE avait même plutôt recommandé de préciser que la définition de système de paiements inclut une référence expresse aux systèmes relevant de la directive finalité (Modification N° 7, p. 22).*

[225] *Sous réserve toutefois de MasterCard, qui est agréé comme établissement de paiement.*

[226] *Cadre de surveillance de l'Eurosystème pour les instruments, systèmes et dispositifs de paiement électronique (« **Cadre PISA** »), novembre 2021, https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf. Les payment schemes qui sont supervisés par la BCE dans le Cadre PISA comprennent, notamment, MasterCard Europe et Visa Europe, voir la liste : https://www.ecb.europa.eu/paym/pdf/2022-10-04-List_overseen_schemes.lt.pdf. Voir également, le Règlement (UE) n° 795/2014 de la Banque centrale européenne du 3 juillet 2014 concernant les exigences de surveillance applicables aux systèmes de paiement d'importance systémique (/2014/28), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014R0795. Adde, , « Oversight framework for card payment schemes – standards », janvier 2008.*

[227] *Tels que Mastercard qui dispose d'un agrément en qualité d'EP en Belgique.*

[228] *Tels que Visa Europe (cf., liste des schémas du cadre de surveillance PISA tenue par la BCE, https://www.ecb.europa.eu/paym/pdf/2022-10-04-List_overseen_schemes.en.pdf.)*

Malgré cela, l'ABE relève que les systèmes de paiement de cartes jouent un rôle crucial dans le respect, par les PSP participant aux systèmes, de certaines exigences légales découlant de la DSP2, telles que l'authentification forte du client (SCA), en raison des protocoles de communication qu'ils leur fournissent et qui sont utilisés par les PSP pour l'application de ces exigences.[229] De fait, le protocole « *3D secure* », qui est un système de sécurisation des paiement en ligne créé originellement par Visa et Mastercard, s'est imposé comme le standard en matière d'authentification des paiement par carte, ce qui pose question en termes, non seulement de monopole de fait dans un secteur d'activité théorique pour l'union des services de paiement, mais également de souveraineté européenne, compte tenu de la nationalité de ces deux acteurs.

En définitive, une clarification de l'articulation entre la DSP2 et le cadre de supervision des systèmes de paiement de la BCE serait nécessaire, en précisant que l'exclusion contenue dans la DSP2 ne s'applique qu'aux systèmes soumis à la directive finalité ainsi qu'à ceux qui n'y étant pas soumis, sont supervisés par la , de telle sorte que seul un système faisant l'objet d'une supervision dans le cadre du droit de l'Union bénéficie de l'exclusion. Accessoirement, on peut se poser la question de savoir s'il ne serait pas également nécessaire de préciser, dans la définition de système de paiement prévue dans la DSP2, que l'opérateur du système, dont la notion devrait être précisée, devrait avoir son siège dans l'Union.

5.3 - Recommandations du HCJP

Le HCJP propose de formuler les recommandations suivantes :

Recommandation n° 9 : le HCJP recommande de clarifier les notions d'« *initiation d'opération de paiement* » et d'« *instrument de paiement* », en vue de préciser les conditions dans lesquelles : (i) s'agissant des paiements par carte et ; (ii) plus généralement les solutions technologiques apportées par les prestataires de services techniques peuvent se distinguer des services de paiement fournis par les PSP.

Recommandation n° 10 : clarifier l'articulation de la réglementation applicable en matière de sous-traitance, particulièrement entre DORA et la DSP2.

Recommandation n° 11 : clarifier la définition de système de paiement, afin de lier cette exclusion à la soumission du système de paiement au cadre de supervision des systèmes et schémas de paiement de l'Union.

[229] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 June 2022, n° 83.*

VI. Exclusions du champ de la DSP - Exclusion intragroupe

6.1 - Enjeux liés à l'exclusion intragroupe

La gestion centralisée de la trésorerie[230] constitue une pratique courante au sein des groupes de sociétés, notamment internationaux. Elle peut prendre plusieurs forme : soit elle repose sur des mouvements effectifs de trésorerie entre les sociétés du groupe, dont l'une d'elles assume le rôle d'agent centralisateur – usuellement, on la qualifie de société « *pivot* » (cette forme corresponde à une centralisation « *réelle* » des flux financiers) ; soit elle repose sur la fusion des échelles d'intérêts dus par les sociétés du groupe sur un compte centralisateur tenu par la société pivot (il s'agit là d'une centralisation dite « *notionnelle* »).[231] En France, la centralisation de trésorerie ne fait pas l'objet d'un cadre juridique dédié. Toutefois, comme elle implique généralement la réalisation de certaines opérations de banques soumises au monopole bancaire, tant au titre d'opérations de crédit effectuées à titre habituel que de la réception de fonds remboursables du public,[232] elle fait l'objet de dispositions dédiées prévoyant des exceptions à ce monopole.[233]

Mais la centralisation de trésorerie n'implique pas que la seule réalisation d'opérations de banque.[234] Elle s'accompagne de la réalisation d'opérations de paiement, impliquant la fourniture de services de paiement, au sens de la DSP. Cela d'autant plus que l'instauration d'un marché européen unique pour les paiements en euros (zone « SEPA ») a ouvert de nouvelles perspectives en matière de gestion des liquidités au sein des groupes de sociétés. Dans ce cadre, la société pivot est chargée de centraliser les paiements pour le compte de l'ensemble des sociétés du groupe membre du pool de trésorerie (en pratique, le terme de « *payment factory* » est souvent employé). Cette centralisation des paiements joue dans les deux sens : la société pivot peut aussi bien effectuer des paiements au profit de tiers pour le compte d'une société du groupe (paiement qualifié de POBO (*payment on behalf of*)) que recevoir d'un tiers un paiement dû à une autre société du groupe (on parle alors de paiement ROBO ou COBO (*reception ou collection on behalf of*)).

---

[230] Aussi appelée « cash pooling », omnium de trésorerie, etc.

[231] Voir pour une description plus détaillée : Banque de France, « Le cash pooling », V15/11/2016, https://entreprises.banque-france.fr/sites/default/files/bdf_reffin_chap6_603.pdf.

[232] Respectivement, article L. 311-1 et L. 511-5 du CMF.

[233] Articles L. 312-2, §1° et L. 511-7, §3° du CMF.

[234] Selon l'acception actuelle de cette notion, découlant de la transposition de la DSP1. Les opérations de banques n'incluent, depuis lors, que les services bancaires de paiement, à côté de la réception de fonds remboursables du public et des opérations de crédit.

6.2 - Quel est le régime juridique actuel ?

6.2.1 - Dans la DSP2 (et les autres textes européens pertinents)

En France, avant la transposition de la DSP1, les actuels services de paiement étaient contenus dans la notion de « *gestion des moyens de paiement* » qui relevait du monopole bancaire. Par conséquent, les exceptions précitées applicables en matières bancaires étaient alors suffisantes à couvrir toutes les opérations bancaires (y compris, donc, les services de paiement) réalisées dans le cadre d'une gestion de trésorerie centralisée au sein d'un groupe de sociétés.[235] En séparant les services de paiement des services bancaires (et, partant, du monopole y relatif), la DSP1 a modifié la situation, de sorte qu'une exception spécifique au monopole des PSP a été rendue nécessaire.

La DSP1 a donc offert la possibilité aux États membres de l'Union européenne d'exclure du champ d'application du régime des services de paiement les opérations de paiement « *entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, sans qu'aucun autre prestataire de services de paiement qu'une entreprise du même groupe ne fasse office d'intermédiaire* » (« ***Exclusion Intragroupe*** »). Ainsi, dans les États membres ayant transposé l'Exclusion Intragroupe, les règles applicables aux services de paiement rendus dans cet État membre ne s'appliquent pas aux opérations de paiement réalisées entre entités du même groupe (par exemple, il n'est pas nécessaire de disposer d'un agrément, *a minima*, d'établissement de paiement pour fournir lesdits services). La DSP2 a repris à son article 3(n) cette exclusion sans changement.

Toutefois, on peut constater que l'Exclusion Intragroupe ne vise que les opérations de paiement au sein du groupe de sociétés, mais pas la fourniture de services de paiement. La nuance est importante, car, si les services de paiement fournis par une société du groupe à une autre au titre de la réalisation de telles opérations sont nécessairement couverts par cette exclusion, il n'en est pas de même à l'égard des mêmes services de paiements fournis en relation avec des opérations de paiement lorsqu'elles sont exécutées hors du groupe, c'est-à-dire en direction, ou en provenance, de tiers (autrement dit, les paiements POBO et ROBO). En particulier, on rappellera à cet égard que l'activité d'encaissement de fonds pour le compte de tiers implique la fourniture de services de paiement, selon l'ABE et, en France, l'ACPR.[236]

C'est pourquoi la DSP2 précise, dans son considérant n° 17, que l'Exclusion Intragroupe peut s'appliquer à la centralisation d'ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale : « *L'espace unique de paiements en euros (SEPA) a facilité la mise en place*

[235] *Voir supra, note de bas de page n° 233.*

[236] *Voir supra section 4 (Champ d'application matériel de la DSP2 – Encaissement de fond pour le compte de tiers).*

de centres de paiement et de centres d'encaissement à travers l'Union, permettant une centralisation des opérations de paiement d'un même groupe. À cet égard, les opérations de paiement entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, effectuées par un prestataire de services de paiement faisant partie du même groupe devraient être exclues du champ d'application de la présente directive. La centralisation des ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure à un prestataire de services de paiement ne devrait pas être considérée comme un service de paiement aux fins de la présente directive ».

Pour autant, cette approche consistant à clarifier la substance du texte de la directive par voie de considérant pose deux difficultés. La première est d'ordre méthodologique. En effet, cette précision ne vaut que comme règle d'interprétation et ne figure pas dans le texte lui-même de l'Exclusion Intragroupe. Or dans, dans le cadre de la transposition d'une directive, ses considérants ne sont que très rarement transposés et il en résulte une incertitude quant à leur portée, lorsque, non transposés, ils sont invoqués devant les tribunaux ou les autorités de supervision. D'ailleurs, on verra que les approches retenues par certains États membres, de transposer ou non le considérant n° 17 ou de lui donner une portée normative, sont variables,[237] ce qui nuit à la cohérence des textes de transposition de la directive au sein de l'Union et crée de réelles difficultés pour les groupes de sociétés ayant mis en place une gestion centralisée pan-européenne de leur trésorerie.

La deuxième concerne la substance même de l'interprétation portée par ce considérant. En effet, alors qu'il est fait référence à « *la mise en place de centres de paiement et de centres d'encaissement*[238] *à travers l'Union, permettant une centralisation des opérations de paiement d'un même groupe* », ce qui inclut bien tant les paiements POBO que les paiements ROBO, la conclusion du considérant est plus ambiguë quant à savoir si les paiement POBO et ROBO sont exclus du champ de la directive : « *La centralisation des ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure à un prestataire de services de paiement ne devrait pas être considérée comme un service de paiement aux fins de la présente directive* ». Une lecture littérale de cette phrase laisse penser que les paiements ROBO sont hors du champ de l'Exclusion Intragroupe.

Se pose dès lors la question de la portée exacte de cette exclusion.

---

[237] *Voir infra paragraphe 6.2.2.*

[238] *Soulignement ajouté.*

6.2.2 - Dans la législation des États membres

En France tout d'abord, l'Exclusion Intragroupe a été transposée en reprenant verbatim l'article 3(n) de DSP2, en ajoutant toutefois la précision apportée par le considérant 17 : « *N'est pas considérée comme un service de paiement (...) 4° La réalisation d'opérations de paiement entre une entreprise mère et sa filiale, ou entre filiales d'une même entreprise mère, ou au sein d'un groupe au sens du h de l'article L. 133-4, sans qu'aucun autre prestataire de services de paiement qu'une entreprise du même groupe ne fasse office d'intermédiaire, ainsi que la centralisation des ordres de paiement pour le compte d'un groupe par une entreprise mère ou sa filiale pour transmission ultérieure à un prestataire de services de paiement* ».[239]

Or, au sein de l'Union, l'Exclusion Intragroupe n'a pas été transposée de manière uniforme.

Certains pays reconnaissent une portée large à l'Exclusion Intragroupe : c'est le cas, par exemple, de l'Italie qui a transposé l'Exclusion Intragroupe en y incluant la centralisation des ordres de paiement[240], ou encore de l'Allemagne, dans une moindre mesure. En effet, bien que le droit allemand précise que l'Exclusion Intragroupe ne s'applique pas quand une entité du groupe effectue ou reçoit des paiements au bénéfice d'une entité extérieure au groupe, il existe une pratique d'exclusion convenue entre la BaFin et l'Association des Trésoriers Allemands (*Association of German Treasurers*) au titre de laquelle les entités d'un même groupe ne sont autorisées à réaliser des mouvements de trésorerie (*e.g. cash pooling*) que si toutes les entités sont soumises aux mêmes règles de gestion du risque.[241]

En revanche, en Espagne, au Luxembourg et en Pologne, l'Exclusion Intragroupe a été transposée en reprenant uniquement la rédaction étroite de l'article 3(n) de la DSP2, sans reprendre le considérant n° 17 de la DSP2 : la centralisation des ordres de paiement n'est donc pas *a priori* incluse dans le périmètre de l'Exclusion Intragroupe.

6.3 - Recommandations du HCJP

La centralisation des ordres de paiement et des paiements via une centrale de trésorerie (tant en ce qui concerne les paiements POBO et ROBO) est, non seulement, une pratique répandue dans les

[239] *Article L. 314-1 III 4° du CMF.*

[240] *Article 2(2)(p) du Legislative Decree n° 11/2010.*

[241] *Site internet de la BaFin, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html;jsessionid=26C2E6B0C4B5FB17615CA7C49D3E0B8C.1_cid500?nn=9450978.*

groupes de sociétés, mais au surplus qui ne reste pas confinée aux frontières d'un seul État membre. Or les différences de transposition au sein de l'Union, ainsi que l'incertitude juridique quant à la portée du considérant n° 17 de la DSP2 (transposé ou non) en affectent la sécurité juridique. Afin de réduire cette insécurité, il serait recommandé de préciser, sans ambiguïté, que l'Exclusion Intragroupe s'applique à la centralisation des paiements reçus, ainsi qu'au bénéfice des tiers, pour le compte d'entités appartenant au même groupe afin d'harmoniser la législation des États membres.

Recommandation n° 12 : le HCJP recommande de modifier la DSP2 afin de préciser dans le texte de l'Exclusion Intragroupe que cette exclusion s'applique à la centralisation des paiement reçus de tiers, ainsi qu'au bénéfice des tiers, pour le compte d'entités appartenant même groupe.

VII. Notion de compte de paiement

7.1 - Enjeux liés à la définition du compte de paiement

L'une des innovations de la DSP1 a été la création de la notion de « *compte de paiement* », reprise sans changement dans la DSP2. Le compte de paiement se définit comme « *un compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et qui est utilisé aux fins de l'exécution d'opérations de paiement* ».[242] Le compte de paiement se caractérise par sa finalité : celle d'exécuter toute « *action, initiée par le payeur ou pour son compte ou par le bénéficiaire, consistant à verser, à transférer ou à retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire* »,[243] à savoir par exemple, le retrait ou le versement d'espèces, les virements, les prélèvements, etc.

Depuis la DSP1, le compte de paiement est devenu une notion essentielle utilisée par un certain nombre de textes européens, notamment de niveau 1 : le règlement (UE) 260/2012, définissant les standards techniques applicables aux opérations de virements et prélèvements en euros (Règlement SEPA) et la directive 2014/92/UE, sur les comptes de paiement (Directive PAD), le règlement (UE) 2015/751, sur les frais d'interchange pour les paiements basés sur une carte de paiement (Règlement Interchange), le règlement (UE) 2015/847, sur les informations accompagnant les transferts de fonds et le Règlement (UE) 2021/1230, sur les paiements transfrontaliers. On notera également la DME2.

Pour autant, la notion de compte de paiement n'est pas essentielle à la DSP2. En effet, la directive s'attache à encadrer la fourniture de services de paiement dans l'Union par les prestataires de services de paiement.[244] D'ailleurs, on observera que la tenue d'un compte de paiement ne constitue pas, par elle-même, un service de paiement.[245]

Cela étant posé, comme le relèvent la Commission européenne[246] et l'ABE[247], la notion de compte de paiement est sujette à controverse.

---

[242] *Article 4(12) de la DSP2 (anciennement article 4(14) de la DSP1). Transposé à l'article L. 314-1- I du CMF.*

[243] *Article 4(5) de la DSP2, transposée à l'article L. 133-1-I du CMF. Voir G. Goffinet, « Le régime des comptes de paiement vu par le régulateur », Banque & Droit, novembre-décembre 2016, hors-série « Nouveaux comptes et intérêts négatifs », p. 21. Voir également, L. de Pellegars, « Le compte de paiement », Banque & Droit n° 134, novembre-décembre 2010, p. 14 ; D. Stucki et N. Kanhonou, « Le compte de paiement : une notion juridique stable pour une utilisation évolutive », Banque & Droit, hors-série, novembre-décembre 2019, p. 18 ; P. Storrer, « Brêves remarques sur le compte de paiement », Revue Banque n° 788, 13 octobre 2015.*

[244] *Articles 1 et 2 de la DSP2.*

[245] *Cf. la liste des services de paiement figurant à l'annexe 1 de la DSP2.*

[246] *DG FISMA, op. cit., spec. § 5.1.4, p. 111 : « Surely the most controversial across all stakeholders is the definition of "payment accounts": this is a key definition […] ».*

[247] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 juin 2022.*

D'abord, parce que, au niveau des textes européens, la DSP2 ne dispose pas du monopole de sa définition. En effet, depuis la DSP1, d'autres textes législatifs sont venus définir, pour les besoins de leur application respective, le compte de paiement de manière autonome. De fait, il n'existe pas une définition unique de compte de paiement, ce qui peut paraître paradoxal s'agissant d'une notion importante en matière de réglementation des services de paiement au sens large, et qui plus est, contenue dans une simple directive alors que des règlements européens (Règlement SEPA et Règlement Interchange, pour ne citer que ceux-ci), d'application directe dans la législation des États membres, font référence à cette notion.[248]

Or, on relèvera en particulier que le Règlement SEPA[249] associe indissociablement le numéro IBAN[250] à un compte de paiement.[251] En d'autres termes, aux fins d'exécution d'une opération de paiement consistant en un virement ou un prélèvement, [252] tout compte de paiement doit obligatoirement disposer d'un numéro IBAN. Par conséquent, si tout compte de paiement entrant dans le champ du Règlement SEPA[253] doit revêtir un numéro IBAN, l'inverse ne semble pas être vrai. En effet, un compte disposant d'un numéro IBAN n'est pas nécessairement un compte de paiement, car un tel numéro peut être attribué à tout type de compte.

Ensuite, parce qu'en créant le compte de paiement et en le soumettant à une réglementation autonome, distincte de celle qui s'appliquait généralement au domaine bancaire[254], la DSP a donné lieu à des conflits de frontières avec des notions voisines préexistantes, comme le compte « *bancaire* »[255],

---

[248] Sur la proposition visant à transformer la DSP2 en un règlement européen, voir supra paragraphe 1 (Élévation de la directive en règlement).

[249] Qui établit les règles pour les virements et les prélèvements libellés en euros dans l'Union lorsque tant le prestataire de services de paiement du payeur que celui du bénéficiaire, ou l'unique prestataire de services de paiement intervenant dans l'opération de paiement, sont situés dans l'Union.

[250] International bank account number, défini comme « un numéro de compte de paiement qui identifie sans équivoque un compte de paiement individuel ouvert dans un État membre, dont les éléments sont spécifiés par l'Organisation internationale de normalisation (ISO) » ; (article 2(15) du Règlement SEPA). L'IBAN est en quelque sorte la plaque d'immatriculation d'un compte bancaire : il permet de l'identifier. Il consiste en une variété de signes alphanumériques comprenant au minimum quatorze caractères, mais pouvant en comporter jusqu'à trente-quatre. La longueur de l'IBAN dépend du pays. En France, les codes IBAN comptent vingt-sept caractères. Les deux premiers caractères représentent le code du pays d'origine (par exemple, FR pour la France). Voir le site de l'ISO : https://www.iso.org/obp/ui/#iso:std:iso:13616:-1:ed-2:v1:en.

[251] Article 5(1)(a) du Règlement SEPA, renvoyant au paragraphe 1(a) de son annexe.

[252] Pour autant que le PSP du payeur et celui du bénéficiaire (ou l'unique PSP intervenant dans l'opération de paiement) soient situés dans l'Union.

[253] Voir en particulier les exceptions prévues à l'article 1(2) du Règlement SEPA.

[254] Cf. article L. 311-1 du CMF avant la DSP1 : la gestion de moyens de paiement relevait du monopole bancaire.

[255] Plus précisément, le compte de dépôt. Le terme compte bancaire, d'usage familier et historique ne correspond pas à une réalité juridique précise. Par conséquent, celle de compte de dépôt, plus précise, lui sera préférée.

ou de nouveaux comptes, comme le « *compte spécifique de monnaie électronique* » auquel la DME2 fait allusion.[256] Enfin, compte tenu de la liberté d'interprétation qu'offre l'absence d'une définition conceptuelle unique précise, il est parfois difficile de distinguer un compte de nature technique (ou comptable) d'un compte de paiement.

7.1.1 - Compte de dépôt et compte de paiement

S'agissant du compte de dépôt en premier lieu, il s'agit de bien comprendre en quoi un compte de paiement s'en distingue ou pas.

Contrairement au compte de paiement, le compte de dépôt n'est pas défini par la loi (dans les textes européens ou dans la loi française). D'ailleurs, la notion de compte de dépôt est suffisamment protéiforme pour englober différents types de comptes, lesquels d'ailleurs ne connaissent pas d'acceptions officielles ou réglementées qui les caractériseraient de manière générale. Ainsi, on peut évoquer l'existence de comptes de dépôt *stricto sensu* (en pratique souvent désignés comme des comptes courants), de comptes chèques, de comptes de dépôt à vue, etc.[257] Ce sont des comptes généralement utilisés dans la vie courante, pour domicilier ses revenus, payer ses dépenses courantes, etc. À ces comptes sont généralement associés des moyens de paiement, tels que la carte de paiement et le carnet de chèques.[258] On les distingue des comptes d'épargne qui, sous des vocables différents,[259] ne sont pas, en général, affectés aux dépenses courantes et ne sont alimentés qu'à partir du compte courant de leur titulaire (ou débités qu'en direction de ce même compte), originellement au sein de la même banque,[260] ce qui n'est toutefois plus le cas depuis la

[256] *Voir infra paragraphe 7.1.2.*

[257] *Voir toutefois la décision de caractère général n° 69-02 du 8 mai 1969 du Conseil national du crédit relative aux conditions de réception des fonds par les banques (la Décision CNC de 1969), qui opère une distinction entre une première catégorie, les comptes à vue et une seconde catégorie, les comptes sur livret ou à terme. Cette décision adopte une conception négative du compte à vue. Est ainsi un compte à vue un compte qui ne respecte pas les conditions applicables à la seconde catégorie de comptes.*

[258] *On voit déjà poindre le hiatus entre deux régimes juridiques distincts : si l'émission d'une carte de paiement (ou de crédit) constitue en effet un service de paiement soumis à la DSP2 (service n° 5, Annexe 1, DSP2), l'émission (et l'encaissement) des chèques est exclu de son champ (article 3(g) de la DSP2), et relève, en France, des services bancaires de paiement (article L. 311-1 du CMF) qui ressortissent du monopole bancaire (article L. 511-5, al. 2 du CMF).*

[259] *En France, comptes sur livret (non réglementés), comptes d'épargne réglementée (Livret A, Livret de Développement Durable et Solidaires (LDDS), etc.).*

[260] *En France, voir la Décision CNC de 1969 : concernant les comptes sur livret : « Les opérations enregistrées sur des comptes sur livret sont limitées à des versements ou des retraits au profit du titulaire ou à des virements de ou à son compte à vue » (article 2(B)(2)), et les comptes à terme : « Un compte distinct doit être ouvert pour chaque opération de dépôt à terme ; chacun de ces comptes ne peut enregistrer que l'écriture de virement ou de versement des fonds à bloquer, les écritures d'arrêté de compte et l'écriture de solde de compte à l'échéance prévue » (article 2(C)(2)).*

fin de l'année 2022.[261] Cela étant dit, il ne s'agit pas là d'une distinction absolue, puisqu'un compte d'épargne peut également être utilisé pour des dépenses courantes et permettre ainsi l'exécution d'opérations de paiement à son débit.[262] Finalement, le point commun entre tous les comptes dits « *bancaires* » est le fait, pour la banque, de recevoir les dépôts ou d'autres fonds remboursables de ses clients. Ces notions ne sont pas non plus définies dans les textes européens.[263] La CJCE considère pour sa part que le caractère remboursable, intrinsèque ou non, est une caractéristique essentielle du dépôt.[264] Le libre usage qui est accordé à l'établissement de crédit qui les reçoit est un critère proprement distinctif, ce que précise le droit français.[265]

Dès lors, suivant la définition littérale du compte de paiement contenue dans la DSP2, un compte de dépôt qui permet la réalisation d'opérations de paiement à son débit ou son crédit devrait donc nécessairement être un compte de paiement et l'établissement de crédit teneur du compte un PSP, au sens de la DSP2.[266] L'inverse n'est, en revanche, pas vrai pour un compte de paiement tenu par un établissement de paiement. En effet, en faisant sortir la fourniture des services de paiement du champ du monopole bancaire de la réception des dépôts[267] par la création d'une nouvelle catégorie d'acteurs que sont les établissements de paiement,[268] le législateur européen interdit corrélativement à ces derniers de recevoir des dépôts ou d'autres fonds remboursables du public, similairement aux établissements de monnaie électronique.[269] Cela dit, la frontière peut parfois sembler ténue en apparence : lorsque l'établissement reçoit des fonds des utilisateurs en vue de l'exécution

---

[261] Arrêté du 10 novembre 2022 modifiant la Décision CNC de 1969 qui permet à présent des virements entre des comptes appartenant au même titulaire dans différents établissements.

[262] En France, voir l'article R. 221-5-II du CMF concernant le Livret A. Pour autant, comme le Livret A n'est pas considéré comme un compte de paiement au sens de la DSP2, car sa finalité est l'épargne et non la réalisation d'opérations de paiement (G. Richard, « Nouveau droit d'accès aux comptes et aux données des comptes », Banque & Droit, hors série, mars 2019, p. 15 ; P. Storrer, « Brèves remarques sur le compte de paiement », Revue Banque n° 788, 13 octobre 2015.).

[263] L'article 9 de la CRD, qui est le siège du monopole de la réception des dépôts ou d'autres fonds remboursables du public, ne définit aucune de ces notions. Le paragraphe (14) du préambule de la CRD se contente d'indiquer la réception de fonds remboursables du public peut prendre la formes, telles que l'émission continue d'obligations d'autres titres comparables. On ne trouve pas non plus de définitions de ces notions dans le Règlement CRR.

[264] Voir CJCE, Affaire C-366/97, Romanelli, 11 février 1999. Également, article L. 312-2 du CMF.

[265] Article L. 312-2 du CMF : « Sont considérés comme fonds remboursables du public les fonds qu'une personne recueille d'un tiers, notamment sous la forme de dépôts, avec le droit d'en disposer pour son propre compte mais à charge pour elle de les restituer ».

[266] Voir les articles 1(a) et 4(11) de la DSP2.

[267] Posé par l'article 9(1) de la CRD, transposé à l'article L. 511-5, al. 1er du CMF.

[268] Paragraphe (10) du préambule de la DSP1.

[269] Article 18(3) et (5) de la DSP1. Cela entraîne également, pour l'établissement, s'il n'a pas opté pour une police d'assurance ou une garantie, l'obligation de cantonner ces fonds dans un compte séparé ouvert auprès d'un établissement de crédit ou de les investir en actifs à faible risque, liquides et sûrs (article 10(1)).

d'opérations futures,[270] l'établissement de paiement ne reçoit-il pas une forme de dépôt, d'autant plus si, comme la DSP2 l'y autorise, les fonds sont protégés par une police d'assurance ou une garantie, plutôt que par le biais du cantonnement ?[271] En réalité, il reste que l'EP ne peut employer les fonds reçus des utilisateurs de services de paiement à d'autres fins que la fourniture de services de paiement, car il ne peut tout simplement pas en disposer pour son propre compte.[272]

Pour autant, peut-on affirmer, comme il est dit plus haut, qu'un compte de dépôt est nécessairement un compte de paiement ? La définition finaliste est-elle suffisante à les distinguer lorsque le compte de dépôt ne présente pas les fonctionnalités d'un compte de paiement ? La question s'est précisément posée à propos du compte d'épargne qui, lorsqu'il n'est destiné qu'à une fonction d'épargne, devrait échapper à la qualification de compte de paiement. Pourtant, on ne peut qu'admettre qu'au moins deux opérations de paiement sont réalisées, d'une part à son crédit, lorsque son titulaire l'alimente, puis à son débit, lorsque ce même titulaire retire son épargne du compte.[273] Mais on relèvera que ces opérations ont souvent pour payeur et bénéficiaire la même personne, à savoir, le titulaire, qui utilise deux comptes lui appartenant : son compte de dépôt – compte de paiement, devrait-on dire – et son compte d'épargne. Dans le silence de la DSP2, la Directive PAD, prend le parti de les exclure de son champ d'application (qui certes est plus étroit que celui de la DSP2).[274] Cette approche est assez généralement partagée en doctrine,[275] quoique discutable compte tenu du fait qu'un compte d'épargne peut permettre l'exécution d'opérations de paiement.[276]

7.1.2 - Compte spécifique de monnaie électronique et compte de paiement

En second lieu, la DME2 a créé, de manière incidente, le concept de compte de monnaie électronique, en se bornant à indiquer que « *la définition de la monnaie électronique devrait comprendre à la fois*

---

[270] *Article 10(2) de la DSP2 (et, en France, article L.522-17-II du CMF).*

[271] *Article 10(1)(b) de la DSP2.*

[272] *Voir paragraphe (34) du préambule de la DSP2, en lien avec l'article L. 312-2 du CMF précité.*

[273] *Ce qui manifeste la fourniture des services n° 1, 2 et 3(c) de l'annexe 1 de la DSP2 par la banque teneuse de compte.*

[274] *Paragraphe (12) du préambule de la Directive PAD, sauf s'ils « devaient être utilisés pour exécuter des opérations de paiement quotidiennes et s'ils devaient comporter toutes les fonctions » attribuées au compte de paiement par la DSP2. Voir infra, l'Arrêt ING DiBA au paragraphe 7.2.2 du présent rapport.*

[275] *Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), Rapport, « Analyse nationale des risques de blanchiment de capitaux et du terrorisme en France », janvier 2023, spéc. p. 79 : « Le compte de paiement est défini au I de l'article L. 314-1 du Code monétaire et financier et permet notamment les dépôts, mais tous les comptes de dépôt ne sont pas des comptes de paiement (exemple : compte d'épargne). » ; G. Richard, « Nouveau d'accès aux comptes et aux données des comptes », Banque & Droit, hors-série, mars 2019, p. 15 ; P. Storrer, « Brèves remarques sur le compte de paiement », Revue Banque, n° 788, 13 octobre 2015.*

[276] *Voir note de bas de page n° 262 ci-dessus.*

la monnaie électronique ayant pour support un dispositif de paiement que le détenteur de monnaie électronique a en sa possession et celle qui est stockée à distance sur un serveur et gérée par le détenteur de monnaie électronique par l'intermédiaire d'un compte spécifique de monnaie électronique »,[277] sans le définir[278] mais tout en reconnaissant à ce compte *sui generis* la capacité d'y stocker de la monnaie électronique. Il résulte de la définition de monnaie électronique que celle-ci peut être émise sur différents supports, à savoir : soit sur un support physique susceptible de possession (tel qu'une carte), soit sur un support logiciel (dans lequel des comptes informatiques sont créés) où sont inscrites les unités de monnaie électronique. En réalité, peu importe en pratique, car si la monnaie électronique n'est pas stockée dans une carte de paiement, l'utilisateur ouvre un compte auprès de l'émetteur de monnaie électronique afin de se voir créditer la monnaie électronique émise par celui-ci,[279] fréquemment qualifié en pratique de *wallet* ou *e-wallet*, compte auquel peuvent-être associés des instruments de paiement de type carte de paiement sans que ceux-ci ne stockent directement la monnaie électronique.[280]

Si, d'un point de vue juridique, ce compte ne peut être confondu avec un compte de dépôt, de la même manière qu'un compte de paiement tenu par un établissement de paiement ne peut servir de réceptacle aux dépôts du public,[281] le solde de ce compte de monnaie électronique constitue pourtant bien une créance de remboursement contre l'établissement de monnaie électronique,[282] ce qui le rapproche de la monnaie scripturale, c'est-à-dire du solde d'un compte de dépôt.[283] D'ailleurs, le compte de monnaie électronique remplit les mêmes fonctions, au-delà même de simplement stocker la valeur monétaire sous forme électronique, c'est-à-dire, celles de permettre l'exécution d'opérations de paiement, à savoir en particulier, de transférer la créance de solde du compte appartenant au titulaire (payeur) à une autre personne (bénéficiaire).[284] Toutefois, les modalités de transfert entre des comptes de monnaie électronique et des comptes de paiement sont juridiquement différentes, en particulier lorsque les transferts rentrent dans le champ du Règlement SEPA.

---

[277] *Considérant n° 8 de la DME2. Cette notion n'existait pas sous l'empire de la DME1.*

[278] *D'ailleurs, la Banque de France parle plus volontiers de portefeuille de monnaie électronique (https://particuliers.banque-france.fr/info-banque-assurance/compte/les-differents-types-de-comptes).*

[279] *Voir les conditions générales de PayPal, https://www.paypalobjects.com/ua/FR_fr_FR/ua.pdf. À noter que c'est un établissement de crédit. Le compte est parfois aussi qualifié de wallet, voir les conditions générales de Lydia, https://www.lydia-app.com/info/cgu-service-lydia-iban/.*

[280] *ABE, « Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) », EBA/Op/2022/06, 23 juin 2022.*

[281] *Article 6(2) et (3) de la DME2.*

[282] *Article 2(d) de la DME2 : la monnaie électronique constitue « une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur ».*

[283] *Sans toutefois pouvoir être un moyen d'épargne (considérant n° 13 de la DME2). Cependant, on remarquera que le parallèle trouve sa limite dans le fait que, alors qu'un compte de dépôt fait naître un droit de créance du titulaire du compte contre le teneur du compte (et non contre l'émetteur de la monnaie elle-même), la monnaie électronique constitue sur un droit de créance contre le seul émetteur de la monnaie électronique.*

[284] *Voir par exemple l'article 4.2 (Fonctionnement du compte) des conditions générales de Mangopay ; article 3 (Envoi d'argent) des conditions générales de PayPal.*

En revanche, il est permis de se demander s'il ne constitue pas un compte de paiement.[285] En effet, la DME2 entretient l'ambiguïté lorsqu'elle précise que la définition de monnaie électronique « *devrait couvrir toutes les situations dans lesquelles un prestataire de services de paiement émet en contrepartie de fonds une valeur stockée prépayée, qui peut être utilisée à des fins de paiement car elle est acceptée par des tiers en tant que paiement* ». Au surplus, la DSP2 elle-même prévoit que la monnaie électronique puisse être stockée sur un compte de paiement.[286] De son côté, le considérant n° 12 de la Directive PAD exclut, à titre réfragable, les comptes de monnaie électronique du champ des comptes de paiement en raison des fonctionnalités généralement plus limitées de ces comptes. Enfin, le Règlement Interchange ne précise-t-il pas également que le compte de paiement est un « *compte détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et servant à exécuter des opérations de paiement, y compris au moyen d'un compte spécifique de monnaie électronique au sens de l'article 2, point 2, de la directive 2009/110/CE du Parlement européen et du Conseil* »?[287] Dès lors, la frontière entre le moyen de paiement constitué par la monnaie électronique et les instruments de paiement utilisés pour transférer des fonds depuis, ou en direction, du compte de paiement devient alors très fine, d'autant plus lorsque le compte de paiement peut être crédité de sommes destinées à l'exécution d'opérations de paiement futures.[288] Pour finir, comme le remarquait un auteur en 2010, « *la différence entre le compte de monnaie électronique et le compte de paiement deviendra alors très ténue si l'on considère le développement en parallèle des moyens de paiement dématérialisés adossés à des comptes de paiement (transmission d'ordre par téléphone portable…). En effet, comment distinguer le titulaire d'un compte de paiement qui transmet son ordre par une carte virtuelle attachée à un compte de paiement de celui émettant son ordre à partir d'un numéro de compte de monnaie électronique ?* ».[289] Treize ans plus tard, la DG FISMA ne dit pas autre chose.[290] Selon les modèles de fonctionnement de monnaie électronique, certains comptes de monnaie électronique pourraient être qualifiés de comptes de paiement lorsque leurs fonctionnalités sont importantes et comparables à un compte de paiement.

7.1.3 - Compte technique et compte de paiement

La notion de compte dit « *technique* » est, quant à elle, plus difficile encore à appréhender, car elle recouvre des réalités très différentes, en fonction des objectifs que ce type de compte cherche

---

[285] *Voir M. Roussille, « La notion de compte de paiement », Banque et droit, novembre-décembre 2016, hors-série « Nouveaux comptes et intérêts négatifs », p. 12. Spéc : « (…) le compte de monnaie électronique est-il par principe un compte de paiement, dès lors qu'il a vocation à permettre à son titulaire de recevoir des unités de monnaie électronique ou de régler des créanciers en unités de monnaie électronique. La notion de compte de paiement traduit ainsi la soumission à un régime qui se cumule avec les règles spécifiques applicables à chaque type de comptes ».*

[286] *Article 63(3) de la DSP2.*

[287] *Article 2(22) du Règlement Interchange, définissant le compte de paiement. Voir également, P. Storrer, « Brèves remarques sur le compte de paiement », Revue Banque, n° 788, 13 octobre 2015.*

[288] *Voir supra note de bas de page n° 270.*

[289] *L. de Pellegars, « Le compte de paiement », op. cit., p. 16.*

[290] *DG FISMA, op. cit., p. 40.*

à poursuivre.[291] Au surplus, il convient de ne pas s'y tromper : en matière de comptabilité à partie double, toutes dettes et créances donnent lieu à des écritures au débit et au crédit de comptes comptables (notamment comptes de tiers : clients, fournisseurs, créanciers de tous types, etc.).[292] Ces comptes doivent-ils nécessairement être qualifiés de compte de paiement ?

Les situations factuelles étant spécifiques, une analyse au cas par cas, au travers de quelques exemples, s'avère nécessaire.

Un premier exemple peut être tiré du fait que, depuis quelques années, des grandes banques internationales proposent à leurs clients, souvent de grands groupes industriels, l'ouverture de comptes techniques ou administratifs, dits « *virtuels* », destinés à faciliter la gestion de leur trésorerie.[293] Concrètement, une banque tenant le compte de paiement d'une société (appelé compte maître ou parfois compte physique) propose à son client d'ouvrir des comptes, dits virtuels, désignant des filiales de cette société. À chaque filiale est ainsi associé un de ces comptes virtuels. Ces comptes sont destinés à enregistrer les opérations de débit et de crédit correspondant à des paiements qui seront réalisés ou reçus par la société à partir du compte maître, agissant au nom et pour le compte de ses filiales.[294] À ces comptes peuvent être associées des références IBAN.[295] La question s'est posée de savoir si ces comptes virtuels constituent des comptes de paiements soumis aux dispositions de la DSP2, en particulier dans le contexte où de tels comptes se voient attribuer une référence IBAN (qualifiée également de virtuelle) et que, dans certains cas, les filiales auxquelles sont attribuées ces comptes peuvent notifier des ordres de paiement à la banque tenant le compte maître au nom de la société qui en est titulaire.

---

[291] D'ailleurs il n'existe pas, en tant que telle, une acceptation ni unique, ni officielle : en pratique ces comptes sont souvent qualifiés de comptes virtuels, d'attente, intermédiaires, etc.

[292] Règlement ANC n° 2014-03 du 5 juin 2014 relatif au plan comptable général. Comptes de classe 4 (compte de tiers).

[293] Voir par exemple : Oracle, « Virtual accounts », white paper, novembre 2018, https://www.oracle.com/us/financial-services/fs-virtual-account-management-wp-5248866.pdf ; BNP Paribas, https://cashmanagement.bnpparibas.com/our-solutions/trends-vision/np-paribas%E2%80%99s-virtual-account-management-platform-offers-countless ; JPMorgan, https://www.jpmorgan.com/solutions/payments/solutions/virtual-account-management ; Deutsche Bank, https://corporates.db.com/solutions/corporate-bank-solutions/cash-management/virtual-accounts ; Goldman Sachs, https://www.goldmansachs.com/what-we-do/transaction-banking/insights/virtual-account-management.pdf ; etc.

[294] POBO (payment of behalf of) et ROBO (receipt on behalf of) payments. L'intérêt de ces comptes reside dans ce qu'est faite l'économie d'ouvrir autant de comptes physiques que de filiales, voire pour chaque business units au sein de celles-ci ou, dans une approche matricielle, au sein d'une géographie particulière (voir p. ex. Goldman Sachs et Deloitte, « Virtual Account Management: A foundational imperative for cash concentration », 2020, p. 2).

[295] Voir ci-dessus, note de bas de page n° 250. Il s'agit d'un standard technique qui n'a donc pas de valeur juridique obligatoire. Toutefois, cette norme est utilisée par le Règlement SEPA, qui le définit comme « un numéro de compte de paiement qui identifie sans équivoque un compte de paiement individuel ouvert dans un État membre, dont les éléments sont spécifiés par l'Organisation internationale de normalisation (ISO) » (article 2(15) du Règlement SEPA) et lui attribue une obligatoire pour les comptes de paiement concernant les virements et les prélèvements (article 5(a) du Règlement SEPA).

Si l'on s'en tient à la définition finaliste du compte de paiement,[296] alors, dans ce contexte, ces comptes virtuels ne devraient pas être qualifiés de tels. En effet, ces omptes n'ont d'autre vocation que le suivi administratif et comptable des paiements reçus ou effectués pour le compte des filiales dans le cadre de la gestion des flux au sein de la *payment factory* du groupe de sociétés concerné, et les opérations de paiement ne sont exécutées qu'au crédit ou au débit du compte maître, les écritures réalisées sur les comptes virtuels n'en étant que le reflet.[297]

Un deuxième exemple peut être tiré du modèle des EP et EME qui mandatent des agents, tels que des places de marchés. Dans ce modèle, les fonds des utilisateurs de services de paiement (généralement des personnes morales) sont encaissés sur un seul compte ouvert au nom de l'agent (compte appelé aussi « *master account* »). À ce compte sont attachés indirectement des cartes de paiement appartenant aux utilisateurs. Plus exactement, entre le « *master account* » et les cartes de paiement s'interposent des comptes « *techniques* », ouverts au nom du titulaire de chaque carte de paiement. Ces comptes, comportant un solde égal à zéro, servent principalement à ségréger les flux de paiement par porteur de carte. Toutefois, des fonds transitent par ces comptes car lors d'une opération de paiement par carte, le montant de l'achat est débité du « *master account* », crédité sur le compte dit « *technique* », ou de passage, et transféré in fine sur le compte de règlement de l'EP ou EME pour transmission au système de paiement par carte. L'enregistrement des flux en entrée et en sortie sur ce compte et l'exécution de l'opération de paiement par carte depuis ce compte, permettent, selon l'ACPR, de retenir la qualification de compte de paiement.

Un troisième exemple est celui de l'externalisation du service d'émission de carte par un PSP vers un autre PSP, membre du réseau Mastercard ou Visa par exemple. D'un point de vue technique, les cartes de paiement doivent être attachées à un compte. Le PSP, émetteur de la carte, rattache ces cartes à des comptes techniques ouverts dans ses livres (aussi appelés « *comptes miroirs* »). Ces comptes sont ouverts soit au nom du PSP partenaire (avec des sous-comptes au nom de chaque porteur de carte), soit au nom de chaque porteur de carte. Ces comptes techniques sont généralement préalimentés soit par le PSP qui est en relation contractuelle avec les utilisateurs, soit par le PSP, émetteur de la carte. Il s'agit d'une avance de paiement à titre onéreux. Or, ici encore, selon l'ACPR, l'enregistrement des fonds sur ces comptes et l'exécution de l'opération de paiement par carte depuis ces comptes entrainent une qualification de comptes de paiement.

Les enjeux liés à la qualification de compte de paiement sont donc nombreux et importants au regard des conséquences qui découlent, notamment, de l'application de la DSP2, ainsi que d'autres

[296] *Notamment à la lumière de l'Arrêt ING DiBa (voir infra paragraphe 7.2.2).*

[297] *Les opérations de paiement ne peuvent en effet être effectuées directement depuis les comptes virtuels et le recours à un compte intermédiaire (le compte maître) est nécessaire. Cela correspond à la situation décrite par l'arrêt ING DiBa (cf. considérants n° 32 et 33 de la décision).*

textes.[298] On peut mentionner, sans prétendre à l'exhaustivité :

(i) l'obligation d'agrément (en qualité d'établissement de paiement, de crédit ou de monnaie électronique). En effet, même si la tenue d'un compte de paiement ne constitue pas à proprement parler un service de paiement, dont la fourniture à titre de profession habituelle requiert un agrément,[299] la tenue d'un tel compte emporte nécessairement la fourniture de certains services de paiement qui y sont associés ;[300]

(ii) la possible nullité ou l'inefficacité de certaines clauses contractuelles si elles se trouvent en conflit avec les dispositions d'ordre public de la DSP2 ;[301]

(iii) l'obligation faite pour un PSP gestionnaire de compte (PSPGC) d'appliquer l'authentification forte (SCA) du titulaire du compte ;[302] et

(iv) la facilitation de la fourniture des services d'informations sur les comptes et d'initiation de paiement sur les comptes[303] (l'*open banking*)[304] et le respect des contraintes techniques qui en découlent.[305]

7.2 - Quel est le régime juridique actuel ?

7.2.1 - Dans la DSP2 (et les autres textes européens pertinents)

Si le siège historique de la définition de compte de paiement est la DSP1 (remplacée par la DSP2), cette notion se retrouve également définie de manière autonome dans d'autres textes législatifs pour leurs propres besoins (Règlement SEPA, Directive PAD et Règlement Interchange)[306].

Ces textes ont certes des finalités et, parfois, des champs d'application distincts. Ainsi, la Directive PAD ne s'applique qu'aux comptes de paiement détenus par des consommateurs et vise, notamment, à faciliter la transparence et la comparabilité des frais liés aux comptes de paiement, ainsi que le

[298] *Tels que le Règlement SEPA par exemple.*

[299] *Article 37(1) de la DSP2, transposé à l'article L. 521-2 du CMF.*

[300] *G. Goffinet, op. cit., spéc. p. 22.*

[301] *C'était précisément l'objet du litige au fond en droit autrichien qui a donné lieu à la question préjudicielle soumise à la CJUE dans l'Arrêt ING DiBa cité infra.*

[302] *Article 97(1)(a) de la DSP2.*

[303] *Respectivement, services n° 8 et 7 de l'annexe I de la DSP2.*

[304] *Articles 66 et 67 de la DSP2.*

[305] *Prévues dans le règlement délégué 2018/349.*

[306] *Voir Annexe VI pour les définitions.*

changement de compte.[307] Si, de prime abord, les définitions respectives du compte de paiement sont en substance identiques à celles de la DSP2, il convient d'y regarder de plus près s'agissant de la Directive PAD. En effet, son considérant n° 12 fixe une règle d'interprétation inconnue des autres textes précités : « *L'ensemble des dispositions de la présente directive devraient s'appliquer aux comptes de paiement permettant aux consommateurs d'effectuer les opérations suivantes : verser des fonds, retirer des espèces et exécuter des opérations de paiement, y compris l'exécution de virements, en faveur de tiers, ou être les bénéficiaires de telles opérations de la part de tiers* ».[308]

7.2.2 - Jurisprudence européenne

Par un arrêt du 4 octobre 2018, saisie d'une question préjudicielle, la CJUE s'est prononcée sur la définition du compte de paiement contenue dans la DSP1 à l'aune de la Directive PAD précitée (l'« ***Arrêt ING DiBA*** »).[309]

Selon la Cour, la possibilité d'effectuer, à partir d'un compte, des opérations de paiement en faveur d'un tiers *ou*[310] de bénéficier de telles opérations effectuées par un tiers est un élément constitutif de la notion de compte de paiement sur la base de l'article 1(6) de la Directive PAD.[311] Dès lors, un compte à partir duquel de telles opérations de paiement ne peuvent être effectuées directement, mais pour la réalisation desquelles le recours à un compte intermédiaire (par exemple, un compte de dépôt) est nécessaire ne peut donc être considéré comme étant un compte de paiement, au sens

[307] *Article 1(1) de la Directive PAD.*

[308] *Considérant n° 12 du préambule de la Directive PAD. Voir également, en ce sens, l'article 1(6) de la Directive PAD qui précise : « La présente directive s'applique aux comptes de paiement permettant aux consommateurs d'effectuer au moins les opérations suivantes : a) verser des fonds sur un compte de paiement ; b) retirer des espèces d'un compte de paiement ; c) exécuter des opérations de paiement, y compris des virements, en faveur d'un tiers et être les bénéficiaires de telles opérations effectuées par un tiers. »*

[309] *CJUE, Affaire C-191/17, Bundeskammer für Arbeiter und Angestellte contre ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG. Voir commentaire P. Storrer, « Le rendez-vous manqué entre la CJUE et le compte de paiement », Banque & Droit, n° 182, novembre-décembre 2018, p. 50. Voir également, Bird & Bird, https://www.twobirds.com/en/insights/2018/global/the-cjeu-provides-clarity-on-the-definition-of-a-payment-account.*

[310] *Si la version française de la décision de la CJUE utilise le terme alternatif « ou », des membres du groupe de travail font remarquer qu'il s'agirait d'un problème de traduction de la version française de la décision par rapport à la version originale allemande concernant la traduction du mot « beziehungsweise » (respectivement) dans le paragraphe (31) de la décision. L'article 1(6) de la Directive PAD, sur laquelle la CJUE se base, vise les comptes de paiement permettant d'exécuter des opérations de paiement, y compris des virements, en faveur d'un tiers et être les bénéficiaires de telles opérations effectuées par un tiers. À titre d'exemple, les versions italiennes et espagnoles de la décision de la CJUE confirment cette hypothèse en ce que ces versions font du cumul de la possibilité d'exécuter des opérations de paiement envers des tiers et la possibilité de recevoir de telles opérations le critère de caractérisation d'un compte de paiement.*

[311] *Considérant n° 31.*

de la Directive PAD et, en conséquence, au sens de la DSP1.[312] On notera que la notion de tiers n'est toutefois pas reprise dans la décision elle-même.[313]

7.2.3 - Dans la législation des États-membres

Une analyse multi juridictionnelle a été conduite dans sept pays concernant : (i) la définition et l'interprétation locales de la notion de compte de paiement[314]; et (ii) les éventuelles précisions attendues dans chacune des juridictions.

La définition du compte de paiement prévue par la DSP2 est reprise fidèlement dans les sept juridictions interrogées. Toutefois, dans quatre des sept juridictions interrogées, des précisions sur la définition du compte de paiement ont été apportées par le régulateur ou par le législateur, ainsi[315] :

(i) en Allemagne, le régulateur a notamment précisé : (*x*) qu'un compte est qualifié de compte de paiement s'il permet l'exécution d'opérations de paiement ; (*y*) que les comptes de dépôt, les comptes d'épargne en ligne et les comptes tenus par un émetteur de monnaie électronique pour comptabiliser la monnaie électronique en circulation de l'émetteur (*shadow accounts*) ne sont pas des comptes de paiement ; et, enfin (*z*) s'agissant des comptes internes et techniques, qu'ils peuvent entrer dans la qualification de compte de paiement s'ils permettent de documenter l'obligation de paiement qui existe entre le détenteur du compte et un tiers – par conséquent les comptes techniques tels que les comptes de facturation pour les cartes de crédits ou les comptes d'attente ne sont pas des comptes de paiement, car ils ne sont pas destinés aux opérations de paiement ;

(ii) au Luxembourg, le superviseur a notamment précisé que : (*x*) sont des comptes de paiement, les comptes qui permettent l'exécution d'opérations de paiement ; et (*y*) les comptes et portefeuilles de monnaie électronique sont des comptes de paiement – sur ce point le Luxembourg et l'Allemagne ont donc une position divergente ;

(iii) aux Pays-Bas, le régulateur a notamment précisé que pour qualifier un compte d'épargne en compte de paiement, il convenait d'identifier s'il était possible de réaliser des opérations de paiement via ce compte ; et

---

[312] Considérant n° 32.

[313] « Par ces motifs, la Cour (cinquième chambre) dit pour droit : L'article 4, point 14, de la [DSP1] doit être interprété en ce sens que ne relève pas de la notion de « compte de paiement » un compte d'épargne qui permet de disposer de sommes déposées à vue et à partir duquel des opérations de versement et de retrait ne peuvent être effectuées que par l'intermédiaire d'un compte courant. »

[314] Allemagne, Belgique, Espagne, Italie, Luxembourg, Pays-Bas, Pologne.

[315] Pour plus d'informations, voir Annexe II du présent rapport.

(iv) en Pologne, le législateur a précisé que le compte bancaire et le compte d'épargne peuvent être également des comptes de paiement, si ces comptes sont utilisés pour réaliser des opérations de paiement.

Il ressort de ces précisions que le critère clef pour qualifier un compte de paiement consiste en la possibilité de réaliser des opérations de paiement directement à partir dudit compte. Cette position est en ligne avec l'Arrêt ING DiBa.

Dans les sept juridictions interrogées, il n'a pas été identifié de jurisprudence locale en lien avec la définition du compte de paiement. La jurisprudence créée par l'Arrêt ING DiBA étant donc la seule applicable.[316]

Les clarifications attendues dans le cadre de la DSP3 sont les suivantes :

(A) pour l'Allemagne et la Pologne[317] : il n'a pas été identifié de clarification attendue ;

(B) pour le Luxembourg : les clarifications attendues sont celles mentionnées par l'ABE, *e.g.* avoir une définition du compte de paiement plus détaillée avec des critères et/ou des références à des caractéristiques spécifiques ainsi qu'une clarification de la notion de « tiers », tout en précisant que la nouvelle définition devrait assurer une neutralité du modèle économique et faciliter le développement de solutions de paiement différentes et innovatrices ;

(C) pour les autres juridictions, il conviendrait : (*x*) de préciser les éléments techniques du compte de paiement (Pays-Bas) et le distinguer des autres types de comptes, *e.g.* comptes courants (France, Italie) ou d'épargne (Belgique) ; (*y*) de prévoir une définition des comptes miroirs, des comptes techniques ou encore des comptes d'intermédiation (Espagne, France, Italie) ; et (*z*) d'indiquer, si certains instruments, tels que les cartes prépayées, les portefeuilles (*wallets*) et les portefeuilles de monnaie électronique (*e-wallets*) peuvent être qualifiés de comptes de paiement et donc se voir appliquer les règles relatives au compte de paiement[318] (Espagne).

Le détail de l'analyse multi juridictionnelle se trouve en Annexe III du présent document.

---

[316] *Arrêt ING-DiBa.*

[317] *Juridictions dans lesquelles des clarifications à la définition du compte de paiement ont été apportées.*

[318] *Cela rejoindrait donc l'actuelle position du Luxembourg.*

7.3 - Recommandations du HCJP

Sur la question de savoir si une définition unique du compte de paiement au sein des différents textes qui y font référence ou le redéfinissent, un consensus s'est dégagé au sein du groupe de travail en faveur d'une réponse positive. Le siège de cette définition devrait rester la DSP2.[319]

Recommandation n° 13 : le HCJP recommande de ne retenir qu'une seule et unique définition de compte de paiement qui serait contenue dans la DSP, les autres textes pertinents (en particulier, la Directive PAD, le Règlement SEPA et le Règlement Interchange) devant y faire référence.

Ensuite, sur le fond, les avis au sein du groupe de travail sont partagés.

Certains membres sont en faveur du maintien du *status quo*, ce qui signifie que la définition du compte de paiement contenue dans la DSP2 doit rester interprétée à la lumière de l'Arrêt ING DiBA.

Or cet arrêt dit deux choses : *d'une part*, qu'un compte à partir duquel des opérations de paiement ne peuvent être effectuées directement, mais nécessitent le recours à un compte intermédiaire n'est pas un compte de paiement ; et *d'autre part*, que la possibilité d'effectuer des opérations de paiement en faveur d'un tiers[320] ou de bénéficier de telles opérations effectuées par un tiers est un élément constitutif du compte de paiement.

Concernant le premier point, le groupe de travail convient du fait que cette condition est essentielle à la qualification du compte de paiement.

Le second point fait en revanche l'objet de vifs débats au sein du groupe. La notion de tiers est en effet susceptible de deux interprétations différentes. Selon une première interprétation, le tiers (payeur ou bénéficiaire) serait toute personne qui n'est pas le titulaire du compte au sujet duquel la qualification de compte de paiement est en question. Ainsi, si ce compte ne peut être alimenté que par des fonds provenant de tout autre compte appartenant au même titulaire, y compris si ce dernier compte est ouvert auprès d'un autre PSP, ni débité autrement qu'au profit de tout autre compte appartenant à ce titulaire, alors il ne peut s'agir d'un compte de paiement. Cette interprétation devrait être considérée comme conforme aux prévisions de l'Arrêt ING DiBA, compte tenu de la situation factuelle dont la Cour a été saisie.[321]

---

[319] *La recommandation s'étend à d'autres concepts utilisés et parfois redéfinis dans ces textes dans la mesure où une définition commune et unique est pertinente.*

[320] *Voir note de bas de page n° 309.*

[321] *Voir le considérant n° 12 : « ING-DiBa Direktbank Austria propose des comptes d'épargne en ligne à partir desquels ses clients peuvent effectuer, au moyen d'un service télébancaire, des versements et des retraits. Ces virements doivent toujours être effectués par l'intermédiaire de comptes de référence ouvert au nom de ces clients. Ces comptes de référence sont des comptes courants que lesdits clients peuvent également détenir dans une banque autre qu'ING-DiBa Direktbank Austria. (…) ».*

Selon une seconde interprétation, la notion de tiers devrait être associée, non seulement à toute autre personne que le titulaire lui-même, mais également, à ce dernier au titre de tout compte ouvert auprès d'un autre PSP que celui qui tient le compte en question. Ainsi, même en cas d'opération de paiement entre des comptes ouverts auprès de PSP distincts mais appartenant à la même personne, ces comptes seraient tous des comptes de paiement. Cette dernière interprétation a les faveurs de l'ACPR, en raison du fait que la première interprétation aurait pour effet de restreindre le champ des obligations des PSP gestionnaires de compte en matière d'*Open Banking*.[322] La FBF partage le même avis, avec quelques nuances, considérant pour sa part qu'un compte de paiement utilisé pour effectuer des opérations de paiement en faveur d'un autre compte ouvert au nom du même titulaire dans un même établissement ou dans des établissements différents, reste un compte de paiement, dès lors que la réglementation attachée à ce compte ne lui interdit pas d'effectuer des opérations de paiement en faveur d'un tiers ou de bénéficier de telles opérations effectuées par un tiers.

En conclusion, les avis du groupe de travail restent partagés sur cette question. Le groupe de travail se limite donc à recommander au législateur européen et à l'ABE d'approfondir l'analyse afin de conclure sur l'opportunité d'inclure ou non dans la DSP une référence à la notion de tiers dans la définition du compte de paiement, et de prendre expressément parti aux fins de sécurité juridique. Il est en effet rappelé qu'à défaut de précision dans le texte de la DSP3, la notion de compte de paiement devant continuer de s'interpréter à la lumière de l'Arrêt ING DiBA qui inclut cette référence à la notion de tiers.

Recommandation n° 14 : le HCJP recommande :

- de modifier de modifier la DSP2 (soit dans les considérants, soit dans la définition de compte de paiement) afin de préciser qu'un compte à partir duquel des opérations de paiement ne peuvent être effectuées directement, mais nécessitent le recours à un compte intermédiaire n'est pas un compte de paiement ; et

- au législateur européen et à l'ABE, d'évaluer de manière plus approfondie si la notion de tiers est pertinente au regard de la définition de compte de paiement, et de prendre expressément parti aux fins de sécurité juridique.

[322] *Selon l'ACPR, une telle restriction aurait, selon elle, comme conséquence un affaiblissement de la protection des utilisateurs des services de paiement (par un recours massif au web scrapping) ainsi qu'un risque financier supplémentaire pour les établissements de paiement et les établissements de monnaie électronique car, en cas de perte de données des utilisateurs des services de paiement, ces prestataires seraient responsables et devraient en conséquence indemniser leurs clients. Par ailleurs, une telle recommandation irait à l'encontre des recommandations de l'ABE ainsi que de celles des institutions européennes et nationales compétentes en matière de protection des données personnelles (l'EDPB et la CNIL ont ainsi recommandé la mise en place et l'utilisation des API par les acteurs financiers pour encadrer et sécuriser l'accès à des données financières et d'assurance, même au-delà des données liées aux comptes de paiement).*

VIII. Responsabilité des PSP

8.1 - Le guichet unique et la répartition de la responsabilité entre le PSPGC et les TPP

8.1.1 - Enjeux et régime juridique actuel

Par principe, chacun est responsable du dommage qu'il a causé par son fait, sa négligence ou par son imprudence (article 1241 du Code civil français). Par exception, le droit français prévoit des cas de responsabilité du fait d'autrui (article 1242 du Code civil français).

Ces situations trouvent notamment leur justification dans la volonté de protéger la victime. Les cas de responsabilité du fait d'autrui sont précisément ceux dans lesquels une insolvabilité de l'auteur du dommage est à redouter (enfant mineur, préposé, domestique, etc.).[323]

L'ensemble des hypothèses de responsabilité pour autrui présentent une similitude essentielle : la personne civilement responsable exerce une autorité sur la personne de l'auteur du dommage. La responsabilité pour autrui apparaît ainsi comme une contrepartie de l'exercice de ces pouvoirs.

Ces deux caractéristiques sont absentes du régime fixé par la DSP puisque, d'une part, les prestataires de services de paiement tiers (TPP) ne présentent pas de risque particulier d'insolvabilité (la DSP a au contraire, fixé un certain nombre d'exigences destinées à l'éviter) et, d'autre part, le PSP gestionnaire de compte (PSPGC) n'exerce aucun pouvoir ni contrôle sur les TPP ni sur les opérations qu'ils effectuent et que le PSPGC est obligé d'exécuter.

Ainsi, la responsabilité du PSPGC ne peut pas trouver son fondement dans la responsabilité du fait d'autrui ou d'une interprétation extensive de ce principe. Il s'agit bien d'un régime exorbitant de droit commun dans sa relation avec les TPP.

En effet le PSPGC est contraint, lorsqu'un payeur nie avoir autorisé une opération de paiement initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, à rembourser le payeur immédiatement, et en tout état de cause au plus tard à la fin du premier jour ouvrable suivant, le montant de l'opération de paiement non autorisée.

Si la DSP2 prévoit bien un principe d'indemnisation immédiate du PSPGC par le prestataire de services d'initiation de paiement (PSIP) pour les pertes subies ou les sommes payées en raison du remboursement du payeur lorsque le PSIP est responsable de l'opération de paiement non

[323] *Jérôme Julien, « Responsabilité du fait d'autrui », Répertoire civil Dalloz.*

autorisée[324], l'absence de relations contractuelles entre eux rend ce principe difficile à mettre en œuvre.

Il conviendrait en particulier de compléter le dispositif pour faciliter cette indemnisation, lorsqu'un PSPGC et un PSIP conviennent que l'authentification forte incombera, non au PSPGC mais au PSIP.

Dans cette situation, le groupe de travail propose :

(i) que le PSIP supporte pleinement et effectivement les conséquences de l'opération non autorisée et le remboursement du payeur, sauf accord contraire des parties ;

(ii) de prévoir la contractualisation de la relation entre PSPGC et PSP tiers, en formalisant dans le contrat la part de responsabilité qui incombe à chacun des acteurs en ayant procédé, au préalable, à une segmentation précise de l'opération visée (de sorte qu'*in fine*, chaque protagoniste puisse voir sa responsabilité engagée pour la partie de l'opération qui nécessite son intervention, sauf à ce que celui-ci rapporte la preuve de sa bonne exécution) ; et

(iii) que, dans l'hypothèse où l'opération doive être remboursée par le PSPGC sur la base du principe du guichet unique, le contrat identifie, en amont, les responsabilités de chacune des parties de manière précise ; dès lors, l'exécution du contrat aboutirait à une prise en charge du remboursement de l'opération par la partie défaillante en fonction des obligations mises à sa charge dans un délai fixé contractuellement, nécessairement court (puisque le PSPGC a une obligation de rembourser l'opération non autorisée à J+1). Il en résulterait, en définitive, une clarification opportune des obligations juridiques mises à la charge des acteurs impliqués dans la transaction bancaire.

8.1.2 - Recommandations du HCJP

Recommandation n° 15 :

- le HCJP recommande de compléter l'article 97 de DSP2 par un 6e paragraphe : (i) permettant aux PSP gestionnaires de comptes (PSPGC) et aux prestataires de services d'initiation de paiement (PSIP) de pouvoir convenir que la procédure d'authentification forte incombera, non à le PSPGC mais au PSIP ; (ii) précisant que, dans ce cadre, le PSIP est responsable vis-à-vis de l'utilisateur dans les termes de l'article 73(1) de la DSP2 ; et (iii) que le PSIP doit préalablement en informer l'utilisateur conformément à l'article 52 de la DSP2. La rédaction proposée est la suivante :

[324] *Article 73(2), §2 de DSP2.*

« 6. Par dérogation au paragraphe 5, les prestataires de service de paiement gestionnaires de comptes peuvent convenir avec les prestataires de service d'initiation de paiement que ces derniers se fondent sur leurs propres procédures d'authentification. Les procédures mises en place par ces derniers doivent alors être conformes respectivement aux paragraphes 1, 2 et 3 » ;

- en conséquence il s'agira également de compléter l'article 73(2) de la DSP2 par un 3e paragraphe prévoyant en substance que c'est le PSIP qui supporte l'obligation de rembourser au payeur le montant de l'opération de paiement non autorisée, de la manière suivante :

« Lorsque le PSPGC et le PSIP ont convenu, conformément à l'article 97, que la procédure d'authentification forte incombera au prestataire de services d'initiation de paiement, c'est ce dernier qui rembourse au payeur, dans les conditions du paragraphe 1, le montant de l'opération de paiement non autorisée[325] et rétablit le compte de paiement débité dans l'état ou il se serait trouvé si l'opération de paiement non autorisé n'avait pas eu lieu. »[326]

8.2 - La responsabilité du PSPGC vis-à-vis du client

8.2.1 - Enjeux et régime juridique actuel

8.2.1.1 - Un régime de responsabilité déséquilibré au préjudice des PSP

(i) Les obligations qui pèsent sur l'utilisateur de services de paiement

Les principales dispositions du Code monétaire et financier qui obligent l'utilisateur de services de paiement et qui peuvent écarter son droit au remboursement en cas de manquement intentionnel ou par négligence grave sont rappelées ci-après. Elles sont en définitive assez limitées. L'utilisateur a l'obligation :

(A) de prendre toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées ;[327] et

[325] *Prévoir dans la révision une obligation d'information préalable de l'utilisateur à la charge du PISP sur la prise en charge de la SCA par ce dernier et sa conséquence : les demandes de remboursement devront être dirigées vers lui et non vers le PSPGC.*

[326] *Dans la mesure où il ne semble pas possible pour le PISP de rétablir un compte de paiement qu'il ne détient pas, il conviendrait de revoir cette partie de la disposition qui ne parait pas cohérente.*

[327] *Article L. 133-16 du CMF.*

(B) de signaler sans tarder la perte, le vol, le détournement ou l'utilisation non autorisée de sa carte ou des données qui y sont liées dès qu'il en a connaissance.[328]

(ii) Les obligations qui pèsent sur les PSP

De leur côté et selon les situations, les PSP doivent, en vertu de l'article 73 de la DSP2[329], rembourser immédiatement après en avoir pris connaissance ou en avoir été informés et au plus tard à la fin du premier jour ouvrable suivant, les opérations signalées par l'utilisateur de services de paiement comme non autorisées dans le délai de treize mois suivant la date du débit (sauf bonnes raisons de soupçonner la fraude du client).

Au titre de l'article 74(2) de la DSP2[330], ils doivent rembourser automatiquement les opérations non autorisées en cas d'absence d'authentification forte (sauf agissements frauduleux de l'utilisateur de services de paiement).

Pour échapper à leurs obligations de remboursement, ils doivent démontrer que l'utilisateur de services de paiement a fraudé ou, en cas d'authentification forte, a manqué intentionnellement ou par négligence grave à ses obligations (au titre de l'article 74(1) de la DSP2).

Aux termes de l'article 73 de la DSP2, en cas d'opération de paiement signalée par l'utilisateur de services de paiement comme étant non autorisée, le PSP est tenu de le rembourser au plus tard à la fin du premier jour ouvrable suivant, sauf s'il a de bonnes raisons de soupçonner une fraude de l'utilisateur de services de paiement.[331]

Aux termes de l'article 72(1) de la DSP2,[332] lorsque l'utilisateur de services de paiement nie avoir autorisé une opération de paiement, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe au PSP de prouver que l'opération a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre.

---

[328] Article L. 133-17-I du CMF.

[329] Transposé à l'article L. 133-18 du CMF.

[330] Transposé à l'article L. 133-19-V du CMF.

[331] Cf. également le considérant n° 71 de DSP2 : « Toutefois, s'il existe une forte présomption qu'une opération non autorisée résulte d'un comportement frauduleux de l'utilisateur de services de paiement et lorsque cette présomption repose sur des raisons objectives qui sont communiquées à l'autorité nationale concernée, le prestataire de services de paiement devrait être en mesure de mener une enquête dans un délai raisonnable avant de rembourser le payeur ».

[332] Transposé à l'article L. 133-23, 1° du CMF.

Le PSP supporte donc des contraintes particulièrement lourdes liées au délai prévu pour le remboursement du client (J+1) ainsi qu'à la charge de la preuve qui pèse sur lui, d'autant qu'aux termes du deuxième alinéa de l'article 72(2) de la DSP2,[333] l'utilisation de l'instrument de paiement telle qu'enregistrée par le PSP ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. Le PSP, y compris, le cas échéant, le PSIP, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.

8.2.1.2 - Un régime de la preuve « diabolique »

(i) Aux termes du deuxième alinéa de l'article 72(2) de la DSP2, l'utilisation de l'instrument de paiement telle qu'enregistrée par le PSP ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur.

Une opération de paiement est nécessairement autorisée à partir du moment où l'utilisateur de services de paiement a donné son consentement à celle-ci dans la forme convenue avec le PSP. Peu importe le contexte dans lequel l'utilisateur de services de paiement a donné ce consentement. La qualification du caractère autorisé de l'opération réalisée ne doit s'apprécier qu'au regard de l'exécution de l'opération de paiement.

Le régime de la responsabilité PSPGC organisé à l'article 73 de la DSP2 ne s'applique qu'aux opérations de paiement non autorisées, c'est-à-dire, aux opérations non validées par le client selon la forme ou la procédure prévue au contrat.

Les opérations de paiement autorisées sont donc exclues de son champ d'application.

Aux termes de l'article 64(1) de la DSP2, une opération de paiement est autorisée si le payeur a donné son consentement à son exécution. Ce consentement est donné « *sous la forme convenue entre le payeur et son prestataire de services de paiement* » aux termes de l'article 64(2) de la DSP2.

La forme de ce consentement, valant autorisation, ne peut être inconnue de l'utilisateur de services de paiement d'autant que la réglementation française oblige spécifiquement la banque, dans la convention de compte de dépôt et dans les contrats cadres de services de paiement (par exemple contrat régissant l'utilisation de la carte ou convention cadre régissant les moyens de paiement

[333] *Transposé à l'article L. 133-23, 2° du CMF.*

de manière générale, incluant le virement), à communiquer sur « *La forme et la procédure pour donner le consentement à l'exécution d'une opération de paiement et pour retirer ce consentement, conformément aux articles L. 133-6 et L. 133-7 du Code monétaire et financier* », sous peine des sanctions prévues à l'article L. 351-1 du CMF.[334]

Par ailleurs, le caractère autorisé d'une opération de paiement s'apprécie indépendamment de toute relation sous-jacente. L'article 4(5) de la DSP2[335] définit d'ailleurs l'opération de paiement comme une action, initiée par le payeur ou pour son compte ou par le bénéficiaire, consistant à verser, à transférer ou à retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire.

En pratique, à l'occasion d'une contestation, le juge dans de nombreux cas d'espèce, se pose la question de savoir si l'utilisateur de services de paiement a bien donné son consentement à l'opération et si, le cas échéant, le remboursement doit, de ce fait être écarté. Cette question se pose, en particulier, lorsque l'utilisateur de services de paiement conteste la validation d'un ordre donné, dans un contexte frauduleux ou à la suite d'une manipulation d'un fraudeur.

Puisque l'opération de paiement est indépendante de l'obligation sous-jacente, la contestation ne peut porter que sur le consentement donné à cette opération sans considération de l'obligation sous-jacente. Dans ce cadre, il conviendrait de considérer qu'une opération de paiement est nécessairement autorisée à partir du moment où l'utilisateur de services de paiement a donné son consentement à celle-ci dans la forme convenue avec le PSP. Peu importe le contexte dans lequel l'utilisateur de services de paiement a donné ce consentement. La qualification du caractère autorisé de l'opération réalisée ne doit s'apprécier qu'au regard de l'exécution de l'opération de paiement.

En définitive, il y a lieu de considérer que lorsque le client a utilisé les méthodes mises à sa disposition pour donner son consentement, en particulier par l'utilisation de l'un des dispositifs d'authentification forte mis à sa disposition par le PSPGC conformément à ce qui est convenu avec ce dernier, l'opération doit être considérée comme autorisée.[336] De ce point de vue, la décision récente rendue par la Cour d'appel de Versailles est contestée par la profession bancaire et au demeurant non définitive à ce jour.[337]

---

[334] Cf. articles L. 312-1-1-II et L. 314-12-II du CMF et l'arrêté modifié du 29 juillet 2009 pris en application de ces articles, relatif aux relations entre les prestataires de services de paiement et leurs clients en matière d'obligations d'information des utilisateurs de services de paiement et précisant les principales stipulations devant figurer dans les conventions de compte de dépôt et les contrats-cadres de services de paiement.

[335] Transposé à l'article L. 133-3-I du CMF.

[336] En ce sens, Trib. de com. Saint Nazaire, 15 juin 2022, affaire n° 2021001463 ; Trib. jud. Paris, 8 juin 2022, 9e chambre 2e section, n° RG 19/04840 ; 15 novembre 2022, n° RG 22/02540. Les décisions sont annexées au rapport en Annexe VII.

[337] CA Versailles, 28 mars 2023, RG n° 21/07299. La décision est annexée au rapport.

(ii) Aux termes du deuxième alinéa de l'article 72(2) de la DSP2, l'utilisation de l'instrument de paiement telle qu'enregistrée par le PSP ne suffit pas nécessairement en tant que telle à prouver que le payeur n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière.

En effet, le PSP, y compris, le cas échéant, le PSIP, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement.

La jurisprudence antérieure à la DSP2 considère que l'utilisation d'un système sécurisé tel que requis à l'époque des faits ne permet pas de faire présumer le manquement intentionnel ou la négligence grave du payeur.[338]

Cette solution dégagée par la Cour de cassation[339] est particulièrement stricte. Elle conduit à faire peser, sur la banque, la charge d'une preuve particulièrement difficile à rapporter car dépendant des éléments que le payeur consent à communiquer alors même que le PSP dispose de traces informatiques reconstituant le parcours du paiement ou de l'opération contestée.

Dans la mesure où il appartient au PSP de prouver la fraude ou la négligence grave du payeur, il ne peut à lui seul reconstituer le contexte de la fraude, si l'utilisateur de services de paiement reste taisant sur les circonstances de celle-ci, qui interviennent en amont de l'opération contestées sur des médias auxquels le PSP n'a pas accès. Or, la directive n'impose pas au payeur de fournir des informations sur le contexte dans lequel l'opération frauduleuse a été réalisée.

De la même manière, la preuve négative de l'absence de déficience technique exigée par l'article 72 de la DSP2 apparaît particulièrement difficile à apporter. Celle-ci devrait être limitée à la preuve de l'absence de déficience technique « *détectée et enregistrée par la banque* » ayant pu affecter l'opération dans la mesure où les moyens d'actions et de contrôle de la banque dans le cadre de l'exécution de l'opération de paiement sont nécessairement limités.

En effet, dans le cadre d'une opération de paiement, la banque n'a pas, par exemple, la maîtrise du terminal utilisé par l'utilisateur de services de paiement. Dès lors, une obligation de prouver l'absence de toute déficience, même non détectable par la banque, reviendrait à exiger de la banque qu'elle garantisse le bon fonctionnement d'éléments sur lesquels elle n'a aucun contrôle.

---

[338] *Cass. Com, 18 janvier 2017, n° 15-18102.*

[339] *Cf. également Cass. Com., 12 novembre 2020, n° 19-12112 : la Cour confirme le raisonnement du Tribunal d'instance qui a condamné la banque à rembourser la victime d'un hameçonnage, du fait qu'elle ne démontrait pas l'absence d'une déficience technique au sens de l'article L. 133-23 du CMF.*

8.2.2 - Recommandations du HCJP

La question est débattue au sein du groupe de travail. Selon les représentants de la profession bancaire, il devrait être expressément mentionné dans le cadre de la révision de DSP2 que la mise en œuvre d'une procédure d'authentification forte permet au PSPGC de considérer que l'opération de paiement est présumée autorisée, l'article 73 de la DSP2 n'ayant pas vocation à s'appliquer dans cette situation. Toutefois, au sein du groupe de travail, l'ACPR s'est dite opposée à la proposition d'introduire une présomption simple d'autorisation d'une opération de paiement en cas d'authentification forte, considérant qu'elle serait défavorable pour l'utilisateur de services de paiement.

Un consensus se porte néanmoins au sein du groupe de travail sur l'opportunité d'aménager le délai de remboursement à J+1 fixé à l'article 73(1) de la DSP2 pour les opérations contestées par l'utilisateur de services de paiement. En effet, ce délai ne permet pas aux PSP de mener à bien les investigations afin d'établir le soupçon de fraude ou le cas échéant, le consentement de l'utilisateur à l'opération, notamment en cas d'authentification forte. Il pourrait donc être proposé d'allonger ce délai (entre cinq et quinze jours) afin que les PSP puissent mener ces investigations.

Recommandation n° 16 : le HCJP recommande de modifier l'article 73 de la DSP2, afin d'allonger le délai de remboursement en cas d'opération de paiement non autorisée à cinq (si l'utilisateur du service de paiement est un consommateur) ou quinze (dans le cas contraire) jours ouvrables au lieu de un jour ouvrable comme c'est le cas actuellement, de la manière suivante :

« 1. *Les États membres veillent, sans préjudice de l'article 71, à ce que, en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur rembourse au payeur le montant de cette opération* ~~*immédiatement*~~ *après avoir pris connaissance de l'opération ou après en avoir été informé,* ~~*et en tout état de cause*~~ *au plus tard à la fin du* ~~*premier*~~ ***[cinquième ou quinzième[340]]*** *jour ouvrable suivant, sauf si le prestataire de services de paiement du payeur a de bonnes raisons de soupçonner une fraude et s'il communique ces raisons par écrit à l'autorité nationale concernée. Le cas échéant, le prestataire de services de paiement du payeur rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Cela suppose par ailleurs que la date de valeur à laquelle le compte de paiement du payeur est crédité n'est pas postérieure à la date à laquelle il avait été débité.*

2. Lorsque l'opération de paiement est initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, le prestataire de services de paiement gestionnaire du compte rembourse ~~*immédiatement, et en tout état de cause*~~ *au plus tard à la fin du [cinquième ou quinzième] jour ouvrable suivant, le montant de l'opération de paiement non autorisée et, le cas échéant, rétablit le compte de paiement débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu* ».

[340] *Le délai de quinze jours pourrait être prévu lorsque l'utilisateur n'est pas un consommateur.*

Il convient également de repositionner la valeur de la preuve numérique dans le débat judiciaire.

La dématérialisation accrue de la relation entre les PSP et les utilisateurs de services de paiement s'accompagne nécessairement d'une traçabilité informatique des opérations effectuées avec les éléments d'identification et d'authentification de l'utilisateur de services de paiement. Ces données et paramètres techniques collectés par les logiciels applicatifs utilisés par les PSP retracent chronologiquement les opérations opérées, associées auxdits éléments du client, ce qui sécurise l'affectation de leur occurrence. Ce sont les preuves intrinsèques des opérations de paiement dont le PSP dispose.

En l'état actuel des textes, il incombe au PSP, par application de l'article 72(1) de la DSP2, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations. En ce sens, ce sont également des preuves extrinsèques au PSP que ce dernier doit rapporter.

Bien que la preuve ne puisse se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés, il n'en demeure pas moins que les preuves intrinsèques du PSP doivent également avoir toutes leur place dans la démonstration de l'autorisation ou de la négligence grave.

Le débat judiciaire doit apprécier en toute proportionnalité leur existence technique, et objective qui plus est, notamment en l'absence de déclaration du client éclairant les circonstances précises de la fraude, ou en cas de silence de ce dernier, car les journaux numériques constituent une preuve des opérations intervenues et de leur mode de réalisation (l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et n'a pas été affectée par une déficience technique ou autre).

Recommandation n° 17 : le HCJP recommande la modification de l'article 72 de la DSP2 afin de prévoir que, lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée ou affirme que l'opération de paiement n'a pas été exécutée correctement, le PSP peut apporter la preuve « *qu'il n'a pas détecté une déficience technique ou autre en relation avec le service fourni qui aurait pu affecter l'opération* », et non pas la preuve « *que l'opération en question n'a pas été affectée par une déficience technique ou autre du service fourni par le PSP* ». Les modifications seraient rédigées comme suit :

« 1. Les États membres exigent que, lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe au prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée ***et ~~qu'elle n'a pas été affectée par~~ qu'il n'a pas détecté une déficience technique ou autre en relation avec le service fourni qui aurait pu affecter l'opération.***

Si l'opération de paiement est initiée par l'intermédiaire d'un prestataire de services d'initiation de paiement, c'est à ce dernier qu'incombe la charge de prouver que, pour ce qui le concerne, l'opération en question a été authentifiée et dûment enregistrée ~~***et qu'elle n'a pas été affectée par une déficience technique ou autre du service fourni par le prestataire de services de paiement***~~ ***et qu'il n'a pas détecté une déficience technique ou autre en relation avec le service de paiement qu'il doit assurer.*** *»*

8.3 - Le partage d'informations sur les IBAN frauduleux

8.3.1 - Enjeux et régime juridique actuel

Un aspect clef de la lutte contre la fraude pour assurer la protection de nos clients dans le cadre d'un intérêt public est la nécessité d'envisager des traitements de centralisation de l'identité des fraudeurs et des données de fraude (IBAN de fraudeurs, adresse IP ou numéro de mobiles de fraudeurs), tant au sein des groupes auxquels appartiennent des PSP le cas échéant, qu'en dehors de tels groupes, avec les autres PSP ou les autorités nationales, de police le cas échéant. Les données afférentes à un fraudeur recueillies par un PSP devraient pouvoir être communiquées aux autres PSP afin de les alerter.

Aussi, la réglementation devrait évoluer pour permettre une faculté de partage entre PSP des informations utiles à la lutte contre la fraude.

Associé aux actions de mises en garde des clients, à la sécurisation renforcée des opérations de paiement, cette faculté de partage d'informations constituerait certainement une avancée majeure dans la lutte contre la fraude.

Le partage d'informations devrait prévoir également l'information du PSIP lorsqu'une opération ne peut être réalisée au motif d'une suspicion de fraude.

Outre cette faculté de partage, des règles adaptées et proportionnées devraient être prévues en ce qui concerne les obligations d'information individuelle des personnes suspectées de fraude et faisant l'objet de traitement de données à caractère personnel ayant cette finalité. En effet, une information individuelle des personnes suspectées de fraude pose des difficultés, notamment eu égard aux risques d'incivilités et des violences à l'égard des collaborateurs des PSP, en particulier les collaborateurs dans les agences qu'il convient de protéger. En outre, l'information de ces personnes est susceptible de nuire aux investigations menées par les autorités (TRACFIN, autorités judiciaires) et en définitive aller à l'encontre des dispositifs de lutte contre la fraude.

8.3.2 - Propositions du HCJP

Recommandation n° 19 : le HCJP recommande d'ajouter un nouvel article 26(3) rédigé comme suit :

« Afin de garantir la sécurité des opérations de paiement et la protection des utilisateurs, en particulier la protection de leurs fonds contre les risques de fraude, les autorités compétentes des États membres autorisent, le cas échéant avec le concours de leur banque centrale nationale, les échanges d'informations entre prestataires de services de paiement relatifs à des fraudes, y compris des informations confidentielles et des données à caractère personnel telles que le nom du titulaire d'un compte et/ou les données permettant d'identifier un compte de paiement, ainsi que toute autre information susceptible de permettre de détecter éventuellement l'initiation et l'exécution d'opérations de paiement frauduleuses. Les prestataires de service de paiement ne sont pas obligés de partager ces informations.

Cette faculté d'échanger des informations confidentielles entre les prestataires de services de paiement ne peut être utilisée que pour la seule finalité de lutte contre la fraude.

Le secret professionnel, auquel sont éventuellement tenus les personnes exerçant pour les banques centrales nationales des États membres ou pour les prestataires de services de paiement, n'est pas opposable et ne peut faire obstacle à ce partage d'informations confidentielles.

Ces démarches ne sont pas soumises à de quelconques obligations de résultat ou de divulgation à un tiers autre qu'un prestataire de services de paiement.

Le prestataire de services de paiement ne saurait être responsable pour défaut de consultation ou de partage d'informations ».

IX. Accès aux données

9.1 - Accès aux données par les TPP et principe de « non-discrimination »

9.1.1 - Enjeux et régime juridique

En vertu du principe de non-discrimination prévu à l'article 36(1) du règlement délégué (UE) 2018/389 (« **RTS SCA** »),[341] l'utilisateur de services de paiement doit avoir accès aux données via son prestataire de service d'information sur les comptes (PSIC), ou agrégateur, comme s'il passait par les services mis à disposition par son PSCGC.

Au sein du groupe de travail, les avis sont partagés sur cette question.

Pour les représentants de PSPGC, et en particulier la profession bancaire, le périmètre de la DSP2 et le principe de non-discrimination des TPP doivent être clarifiés. En effet, les PSCGC constatent une tendance à l'élargissement du partage d'informations avec les TPP vers les fonctionnalités accessibles via les services de banque en ligne, dès lors qu'elles portent sur un compte de paiement.

Ainsi, à la demande même du superviseur bancaire, les comptes pour lesquels le titulaire a donné un mandat à un tiers doivent être inclus dans le périmètre d'agrégation des comptes ouverts au nom de ce tiers alors même que le mandat confié par le titulaire du compte à ce tiers ne prévoirait pas cette possibilité. Pour les PSCGC, au titre de la DSP2, seuls les comptes ouverts au nom d'un même utilisateur de services de paiement devraient être concernés par le périmètre d'agrégation. Ils considèrent que cette extension est donc contraire à la définition même du service d'information sur les comptes qui devrait être limité aux comptes de l'utilisateur.[342]

Les opérations à venir concernant les cartes (y compris les paiements par carte à débit différé), les prélèvements et les virements ont également dû être rendues accessibles aux TPP par les PSPGC,

---

[341] *Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.*

[342] *Cf. la définition du service d'information sur les comptes à l'article 4(16) de DSP2 (« un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement ») et l'article 67(2), §d) et §f) de DSP2 (« Le prestataire de services d'information sur les comptes : accède uniquement aux informations provenant des comptes de paiement désignés et des opérations de paiement associées ; n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'information sur les comptes expressément demandée par l'utilisateur de services de paiement, conformément aux règles relatives à la protection des données »).*

ce qui est également contesté par les établissements de crédit au regard de la définition du service d'agrégation d'information sur les comptes.

En définitive, pour la profession bancaire, les informations partageables dans le cadre de DSP2 doivent être strictement déterminables. Seuls le solde d'un compte et les mouvements sur ce compte devraient être dans le périmètre de l'agrégation.

Pour les représentants d'agrégateurs (PSIC) et d'initiateurs (PSIP), au contraire, il a pu être constaté que les PSPGC pouvaient utiliser l'interface dédiée (l'API) pour limiter les données mises à disposition des TPP. En effet, ils considèrent que le principe de minimisation est utilisé par ces dernières pour entraver la qualité de service de ces acteurs. Par exemple lorsque plusieurs interfaces sont utilisées par le PSPGC pour les accès directs des utilisateurs de service de paiement (un site internet et une application mobile), il a été constaté à plusieurs reprises et pour plusieurs acteurs que le contenu de l'API correspondait aux données de l'interface la moins performante. Pour illustrer cette assertion, exemple est pris d'une banque utilisant deux-cent-cinquante-six caractères sur son site internet et trente-deux sur son application mobile pour le message accompagnant l'instruction de virement. Cette banque considère que ce sont les libellés de l'interface mobile qui doivent figurer dans l'API mise à disposition du TPP.

Ces éléments ont été portés à la connaissance de la Haute Autorité de la Concurrence qui les a repris dans son avis n° 21-A-05 du 29 avril 2021 en ces termes : « *Il ressort donc de ce qui précède que la détention par les PSPGC des données des comptes de paiement accessibles en ligne pourrait leur conférer un avantage significatif face à de nouveaux acteurs dans le secteur des paiements, qui sont pour certains fortement dépendants de l'accès à de telles données pour pouvoir opérer sur le marché.* »

Pour ce qui concerne la propriété des données, les représentants de PSIC ont exprimé le souhait de rappeler que les services des acteurs tiers sont fournis à l'utilisateur de services de paiement qui, comme le rappelle la DSP2 dans ses définitions n'est pas simplement le titulaire d'un compte de paiement, mais est plus largement un utilisateur de services de paiement, ce qui inclut donc ceux à qui les services sont fournis par les TPP au même titre que les PSPGC.[343]

Pour ces représentants, il est donc nécessaire que l'information mise à disposition des PSIC ne les mette pas dans une situation où l'utilisateur de services de paiement leur reprocherait une information erronée par rapport à celle fournie par leur PSPGC. Et c'est ce qui a pu être constaté en pratique par des TPP, dans des cas précis lorsque les utilisateurs constatent une différence sur l'information concernant le solde disponible et la liste des opérations qu'ils effectues entre leur PSPGC et leur agrégateur de comptes.

---

[343] *Article 4(10) : « utilisateur de services de paiement », une personne physique ou morale qui utilise un service de paiement en qualité de payeur, de bénéficiaire ou des deux ».*

Si l'AFEPAME comprend que les PSPGC puissent vouloir offrir des informations « à valeur ajoutée » à leurs utilisateurs, cela ne devrait pas en revanche être permis de cacher aux agrégateurs des transactions ou opérations dont l'utilisateur de services de paiement est à l'origine (qu'elles soient différées ou pas).

Pour l'AFEPAME, qui est favorable à la détermination des informations partageables afin d'éviter des divergences d'interprétations entre les différents établissements bancaires, il est primordial cependant de permettre à l'utilisateur de services de paiement de consentir au partage de ses données sans que son PSPGC puisse y faire obstacle. Le champ des informations partageables doit donc être suffisamment large pour permettre à tout PSP (PSPGC comme PSIC) de fournir les différents services souhaités par l'utilisateur de services de paiement.

9.1.1.1 - L'interprétation du principe de « non-discrimination » et la concurrence entre les prestataires

Pour la profession bancaire, l'interprétation large du principe de non-discrimination porte atteinte à la concurrence, à la liberté du commerce et aux investissements réalisés par les PSPGC. Elle considère que le principe de non-discrimination devrait être sans préjudice de la capacité des PSPGC à maintenir un certain niveau d'innovation et à développer un avantage concurrentiel. De son point de vue, le principe de mise à disposition gratuite par les PSPGC de certains services/certaines données au titre de la DSP2 devrait donc être appliqué strictement et ne pas être étendu à d'autres services/données.

Les services en ligne des banques évoluent régulièrement et les représentants de PSPGC au sein du groupe de travail n'approuvent pas, qu'au nom d'un principe de non-discrimination entendu trop largement, les TPP bénéficient d'un droit d'accès inconditionné, gratuit et automatique à ces évolutions, au-delà de ce qui devrait être strictement accessible dans le cadre délimité par la DSP2 et ses textes d'accompagnement.[344]

---

[344] *Article 36(1) de la RTS SCA : « 1. Les prestataires de services de paiement gestionnaires de comptes remplissent chacune des exigences suivantes :*

a) ils fournissent aux prestataires de services d'information sur les comptes les mêmes informations provenant des comptes de paiement désignés et des opérations de paiement associées que celles qui sont mises à la disposition de l'utilisateur de services de paiement en cas de demande directe d'accès aux informations sur le compte, pour autant que ces informations ne comportent pas de données de paiement sensibles ;

b) immédiatement après avoir reçu l'ordre de paiement, ils fournissent aux prestataires de services d'initiation de paiement les mêmes informations sur l'initiation et l'exécution de l'opération de paiement que celles qui sont fournies ou mises à la disposition de l'utilisateur de services de paiement lorsque ce dernier initie directement l'opération ;

c) sur demande, ils fournissent immédiatement aux prestataires de services de paiement la confirmation, sous la forme d'un simple « oui » ou « non », que le montant nécessaire à l'exécution d'une opération de paiement est disponible ou non sur le compte de paiement du payeur. »

En effet, les investissements réalisés par les PSPGC pour offrir une nouvelle fonctionnalité à leurs utilisateurs ou pour améliorer leurs banques en ligne sont engagés dans un objectif de satisfaction de leurs clients et dans un cadre de concurrence avec les autres prestataires. Les PSPGC considèrent donc que les contraindre à partager ces services gratuitement avec des concurrents est inéquitable (sachant que l'accès à une donnée de qualité nécessite des investissements dans des infrastructures spécifiques), contraire au principe de la liberté du commerce et de l'industrie et fausse le jeu de la concurrence.

Pour la profession bancaire, les PSPGC doivent avoir la garantie de pouvoir conserver les avantages concurrentiels que leur procure le développement de nouveaux services et de services innovants. Aussi, les représentants de PSPGC tiennent à ce que tout nouveau service, toute information, toute donnée, en lien avec les comptes de paiement de l'utilisateur de services de paiement et mis à disposition sur sa banque en ligne ne devienne pas accessible aux concurrents sans condition, du seul fait que ce service, cette information, cette donnée, est accessible par l'utilisateur de services de paiement sur sa banque en ligne. Ils sont d'avis que le droit pour les prestataires d'accéder à certaines informations sur les comptes de paiement au titre de DSP2 ne devrait pas s'apprécier au regard de l'ensemble des informations qui sont disponibles pour l'utilisateur sur son interface de consultation.

Ces représentants sont favorables à ce qu'un mécanisme garantisse que ces services innovants et concurrentiels soient en dehors du tronc commun de la DSP2. À défaut, la profession bancaire considère que cet accès élargi aura des effets négatifs sur la capacité des PSPGC à innover et sur le développement de services ayant une plus-value et que *in fine*, cela conduira à faire supporter indirectement les coûts d'innovation par les utilisateurs uniquement.

Pour les membres de l'AFEPAME participant au groupe de travail, la possibilité laissée à la banque de choisir quelles données sont disponibles ou non dans les interfaces mises à disposition des agrégateurs pose un risque majeur en matière de concurrence comme déjà indiqué ci-avant.

Ils constatent que toutes les PSPGC ne voient pas les TPP comme des alliés permettant de compléter les services disponibles aux clients communs des TPP et des PSPGC, que certains acteurs bancaires utilisaient délibérément cette possibilité qui leur est donnée de restreindre les données disponibles pour rendre leurs services plus pertinents que ceux des agrégateurs. Selon les membres de l'AFEPAME, la concurrence saine des différents acteurs devrait les inciter à innover et proposer plus de services intéressant les clients plutôt qu'affecter, au contraire, négativement les services des autres acteurs.

L'AFEPAME considère que le principe de non-discrimination devrait être sans préjudice de la capacité des TPP à maintenir un certain niveau d'innovation et à développer un avantage

concurrentiel. Elle considère que les données qui devraient être disponibles au titre de DSP2 devraient être étendues à l'ensemble des données personnelles et rappelle que les accès aux données ne sont ni automatiques, ni inconditionnés puisqu'ils reposent sur le consentement et l'authentification des propriétaires des données.

Pour l'AFEPAME, les services des TPP et des PSPGC ne sont pas concurrents mais complémentaires. En effet, pour fonctionner, les services d'agrégation ou d'initiation de paiement ont besoin que les utilisateurs aient des comptes dans les PSPGC.

Selon l'AFEPAME, il est important que toute information personnelle, toute donnée personnelle, en lien avec les comptes de paiement de l'utilisateur de services de paiement, mise à disposition sur sa banque en ligne devienne accessible sous conditions. Que cette information, cette donnée, soit accessible par le client sur sa banque en ligne (que ce soit à travers d'un navigateur internet, d'une application mobile, ou d'une interface spécifique du PSPGC) et qu'elle soit relative à un compte de paiement.

Ce principe de non-discrimination aura des effets positifs sur l'innovation, sur la capacité des PSPGC et des TPP à innover et sur le développement de services ayant une plus-value. En effet, les données personnelles sont et doivent rester la propriété des utilisateurs, l'innovation portant uniquement sur la valeur ajoutée apportée par les PSPGC et les TPP plutôt que la simple mise à disposition de l'information. À l'inverse, ce serait de la rétention d'information au détriment de l'utilisateur de services de paiement.

L'AFEPAME pense que l'accès à la donnée ne doit pas constituer en tant que telle un avantage, en revanche elle est d'accord avec la profession bancaire sur le fait que chacun des acteurs (TPP et PSPGC) doit avoir la garantie de pouvoir conserver les avantages concurrentiels que lui procure le développement de nouveaux services et de services innovants.

En conclusion, en désaccord sur le réexamen du principe de non-discrimination prévu à l'article 36(1) de la RTS SCA, les PSPGC et les TPP partagent néanmoins l'idée qu'une liste précise de données type, auxquelles le TPP aurait accès dans le cadre du service d'agrégation couvert par la DSP2, serait utile. Les données figurant sur cette liste, qui pourraient être mise à jour régulièrement, seraient accessibles aux TPP dans le cadre du service précité, à la condition qu'elles soient déjà disponibles en ligne pour l'utilisateur de services de paiement et relatives à son compte de paiement. Néanmoins, les membres du groupe de travail ne s'accordent pas sur les modalités d'établissement de cette liste (soit conventionnelle, soit établie ou reconnue par une autorité officielle). Le groupe de travail n'étant pas en mesure de proposer une recommandation sur cette question, des travaux complémentaires sont nécessaires.

9.1.1.2 - Des règles d'accès aux données différentes pour les utilisateurs selon le statut des PSP

Au sein du groupe de travail, la profession bancaire rappelle que même si les PSIC sont des PSP selon la DSP2,[345] l'article 97 de la DSP2,[346] ne s'applique pas aux PSIC, qui ne gèrent pas de compte de paiement au nom de leurs clients. En effet, ils ne leur proposent pas directement (par exemple via leur propre API) d'accéder à des comptes en ligne mais à des informations en matière de paiement qu'ils ont préalablement collectées auprès d'un ou plusieurs PSPGC. À ce titre, ils ne sont pas soumis à l'obligation d'authentification forte de l'USP qui s'impose uniquement aux PSPGC lorsque le client accède, par exemple, à son compte de paiement en ligne, que ce soit directement ou via un PSIC.

En conséquence, les représentants de PSPGC constatent que l'USP bénéficie d'un accès aux informations détenues par le PSIC sans authentification forte alors que cette authentification forte est exigée du PSPGC en cas d'accès direct par l'utilisateur aux informations de son compte de paiement. Le parcours client ne sera donc pas identique selon que l'utilisateur s'adressera au PSIC ou à son PSPGC. Le parcours client sera plus fluide, car sans procédure d'authentification forte, en cas de consultation des données détenues par le PSIC, et ce quelle que soit la nature des données, sans les limitations qui s'imposent aux PSPGC.

En effet, la profession bancaire rappelle qu'à l'inverse, les dérogations à l'authentification forte, en cas d'accès aux informations sur le compte de paiement directement auprès du PSPGC sont strictement encadrées[347] : absence de données sensibles, solde des comptes de paiement, opérations exécutées durant les quatre-vingt-dix derniers jours. Du point de vue de l'utilisateur, ces différences de parcours ne sont pas cohérentes pour les PSPGC et, parmi eux, les établissements de crédit, lesquels considèrent que les données et les accès aux données devraient être sécurisés de la même façon quels que soient les PSP. Du point de vue de la profession bancaire, l'absence d'authentification forte à la charge des PSIC est porteuse d'un risque accru de fraude et soulève également des questions en termes de concurrence entre ces PSP, soumis à des règles différentes.

Selon l'AFEPAME, il apparaît déraisonnable de considérer que l'utilisateur de services de paiement bénéficie d'un accès aux informations détenues par le PSIC sans authentification forte, alors même qu'au contraire, en pratique, les services des PSIC ne peuvent pas être fournis si l'utilisateur ne procède pas à une authentification forte, à la première connexion pour chacune de ses connexions bancaires et tous les quatre-vingt-dix à cent-quatre-vingts jours pour chacune de ses connexions à ses

[345] *En France, conformément à l'article L. 521-1 du CMF.*

[346] *Transposé en France à l'article L. 133-44 du CMF.*

[347] *Article 10, Réglement délégué (UE) 2018/389 RTS SCA ?*

comptes de paiement. L'AFEPAME ne comprend pas comment les banques peuvent considérer plus fluides des services qui nécessitent des redirections récurrentes vers de multiples authentifications fortes avec des typologies et des parcours très hétérogènes.

En tout état de cause, elle considère qu'il est erroné de penser que les services des PSIC ne sont pas soumis à l'obligation d'authentification forte. Quand bien même l'obligation d'authentification forte de l'utilisateur de services de paiement ne s'impose pas aux PSIC, en pratique leurs services ne peuvent fonctionner sans qu'une authentification forte ne soit effectuée pour chacun des comptes détenus auprès des PSPGC tous les quatre-vingt-dix (ou cent-quatre-vingts jours bientôt).

L'AFEPAME précise que les PSIC seraient favorables à pouvoir bénéficier des mêmes règles que les PSPGC, à savoir pouvoir procéder à une authentification forte des payeurs et de pouvoir les exempter d'authentification forte (en l'absence de tout risque avéré) pendant quatre-vingt-dix/cent-quatre-vingts jours.

9.1.2 - Propositions du HCJP

Les membres du sous-groupe sont en désaccord sur : (i) la nécessité d'un réexamen du principe de non-discrimination prévu à l'article 36(1) de la RTS SCA ; (ii) les modalités d'établissement d'une liste précise de données type accessibles aux TPP dans le cadre du service d'agrégation couvert par la DSP2 ; et (iii) le besoin de mettre en place une obligation légale d'authentification forte à la charge du PSIC lorsque ses USP accèdent aux informations qu'il détient.

Les membres du groupe de travail n'étant pas, à ce stade, en mesure de proposer une recommandation sur ces points, des travaux complémentaires sont nécessaires.

9.2 - La contractualisation permettrait d'encadrer les modalités de réalisation des services

9.2.1 - Enjeux et régime juridique actuel

9.2.1.1 - Des services répondant au besoin du marché, dans le cadre de DSP2 ou au-delà

Au sein du groupe de travail, les représentants de PSPGC ont exprimé le point de vue selon lequel ils se montrent favorables à ce que les services, les informations et les données, accessibles dans le cadre de DSP2 soient strictement délimitées dans le cadre d'un contrat. Ce contrat indiquerait clairement, parmi les données mises à disposition par l'établissement sur son espace banque en ligne, la liste de celles qui entrent spécifiquement dans le périmètre de la DSP2.

Les services, les informations et les données additionnels, qui dépasseraient ce qui est strictement prévu par la DSP2 devraient pouvoir être proposés par les PSPGC à leurs clients, dans une démarche

d'innovation et de concurrence entre les prestataires, et ne devraient être le cas échéant accessibles aux autres prestataires qu'avec l'accord du PSPGC concerné et selon des modalités négociées et convenues contractuellement (cf. notamment les services dits « *premiums* » et *SEPA Payment Account Access* (« **SPAA** »)).[348]

Les représentants de PSPGC soulignent l'importance de laisser chaque acteur développer ses services et des nouvelles fonctions, notamment en considération de la demande et des besoins du marché, et de les contractualiser pour les rendre disponibles. Il leur semble préférable que des nouvelles fonctions soient développées pour répondre à des besoins du marché plutôt qu'à des exigences réglementaires. Le service prévu à l'article 65 de la DSP2, consistant à exiger des PSPGC qu'ils confirment aux PSP des payeurs la disponibilité des fonds en cas de paiements par carte est un exemple de service développé pour répondre à une exigence réglementaire et qui n'a finalement pas été utilisé. Les représentants de PSPGC font remarquer que ce service représente des investissements et des revenus perdus. Ils considèrent donc que cet écueil aurait pu être évité si les PSP eux-mêmes, par contrat, avaient choisi de développer et proposer des services répondant précisément aux attentes. Pour les PSPGC, la gratuité et l'impossibilité de contractualiser avec les TPP n'ont pas permis d'élargir les échanges d'informations avec les TPP, ni la détermination d'un *business model* alors que les coûts de mise en œuvre ont été importants.

À cet égard, les représentants de PSPGC considèrent que les principes posés aux articles 8 et 9 de la proposition de règlement sur les données[349] doivent être soutenus.

L'article 8 prévoit en premier lieu que la mise à disposition de données par « *un détenteur de données* » à un « *destinataire de données* » doit être réalisée dans des conditions équitables, raisonnables et non discriminatoires, de manière transparente et dans des conditions convenues entre les parties. En effet, une clause contractuelle contraignante peut régir l'accès aux données et leur utilisation, la responsabilité et les voies de recours.

Par ailleurs, les représentants de PSPGC posent la question de la mise en place d'une compensation pour la mise à disposition des données par les PSPGC aux TPP. De ce point de vue, ils relèvent que l'article 9 de la proposition de règlement précitée fixe un principe de compensation raisonnable

---

[348] *V. European Payments Council (EPC), SEPA Payment Account Access : « The SEPA Payment Account Access (SPAA) scheme covers the set of rules, practices and standards that will allow the exchange of payment accounts related data and facilitates the initiation of payment transactions in the context of 'value-added' ('premium') services provided by asset holders (i.e. Account-Servicing Payment Service Providers (ASPSPs)) to asset brokers (e.g. Third Party Providers (TPPs)). » (https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/sepa-payment-account-access).*

[349] *Proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) COM/2022/68 final.*

pour la mise à disposition de données entre les détenteurs et un destinataire de données. Les représentants de PSPGC soutiennent un principe de compensation applicable quelle que soit la taille de l'entreprise destinataire (petite, moyenne ou grande). Toutefois, pour eux, une approche de simple indemnisation n'est pas suffisante. La compensation, qui devrait être convenue contractuellement et négociée librement par les parties (sans référence à des lignes directrices ou recommandations des autorités) devrait pouvoir s'établir en fonction du coût de mise à disposition de ces données mais aussi de la valeur effective des données communiquées. Les représentants de PSPGC soulignent que les bases de données et le canal de communication qui permettent la transmission des données à un tiers mobilisent des ressources financières conséquentes. Il ne semble pas équitable que le coût correspondant soit supporté exclusivement par les PSPGC alors que les PSIC valorisent ces données dans le cadre d'une activité commerciale.

De son côté, l'AFEPAME s'oppose à ce que les données DSP2 soient soumises à la nécessité d'un contrat, cette proposition de la profession bancaire contreviendrait au principe selon lequel chacun est libre de disposer de ses données dans les conditions qu'il le souhaite. Ce principe est d'ailleurs repris dans l'article 20(2) du RGPD.[350]

L'AFEPAME craint par ailleurs que certains établissement teneurs de comptes n'adhèrent pas à un tel contrat, comme certains aujourd'hui ont d'ailleurs choisi de ne pas faire d'une API l'interface d'accès dédiée des TPP.

Pour l'AFEPAME, ce n'est pas le simple accord du PSPGC qui doit légitimer ces accès mais bel et bien le consentement de l'utilisateur de services de paiement.

L'AFEPAME ne s'oppose pas en revanche à cette possibilité de contractualiser pour les services, les informations et les données additionnels, qui dépasseraient ce qui est strictement prévus par la DSP2 même si cela est moins évident pour ce qui est des « *données* ». En effet, même si la donnée hors du champ de la DSP2 semble répondre au principe de portabilité énoncé ci-avant et ne devrait pas être soumise au besoin d'un contrat, c'est plutôt le format API de mise à disposition pour lequel les acteurs tiers sont prêts à contractualiser.

L'AFEPAME ne comprend pas pourquoi la profession bancaire considère que la contractualisation est aujourd'hui impossible. Elle rappelle aussi qu'elle s'est toujours montrée en faveur d'une rémunération pour les services additionnels, et n'ayant réussi à aboutir sur ce périmètre, doute du postulat selon lequel la gratuité serait le réel point de blocage.

---

[350] *« Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible. »*

Pour l'AFEPAME, l'obligation de contractualiser pourrait donner un avantage à l'établissement détenteur des données dans la négociation des conditions d'un tel contrat et contrevenir aux principes d'équité et de non-discrimination indiqués ci-avant. De plus, si cela semble applicable aux données autres que les données personnelles, ceci contrevient au RGPD pour ce qui est des données personnelles.

L'AFEPAME souhaite rappeler que les données personnelles sont la propriété des utilisateurs de services de paiement et non des banques ou même des agrégateurs. Considérer la valeur des données personnelles et faire payer le simple accès à cette donnée contreviendrait au principe du RGPD qui est la « *libre circulation des données à caractère personnel* ».

9.2.1.2 - Une contractualisation via des standards sous forme de schéma ?

Pour les représentants de PSPGC, la mise en place de l'équivalent d'un schéma (*scheme*) au niveau européen permettrait certainement d'aboutir à un consensus des autorités de régulation sur l'interprétation des dispositions de la DSP2.

Ils considèrent qu'établir un cadre réglementaire et légitimer la contractualisation entre PSP seraient de nature à renforcer les aspects de sécurité et permettraient de responsabiliser chaque acteur, dans un marché au service des clients. Pour ces prestataires, cela permettrait de régir certains services par contrat, ou en considération de la demande du marché par une sorte de contrat d'adhésion, sous forme par exemple d'un schéma de paiements européen pour ce qui est déjà règlementé par la DSP2 (proposition de se référer aux schémas de paiement SEPA en vue de transposer certains éléments).

Par ailleurs, en permettant de contractualiser, les représentants de PSPGC considèrent qu'ils pourraient ouvrir des fonctionnalités requérant des développements spécifiques et de nouvelles informations aux TPP (par exemple : l'information concernant le cas échéant le caractère différé des opérations cartes et comptes d'épargne).

Une contractualisation *ad hoc* permettrait également de leur point de vue d'encadrer de manière adaptée les services proposés : les mesures de sécurité, l'exclusivité et la propriété intellectuelle/industrielle sur les Services *Premium*.

Face à ces constats, les représentants de PSPGC soulignent que l'initiative portée par l'EPC, dont les travaux sont en cours, visant à lancer un nouveau système de paiement (schéma SPAA) ayant pour objectif de proposer de nouveaux services à valeur ajoutée (services *premium*), répondant à de réels besoins clients, distribués dans un *business model* équitable entre les participants,[351] pourrait répondre à ces objectifs.

---

[351] *Le schéma SPAA prévoit la facturation de l'accès aux données partagées par les PSPGC (voir SEPA Payment Account Access (SPAA) Scheme Rulebook EPC012-22 / Version 1.1, https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-06/EPC012-22%20v1.1%20SEPA%20Payment%20Account%20Access%20Scheme%20Rulebook.pdf).*

En définitive, les PSPGC considèrent que ces standards contractuels pourraient organiser : (i) les accès aux informations et les échanges entre PSP, y compris la compensation raisonnable des coûts de mise à disposition des données et de maintenance des infrastructures ; (ii) les mesures de sécurité ; (iii) les règles de propriété intellectuelle/industrielle ; (iv) les modalités du recueil du consentement du client qui doivent être claires pour les trois parties (le PSPGC, le TPP et le client titulaire du compte, utilisateur de services de paiement) ; (v) le cas échéant, les responsabilités du PSP en charge de la SCA ainsi que la répartition des responsabilités entre les prestataires ; (vi) les principes de rémunération des services additionnels ; et (vii) les modalités de résolution des litiges.

Pour les membres de l'AFEPAME, la contractualisation est déjà légitime et malgré toute l'énergie déjà mise en œuvre pour définir de tels contrats ou schémas, la profession bancaire s'est toujours montrée insatisfaite des résultats des travaux entrepris et réticente à les finaliser.

L'AFEPAME rappelle que les opérations de paiement par carte à caractère différé sont des informations dans le périmètre de la DSP2. Constat est fait que seul un faible nombre d'acteurs de la profession bancaire, en dépit des discussions tripartites et de l'avis de la Banque de France sur le sujet, considère ces informations comme ne faisant pas partie des données DSP2 (en pratique tous les autres établissements teneurs de compte mettent ces données dans leurs API DSP2). Alors même que leurs clients sont insatisfaits et souhaitent explicitement pouvoir consentir au partage de ces informations, ces acteurs maintiennent leurs positions et profitent de la mise en place des API pour verrouiller les services des agrégateurs. L'AFEPAME souhaite rappeler que quand chaque PSPGC a dû engager des coûts et des développements pour la mise en œuvre des API, pour les agrégateurs et initiateurs de paiements, ce sont autant de coûts et de développements que de PSPGC qui leur ont été imposés.

Cela étant dit, l'AFEPAME serait favorable à une évolution de la directive qui permettrait aux PSPGC et aux PSIC de pouvoir convenir par contrat que la procédure d'authentification forte incombe, non au PSPGC mais au PSIC. Le contrat réorganiserait en conséquence les règles et responsabilités définies par la DSP2.

9.2.2 - Propositions du HCJP

Les membres du sous-groupe étant en désaccord sur l'encadrement par contrat des modalités de réalisation des services, le groupe de travail n'est pas en mesure de faire une recommandation sur le sujet.

9.3 - Accès aux données par les TPP : la nécessité de développer le recours aux API ?

9.3.1 - Enjeux et régime juridique actuel

L'encadrement juridique des activités d'agrégation et d'initiation de paiement et l'exigence de mise en place d'un mode de communication sécurisé entre acteurs constituent un apport majeur de la DSP2.

Pour répondre à cette dernière exigence, les banques françaises mettent en avant qu'elles ont, dès novembre 2015, initié une démarche interbancaire visant à répondre à un double objectif : sécuriser l'accès aux données et apporter une solution simple et innovante, en d'autres termes, proposer une API commune permettant d'éviter le contournement des mesures de sécurité, notamment le partage du mot de passe de l'utilisateur qui ne devrait être connu que de celui qui le génère et de celui qui l'utilise.

Les banques françaises soutiennent qu'elles ont travaillé à la définition, au développement et à la mise en production d'un standard d'API qui offre une réponse totalement conforme aux exigences de la directive-cadre et des RTS (normes de sécurité, reposant sur un mode d'accès ouvert à tous les acteurs, standardisé et sécurisé), à la fois en termes d'égalité d'accès pour tous les acteurs et de sécurité pour les données des clients. De ce fait, par cette proposition de standard commun, les banques françaises considèrent qu'elles ont grandement facilité le travail des TPP pour se connecter aux systèmes d'informations bancaires (un seul standard permet d'accéder à l'ensemble des API des banques françaises).

(i) La communauté bancaire française rappelle qu'elle a été la première en Europe à publier les spécifications techniques de son API dès juillet 2017.

(ii) Par cette approche basée sur les API, la DSP2 a permis de poser le socle d'échange technique des données dans un cadre sécurisé.

Lors de la mise en œuvre des API, un important travail a été mené afin de se conformer aux exigences imposées par la directive (texte de niveau 1) et les RTS (normes de sécurité, reposant sur un mode d'accès ouvert à tous les acteurs, standardisé et sécurisé), à la fois en termes d'égalité d'accès pour tous les acteurs et de sécurité pour les données des clients (textes de niveau 2).

Les représentants des banques françaises participant au groupe de travail considèrent que l'approche interbancaire a permis à l'ensemble des TPP de se connecter à l'ensemble des banques françaises en ayant recours à un seul standard. De ces développements et des travaux menés avec les TPP et l'autorité de supervision nationale, elles regrettent néanmoins les éléments suivants :

(A) un manque de clarté entre les RTS, les *guidelines* et les précisions sur les exigences s'ajoutant au fil de l'eau ont rendu les textes très difficiles dans leur mise en œuvre et ont pour de nombreux sujets fait l'objet de multiples interprétations. Ce point de vue est partagé par l'AFEPAME ;

(B) des connexions passives génératrices de coûts, plusieurs banques continuant d'observer que des TPP se connectent à leurs API sans générer la moindre activité (les appels API ayant pour unique finalité de vérifier sa disponibilité, sans générer d'activité) ; et

(C) un taux d'utilisation décevant des API, bien qu'en augmentation, et le maintien de la pratique du *web scrapping*.

Aussi, la profession bancaire propose au HCJP de recommander le développement des API, *d'une part*, en rendant leur utilisation obligatoire, au moins dès lors qu'une API est proposée par le PSPGC, *d'autre part*, en interdisant l'accès aux données d'un utilisateur lorsque les modalités d'accès contournent les mesures de sécurité et s'appuient en particulier sur le partage du mot de passe de l'USP mis à disposition et communiqués par le PSPGC et, *enfin*, en assouplissant les niveaux de certification des API (critères objectifs fixés par la directive) : une solidarité de fait a été établie entre les trois API issues de la DSP2 prescrites par la réglementation. Ainsi, une exemption n'est autorisée que si les trois API (à savoir : information sur les comptes de paiement, initiation de paiement et CBPII)[352] sont conformes aux orientations de l'ABE.[353] Ces orientations manquent selon les représentants de la profession bancaire, de proportionnalité et ne font pas la différence entre, d'une part, un utilisateur consommateur ou non professionnel et, d'autre part, un client professionnel ou une personne morale, pour lesquels les exigences de sécurité et les modes opératoires sont différents, ce qui crée *de facto* un frein à la mise en conformité de certaines API dédiées au service d'initiation de paiement. C'est sur ce point que les niveaux de certification des API devraient être assoupli.

De son côté, l'AFEPAME souhaite préciser que le *web scrapping* et les API sont deux technologies permettant de réaliser les services d'agrégation et d'initiation de paiement, mais que le partage du mot de passe de l'utilisateur n'a rien de spécifique au *web scrapping* en effet, et que certaines banques européennes ont choisi de mettre en œuvre des API basées sur cette même méthode d'authentification. Et la réciproque est tout aussi valable, le *web scrapping* étant tout à fait possible sans partage du mot de passe.

Ainsi la phase d'authentification et la phase d'utilisation de l'interface sont deux choses distinctes et, partant, les quatre modalités suivantes sont possibles :

(1) *web scrapping* via utilisation des identifiants de l'utilisateur ;

(2) API via utilisation d'une redirection vers le PSPGC pour que ce dernier délivre un jeton d'accès à l'API ;

(3) API via utilisation des identifiants de l'utilisateur ; et

(4) *web scrapping* via utilisation d'une redirection vers l'PSPGC pour que ce dernier délivre un jeton d'accès à l'interface utilisateur.

---

[352] *Service de confirmation de la disponibilité des fonds prévu à l'article 65 de la DSP2.*

[353] *ABE, « Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) », EBA/GL/2018/07, 4 December 2018.*

Par ailleurs, estimer que l'API est plus sûre que le *web scrapping*, signifie considérer que les interfaces délivrées par les banques à leurs utilisateurs ne sont pas suffisamment sécurisées (le *screen scrapping* étant par conception soumis exactement aux mêmes mesures de sécurités que les utilisateurs lors de leur utilisation directe des interfaces).

Depuis la mise en œuvre effective de la DSP2 en ce qui concerne l'accès aux données, et que les TPP fournissent leurs API, ces derniers ne peuvent que constater l'hétérogénéité des API mises à disposition par les PSPGC. En pratique, les API de deux PSPGC sont bien plus différentes que leurs interfaces directes (sites internet à disposition des clients). En effet, le standard STET est très ouvert et libre et permet à chaque banque de l'implémenter selon ses propres règles.

Comme déjà indiqué par l'AFEPAME de manière récurrente depuis plusieurs années, le choix des PSPGC de limiter les données accessibles via l'API impose aux TPP de maintenir les accès au mécanisme de secours pour l'accès aux autres données consenties par les clients.

Si un PSPGC souhaite que le *web scrapping* ne soit plus utilisé, il en a la possibilité, ce n'est qu'une question de volonté.

Ainsi, sur les trois recommandations de la profession bancaire, l'AFEPAME n'est pas aligné car, en effet :

(A) le premier point est déjà d'actualité, c'est bien le PSPGC qui choisit l'interface qui doit être obligatoirement utilisée par les TPP (cf. article 31 de la RTS SCA), cette recommandation n'a pas lieu d'être ;

(B) le second point n'est que la réciproque du premier et n'a donc pas d'intérêt en tant que tel pour ce qui concerne les choix de la profession bancaire. En revanche, certains PSPGC (français et européens) ayant choisi la méthode du *web scrapping* « *authentifié* » ou d'API « *with Embedded Authentification* » comme réponse à l'article 31 de la RTS SCA, cette recommandation les mettrait en difficulté ; et

(C) enfin, l'AFEPAME ne peut que constater la réelle différence de qualité entre les API « *certifiées* » (exemptées de mécanisme de secours) et recommande le maintien du niveau actuel. D'autant plus qu'il a déjà été atteint par une majorité des banques françaises.

L'AFEPAME recommande la mise à disposition de l'intégralité des données personnelles des USP pour mieux différentier les accès directs des utilisateurs et ceux des TPP.

9.4 - Recommandations du HCJP

En l'absence de consensus à ce stade, le groupe de travail n'étant pas en mesure de proposer des recommandations, des travaux complémentaires sont nécessaires.

X. L'accès aux données par les PSP et la protection des donnés à caractère personnel

10.1 - Une approche en conformité avec les principes posés par le RGPD

10.1.1 - Enjeux et régime juridique actuel

Il faut impérativement s'attacher aux finalités de l'opération et procéder à un partage de données correspondant uniquement à ces finalités.

Ainsi, sur la question de l'accès aux données des comptes de paiement détenus par un utilisateur spécifiquement, conformément au RGPD, les données personnelles traitées afférentes aux comptes de l'utilisateur doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).

En conséquence, une délimitation claire des types de données concernées dans le cadre de l'accès des TPP et la limitation de la circulation inutile des données qui en résulterait rentrerait finalement dans le cadre du respect du principe de minimisation et irait dans le sens de la protection des données.

L'AFEPAME est parfaitement alignée sur ce point avec la FBF et précise que c'est bien à l'utilisateur de service de paiement qu'il incombe de délimiter les données concernées afférentes à ses comptes de paiement et non aux PSPGC. En aucun cas, ce principe de minimisation ne devrait être avancé pour entraver les services des TPP.

Sur cette approche de conformité avec les principes posés par le règlement européen de protection des données, les banques soulignent l'importance du consentement de l'utilisateur d'un service d'information sur les comptes. Elles proposent, dans un souci de bonne gestion de ses droits et dans un objectif de protection efficace de ses données à caractère personnel de compléter l'article 67 de la DSP2 afin de permettre à l'utilisateur d'un service d'information sur les comptes de révoquer auprès de son PSIC le consentement donné à un TPP (« *droit de révocation* »). Elles sont favorables à la mise en place d'un tableau de bord dans les interfaces en ligne des banques, afin que les USP puissent disposer d'une voie centralisée pour identifier à la source les TPP avec lesquels ils partagent leurs données et révoquer facilement les consentements qui ne sont plus d'actualité.

L'AFEPAME considère qu'une telle possibilité supposerait que les PSPGC et les PSIC puissent convenir par contrat que la procédure d'authentification forte incombe, non à le PSPGC mais au PSIC, le contrat réorganisant en conséquence les règles et responsabilités définies par la DSP2. En

l'absence d'accord sur ce point entre les PSP[354], l'AFEPAME ne peut pas soutenir la démarche proposée par les banques, considérant que l'intérêt pour l'utilisateur de services de paiement de pouvoir révoquer le consentement donné auprès du PSPGC n'a de sens que si les accès sont maintenus dans la durée sans intervention du PSPGC dans son renouvellement.

10.1.2 - Recommandations du HCJP

En l'absence de consensus à ce stade, le groupe de travail n'étant pas en mesure de proposer des recommandations, des travaux complémentaires sont nécessaires.

10.2 - La révision de l'article 94 de la directive DSP2

10.2.1 - L'articulation des dispositions des Articles 94.2 de la DSP2 et 6.1 du RGPD

10.2.1.1 - Enjeu et régime juridique

Concernant l'articulation avec le RGPD, l'article 94.2 devrait être supprimé.

Le traitement des données personnelles par les PSP ne s'appuie pas sur le seul consentement de l'utilisateur, mais plus souvent sur d'autres fondements que sont l'exécution du contrat, le respect d'une obligation légale ou l'intérêt légitime.

En revanche, le consentement doit demeurer une base légale possible.

Le chapitre 4 du Titre IV de la DSP2 (article 94) traite de la protection des données (à caractère personnel). Les objectifs de cet article sont notamment : (i) de souligner l'importance d'un bon encadrement du traitement des données personnelles effectué par les PSP ; et (ii) d'assurer une bonne articulation entre la DSP2 et des règlementations spécifiques relatives au traitement des données personnelles (notamment le RGPD).

Cette volonté du législateur européen se manifeste également dans les considérants de la DSP2 :

(A) considérant n° 89 : lorsque des données à caractère personnel font l'objet d'un traitement aux fins de la directive, la finalité du traitement devrait être précisée, la base juridique applicable devrait être nommée, les exigences de sécurité applicables du RGPD mises en œuvre, et les principes de nécessité, de proportionnalité, de limitation de la finalité et de la

[354] *Cf. supra.*

durée proportionnée de conservation devraient être respectés. De même, la protection des données dès la conception et la protection des données par défaut devraient être intégrées dans tous les systèmes de traitement des données développés et utilisés dans le cadre de la DSP2 ; et

(B) considérant n° 93 : les services d'initiation de paiement et les prestataires de services d'information sur les comptes d'une part, et le prestataire de services de paiement gestionnaire du compte d'autre part, doivent respecter les nécessaires exigences de protection des données et de sécurité prescrites ou visées dans la directive ou incluses dans les normes techniques de réglementation.

Sur le principe, le fait d'intégrer dans les textes une articulation entre la DSP2 et le RGPD est à saluer. Néanmoins, l'article 94 dans sa rédaction actuelle présente quelques problématiques d'interprétation et d'application : (i) le terme « *données à caractère personnel* » n'est pas défini dans l'article 4 de la DSP2. Pourtant et afin d'éviter toute confusion avec d'autres termes à résonnance semblable (par exemple données de paiement sensibles, données de sécurité personnalisées), un renvoi vers la définition du RGPD serait utile ; et (ii) l'article 94(2) n'est pas clair et semble être redondant par rapport à d'autres dispositions de la DSP2 et du RGPD.

L'EDPB précise que le consentement donné en vertu de l'article 94(2) ne doit pas être confondu avec le consentement en vertu de l'article 6(1)(a) du RGPD :

« *Le consentement explicite au sens de l'article 94, paragraphe 2 de la DSP2 devrait donc être considéré comme une exigence supplémentaire de nature contractuelle en relation avec l'accès à des données à caractère personnel et avec leur traitement ultérieur et leur conservation, aux fins de fournir des services de paiement, et n'est donc pas identique au consentement (explicite) au sens du RGPD (point 36 opinion EDPB). En particulier, le consentement en vertu de l'article 94 § 2 ne constitue pas une base légitime de traitement des données personnelles dans le sens du RGPD et s'ajoute au consentement potentiellement nécessaire en vertu de ce dernier.* »

Si on comprend aisément que le consentement en vertu de l'article 94(2) est distinct du consentement en vertu du RGPD, on voit mal, quelles sont la fonction/l'utilité de ce paragraphe :

(1) si la fonction de ce paragraphe est d'assurer la protection des données personnelles de l'utilisateur, cet objectif est déjà pleinement assuré par le renvoi vers les textes spécifiques/le RGPD dans l'article 94(1). Plus encore, le paragraphe 2 prête à confusion car on pourrait penser (à tort et contrairement à ce qui précise l'EDPB) que la base légitime de traitement des données personnelles dans le cadre de la DSP2 est en toutes circonstances le consentement de l'utilisateur ;

(2) si la fonction de ce paragraphe est d'assurer que l'utilisateur donne son consentement contractuel à la fourniture des services de paiement (dans le sens du droit civil commun), l'article est mal

rédigé et redondant. Si telle est sa véritable fonction, l'article ne devrait pas parler du traitement et de la conservation des données personnelles, mais d'un consentement contractuel « *général* » et ne devrait pas être intégré dans un chapitre qui s'intitule « *Protection des données* ». De surcroît, les articles 64, 66 et 67 règlent déjà la problématique du consentement dans le sens du droit civil.

Pour toutes ces raisons, le groupe de travail recommande de supprimer l'article 94(2) de la DSP2.

10.2.1.2 - Recommandation du HCJP

Recommandation n° 19 : le HCJP recommande la suppression de l'article 94(2) de la DSP2.

10.2.2 - La délimitation des responsabilités entre PSP en matière de protection des données

L'article 94 de DSP2 qui soumet les traitements des données à caractère personnel aux fins de la directive au respect de la directive 95/46/CE et aux règles nationales transposant cette directive, s'adresse à tous les PSP, ce qui inclut les TPP.

Or, dans le cadre de l'accès aux données, la répartition des responsabilités concernant le traitement des données, la minimisation de traitement etc., n'est pas toujours claire.

Si le PSP gestionnaire du compte est habituellement responsable de traitement dans le sens du RGPD, le TPP est aussi tenu de respecter les règles du RGPD.

Certaines obligations sont par ailleurs précisées par la DSP2 à cet égard (voir par exemple les articles 66 et 67 : obligation d'accéder uniquement aux données nécessaires à la prestation du service). Cependant, dans le cadre d'une fuite des données ou d'un autre cas de non-respect du RGPD – comment est réglée la question de la responsabilité ?

Ce point pourrait être traité dans le cadre du contrat entre le TPP et le PSP teneur du compte.

Pour l'AFEPAME, chacun des acteurs est responsable des traitements qu'il effectue sur les données. Le TPP n'est pas le sous-traitant des PSPGC. La notion de responsable de traitement n'a pas à être traitée dans la DSP2 et doit rester du ressort du RGPD. Le RGPD ne prévoit pas par ailleurs la nécessité d'un contrat pour encadrer la responsabilité de chacun (ce n'est qu'une des bases légales possibles). Pour l'AFEPAME, il n'est pas nécessaire de mettre en place un contrat, pour qu'un agrégateur soit responsable d'une fuite de données dont il est à l'origine, ou de son non-respect du RGPD.

10.2.2.1 - Données de paiement et données sensibles au sens du RGPD

(i) Enjeux et régime juridique

Le groupe de travail est en désaccord avec l'assimilation quasi automatiques qui est faite par le comité européen de protection des données (« **CEPD** ») des données de paiement à des données sensibles au sens du RGPD .

En effet, les données relatives aux transactions financières ne sont pas mentionnées à l'article 9(1) du RGPD en tant que catégorie particulière de données à caractère personnel. Néanmoins, les lignes directrices du CEPD[355] semblent présumer que les données relatives aux transactions financières pourraient être des catégories particulières de données à caractère personnel au sens du RGPD, au motif que les opérations[356] financières peuvent révéler des informations sensibles au sujet d'une personne concernée et que les chances qu'un prestataire de services qui traite des informations sur les opérations financières d'une personne concernée traite aussi des catégories particulières de données à caractère personnel sont considérables. En conséquence, le CEPD recommande d'au moins recenser et catégoriser précisément le type de données à caractère personnel qui sera traité et de réaliser une analyse d'impact qui ne s'impose normalement selon le RGPD que lorsqu'un type de traitement, compte tenu de sa nature, de sa portée, du contexte et de ses finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Ces recommandations ne nous paraissent pas justifiées s'agissant de traitements en lien avec la fourniture de services de paiement et de services financiers en général, et vont au-delà de ce que prévoit le RGPD et la DSP2. La déduction de données sensibles au sens de l'article 9(1) du RGPD à partir des données relatives aux transactions financières d'un USP nécessiterait que le responsable de traitement procède intentionnellement et spécifiquement à un traitement de données ayant pour finalité la déduction de données sensibles au sens du RGPD. Dans une telle situation, les responsables du traitement appliqueraient en effet les conditions requises à l'article 9 du RGPD (recueil du consentement explicite de la personne concernée sauf application d'une dérogation). Toutefois, lorsque les données relatives aux transactions financières ne sont pas traitées pour en déduire une donnée sensible au sens du RGPD, alors l'article 9(1) du RGPD ne devrait pas s'appliquer, ces données ne constituant pas par nature une donnée sensible au sens du RGPD. Un

[355] *Constitue un traitement de données sensibles au sens du RGPD un traitement de données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.*

[356] *Lignes directrices 6/2020 relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, Version 2.0, adoptées le 15 décembre 2020.*

principe de ce type est retenu au considérant n° 51 du RGPD à propos des photographies écartant ainsi l'assimilation systématique d'un traitement incluant une photographie à un traitement de données sensibles au sens du RGPD,[357] principe qui devrait valoir également pour les traitements en lien avec la fourniture de services de paiement. Le groupe de travail note également que les mesures techniques recommandées par le CEPD, particulièrement difficiles à mettre en œuvre en pratique, seraient susceptibles d'avoir un effet négatif sur la protection des données à caractère personnel de l'USP, en ce sens que leur mise en œuvre impliquerait nécessairement le traitement de données sensibles.

En conséquence, pour éviter toute confusion, la DSP2 incluant une définition des « *données de paiement sensibles* »,[358] le groupe de travail recommande une nouvelle formulation et définition (le cas échéant) de cette notion, afin de la distinguer de celle de « *donnée sensible* » au sens du RGPD.

(ii) Recommandation du HCJP

Recommandation n° 20 du HCJP : le HCJP recommande de remplacer l'article 4(32) de la DSP2 par l'article 4(32) ci-dessous :

« *Donnée de paiement protégée : des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude et qui nécessitent un niveau de protection adapté*. »

10.3 - L'accès aux données et l'articulation avec eIDAS

10.3.1 - Enjeux et régime juridique

La Commission européenne, dans sa proposition de règlement,[359] envisage la possibilité au travers des cas d'usages actuellement étudiés qu'il y ait une fonction paiement dans le *digital identity*

[357] *Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique.*

[358] *Article 4(32) : « Données de paiement sensibles : des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude. En ce qui concerne les activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes, le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles ».*

[359] *Proposition de règlement du parlement européen et du conseil modifiant le règlement (UE) 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique COM/2021/281 final (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0281).*

wallet (« **DIW** »), en plus de la fonction identification. Cette révision du Règlement eIDAS[360] pourrait donc conduire à rendre obligatoire l'acceptation du DIW par les PSP en tant que solution d'authentification tierce qui devra être obligatoirement proposée (en concurrence avec les autres méthodes d'authentification proposées par le PSP).

10.3.1.1 - Problème de la responsabilité

Or, aujourd'hui dans le cadre de la DSP2, quand l'initiation de paiement est faite, le PSPGC contrôle la solution de SCA utilisée.

Demain avec une identification réalisée via le DIW (et donc à la main des États membres), le PSPGC ne sera plus maître de la solution de SCA lorsque l'utilisateur de services de paiement choisira d'utiliser le DIW comme solution d'authentification forte. Des questions de responsabilité se poseront donc en cas d'usurpation d'identité et d'opérations frauduleuses.

10.3.1.2 - Problème de la traçabilité

Autre problème : les États membres n'ont, en l'état actuel de la rédaction du projet de texte de révision d'eIDAS, pas la possibilité de tracer les usages du DIW. En cas d'initiation de paiement, la DSP2 impose une authentification dynamique (« *dynamic linking* », ou lien dynamique entre l'opération, le montant et le bénéficiaire données).[361] Cela ne sera plus possible.

10.3.1.3 - Les conséquences opérationnelles de l'introduction d'une fonction paiement dans le DIW en plus de sa fonction d'identification.

Comme indiqué par les trois associations bancaires européennes dans leur déclaration publique du 11 avril 2023,[362] l'utilisation du portefeuille d'identité numérique comme solution d'authentification en matière de paiement nécessiterait des investissements considérables non seulement dans le secteur financier, mais aussi pour le réseau d'acceptation des paiements dans son ensemble. Cela

---

[360] *Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE , https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=hr.*

[361] *Cf. article 97(2) de la DSP2 : « En ce qui concerne l'initiation des opérations de paiement électronique visée au paragraphe 1, point b), les États membres veillent à ce que, pour les opérations de paiement électronique, les prestataires de services de paiement appliquent l'authentification forte du client comprenant des éléments qui établissent* ***un lien dynamique entre l'opération, le montant et le bénéficiaire données.*** *»*

[362] *European Association of Co-operative Banks and European Savings and Retail Banking Group, « European Credit Sector Associations call for removing payments from the scope of the Digital Identity Regulation » (https://www.ebf.eu/ebf-media-centre/european-credit-sector-associations-call-for-removing-payments-from-the-scope-of-the-digital-identity-regulation/).*

pourrait entraîner des coûts disproportionnés pour les commerçants et les industries de services qui acceptent les paiements par carte. Les banques considèrent qu'il serait préférable de capitaliser sur les solutions d'authentification existantes mises en place à la suite de la DSP2, qui doivent rester lisibles et interactives avec les clients dans l'espace numérique.

Compte tenu des éléments précédents, les membres de la profession bancaire participant au groupe de travail sont favorables à l'exclusion du DIW comme solution d'authentification en matière de paiement du champ d'application d'eIDAS révisé, ce qui permettrait d'éviter les difficultés, les problèmes de responsabilité et de traçabilité précités. Le groupe étant en désaccord sur ce dernier point et n'étant pas en mesure de formuler une recommandation, des travaux complémentaires sont donc nécessaires.

10.3.2 - Recommandation du HCJP

Recommandation n° 21 : le HCJP recommande :

- concernant l'authentification forte de l'utilisateur (SCA) et les *digital identity wallets* (DIW) : considérant que le PSPGC ne peut pas être responsable d'une solution technique d'identification et de SCA dont il n'a pas le contrôle et qui lui est imposée par la réglementation, la révision de DSP2 pourrait prévoir qu'en cas de recours à une solution tierce telle que le DIW, le consentement de l'utilisateur à l'exécution des opérations de paiement ne pourra pas être contesté par ce dernier auprès du PSPGC. Au mieux, en cas de contestation, le PSPGC ne pourra être tenu qu'à une obligation d'assistance dans la récupération des fonds auprès du PSP du bénéficiaire ;

- l'exigence d'authentification forte dynamique requise par la DSP2 lors de l'initiation de l'opération de paiement devra être compatible avec la solution d'authentification proposée par le DIW et s'imposant aux PSPGC ; et

- en ce qui concerne l'articulation entre les révisions respectives de la DSP2 et du Règlement eIDAS, compte tenu des impacts du projet de révision du Règlement eIDAS sur les paiements, il semble indispensable que la cohérence entre la révision de ce texte et celle de la DSP2 soit assurée. En conséquence, il devrait être recommandé que la révision de la DSP2, qui devra prendre en compte la révision du Règlement eIDAS, n'intervienne que lorsque la révision de ce dernier texte sera complétement stabilisée.

ANNEXE 1

Glossaire

GLOSSAIRE

ABE : Autorité bancaire européenne.

ACPR : Autorité de contrôle prudentiel et de résolution.

AEMF : Autorité européenne des marchés financiers.

Arrêt ING DiBA : CJUE, Affaire C-191/17, *Bundeskammer für Arbeiter und Angestellte* contre ING-DiBa Direktbank Austria *Niederlassung der* ING-DiBa AG.

Arrêt DenizBank : CJUE, *DenizBank AG c/ Verein für Konsumenteninformation*, Affaire C-287/19, 11 novembre 2020.

API : *Application programming interface*, interface de programmation. Banque centrale européenne.

CJUE : Cour de justice de l'UE.

CMF : Code monétaire et financier.

COBO : *Collection on behalf of*, ou collecte pour le compte de.

CPCE : Code des procédures civiles d'exécution.

CRD : Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement.

CRR : Règlement (UE) 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) 648/2012.

Directive PAD : Directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base.

DIW : *Digital identity wallet*.

DME1 : Directive 2000/46/CE du Parlement européen et du Conseil du 18 septembre 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.

DME2 : Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE.

DORA : Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) 1060/2009, (UE) 648/2012, (UE) 600/2014, (UE) 909/2014 et (UE) 2016/1011.

DSP : sur les services de paiement, sans distinction selon qu'il s'agit de la DSP1 ou de la DSP2.

DSP1 : Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.

DSP2 : Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015, concernant les services de paiement dans le marché intérieur.

EEE : Espace économique européen.

EME : Établissement de monnaie électronique.

EP : Établissement de paiement.

HCJP : Haut Comité Juridique de la Place Financière de Paris.

LCB-FT : Lutte contre le blanchiment et le financement de terrorisme.

PISA : « *Oversight framework for electronic payments, schemes and arrangements* », cadre de surveillance de l'Eurosystème pour les instruments, systèmes et dispositifs de paiement électronique, novembre 2021 (https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf).

PSIP : *Payment initiation service provider*, prestataire de service d'initiation de paiement.

POBO : *Payment in behalf of*, paiement pour le compte de.

Proposition DSP3 : Proposition de Directive du Parlement Européen et du Conseil concernant les services de paiement et les services de monnaie électronique dans le marché intérieur modifiant la directive 98/26/CE et abrogeant les directives 2015/2366/UE et 2009/110/CE la directive 98/26/CE et abrogeant les directives 2015/2366/UE et 2009/110/CE, COM(2023) 366 final (https://finance.ec.europa.eu/document/download/e1a54147-429c-49e6-bce3-a65af5d26b5e_en?filename=230628-proposal-payment-services-directive_en.pdf).

Proposition Euro Digital : Proposition de Règlement du Parlement Européen et du Conseil sur l'établissement de l'euro numérique, COM(2023) 369 final (https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-regulation_en.pdf).

Proposition de Règlement RSP : Proposition de Règlement du Parlement Européen et du Conseil concernant les services de paiement dans le marché intérieur et modifiant le règlement (UE) n° 1093/2010, COM(2023) 367 final (https://finance.ec.europa.eu/document/download/82406ae1-3dde-43d5-879d-83683a8d09e6_en?filename=230628-proposal-payment-services-regulation_en.pdf).

PSPGC : Prestataire de service de paiement gestionnaire de compte.

PSIC : Prestataire de service d'information sur les comptes.

PSIP : Prestataire de services d'initiation de paiement.

PSP : Prestataire de services de paiement.

PST : Prestataire de services techniques.

Règlement eIDAS : Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Règlement Interchange : Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

Règlement MAR : Règlement (UE) 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission.

MiCA : Règlement (UE) 2023/1114 du Parlement Européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937.

Règlement SEPA : Règlement (UE) 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009.

RGPD : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

RTS SCA : Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

ROBO : *Reception on behalf of*, réception pour le compte de.

SCA : *Strong customer authentification*, authentification forte du client.

TPP : *Third party provider*, ou prestataire de services tiers.

UE : Union européenne.

USP : Utilisateur de services de paiement.

ANNEXE 2

Composition du groupe de travail

COMPOSITION DU GROUPE DE TRAVAIL
sur la révision de la directive sur les services de paiement 2 (DSP2)

PRÉSIDENT

- **Frédérick Lacroix,** Avocat Associé, Clifford Chance, membre du HCJP

RAPPORTEURS

- **Hélène Kouyaté,** Avocate Counsel, Clifford Chance
- **Laura Chambeaud,** Juriste, Clifford Chance

MEMBRES

- **Charlotte Ast,** Adjointe au chef du bureau Finance durable, droit des sociétés, comptabilité et gouvernance des entreprises, Direction générale du Trésor
- **Louis-Auguste Barthout,** Avocat, Clifford Chance
- **Louise Baroin,** Avocate, Kramer Levin Naftalis & Frankel
- **Mathilde Bonneau,** PayPal
- **Sylvie Bertin-Lê,** BNP Paribas
- **Nathalie Campagne,** Juriste contentieux, BNP Paribas
- **Caroline Cartereau,** Juriste paiement, Crédit Agricole Payment Services
- **Aurore Chevron,** Crédit Mutuel
- **Sophie Clément,** Responsable juridique, La Banque Postale
- **Mia Dassas,** Avocate Associée, Allen & Overy
- **Marie Daulny,** Responsable juridique et Contentieux, Fortuneo
- **Pierre François,** Délégué Général, Association des établissements de paiement et de monnaie électronique (AFEPAME)
- **Gérard Gardella,** Secrétaire Général, HCJP
- **Thomas Gousseau,** Linxo
- **Evelina Gratianu,** ACPR
- **Anne-Victoire d'Herbecourt,** Fintecture
- **Catherine L'Hostis,** Juriste-Conseil, Direction Juridique Groupe, BPCE
- **Muriel Kah,** Crédit Mutuel
- **Hélène Lair,** Société Générale

- **Daniel Laiter,** Juriste regulatory, BNP Paribas
- **Severine Loretti,** Juriste regulatory, BNP Paribas
- **Alexandre Loyer,** Mangopay
- **Alexandra Marais,** ACPR
- **Delphine Marchand,** PSL Counsel, Allen & Overy
- **Francesco Martucci,** Professeur agrégé, Université Paris Panthéon-Assas, membre du HCJP
- **Paulo Mendes,** Head of Product Legal & Regulatory Affairs, Swile
- **Jérôme Raguenes,** Directeur Numérique, Paiements et Résilience Opérationnelle, Fédération bancaire française (FBF)
- **Pauline Robin,** Avocate, Allen & Overy
- **Myriam Roussille,** Professeur agrégé, Université du Mans et Directrice de l'institut d'études judiciaires du Mans
- **David Sabban,** Direction générale du Trésor, adjoint à la cheffe du bureau Bancfin4
- **Pierre Storrer,** Avocat Associé, Storrer & Associés
- **Jerome Traisnel,** CEO, Slimpay
- **Hubert de Vauplane,** Avocat Associé, Kramer Levin Naftalis & Frankel
- **Jonathan Vincent-Lafont,** BNP Paribas
- **Stéphane Yvon,** Chargé de missions, Juridique et conformité, FBF