Chronique

Nouveaux moyens de paiement, banque digitale et protection des données

PIERRE STORRER*
Avocat au Barreau de Paris
Kramer Levin Naftalis
& Frankel LLP

MYRIAM ROUSSILLE
Agrégée des facultés de Droit
Professeur
Université du Mans
IRJS Sorbonne Affaires-Finance

L'harmonisation modulaire de la réglementation européenne : le cas d'école de la DSP 2

Le 14 septembre 2019, les mesures phares de la DSP 2 devaient entrer en application : mais en guise de grand moment, cette date marque, en matière de communication sécurisée, la publication, en France, d'une liste des établissements exemptés de l'obligation de mettre en place des mesures de secours ; surtout, l'exigence d'authentification forte du client a été reportée.

Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, 21 June 2019.

Liste de publication des établissements exemptés de l'obligation de disposer d'un mécanisme de secours d'API, publiée le 12 septembre 2019.

Introduction par Myriam Roussille

De l'optimisme contrarié. La réalité économique s'accommode décidément bien mal de la tyrannie normative. Et quand les textes entendent imposer des changements aux implications pratiques fortes, supposant notamment des investissements techniques ou des avancées technologiques, il n'est pas rare que les calendriers plient sous la contrainte des faits.

L'histoire récente des grands textes « révolutionnaires » du droit bancaire et financier le prouvent. MIF, EMIR et désormais la DSP 2 ont ainsi conduit les autorités à devoir reporter, parfois à de nombreuses reprises, l'entrée en application des textes.

Ce report est parfois le résultat « mécanique » du laps de temps pris pour arrêter les mesures d'applications. L'adoption des standards techniques, dits aussi « RTS », fait en amont l'objet de consultations et de négociations souterraines entre les parties prenantes ; or, la guerre des lobbies est chronophage et trancher entre les conflits d'intérêts l'est tout autant. En outre, on sait que les autorités européennes de surveillance (EBA en matière de paiement ou ESMA pour ce qui relève de la finance de marché) n'ont pas de pouvoir normatif direct, leurs propositions de RTS devant être formellement adoptées par la Commission, le Parlement ayant un droit de veto, ce qui peut d'autant en retarder la mise en place.

Quand nécessité fait loi... Mais le report d'entrée en application des grands textes, et ainsi des mesures structurelles qui y sont associées, résulte souvent d'un constat : les acteurs, parfois même publics, qui doivent mettre en place les mesures décrétées à Bruxelles ne sont pas prêts. La supériorité de la règle européenne dans la hiérarchie des normes n'y change rien : si la migration opérationnelle vers de nouveaux dispositifs est trop lourde, les autorités sont bien obligées de se résigner à laisser passer du temps. Et là, curiosité, plutôt que d'instituer un calendrier unique – report de la date de bascule – les autorités laissent aux autorités nationales des possibilités d'aménagement peu compatibles avec la volonté d'unification des règles et d'égalité entre les acteurs.

Du pouvoir des autorités. En outre, la lourdeur des nouveaux dispositifs combinée à l'approche par les risques – nouveau credo des autorités européennes – pousse les autorités européennes à reconnaître aux autorités nationales une faculté d'exemption. La DSP 2 signe ainsi le « tout pouvoir » des autorités de supervision : l'harmonisation par la règle laisse place à la modulation par l'administration.

Au 14 septembre 2019, date à laquelle les nouvelles mesures de la DSP 2, communication sécurisée et authentification forte, devaient entrer en application partout

dans l'Union, on constate donc une mosaïque de situations : outre les différences entre les pays, les acteurs relevant d'un même État d'origine ne sont en réalité pas tous dans des positions identiques, certaines bénéficiant d'exemption d'autres non, qui étant déjà prêts au prix de lourds investissements qui profitant de la tolérance des autorités pour se conformer.

I. Authentification forte et DSP 2 : une histoire de "*supervisory flexibility*"

Par Pierre Storrer[1]

Une affaire de temps. On avait déjà regretté l'entrée en application en deux temps de la DSP 2 : le temps juridique du 13 janvier 2018 et le temps technique des RTS (ou *Regulatory technical standards*) on SCA and CSC (*strong customer authentication and common secure communication*) du 14 septembre 2019, portées par le règlement délégué (UE) 2018/389 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.

Il faut croire que le temps est désormais à la politique, celle du « *temps additionnel* » (on se croirait presque dans une compétition sportive), comme l'évoque l'EBA dans son opinion du 21 juin 2019 ; celle, aussi, des intérêts catégoriels (prestataires de services de paiement, d'un côté, e-commerçants, de l'autre) et, surtout, nationaux, car, on y est, chacun des États y va de sa propre « *prolongation* », tout en affirmant haut et fort que le 14 septembre était une date intangible et que le pire serait de ne pas s'entendre sur un nouveau temps commun.

Quoi qu'il en soit, du temps, à proprement parler, il n'en manquait pas : on ne nous fera pas croire le contraire, pour peu que l'on se remémore que la proposition de DSP 2 date de juillet 2013 ; de la bonne volonté, en revanche, on peut douter qu'elle fût toujours présente. À moins, mais faudrait-il encore le faire valoir, que cette affaire d'authentification forte du client ne soit une aberration économique – en l'état de la technologie –, pour cela qu'elle perturberait par trop la fluidité du parcours client.

Quand l'EBA siffle… la récréation. Il y eut d'abord cette étude menée pour le compte de l'établissement de monnaie électronique de droit anglais, et depuis peu de droit irlandais, *Stripe : The Impact of SCA - Shaking up Europe's online economy*, datée de mai dernier, qui a évalué à 57 milliards d'euros (tout de même !) – soit à peu près 10 % des 592 milliards d'euros de ventes en lignes prévues dans l'Union européenne pour 2019 – la perte que l'économie européenne du e-commerce enregistrerait dans les douze mois suivant la mise en œuvre de l'authentification forte.

Sans nécessairement y voir une relation de cause à effet, l'Autorité bancaire européenne publia, le 21 juin suivant, son opinion sous commentaire, relative à la seule authentification forte alors que, un an plus tôt, elle se prononçait sur les deux volets, manifestement indissociables, de la sécurisation des paiements électroniques : authentification forte et communication commune et sécurisée[2]. Le point 12 de l'opinion du 21 juin 2019 est un modèle d'antiphrase (nous soulignons) : "*The EBA reiterates that the application date of the RTS, as published in the Official Journal of the EU, is 14 September 2019, by which date all PSPs have to comply with the requirements set out therein. However, the EBA acknowledges the complexity of the payments markets across the EU and the necessary changes (including those described in this opinion) required to enable the issuer to apply SCA, in particular those required by actors that are not PSPs, such as e-merchants, which may be challenging and may lead to some actors in the payments chain not being ready. PSPs have a self-interest in ensuring that merchants, and all relevant actors in the payments chain, take all necessary steps. In addition, even if there were a liability shift to the payee or the payee's PSP for failing to accept SCA, as articulated in Article 74(2) of PSD2, this could not be considered an alleviation of PSPs' obligation to apply SCA in accordance with and as specified in Article 97 of PSD2. The EBA also acknowledges that a key component for the successful application of SCA is to explain and make customers aware of such changes and that it is paramount for customers to be able to continue making payments, including online.*"

L'heure de la récréation peut donc sonner, au point 13 (nous soulignons encore) : "*The EBA therefore accepts that, on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, CAs may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA, such as those described in this Opinion, and acquirers to migrate their merchants to solutions that support SCA. This supervisory flexibility is available under the condition that PSPs have set up a migration plan, have agreed the plan with their CA, and execute the plan in an expedited manner. CAs should monitor the execution of these plans to ensure swift compliance with the PSD2 and the EBA's technical standards and to achieve consistency of authentication approaches across the EU.*"

And so what? Ce n'est pas seulement la liberté prise avec la *end date* du 14 septembre 2019 qui étonne : après tout, la réalité (économique) est plus forte qu'un texte de loi. Outre le fait qu'il ait fallu attendre l'été pour s'apercevoir d'une telle difficulté insurmontable, c'est plutôt la méthode empruntée par l'EBA qui crée la surprise. Car ne nous y trompons pas : l'Autorité bancaire européenne ne procède pas elle-même à un report d'échéance mais autorise chacune des autorités compétentes des États membres, chacun de leur côté, en ordre dispersé, à fixer un *« temps additionnel »*. Elle ajoute, plus étonnant encore, que cette prolongation doit émaner des prestataires de services de paiement (PSP), sous forme de plan de migration agréé par leur autorité compétente ! Cette déconstruction du schéma initial de normalisation a désormais un nom : la *supervisory flexibility*.

1. Achevé de rédiger le 14 septembre 2019.

2. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, EBA-Op-2018-04, 13 June 2018.

Or ce n'est pas seulement l'unité de temps qui vole ainsi en éclats : c'est celle, sinon de la DSP 2 tout entière, du moins de son volet de sécurisation des paiements électroniques et de l'accès aux comptes, qui devaient marcher ensemble sur les deux jambes de l'authentification forte et de la communication commune et sécurisée. D'autant que l'on eût cru que la mise en place des APIs aurait été plus délicate (technologiquement) que celle des protocoles d'authentification. Pourquoi, dès lors, l'EBA n'a-t-elle pas organisé un nouveau calendrier de mise en œuvre de l'ensemble des mesures de sécurisation ? Se pourrait-il qu'une deuxième opinion s'intéressât bientôt à la date d'entrée en application des interfaces de communication ? Car après l'étude commandée par Stripe, voici qu'un tout jeune établissement de paiement suédois spécialisé dans l'initiation de paiement et l'information sur les comptes (dont le métier suppose donc l'accès aux comptes tenus par les banques, essentiellement) : *Tink*, a publié le 21 août dernier une lettre ouverte aux autorités nationales compétentes afin de leur faire part de cette « évidence » : *"Two thirds of financial institutions in Europe published their PSD2 APIs in time for the June deadline. Yet not a single one meets the requirements ans standards to be compliant*[3]."

Où l'on assiste alors à une « *sortie de la classe européenne* » à l'image de tous les départs en récréation : les uns et les autres vont en ordre dispersé, chacun dans sa direction et à son rythme. Anglais, allemands, belges, luxembourgeois, etc., y sont allés d'un communiqué de leur autorité de supervision, annonçant tantôt un plan de migration à 18 mois (FCA anglaise), mais le plus souvent sine die (Bafin allemande, Banque nationale de Belgique) ou, parfois, en s'inquiétant qu'« *étant donné la nature transfrontalière du e-commerce, l'adoption d'une date butoir de mise en conformité commune et harmonisée au niveau européen est jugée essentielle* » (CSSF luxembourgeoise), etc.

En France, nous guettions une prise de position de l'ACPR, autorité compétente nationale au sens du système européen de surveillance financière (SESF). Et bien non, c'est sous l'égide de l'Observatoire de la sécurité des moyens de paiement (OSMP, rattaché à la Banque de France) que s'est élaboré le « *plan de migration* » français – puisque c'est de cela dont il s'agit –, en deux temps. Le premier temps fut la publication, début juillet (donc assez tôt), du Rapport annuel de l'OSMP 2018, dont le chapitre Ier exposait un « *plan de migration des solutions d'authentification forte reposant sur la réception d'un code temporaire reçu par SMS (SMS OTP)* », dont le calendrier prévoyait que cette migration devrait être aboutie pour l'essentiel d'ici décembre 2020 et complètement achevée en trois ans (juin 2022). Dans un second, le 11 septembre dernier, ce même Observatoire invitait la presse pour lui présenter un « *Plan de migration de la Place française* » complété d'un volet, manifestement absent du Rapport, à l'attention des acteurs professionnels de la chaîne des paiements (schemes, prestataires de services de paiements acquéreurs et émetteurs, prestataires d'acceptation technique ou PAT e-commerçants), qui prévoit – à échéance de mars 2021 – la mise à niveau d'une architecture technique de Place « *3D-Secure* ».

Ce ne sont donc pas une mais deux migrations qui se dérouleront sur le territoire français, parallèlement, selon leur propre calendrier : l'une concernant les émetteurs et le déploiement de leurs solutions d'authentification forte du client, l'autre intéressant les différents acteurs du paiement et l'évolution du socle technique 3D-Secure. Tout ça pour ça : avions-nous besoin d'une directive, de RTS, de règlements délégués, d'opinions, etc., pour parvenir à une telle cacophonie ?

II. Communication sécurisée : publication des établissements exemptés de l'obligation de disposer d'un mécanisme de secours d'API

Par Myriam Roussille

Exemption de l'obligation de disposer d'un mécanisme de secours d'API. On le sait, la révolution introduite par la DSP 2 résulte de l'ouverture de l'accès aux données de paiement, souvent résumée sous l'expression *open banking*. Les prestataires teneurs de compte (compte de paiement) (*Account Servicing Payment Service Providers* – ASPSP) ont dû mettre en place un dispositif de communication sécurisée, la date du 14 septembre n'ayant pas sur ce point été reportée. Le règlement délégué qui complète la DSP 2[4] a fixé, il y a 18 mois (délai jugé trop court par certains), les spécifications que doivent aujourd'hui remplir les interfaces (*Application Programming Interface* – API). Tout prestataire gestionnaire de comptes doit proposer au moins une API pour permettre aux prestataires tiers (prestataires de service d'information sur les comptes dits « PSIC », prestataires de service d'initiation de paiements « PSIP » et émetteurs de cartes) qui le demandent d'accéder aux comptes qu'ils gèrent : si cette interface peut être la même que celle mise à disposition des utilisateurs de services de paiement (« l'*interface utilisateurs* »), elle peut aussi être dédiée[5]. Dans cette seconde hypothèse, l'API dédiée est supposée offrir à tout moment le même niveau de disponibilité et de performances que l'interface utilisateurs[6]. À défaut, un « *mécanisme de secours* »[7] doit être mis en place afin de permettre aux trois types prestataires tiers (PSIP, PSIC et émetteurs de carte) d'utiliser l'interface utilisateurs[8]. Du moins en principe, car le

3. *An open letter from Tink to European National Competent Authorities* (NCAs), *calling for flexibility around the PSD2 implementation deadline*, 21 août 2019.

4. Règl. 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. Sur ce texte, lire P. Storrer, « Derrière la DSP 2 : le règlement Authentification forte et Communication sécurisée », *Revue Banque* n° 820, mai 2018, p. 86 ; M. Roussille, « La DSP 2 bientôt pleinement applicable : les normes techniques enfin publiées », *Banque et Droit* n° 179, mai-juin 2018, p. 48.

5. Règl. délégué (UE) 2018/389, art. 31.

6. Règl. délégué (UE) 2018/389, art. 32.4.

7. Peuvent être exemptés par leur autorité compétente de l'obligation de mettre en place un mécanisme d'urgence, les PSPGC qui proposent une interface dédiée en tous points conforme à l'ensemble des obligations de l'article 32.

8. Le gestionnaire doit organiser un mécanisme de secours destiné à prendre le relai en cas d'indisponibilité imprévue ou de panne de l'interface, pour que les PSP puissent recourir aux interfaces utilisateurs, sous condition de respecter un certain nombre d'exigences, dont celles de justifier à leur autorité nationale compétente, sur demande, un tel recours ainsi que d'informer le PSPGC : Règl. délégué (UE) 2018/389, art. 33.

règlement précise que « *les autorités compétentes, après avoir consulté l'ABE pour assurer l'application cohérente* [de certaines conditions citées par le texte], *exemptent les prestataires de services de paiement gestionnaires de comptes qui ont choisi une interface dédiée de l'obligation de mettre en place le mécanisme d'urgence* »[9].

Publication de la liste : peu d'exemptés… C'est pourquoi le 12 septembre 2019, la Banque de France a publié la liste des établissements exemptés de l'obligation de disposer d'un mécanisme de secours d'API. 6 établissements y figurent, soit moins de 2 % des établissements en France d'après la presse, ce qui laisse pour le moins dubitatif. Toutefois, cela ne veut pas dire que les autres banques ne sont pas prêtes, car il fallait que les API mises à disposition attestent de 3 mois d'utilisation en production, preuves à l'appui à fournir à l'ACPR. C'est donc la course du temps. Une drôle de course, dans lesquels les acteurs des paiements se sont lancés et dont les contraintes se trouvent au dernier moment desserrées… en matière d'authentification forte. ■

SERVICES DE PAIEMENT – DSP 2 – HARMONISATION – AUTORITÉ BANCAIRE EUROPÉENNE – AUTORITÉS NATIONALES – COMMUNICATION SÉCURISÉE – MESURES DE SECOURS – EXEMPTION – AUTHENTIFICATION FORTE.

9. Règl. délégué (UE) 2018/389, art. 33.6. Le texte précise, à son considérant 24 : « *Certains prestataires de services de paiement gestionnaires de comptes seront exemptés de l'obligation de proposer un tel mécanisme de secours par l'intermédiaire de leurs interfaces clients, si leurs autorités compétentes établissent que leurs interfaces dédiées satisfont à des conditions spécifiques assurant une concurrence sans entraves. Dans le cas où les interfaces dédiées exemptées ne satisferaient pas aux conditions requises, les dérogations octroyées doivent être annulées par les autorités compétentes concernées.* »

Market et acquisition d'opérations de paiement (SP 5) : l'ACPR scelle sa position

La publication par l'ACPR, dans sa revue de septembre 2019, d'un article intitulé « À quoi correspond le service d'acquisition d'opérations de paiement (SP5) ? » marque sa volonté de consolider la position qu'elle a toujours adoptée pour les *marketplaces* et autres acteurs pratiquant l'encaissement pour compte de tiers. L'article a pour principal intérêt de viser les opérations exclues du SP 5.

« À quoi correspond le service d'acquisition d'opérations de paiement (SP5) ? », *Revue de l'ACPR*, sept. 2019 : https://acpr.banque-france.fr/sites/default/files/medias/documents/sp5.pdf.

Commentaire de Myriam Roussille.

Besoin de clarification. Dans sa revue de septembre 2019, l'ACPR a publié un article intitulé « À quoi correspond le service d'acquisition d'opérations de paiement (SP5) ? ». Le sujet a, on le sait, un temps défrayé la chronique, les e-commerçants exploitant des places de marché (*marketplaces*) s'étant vus enjoindre par l'ACPR, à l'automne 2013, de se conformer aux contraintes statutaires posées à l'époque par la DSP 1[1]. Les autorités françaises avaient unanimement retenu que l'encaissement de fonds pour compte de tiers constitue un service de paiement[2], alimentant un débat d'autant plus vif que toutes les autorités en Europe n'adoptaient pas toutes le même point de vue[3]. Le débat n'a duré qu'un temps seulement, car l'ACPR était en position d'imposer sa vision. Le superviseur a toujours raison.

Compte tenu des divergences en Europe à cette époque, les autorités européennes se sont emparées du sujet et ont entendu clarifier la question dans la DSP 2 en reformulant le service en « *service d'acquisition d'opérations de paiement* ». Y sont-elles parvenues ? On peut en douter… car l'expression n'est pas plus limpide que celle d'« *acquisition d'instruments de paiement* »[4] employée par la DSP 1 auparavant. Et il aura fallu attendre plus de 4 ans depuis la publication de la nouvelle directive pour que l'ACPR précise, au détour d'un article publié dans sa revue, son interprétation du fameux service 5 dans le dessein, à demi-mot assumé (par le schéma illustrant le service), de justifier ses exigences à l'égard des *marketplaces*.

L'ACPR prête à la DSP 2 une vertu de clarification du service de paiement 5 (SP5). Mais le législateur français avait déjà contribué à brouiller l'analyse : en guise d'« *acquisition d'instruments de paiement* » visée par la DSP 1[5], il l'avait à l'époque (en 2009) qualifié d'« *acquisition d'ordres de paiement* »[6] ; la DSP 2 évoque désormais le « *service d'acquisition d'opérations de paiement* ».

1. Les autorités françaises ont précisé leur position quant à l'activité d'encaissement pour compte de tiers début 2013 à l'occasion, s'agissant de l'ACPR et de l'AMF (Guide du financement participatif (*crowdfunding*) à destination des plates-formes et des porteurs de projet, publié par l'ACPR et l'AMF le 14 mai 2013, p. 2., de publication d'un guide sur le financement participatif, et s'agissant de la cour d'appel de Paris, d'un litige opposant une banque à une plate-forme d'échange en bitcoins (CA Paris, 26 sept. 2013, ch. 1, n° 11/15269, SA Crédit industriel et commercial c/ SAS Macaraja : Th. Bonneau, « Une société qui utilise un compte bancaire sur lequel transitent des bitcoins est-elle un prestataire de service de paiement ? », *JCP* E 2014, 1091).
2. Ce que l'ACPR a confirmé par la suite : ACPR, position 2014-P-01, 29 janv. 2014 relative aux opérations sur Bitcoins en France – P. Storrer, « Retour sur le *bitcoin* », in *Actualité janv.-févr. 2014* : Banque n° 770, mars 2014, p. 88 et s., spéc. p. 89. Voir aussi : « La régulation des nouveaux intervenants du marché des services de paiement », *Revue de l'ACPR* n° 21, janv.-févr. 2015.
3. Sur le sujet, voir : P. Storrer, « L'encaissement de fonds pour le compte de tiers vaut-il fourniture de services de paiement ? », *Revue Banque* n° 777, 2014, p. 86 ; M. Roussille, « *Marketplaces* et services de paiement : jusqu'où ira l'impérialisme de l'ACPR ? », *Revue de droit bancaire et financier*, nov.-déc. 2014, Focus 23. Et depuis : P. Storrer, « Services de paiement et intermédiation commerciale : qu'est l'encaissement de fonds pour le compte de tiers devenu ? », *Banque et Droit* n° 181, oct. 2018, p. 9.
4. Dir. 2007/64/CE, 13 nov. 2017, annexe (voir le service énuméré au 5°).
5. *Ibid.*
6. L'expression « *acquisition d'ordres de paiement* » retenue en France pouvait prêter, de l'aveu même de l'autorité, prêter à confusion puisqu'elle pouvait recouvrir le recueil d'un ordre de paiement (pour le compte du payeur), opération que fait tout prestataire qui reçoit un ordre de virement, et le service d'acquisition d'ordres de paiement (pour le compte du bénéficiaire) caractéristique des paiements par carte.

L'acquisition d'opération de paiement (SP 5) vise l'encaissement pour le compte de bénéficiaires. Reprenant cette fois la formule exacte de la DSP 2[7], l'article D. 314-2 définit, en son 4°, le « *service d'acquisition d'opérations de paiement* » comme « *un service 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* ». Le service 5 est donc un service fourni aux bénéficiaires par lequel le PSP s'engage à réceptionner pour le compte de ceux-ci les fonds issus d'opérations de paiement et à les mettre à leur disposition : autrement dit, il s'agit d'opérations d'encaissement.

Le raisonnement est net, même s'il n'est pas directement formulé par l'ACPR : toute personne (et non pas seulement tout PSP agréé comme tel – sinon, la question ne se poserait pas) qui encaisse les fonds pour le compte de bénéficiaires et qui les leur transfère sur un compte tenu par un PSP dans le cadre d'ordres de paiement permanents accomplit donc le service d'acquisition d'opérations de paiements. L'ACPR formalise donc ni plus ni moins la position qu'elle avait arrêtée depuis 2013, une époque où de son aveu même ni la loi, ni la DSP ne permettaient clairement d'asseoir cette interprétation.

7. Dir. (UE) 2015/2366, 25 nov. 2015, art. 4. 44.

Activités exclues du SP 5. L'article n'est pas pour autant dénué d'intérêt, car l'ACPR y précise que certaines activités se trouvent placées en dehors du champ du SP5. Il en va ainsi du recueil du consentement à une opération de paiement ou encore du recueil d'un ordre de paiement, lesquels peuvent en pratique être réalisés soit par des plates-formes, places de marché, soit par des professions réglementées ou encore des gros facturiers[8]. Mais ne pas s'y méprendre, ne manque pas de souligner l'ACPR : ces activités pourront toutefois, le cas échéant, faire l'objet d'une qualification au titre de la fourniture d'un autre service de paiement, tels que l'exécution d'opérations de prélèvements, de virements ou de paiement par carte, s'ils sont associés à un compte de paiement ou à une ouverture de crédit (SP3 et 4 visés aux 3° et 4° de l'article L. 314-1, II du CMF) ! Pour cela, il faut bien sûr que la prestation ne se limite à recueillir un consentement ou instruction, mais bien à l'exécuter. ■

SERVICES DE PAIEMENT – DSP 2 – ACQUISITION D'OPÉRATIONS DE PAIEMENT – ENCAISSEMENT POUR COMPTE DE TIERS.

8. En outre, la DSP précisait dans son considérant n° 10 que « *les services techniques fournis aux prestataires de services de paiement, tels que le simple fait de traiter et de stocker des données ou la gestion des terminaux, ne devraient pas être considérés comme une acquisition. Par ailleurs, certains modèles d'acquisition ne comportent pas de véritable transfert de fonds de l'acquéreur au bénéficiaire, parce que d'autres formes de règlement peuvent être convenues par les parties.* »