



Conseil de
l'Union européenne

**Bruxelles, le 5 juillet 2023
(OR. en)**

11473/23

**EF 213
ECOFIN 732
CODEC 1282**

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	29 juin 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 365 final
Objet:	RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, À LA BANQUE CENTRALE EUROPÉENNE ET AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN sur le réexamen de la directive (UE) 2015/2366 du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur

Les délégations trouveront ci-joint le document COM(2023) 365 final.

p.j.: COM(2023) 365 final



Bruxelles, le 28.6.2023
COM(2023) 365 final

RAPPORT DE LA COMMISSION

**RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, À
LA BANQUE CENTRALE EUROPÉENNE ET AU COMITÉ ÉCONOMIQUE ET
SOCIAL EUROPÉEN**

**sur le réexamen de la directive (UE) 2015/2366 du Parlement européen et du Conseil
concernant les services de paiement dans le marché intérieur**

**RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, À
LA BANQUE CENTRALE EUROPÉENNE ET AU COMITÉ ÉCONOMIQUE ET
SOCIAL EUROPÉEN**

**sur le réexamen de la directive (UE) 2015/2366 du Parlement européen et du Conseil
concernant les services de paiement dans le marché intérieur**

1 Table des matières

1.	INTRODUCTION	3
2.	APPLICATION ET IMPACT DE LA DSP2 EN GÉNÉRAL	3
3.	ASPECTS SPÉCIFIQUES DE LA DSP2	4
3.1.	Banque ouverte	4
3.2.	Champ d'application	6
3.3.	Protection des consommateurs	8
3.4.	Sécurité et prévention de la fraude	10
3.5.	Réduction des risques et questions liées à la concurrence	13
3.6.	Respect effectif des dispositions adoptées	14
3.7.	Autres questions	14
4.	CONCLUSIONS	15

ACRONYMES

AIS	Service d'information sur les comptes
AISP	Prestataire de services d'information sur les comptes
API	Interface de programme d'application
ASPSP	Prestataire de services de paiement gestionnaire de comptes
DAB	Distributeur automatique de billets
DORA	Règlement sur la résilience opérationnelle numérique
ABE	Autorité bancaire européenne
EDIW	Portefeuille européen d'identité numérique
BCE	Banque centrale européenne
EEE	Espace économique européen
DME	Directive sur la monnaie électronique
EMI	Établissement de monnaie électronique
RGPD	Règlement général sur la protection des données
IBAN	Numéro de compte bancaire international
IP	Paiement instantané
MIT	Opération initiée par un commerçant
MOTO	Opérations initiées par correspondance ou par téléphone
ACN	Autorité compétente nationale
OB	Banque ouverte
OF	Finance ouverte
PI	Établissement de paiement
PISA	Cadre de surveillance des instruments, des régimes et des dispositifs de paiement électronique (cadre PISA)
POS	Point de vente
DSP2	Deuxième directive sur les services de paiement
PSP	Prestataire de services de paiement
PSU	Utilisateur de services de paiement
RPS	Stratégie en matière de paiements de détail
RTS	Norme(s) technique(s) de réglementation
SCA	Authentification forte du client
SEPA	Espace unique de paiements en euros
DCDR	Directive concernant le caractère définitif du règlement
TMM	Mécanisme(s) de contrôle des opérations
TPP	Prestataire de services de paiement tiers
TSP	Prestataire de services techniques

1. INTRODUCTION

La deuxième directive sur les services de paiement (DSP2¹) fournit un cadre pour tous les paiements de détail effectués dans l'UE, au niveau national et transfrontière, en euros et dans d'autres monnaies. La première directive sur les services de paiement (DSP1²), adoptée en 2007, avait établi un cadre juridique harmonisé pour la création d'un marché européen intégré des paiements. S'appuyant sur la DSP1, la DSP2 a permis de lever les obstacles à de nouveaux types de services de paiement et d'améliorer le niveau de protection et de sécurité des consommateurs. La clause de réexamen de la DSP2 (article 108, voir l'appendice 1) imposait à la Commission de soumettre, au plus tard le 13 janvier 2021, un rapport sur l'application et l'impact de la directive, notamment en ce qui concerne les frais, le champ d'application, les seuils d'application et l'accès aux systèmes de paiement. Ce réexamen n'a pas pu avoir lieu dans les temps en raison de la transposition tardive de la directive par certains États membres et du retard pris dans l'application de certaines de ses règles, telles que celles concernant l'authentification forte du client (voir le point 3.4 ci-dessous)³. L'évaluation de la DSP2 n'a donc eu lieu qu'en 2022⁴. À la suite de cette évaluation, et à la lumière de sa communication de 2020 sur une stratégie en matière de paiements de détail pour l'UE⁵, la Commission a décidé de réviser la DSP2. Le présent rapport de réexamen accompagne les deux propositions législatives visant à réviser la DSP2⁶.

2. APPLICATION ET IMPACT DE LA DSP2 EN GÉNÉRAL

Ces dernières années, le marché des services de paiement a connu de nombreux changements. Les paiements électroniques dans l'UE n'ont cessé de progresser, atteignant 240 mille milliards d'euros en valeur en 2021 (contre 184 200 milliards d'euros en 2017)⁷. Parallèlement à l'utilisation croissante des cartes, de nouveaux prestataires ont profité des technologies numériques pour entrer sur le marché. Par exemple, les PSP non bancaires, comme les établissements de paiement et les établissements de monnaie électronique, sont désormais largement présents. Les services de banque ouverte, notamment les services d'information sur les comptes et d'initiation de paiement, ont considérablement augmenté au cours de cette période (voir point 3.1 ci-dessous).

Le rapport d'évaluation de la DSP2 a conclu que la DSP2 n'avait pas toujours obtenu le même succès dans la poursuite de ses objectifs. L'un des domaines où elle a manifestement eu une incidence positive est la prévention de la fraude, grâce à l'introduction de l'authentification forte du client; bien qu'elle soit plus difficile à mettre en œuvre que prévu, l'authentification forte du client a déjà eu une des effets significatifs sur la réduction de la fraude. La DSP2 a également été particulièrement efficace en ce qui concerne son objectif d'accroître l'efficacité, la transparence et le choix des instruments de paiement pour les utilisateurs de services de paiement. Toutefois, l'évaluation a révélé que l'efficacité de la DSP2 pour

¹ Directive (UE) [2015/2366](#) du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

² Directive [2007/64/CE](#) du 13 novembre 2007 concernant les services de paiement dans le marché intérieur.

³ La plupart des règles de la DSP2 sont applicables depuis janvier 2018, mais celles relatives à l'authentification forte du client ne s'appliquent que depuis septembre 2019.

⁴ Le rapport d'évaluation figure à l'annexe 5 de l'analyse d'impact, SWD 2023/231 final. Cette évaluation est fondée en partie sur un rapport d'un contractant, VVA/CEPS, disponible via [ce lien](#).

⁵ [COM\(2020\)592 final](#) du 24.09.2020.

⁶ COM (2023) 366 final et COM(2023) 367 final.

⁷ BCE, Statistical Data Warehouse, [Payments Statistics Report](#), juillet 2022.

parvenir à des conditions de concurrence équitables était limitée, notamment, par la persistance d'un déséquilibre entre les PSP bancaires et non bancaires lié au manque d'accès direct de ces derniers à certains systèmes de paiement clés. Malgré l'émergence de centaines de nouveaux prestataires non bancaires au service de millions de clients, les services de banque ouverte dans l'UE ont connu un succès mitigé, avec des problèmes liés à la performance des interfaces d'accès aux données pour les prestataires de ces services. Bien que les prestations transfrontières de services de paiement soient en augmentation, la plupart des systèmes de paiement (en particulier les systèmes de cartes de débit) restent pour l'essentiel nationaux. Aucune nouvelle solution de paiement entièrement paneuropéenne n'a encore vu le jour. L'initiative européenne pour les paiements (EPI)⁸ travaille actuellement à sa première solution de paiement paneuropéenne. Les baisses de coûts escomptées pour les commerçants, grâce à de nouveaux moyens de paiement moins chers basés, par exemple, sur la banque ouverte, ne se sont pas encore pleinement concrétisées. Dans l'ensemble, l'évaluation conclut que, malgré certaines lacunes, le cadre actuel de la DSP2 a permis de progresser dans la réalisation de ses objectifs.

Ces questions, parmi d'autres, sont traitées plus en détail à la section 3 ci-dessous, qui inclut les questions sur lesquelles l'article 108 de la DSP2 met l'accent et qui résume les résultats du réexamen de la DSP2 de manière plus générale.

3. ASPECTS SPÉCIFIQUES DE LA DSP2

3.1. Banque ouverte

Par «banque ouverte», on entend le processus par lequel des prestataires de services d'information sur les comptes (AISP) et des prestataires de services d'initiation de paiement (PISP), collectivement appelés «prestataires de services de paiement tiers» ou TPP, fournissent aux utilisateurs, ou facilitent la fourniture, des services réglementés par la DSP2 qui reposent sur l'accès, à la demande de ces utilisateurs, aux données de leurs comptes détenues par des prestataires de services de paiement gestionnaires de comptes (ASPSP). Bien que la banque ouverte ait existé dans l'UE avant la DSP2, les TPP opéraient dans un environnement largement non réglementé. La DSP2 a donné à la banque ouverte un cadre réglementaire stable, offrant des garanties pour les utilisateurs. Elle a imposé aux ASPSP l'obligation de faciliter l'accès des TPP aux données de paiement sans aucune obligation contractuelle, dans le but de stimuler le développement de la banque ouverte, tout en prévoyant des mesures visant à renforcer la sécurité et la protection des utilisateurs.

Une tendance au développement des services de banque ouverte avait déjà pu être observée avant la DSP2, et ce marché a continué de croître depuis 2018. Le nombre de TPP et d'utilisateurs de services de banque ouverte dans l'UE n'a cessé d'augmenter, avec près de 19 millions d'utilisateurs en 2021⁹. Le cadre juridique a légitimé l'accès réglementé des TPP aux comptes de paiement et garanti la sécurité des utilisateurs et de leurs données. Toutefois, l'évaluation de la DSP2 a révélé des problèmes récurrents en ce qui concerne l'accès effectif et efficient des TPP aux données détenues par les ASPSP. Les TPP restent confrontés à des obstacles importants et signalent fréquemment que les interfaces conçues pour faciliter leur accès aux données¹⁰ sont de qualité et de performances variables. Les ASPSP font état de

⁸ Voir <https://www.epicompany.eu/>.

⁹ Chiffre fourni par Juniper research, [cité par Statista](#). Il n'existe pas de statistiques officielles sur les activités de banque ouverte dans l'UE.

¹⁰ Généralement des API, puisque la grande majorité des ASPSP ont opté pour une API comme interface de banque ouverte.

coûts de mise en œuvre importants pour la mise au point des API¹¹ et regrettent que le cadre législatif de la DSP2 les empêche de facturer aux TPP l'utilisation de ces API pour accéder aux données des clients. Les ASPSP expriment également souvent leur mécontentement face à la faible utilisation de leurs API par les TPP et au fait que certains continuent d'utiliser leur interface client au lieu des API.

Dans ce contexte, le choix opéré par la Commission à la suite du réexamen de la DSP2 consiste à apporter un certain nombre de modifications ciblées au cadre de banque ouverte afin d'en améliorer le fonctionnement, tout en évitant des changements radicaux susceptibles de déstabiliser le marché ou d'occasionner d'importants coûts de mise en œuvre supplémentaires. Malgré l'existence de normes API différentes dans l'UE¹², la Commission juge préférable de ne pas imposer au niveau de l'UE une nouvelle interface d'accès aux données entièrement normalisée. Cela présenterait certes des avantages évidents en termes d'accès des TPP aux données. Mais l'adaptation à une nouvelle norme représenterait un coût élevé pour l'ensemble du marché. Les normes API de la DSP2 en vigueur dans l'UE, bien qu'elles présentent encore certaines différences, ont fortement convergé au fil du temps. Et l'un des deux principaux organes de normalisation des API affirme représenter 80 % des API de banque ouverte en Europe¹³. En outre, bien qu'il subsiste des différences (souvent dues à des adaptations que les ASPSP apportent aux normes principales), les «agrégateurs» d'API offrent déjà aux TPP un point d'accès unique qui leur permet de se connecter simultanément à une multitude d'API différentes. C'est pourquoi la Commission, largement soutenue par le marché, estime que les coûts liés à l'introduction d'une nouvelle norme API unique dans l'UE l'emporteraient globalement sur ses avantages.

La Commission ne voit pas non plus l'intérêt de modifier la règle par défaut de la DSP2 consistant à autoriser l'accès des TPP aux données sans entrer obligatoirement dans une relation contractuelle, et donc sans devoir verser de compensation financière aux ASPSP. Un changement aussi radical dans l'écosystème de la banque ouverte pourrait en effet être très perturbateur, sans aucune garantie d'amélioration rapide et significative du fonctionnement des interfaces. Le marché devrait toutefois être libre de conclure des accords, assortis d'un mécanisme de compensation, pour les services allant au-delà de ceux réglementés par la DSP2 révisée¹⁴, mais il devrait toujours être possible pour tout TPP de bénéficier des services «de base» de la DSP2 sans accord contractuel préalable, et sans frais. Du reste, les actes de révision de la DSP2 imposeront de nouvelles exigences minimales relatives aux performances des interfaces dédiées, qui comprendront notamment l'interdiction d'un ensemble non limitatif d'obstacles à la banque ouverte, afin de garantir aux TPP un accès optimal aux données, dans l'intérêt de leurs clients.

Actuellement, avec la DSP2, les ASPSP doivent maintenir, sauf s'ils bénéficient d'une dérogation, deux interfaces de données de banque ouverte, une interface principale et une «interface de repli». Toutefois, ce régime assez complexe devrait être rationalisé: si les ASPSP proposent des interfaces dédiées conformes fournissant aux TPP les données dont ils ont besoin pour assurer le service à leurs clients, il n'y a aucune raison de maintenir cette

¹¹ Selon un rapport du contractant VVA/CEPS de la Commission, plus de deux milliards d'euros de coûts de mise en œuvre ponctuels.

¹² Il existe essentiellement dans l'UE deux grandes normes API conformes à la DSP2 (la norme du «Berlin Group» et la norme «STET»).

¹³ [COMMUNIQUÉ DE PRESSE \(en anglais\) — Le Berlin Group apporte son soutien à de nouveaux systèmes de paiement européens \(berlin-group.org\)](#)

¹⁴ Tels que les services du système d'accès aux comptes de paiement SEPA (SPAA) dont discutent actuellement les acteurs du marché. [Accès à un compte de paiement SEPA | Conseil européen des paiements](#)

exigence de deux interfaces. Les ASPSP ne devraient être tenus de proposer en permanence qu'une seule interface de banque ouverte «dédiée»¹⁵. Toutefois, la levée de l'obligation de proposer en permanence une interface de repli, que de nombreux TPP utilisent encore souvent en raison de la qualité sous-optimale de certaines API, doit impérativement s'accompagner d'une amélioration substantielle du niveau de performance des interfaces et d'un régime strict de contrôle de l'application des règles. Il s'agit là de deux conditions préalables indispensables à la simplification du paysage actuel et à l'abandon de l'exigence de maintien d'une interface de «repli» permanente. Cela étant, même si elles sont de grande qualité, les API peuvent parfois tomber en panne et, dans ces circonstances, les TPP doivent se voir offrir un moyen de poursuivre leurs activités grâce à un accès temporaire d'urgence aux données. Enfin, afin d'accroître la confiance des consommateurs dans la banque ouverte, de faciliter leur utilisation des services de banque ouverte et d'améliorer leur protection, les banques et les autres ASPSP seront tenus de proposer à leurs clients qui utilisent ces services un outil informatique (un «tableau de bord») leur permettant de voir en un coup d'œil les droits d'accès aux données qu'ils ont accordés, et à qui, et s'ils le souhaitent, de supprimer les droits d'accès des TPP à leurs données.

Parallèlement aux deux propositions de révision de la DSP2, la Commission présente une proposition législative sur l'accès aux données d'information financière (FIDA), qui étend l'obligation de donner accès à d'autres données financières que les seules données relatives aux comptes de paiement («finance ouverte»). La Commission a examiné la possibilité de transférer les prestataires de services d'information sur les comptes de la DSP vers le futur cadre FIDA. Bien qu'un tel transfert puisse, en définitive, apparaître logique, compte tenu de la nature des activités de ces prestataires, il existerait un risque important de perturbation et d'interruption de leurs droits d'accès aux données si ce transfert intervenait prématurément, c'est-à-dire avant la mise en place d'un «système», qui constitue un préalable à toute activité de finance ouverte¹⁶. Il n'existe actuellement aucun système de ce type sur le marché de la banque ouverte, même si des acteurs du marché y travaillent actuellement. La Commission juge donc préférable d'adopter une approche par étapes et de ne prévoir un tel transfert que lorsque le cadre FIDA sera pleinement opérationnel, et uniquement une fois que les conditions d'un transfert sans accroc seront jugées remplies.

3.2. Champ d'application¹⁷

De nouveaux moyens de paiement ont été mis au point depuis l'adoption de la DSP2, tels que les paiements instantanés ou les jetons de monnaie électronique (un type de crypto-actif¹⁸). Parmi les autres produits nouveaux figurent les portefeuilles électroniques (et en particulier les portefeuilles numériques de type «pass-through», à transfert direct d'informations) qui permettent, par tokenisation, d'utiliser un instrument de paiement sur appareil mobile pour effectuer des paiements en ligne ou sans contact. L'on a également vu apparaître de nouveaux services qui, sans être eux-mêmes des services de paiement, facilitent la fourniture de tels services, comme les services de paiement différé (BNPL, pour «Buy Now, Pay Later») ou la «demande de paiement» (RTP, pour «Request-to-Pay»).

¹⁵ Sauf si, pour des raisons de proportionnalité, leur autorité de surveillance les dispense de disposer d'une interface dédiée compte tenu de leur modèle économique.

¹⁶ Voir la proposition de règlement de la Commission 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 du 23 février 2022.

¹⁷ Cette section correspond au mandat défini à l'article 58, paragraphe 2, du règlement DORA; voir l'appendice 2.

¹⁸ Ils sont réglementés, de même que d'autres crypto-actifs qui ne se prêtent pas à une utilisation comme moyen de paiement, par le règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs (MiCA).

La plupart des fournisseurs de ces nouveaux services sont exclus du champ d'application de la DSP2, en tant que «prestataires de services techniques» ou TSP. Ces TSP incluent les opérateurs de systèmes de paiement et des prestataires de services comme les spécialistes du traitement des paiements ou les passerelles de paiement qui, bien que n'étant pas des PSP eux-mêmes, fournissent leur appui aux PSP réglementés pour la prestation de ces services. Depuis la DSP2, certains de ces TSP ont acquis un rôle très important dans la chaîne de paiement, et certains d'entre eux, comme les gros sous-traitants qui traitent les données de paiement, ont même acquis un statut quasi-systémique dans certains États membres. Cette situation peut évidemment engendrer de nouveaux risques dans le paysage des paiements de l'UE.

Dans ce contexte, le règlement sur la résilience opérationnelle numérique (DORA) est pertinent¹⁹. Les PSP au sens de la DSP2 sont inclus dans le champ d'application du règlement DORA, dont les dispositions leur sont directement applicables. Par contre, les opérateurs de systèmes de paiement, qui ne sont actuellement pas soumis à un régime d'agrément au titre de la DSP2²⁰, ne relèvent pas du règlement DORA, qui ne s'applique qu'aux entités financières réglementées et surveillées en vertu de la législation de l'UE. Le règlement DORA a chargé la Commission de réfléchir, dans le cadre du réexamen de la DSP2, à l'inclusion des *«opérateurs de systèmes de paiement et des entités participant aux activités de traitement des paiements»* dans le champ d'application de la DSP2, ce qui permettrait de les inclure aussi dans le champ d'application du règlement DORA²¹.

La Commission est parvenue à la conclusion qu'une telle inclusion serait, à ce stade, prématurée. Il n'existe pas d'opinion dominante sur cette question parmi les parties intéressées, qu'elles soient privées ou publiques, consultées par la Commission lors de son réexamen de la DSP2, et aucun préjudice ou risque clair pour les consommateurs ou d'autres acteurs du marché n'a encore été observé. Bon nombre des services actuellement exclus et de leurs prestataires sont déjà soumis — ou sont sur le point de l'être — à la surveillance de la Banque centrale européenne/de l'Eurosystème (en application de l'article 127, paragraphe 2, du traité). Les mécanismes et les «dispositifs» (tels que les portefeuilles numériques) sont couverts par le nouveau cadre de surveillance «PISA» de l'Eurosystème, qui est actuellement en cours de déploiement. Il y aurait donc un risque important de cumul, si un nouveau niveau de surveillance de l'UE était ajouté au niveau existant de surveillance de la BCE/de l'Eurosystème, sans preuve solide de sa nécessité. En outre, la principale logique de la DSP2 est de réglementer les services fournis aux utilisateurs finaux (consommateurs, commerçants) et non les services liés à l'exploitation d'infrastructures de paiement, ni les services soutenant l'exécution de services de paiement sans être eux-mêmes des services de paiement (par exemple, les services de traitement des données de paiement, d'exploitation de terminaux de paiement, les services en nuage, etc.) ou les services qui ne font que faciliter l'utilisation d'un instrument de paiement, sans qu'aucun service de paiement réglementé n'entre en jeu. La législation de l'UE sur les services financiers a tendance à traiter les questions relatives aux

¹⁹ Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.

²⁰ Toutefois, l'un des articles de la DSP2, l'article 35, impose des exigences aux opérateurs de systèmes de paiement.

²¹ Article 58, paragraphe 2, du règlement DORA. Voir l'appendice 2.

consommateurs et les questions relatives aux marchés de gros et aux infrastructures dans des actes législatifs distincts²².

La Commission est toutefois pleinement consciente de l'importance croissante de ces opérateurs non surveillés pour la prestation de services de paiement, ainsi que des risques que leurs activités peuvent comporter pour les systèmes de paiement et la stabilité financière. C'est pourquoi elle procédera, dans les trois ans suivant son entrée en application, à un réexamen approfondi de la législation révisée, sur la base d'éléments concrets et en étroite coopération avec la BCE/l'Eurosystème, afin d'évaluer en particulier si un régime d'agrément et de surveillance spécifique de l'UE pour certaines des entités exclues jusqu'à présent est nécessaire, en plus du régime de surveillance existant. Ce laps de temps est nécessaire pour recueillir suffisamment d'éléments concernant la mise en œuvre de cette législation.

Ces considérations expliquent que la proposition de révision de la DSP2 ne comporte que des clarifications indispensables des dispositions relatives au champ d'application de la DSP2, là où il existe actuellement des ambiguïtés, mais sans modifier substantiellement ce champ d'application.

L'accès aux espèces est l'une des priorités de la Commission. La nouvelle proposition contribue à la réalisation de cet objectif en facilitant cet accès. Actuellement, en vertu de la DSP2, un détaillant peut, même s'il n'est pas agréé en tant que PSP, fournir des espèces à un client, mais uniquement en association avec un achat («retrait d'espèces à l'achat»). Afin d'améliorer encore l'accès aux espèces, la Commission propose de permettre aux détaillants d'offrir ce service même en l'absence d'achat, sans devoir obtenir d'agrément en tant que PSP ou sans être l'agent d'un établissement de paiement. Cette possibilité est subordonnée à certaines conditions, telles qu'un plafond de 50 euros²³ par retrait et l'obligation de déclarer les frais éventuellement facturés.

La délivrance d'espèces par l'intermédiaire de DAB nécessite en général un agrément de PSP, mais la DSP2 prévoit une exception pour certains exploitants de DAB non bancaires, sous réserve de conditions précises²⁴. Cette exception s'est révélée difficile à mettre en pratique. Il est donc proposé de la supprimer, mais d'inclure dans le champ d'application les exploitants de DAB qui ne gèrent pas de comptes de paiement, en leur appliquant un régime d'immatriculation plus léger et un niveau de réglementation approprié (par exemple, la transparence des frais sera requise).

3.3. Protection des consommateurs

i. Règles relatives aux frais²⁵

La DSP2 permet aux bénéficiaires d'imposer des frais aux payeurs afin de les orienter vers l'utilisation d'instruments de paiement spécifiques («surfacturation»). Elle leur interdit toutefois d'appliquer des frais pour l'utilisation d'instruments de paiement pour lesquels les commissions d'interchange sont réglementées par le règlement sur les commissions

²² Voir par exemple la directive MiFID (directive 2014/65/UE du 15 mai 2014 concernant les marchés d'instruments financiers) et le règlement relatif aux dépositaires centraux de titres [règlement (UE) n° 909/2014] dans le domaine des valeurs mobilières.

²³ Cette limite vise notamment à maintenir une concurrence loyale avec les distributeurs automatiques de billets et à éviter que les magasins se trouvent rapidement à court d'espèces.

²⁴ Article 3, point o), de la DSP2.

²⁵ Cette section correspond au mandat défini à l'article 108, point a), de la DSP2; voir l'appendice 1.

d'interchange²⁶, c'est-à-dire pour les cartes de débit et de crédit de consommateurs émises dans le cadre de systèmes de cartes quadripartites, et pour les services de paiement relevant du règlement SEPA²⁷, à savoir les virements et les prélèvements en euros. Les États membres sont actuellement autorisés à interdire ou à limiter plus largement la surfacturation, option qui a été utilisée par plus de la moitié d'entre eux. La Commission estime qu'il n'est pas nécessaire d'aligner davantage ou de modifier les pratiques tarifaires entre les États membres, étant donné que l'interdiction de surfacturation s'applique déjà à 95 % des paiements dans l'UE. Cette conclusion est soutenue par la plupart des participants à la consultation publique. Toutefois, l'interdiction de la surfacturation prévue par la DSP2 ne s'applique pas actuellement aux virements et aux prélèvements libellés dans des monnaies de l'UE autres que l'euro. Cette restriction n'étant pas clairement justifiée, la Commission propose d'étendre l'interdiction de la surfacturation à tous les virements et prélèvements, dans toutes les monnaies.

ii. Règles relatives aux opérations avec les pays tiers²⁸

La DSP2 s'applique aux opérations de paiement effectuées au sein de l'UE ainsi qu'en provenance et à destination de pays tiers dans n'importe quelle monnaie (y compris les monnaies de pays tiers); toutefois, ses dispositions sont limitées aux parties d'une opération qui sont effectuées dans l'UE. Les frais et la transparence des frais pour les paiements intra-UE sont régis par le règlement concernant les paiements transfrontaliers²⁹, mais ce règlement ne s'applique pas aux opérations de transmission de fonds et aux virements effectués depuis l'UE vers des pays tiers. Lorsqu'une conversion monétaire est nécessaire, les coûts qu'elle entraîne représentent souvent une part importante du coût total de l'opération. Pour les opérations réalisées depuis l'UE vers des pays tiers, en l'absence de transparence totale des coûts et des frais, il est difficile pour les consommateurs de comparer les tarifs de différents prestataires; ils risquent donc de choisir un prestataire qui n'est pas le plus adapté à leurs besoins. En outre, en vertu de l'actuelle DSP2, les PSP ne sont pas tenus de fournir à l'utilisateur de services de paiement une estimation du délai maximal d'exécution de ces opérations.

L'un des objectifs de la feuille de route du G20 sur les paiements transfrontaliers³⁰ est de promouvoir la concurrence et de réduire les frais pour les virements internationaux et les transmissions de fonds. La Commission propose donc d'imposer, pour les virements et transmissions de fonds de l'UE vers des pays tiers, l'obligation d'informer les utilisateurs de ces services des frais estimés de conversion monétaire, comme c'est déjà le cas pour les opérations intra-UE, et du délai estimé de réception des fonds par le PSP du bénéficiaire dans le pays tiers. La Commission ne propose toutefois pas de fixer un délai maximal pour l'exécution des virements et transmissions de fonds de l'UE vers des pays tiers, car cela dépend en partie de banques situées en dehors de l'UE, qui ne sont pas soumises à sa réglementation.

²⁶ Règlement (UE) 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

²⁷ Règlement (UE) n° 260/2012 du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros.

²⁸ Cette section correspond au mandat défini à l'article 108, point b), de la DSP2; voir l'appendice 1. On entend par «pays tiers» les pays qui ne font pas partie de l'Espace économique européen.

²⁹ Règlement (UE) 2021/1230, qui contient des obligations de transparence pour le montant total estimé et les frais de conversion monétaire applicables.

³⁰ <https://www.fsb.org/wp-content/uploads/P131021-1.pdf>.

iii. Seuils relatifs à l'exclusion des réseaux de communications électroniques³¹

La DSP2 exclut de son champ d'application les opérations de paiement effectuées par un fournisseur de réseau de communications électroniques à partir ou au moyen d'un appareil électronique, ou pour l'achat de contenu numérique ou de services vocaux (par exemple, les sonneries, la musique et les services de SMS à taux majoré), et qui sont facturées à l'abonné. Cette exclusion est limitée à 50 euros par opération et à 300 euros par mois. Dans le cadre de son réexamen de la DSP2, la Commission n'a relevé aucun problème lié aux niveaux actuels des différents seuils qui y sont fixés. Compte tenu des éléments d'appréciation reçus lors de son réexamen, la Commission ne propose pas de modifier ces seuils, mais continuera de surveiller leur adéquation.

iv. Règles relatives au blocage de fonds³²

Lorsqu'une carte de paiement est utilisée pour le paiement d'un montant incertain (par exemple dans une station-service, un hôtel ou pour une location de voiture), les fonds sont normalement bloqués sur la carte par le prestataire de services de paiement du payeur après accord du payeur. Les fonds bloqués ne sont pas disponibles pour les dépenses de l'utilisateur jusqu'à leur déblocage, ce qui peut entraîner des difficultés financières. Les éléments d'appréciation montrent que les fonds bloqués peuvent être disproportionnés ou déraisonnablement élevés par rapport au montant final, s'il est connu. Le problème des montants bloqués excessifs ne peut être résolu par l'introduction de plafonds, étant donné que différentes situations peuvent nécessiter des montants bloqués très différents (achat de carburant, location de voiture, séjour à l'hôtel, etc.). C'est l'opinion partagée par la majorité des parties intéressées lors de la consultation publique³³. Un autre problème connexe concerne les variations dans le calendrier du déblocage des fonds bloqués non utilisés, qui pourrait, selon les retours d'information reçus, prendre jusqu'à plusieurs semaines pour que les fonds soient libérés, voire être subordonné à une demande explicite du payeur. Dans ce contexte, la Commission propose des modifications afin d'accélérer le versement des fonds bloqués non utilisés et d'exiger que le montant bloqué soit proportionné au montant final attendu, plutôt que de proposer l'introduction de montants maximaux absolus.

3.4. Sécurité et prévention de la fraude

Dans le domaine de la fraude, la principale innovation de la DSP2 a été l'introduction de l'authentification forte du client (SCA), qui repose sur deux facteurs d'authentification fondés sur la connaissance (par exemple d'un mot de passe), la possession (par exemple d'une carte) ou l'inhérence (par exemple d'une empreinte digitale). La DSP2 impose aux PSP d'appliquer l'authentification forte du client lorsque le payeur souhaite accéder à un compte de paiement en ligne, initier une opération de paiement électronique ou exécuter une action grâce à un moyen de communication à distance susceptible de comporter un risque de fraude au paiement ou d'une autre utilisation frauduleuse. L'évaluation effectuée par la Commission montre que l'authentification forte du client a déjà été très efficace pour réduire la fraude. Par exemple, en ce qui concerne les paiements par carte à distance, les opérations avec authentification forte présentent un niveau de fraude de 70 % à 80 % inférieur à celui des opérations sans SCA³⁴. Toutefois, l'introduction progressive de la SCA par le marché a été difficile, ce qui a entraîné des retards importants dans son déploiement complet. Les acteurs

³¹ Cette section correspond au mandat défini à l'article 108, point d), de la DSP2; voir l'appendice 1.

³² Cette section correspond au mandat défini à l'article 108, point f), de la DSP2; voir l'appendice 1.

³³ Les réponses à la consultation publique sont disponibles sur [ce lien](#).

³⁴ Autorité bancaire européenne, *Discussion paper on EBA's preliminary observations on selected payment fraud data under PSD2*, as reported by the industry, EBA/DP/2022/01, 17 janvier 2022 (en anglais).

du marché insistent régulièrement sur les coûts qu'elle a entraînés³⁵ et nombre d'entre eux préféreraient une approche davantage ciblée sur la finalité des opérations électroniques, afin de réduire les frictions liées à la SCA. La Commission reconnaît que l'introduction de la SCA aurait pu être plus fluide et aurait certainement pu être mieux anticipée par le marché, qui a largement sous-estimé la complexité et l'incidence de cette migration. Elle n'a toutefois pas l'intention de modifier son approche concernant l'authentification forte du client, compte tenu des résultats très positifs qu'elle a déjà permis d'obtenir en ce qui concerne les niveaux de fraude et compte tenu du fait que, aujourd'hui et après son introduction progressive, elle est devenue familière pour la plupart de ses utilisateurs.

L'introduction de la SCA a posé des problèmes concrets à de nombreux consommateurs de l'UE, en les gênant dans l'exécution de paiements électroniques. La Commission estime que la SCA devrait être à la portée de tout un chacun, indépendamment de son état de santé, de son âge ou de sa situation. Les PSP doivent donc proposer des solutions d'authentification forte accessibles à tous leurs clients et pas seulement à ceux qui, par exemple, possèdent un smartphone ou sont à l'aise avec ces technologies. Conformément à l'acte législatif européen sur l'accessibilité³⁶, la Commission imposera donc aux PSP de faciliter l'authentification forte du client, notamment pour les personnes handicapées, les personnes âgées et les autres personnes à qui cette authentification pose des difficultés.

Malgré son succès, l'authentification forte du client ne permet pas de lutter contre tous les types de fraude. Face à l'émergence de nouvelles formes de fraude sur lesquelles l'authentification forte du client n'a que peu d'effet, en particulier la fraude à «l'ingénierie sociale», dans laquelle les fraudeurs manipulent leur victime pour qu'elle révèle ses identifiants ou envoie des fonds à un bénéficiaire illégitime, la Commission propose de nouvelles mesures tant en matière de prévention de la fraude que de réparation³⁷. Il s'agit notamment d'améliorer l'application de la SCA (par exemple en précisant dans quels cas une opération peut être considérée comme une opération initiée par un commerçant ou comme une commande par courriel ou par téléphone), de créer une base juridique permettant aux PSP de partager des informations sur les fraudes dans le plein respect du RGPD, comme le demandent tous les acteurs du marché, d'obliger les PSP à mener des actions d'éducation pour sensibiliser davantage les clients à la fraude aux paiements, et d'étendre à tous les virements, et pas uniquement aux paiements instantanés, les services de vérification du numéro IBAN et du nom, qui ont déjà prouvé leur efficacité face à la fraude et aux erreurs sur les marchés où ils ont été introduits³⁸.

La DSP2 a introduit un droit à remboursement pour les consommateurs, mais uniquement en ce qui concerne les virements non autorisés, c'est-à-dire ceux pour lesquels le payeur n'a pas

³⁵ Selon un rapport du contractant VVA/CEPS, ces coûts de mise en œuvre ponctuels représenteraient plus de cinq milliards d'euros, mais ils seraient compensés par une réduction annuelle des fraudes de près de un milliard d'euros par an.

³⁶ Directive (UE) 2019/882 du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services.

³⁷ Les services de la Commission ont estimé le montant de la fraude à l'ingénierie sociale à 323 millions d'euros par an, d'après des données de l'ABE. Voir l'analyse d'impact accompagnant la proposition de la Commission sur les paiements instantanés, SWD(2022) 546 final.

³⁸ Ces services, qui existent au niveau national dans certains États membres, alertent le payeur, avant qu'un paiement ne soit finalisé, de toute divergence entre le numéro de compte (IBAN) et le nom du bénéficiaire. L'obligation pour les PSP d'offrir un tel système figure déjà (mais uniquement pour les virements instantanés en euros) dans la proposition législative de la Commission sur les paiements instantanés [COM(2022) 546 final du 26.10.2022].

consenti à l'exécution de l'opération de paiement. Elle ne couvre toutefois pas les types de fraude qui sont apparus depuis son adoption et qui sont de plus en plus répandus, tels que la fraude à l'ingénierie sociale mentionnée plus haut. Si l'authentification forte du client introduite par la DSP2 a déjà entraîné une réduction significative du niveau des fraudes liées aux opérations de paiement non autorisées, elle est globalement sans effet sur ces nouveaux types de fraude. La Commission estime qu'avec l'ingénierie sociale, la distinction entre opérations autorisées et opérations non autorisées devient de plus en plus floue et complexe à appliquer dans la pratique, ce qui soulève également des questions juridiques sur le point de savoir si une opération peut être considérée comme autorisée au seul motif qu'une authentification forte du client a été exécutée.

La Commission estime que toute modification du cadre de responsabilité établi par la DSP2 devrait contribuer à réduire la fraude mais ne pas créer de nouvel aléa moral, ce qui pourrait être le cas d'un droit général au remboursement, ni simplement réaffecter les conséquences financières de la fraude. Elle propose donc d'accorder aux consommateurs des droits au remboursement supplémentaires allant au-delà des opérations non autorisées, mais uniquement dans certaines situations spécifiques, et sous certaines conditions. La logique suivie par la Commission est qu'un remboursement peut être justifié dès lors que la responsabilité du prestataire de services de paiement peut être considérée comme engagée du fait de son action ou de son inaction. L'une de ces situations est celle où le consommateur a subi un préjudice causé par une défaillance du service de vérification du numéro IBAN ou du nom. Une autre situation dans laquelle un droit à remboursement serait justifié est celle où un consommateur est victime d'une fraude dans laquelle le fraudeur se fait passer pour un employé de sa banque, par exemple en utilisant le numéro de téléphone ou l'adresse électronique de celle-ci (usurpation d'identité ou d'adresse électronique). Dans ce dernier cas, le prestataire de services de paiement dont des fraudeurs ont détourné les identifiants ou usurpé l'identité de ses employés, pourrait aussi être considéré comme une victime au même titre que le consommateur. Toutefois, dans un nombre croissant d'États membres, les banques, à juste titre préoccupées par l'impact de ces fraudes sur leur réputation et sur la confiance des consommateurs dans le système bancaire, choisissent de plus en plus de rembourser ces opérations frauduleuses basées sur l'usurpation d'identité. Certaines décisions des juridictions nationales semblent suivre la même tendance. Il est toutefois indispensable de prévoir certaines exceptions et garanties à ces droits à remboursement, en particulier en cas de négligence grave du consommateur, ou lorsque le consommateur lui-même participe à l'escroquerie.

La Commission accorde la plus haute importance au problème de la fraude. Elle suivra de près l'évolution de la fraude aux paiements, en coopération avec les organisations de consommateurs, et prête, au besoin, à proposer des ajustements du cadre juridique, y compris en ce qui concerne l'élargissement du transfert de responsabilité. La Commission attend de tous les acteurs de la chaîne de paiement, privés ou publics, réglementés ou non, qu'ils jouent pleinement leur rôle dans la prévention de la fraude. Les commerçants, les systèmes de paiement, les prestataires de services techniques, les opérateurs de réseaux mobiles, les plateformes internet et autres devraient participer pleinement à cet effort collectif, aux côtés des PSP réglementés, et leur responsabilité pourrait également être engagée dans certaines situations.

3.5. Réduction des risques et questions liées à la concurrence³⁹

Le nombre et l'importance des PSP non bancaires ont augmenté depuis l'entrée en vigueur de la DSP2. Ces prestataires peuvent offrir des services de comptes de paiement, mais, à la différence des banques, ils ne peuvent pas accorder de prêts et ils doivent, pour être agréés, protéger les fonds de leurs clients en les déposant auprès d'une banque commerciale. Les établissements de paiement et les établissements de monnaie électronique doivent donc disposer d'un compte auprès d'une banque commerciale. En outre, l'offre de services de paiement nécessite l'accès à des infrastructures de paiement clés qui traitent et règlent les paiements.

Comme l'a signalé l'ABE dans son avis de janvier 2022⁴⁰, les établissements de paiement et les établissements de monnaie électronique ont rencontré des problèmes liés à la «réduction des risques» par les banques commerciales. En ce qui concerne l'accès aux comptes des banques commerciales, bien que celles-ci soient tenues par la DSP2 d'expliquer et de justifier tout refus d'accès opposé à un établissement de paiement ou à un établissement de monnaie électronique, elles fournissent souvent des explications formelles superficielles pour le justifier, ou bien accordent cet accès, mais le retirent par la suite, ce que la DSP2 ne leur impose pas d'expliquer. Cela peut considérablement perturber l'activité des établissements de paiement et des établissements de monnaie électronique.

En outre, la directive sur le caractère définitif du règlement (DCDR⁴¹), dans sa teneur actuelle, interdit aux PSP non bancaires d'accéder aux infrastructures de paiement qui ont été désignées par les États membres en vertu de ladite directive, en ne les mentionnant pas comme participants potentiels. Cela oblige les établissements de paiement et les établissements de monnaie électronique à s'appuyer encore davantage sur les banques commerciales, non seulement pour protéger les fonds de leurs clients, mais aussi pour exécuter les paiements, ce qui entraîne une dépendance structurelle des PSP non bancaires à l'égard des banques et crée des conditions de concurrence inéquitables dénoncées par de nombreux acteurs du marché.

La proposition de la Commission visant à réviser la DSP2 contient donc des mesures visant à remédier à ces lacunes et à rendre les conditions de concurrence plus équitables. Les exigences imposées aux banques en ce qui concerne les services de compte bancaire proposés aux PSP non bancaires seront considérablement renforcées, avec une obligation plus stricte d'expliquer les refus d'accès qui, à la différence de la DSP2, couvrira aussi les retraits de service. Les banques centrales seront également autorisées à fournir des services de compte à des PSP non bancaires, à leur discrétion. La Commission propose en outre de modifier la DCDR afin d'y inclure les établissements de paiement⁴² en tant que participants possibles aux systèmes de paiement désignés. Les règles de paiement révisées comprendront des règles renforcées sur l'admission des établissements de paiement en tant que participants aux systèmes de paiement, assorties d'une évaluation appropriée des risques.

³⁹ Cette section correspond au mandat défini à l'article 108, point c), de la DSP2; voir l'appendice 1.

⁴⁰ [EBA Opinion and annexed report on de-risking.pdf \(europa.eu\)](#)

⁴¹ Directive 98/26/CE du 19 mai 1998 concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres, telle que modifiée.

⁴² Mais pas les établissements de monnaie électronique, dont le statut sera combiné avec celui des établissements de paiement dans le futur cadre; voir point 3.7 ii) ci-dessous.

3.6. Respect effectif des dispositions adoptées

Il est essentiel, pour assurer l'application et la mise en œuvre harmonisées des règles de la DSP2, de veiller à leur respect effectif. Le principe d'une harmonisation complète exige des États membres qu'ils ne conservent pas et n'introduisent pas d'autres dispositions que celles de la DSP2. Or, les règles de la DSP2 ne sont pas interprétées et mises en œuvre de la même manière par les différents acteurs du marché des paiements, bien que des orientations interprétatives non contraignantes soient disponibles, entre autres, sous la forme de questions-réponses ou d'avis et d'orientations de l'ABE⁴³. La surveillance des établissements de paiement s'effectue dans un cadre national, les autorités compétentes nationales étant responsables dans leur juridiction. La concurrence est faussée et comporte des risques d'arbitrage réglementaire lorsque des PSP s'établissent dans un État membre qui applique les règles de la DSP2 d'une manière avantageuse pour eux et qu'ils fournissent à partir de cet État des services transfrontières à destination d'autres États membres ayant des interprétations plus strictes.

Dans ce contexte, il convient de renforcer les pouvoirs d'exécution des autorités compétentes nationales, en particulier dans le domaine des sanctions, et d'assurer l'application uniforme des règles de l'UE en matière de paiements en transformant la majeure partie des règles de la DSP2 en un règlement directement applicable.

3.7. Autres questions

i. Petits établissements de paiement⁴⁴

La DSP2 permet aux États membres de soumettre les petits établissements de paiement à des exigences prudentielles moins strictes, à condition que certains seuils concernant les opérations de paiement exécutées soient respectés⁴⁵. Aucun problème substantiel lié au niveau actuel des seuils n'a été relevé, et la Commission n'a donc aucune raison impérieuse de proposer des modifications de seuils; toutefois, elle propose d'actualiser les seuils pour tenir compte de l'inflation et de le faire périodiquement à l'avenir, par voie d'acte délégué.

ii. Simplification des services de monnaie électronique

La deuxième directive sur la monnaie électronique (DME 2⁴⁶) contient des règles relatives à l'agrément et à la surveillance des établissements de monnaie électronique. La DSP2 contient des règles relatives à l'agrément et à la surveillance des établissements de paiement et établit des droits et obligations ainsi que des exigences de transparence dans la relation entre tous les PSP (y compris les établissements de monnaie électronique) et les utilisateurs de services de paiement. Étant donné que les opérations de paiement utilisant de la monnaie électronique sont déjà très largement réglementées par la DSP2, le cadre juridique applicable aux établissements de monnaie électronique et aux établissements de paiement est déjà relativement cohérent. Toutefois, les établissements de monnaie électronique sont soumis à des exigences assez différentes de celles qui s'appliquent aux établissements de paiement, que ce soit en matière d'agrément, en particulier en termes de capital initial et de capital permanent, qu'en ce qui concerne les concepts clés régissant leurs activités, telles que l'émission, la distribution et le remboursement de monnaie électronique. Les autorités de surveillance ont rencontré des difficultés pratiques pour délimiter clairement les deux régimes

⁴³ [Questionnaire sur le corpus réglementaire unique \(en anglais\) | Autorité bancaire européenne \(europa.eu\)](#)

⁴⁴ Cette section correspond au mandat défini à l'article 108, point e), de la DSP2; voir l'appendice 1.

⁴⁵ Article 108, point e), en liaison avec l'article 32 de la DSP2.

⁴⁶ Directive 2009/110/CE 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, telle que modifiée.

et pour distinguer les produits et services de monnaie électronique des services de paiement proposés par les établissements de paiement. Cela a suscité des craintes d'arbitrage réglementaire et de distorsion des conditions de concurrence, et entraîné des problèmes de contournement possible des exigences de la DME 2, certains établissements émettant de la monnaie électronique profitant de la similitude entre services de paiement et services de monnaie électronique pour ne demander l'agrément qu'en tant qu'établissement de paiement.

L'expérience acquise est désormais suffisante pour conclure qu'il est indiqué de fusionner les deux régimes⁴⁷, en les regroupant en un seul acte législatif et en les harmonisant dans la mesure du possible, tout en laissant une marge de manœuvre pour tenir compte de certaines spécificités, lorsque cela se justifie. Cela permettra de répondre aux craintes et aux difficultés liées à la délimitation des deux cadres juridiques, en particulier au stade de l'agrément. Cela garantira en outre un degré plus élevé d'harmonisation, de simplification et de cohérence dans l'application des exigences légales définies pour les établissements de paiement et les établissements de monnaie électronique, en évitant l'arbitrage réglementaire et en assurant des conditions de concurrence équitables et un cadre juridique à l'épreuve du temps.

4. CONCLUSIONS

À la lumière des résultats du rapport d'évaluation de la DSP2, la Commission conclut, d'une part, que des modifications ciblées sont nécessaires et opportunes, mais, d'autre part, que ces modifications ne doivent pas représenter une révolution, mais une évolution du cadre de l'UE en matière de paiements. Dans certains domaines, tels que le champ d'application de la législation ou la surfacturation, aucun élément concret n'a révélé de problèmes justifiant des changements majeurs et immédiats, même s'il est prévu de procéder à un réexamen, visant en particulier les opérateurs de systèmes de paiement, conformément à la clause de réexamen du règlement DORA. Dans d'autres domaines, par exemple celui de la banque ouverte, compte tenu de l'héritage que représente la DSP2 et des investissements déjà réalisés pour mettre en œuvre ses normes, ainsi que des coûts qu'entraînerait une révision en profondeur de ces exigences, la Commission estime qu'il est essentiel d'écarter toute option pouvant déboucher sur d'importants nouveaux coûts de mise en œuvre et/ou des résultats incertains.

La proposition de révision de la DSP2 représente un ensemble de modifications qui amélioreront le fonctionnement du marché des paiements de l'UE et renforceront considérablement la protection des consommateurs. Ces modifications sont parfaitement conformes aux objectifs de la stratégie de la Commission en matière de paiements de détail et viennent compléter des initiatives en cours telles que la proposition législative sur les paiements instantanés et la proposition relative à la «finance ouverte» (FIDA), que la Commission présente également dans le cadre de la révision de la DSP2.

⁴⁷ Voir le [rapport de la Commission 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.

APPENDICE 1

Article 108 de la directive (UE) 2015/2366

Clause de réexamen

«La Commission soumet, au plus tard le 13 janvier 2021, au Parlement européen, au Conseil, à la BCE et au Comité économique et social européen, un rapport sur l'application et l'impact de la présente directive, et en particulier sur:

- a) l'adéquation et l'impact des règles relatives aux frais telles qu'elles sont fixées à l'article 62, paragraphes 3, 4 et 5;*
- b) l'application de l'article 2, paragraphes 3 et 4, évaluant si les titres III et IV peuvent, si cela est techniquement possible, être intégralement appliqués aux opérations de paiement visées auxdits paragraphes;*
- c) l'accès aux systèmes de paiement, compte tenu notamment du degré de concurrence;*
- d) l'adéquation et l'impact des seuils visés à l'article 3, point l), pour les opérations de paiement;*
- e) l'adéquation et l'impact des seuils visés à l'article 32, paragraphe 1, point a), pour la dérogation;*
- f) l'opportunité, au vu de l'évolution, d'introduire, en complément des dispositions de l'article 75 sur les opérations de paiement dont le montant n'est pas connu à l'avance et pour lesquelles des fonds sont bloqués, des limites maximales pour les montants à bloquer sur le compte de paiement du payeur dans de telles situations.*

Le cas échéant, la Commission accompagne son rapport d'une proposition législative.»

APPENDICE 2

Article 58, paragraphe 2, du règlement (UE) 2022/2554 (DORA)

«Dans le cadre du réexamen de la directive (UE) 2015/2366, la Commission évalue la nécessité de renforcer la cyberrésilience des systèmes de paiement et des activités de traitement de paiements, ainsi que l'opportunité d'étendre le champ d'application du présent règlement aux opérateurs de systèmes de paiement et aux entités participant aux activités de traitement de paiements. À la lumière de cette évaluation, la Commission soumet, dans le cadre du réexamen de la directive (UE) 2015/2366, un rapport au Parlement européen et au Conseil au plus tard le 17 juillet 2023.

Sur la base de ce rapport de réexamen, et après avoir consulté les AES, la BCE et le CERS, la Commission peut présenter, le cas échéant et dans le cadre de la proposition législative qu'elle peut adopter en vertu de l'article 108, deuxième alinéa, de la directive (UE) 2015/2366, une proposition visant à faire en sorte que tous les opérateurs de systèmes de paiement et entités participant à des activités de traitement des paiements fassent l'objet d'une surveillance appropriée, tout en tenant compte de la supervision existante par la banque centrale.»