

# Du droit de donner libre accès à son compte de paiement

DERRIÈRE L'INNOVATION MAJEURE QU'EST LA CRÉATION DES PRESTATAIRES DE SERVICES D'INITIATION DE PAIEMENT ET DES PRESTATAIRES DE SERVICES D'INFORMATION SUR LES COMPTES, SE DÉCOUVRE LA PROMOTION DU COMPTE DE PAIEMENT, BIENTÔT EN LIBRE ACCÈS.

**PIERRE STORRER**

Avocat au barreau de Paris

Kramer Levin Naftalis & Frankel LLP\*



**M**ouvement. L'irruption, dans le paysage réglementaire, de ces nouveaux prestataires de services de paiement (PSP) que sont les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services d'information sur les comptes (PSIC)<sup>1</sup> – on n'oublie pas cette sorte de figure hybride que sont les émetteurs d'instruments de paiement liés à une carte – replace le compte de paiement au cœur du jeu (i.). Son accès par ceux qui ne le tiennent pas se présente ainsi comme l'innovation majeure de la

DSP2 (2.)<sup>2</sup>; en bout de chaîne, la question des données de compte concentre(ra) toute l'attention (3.).

## I. LE COMPTE

**1. De l'idée de compte.** Quel bonheur que d'être (re)tombé sur cette contribution magnifique du Professeur Didier R. Martin, « De l'idée de compte », parue en 1999 dans les *Mélanges de l'AEDBF*. Le ton est d'emblée donné : « Les vieilles idées sont toujours neuves. De sorte que l'idée de compte, née avec le commerce, n'échappe pas à cette perpétuelle jouvence. Spécialement dans l'ordre bancaire où une application systématisée, aussi ancienne que la banque elle-même, la sollicite de pourvoir aussi aux attentes nouvelles de ce métier »<sup>3</sup>. Alors, quelle nouvelle idée de (sur le) compte nous apporterait la DSP2 ? Celle-ci, d'abord et avant tout, que l'utilisateur de services de paiement<sup>4</sup> se réapproprie son compte.

**2. De quelques idées sur le compte.** On connaissait déjà le « compte obligé », sous la forme du fameux droit au compte (DAC)<sup>5</sup> (à noter qu'il s'agit

là de compte de dépôt), en vertu duquel « toute personne physique ou morale domiciliée en France, dépourvue d'un compte de dépôt, a droit à l'ouverture d'un tel compte dans l'établissement de crédit de son choix » (CMF, art. L. 312-1, al. 1<sup>er</sup>)<sup>6</sup>. On y ajouterait volontiers le « compte mobile », au sens du droit à la mobilité bancaire institué par l'article 312-1-7 du CMF qui, faut-il observer, concerne tant le compte de dépôt (et de livret) que le compte de paiement<sup>7</sup>. On y adjoindrait peut-être même une sorte de droit au « compte de cantonnement » pour les établissements de paiement (EP), si c'est de la sorte qu'il faut comprendre la prescription de l'article 36 de la DSP2 : « Les États membres veillent à ce que les établissements de paiement aient un accès objectif, non discriminatoire et proportionné aux services de comptes de paiement des établissements de crédit. Cet accès est suffisamment étendu pour permettre aux établissements de paiement de fournir des services de paiement de manière efficace et sans entraves. » Et puis aussi, pourquoi pas, et sans trop anticiper sur la troisième partie de cet exposé, un « droit à la portabilité des données de compte », comme en existera un des données à caractère

1. On se rappellera que le rapport 2012 du Comité consultatif du secteur financier (CCSF) les nommait *overlays payment service providers* et distinguait les agrégateurs de données des mandataires de paiement (p. 54).

2. Voir encore P. Storrer, « Abécédaire de la DSP2 », *Revue Banque* n° 793, févr. 2016, p. 88.

3. D. R. Martin, De l'idée de compte, *Mélanges AEDBF*, II, 1999, p. 285.

4. C'est l'expression consacrée par la DSP, dont l'article 4, 10 nous dit qu'il est « une personne physique ou morale qui utilise un service de paiement en qualité de payeur ou de bénéficiaire, ou des deux ».

5. Ou du droit à Livret A si l'on suit le texte de l'article L. 221-2 du CMF.

6. DAC qui ne peut toutefois faire obstacle aux règles antiblanchiment, nous apprennent de tous récents (juin 2016) principes sectoriels de l'ACPR relatifs aux obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme dans le cadre du droit au compte.

7. Cf. P. Storrer, « Sur la mobilité du compte de dépôt et du compte de paiement », *Revue Banque* n° 795, avr. 2016, p. 80.

\*Les propos de l'auteur n'engagent que celui-ci.

personnel, au sens où « les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle »<sup>8</sup>.

Droit au compte (de paiement cette fois) et à sa mobilité que l'on trouve consacrés par la directive Comptes de paiement : la directive 2014/92/UE 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<sup>9</sup>. Son considérant 6 peut être relevé, qui souligne que « la disparité des réglementations nationales actuelles peut être une source d'entraves importantes à l'achèvement du marché intérieur des comptes de paiement ». Nous assistons donc à une unification continue : des comptes de paiement (la présente directive), des services de paiement (DSP), à laquelle s'ajoute désormais la dernière pierre du marché unique des services financiers<sup>10</sup>, dans la mesure où, par la grâce de la DSP2, les services de paiement intègrent le champ du Système européen de surveillance financière (SESF), sous la supervision de l'Autorité bancaire européenne (ABE). C'est acquis, le droit des services de paiement n'est plus marginal mais trouve toute sa place à côté de la réglementation des services bancaires et des services d'investissement. Et tout cela en moins de dix ans, faut-il remarquer.

**3. Mon compte est à moi.** Ceci nous paraît caractéristique de la DSP2 : le centre de gravité du compte se déplace, qui n'est plus seulement, ou tellement, la chose de celui qui le

tient (établissement bancaire le plus souvent), pour appartenir davantage à son titulaire, qui en prend la maîtrise. Qui, et c'est remarquable, se voit attribuer la faculté de donner (plus ou moins) libre accès à son compte, accès à d'autres qu'à son gestionnaire. Mais mon compte est davantage à moi, aussi, dans ma relation directe avec mon teneur de compte. De sorte que mon contrat-cadre de services de paiement ne serait plus seulement contrat d'adhésion à prendre ou à laisser. Par exemple, expose le considérant 57 de la DSP2, « il devrait être possible au prestataire de services de paiement et à l'utilisateur de services de paiement d'arrêter, dans le contrat-cadre, les modalités de la transmission des informations fournies par la suite sur les opérations de paiement effectuées, par exemple de convenir que, dans le cadre de services bancaires par l'Internet, toutes les informations relatives au compte de paiement seront accessibles en ligne ».

Droit d'accès au compte de paiement donné par son titulaire à ceux qui ne le tiennent pas, telle est l'innovation majeure apportée par la DSP2, qui n'est toutefois pas sans poser une forte interrogation. Car cet accès est donné à un objet fort mystérieux qu'est le compte de paiement (mystérieuse est sans doute aussi la notion de compte en général), qui n'est jamais défini que comme le compte qui est « utilisé aux fins de l'exécution d'opérations de paiement » (CMF, art. L. 314-1, I, reprenant la définition donnée à l'article 4, 14 de la DSP et reprise à l'article 4, 12 de la DSP2) ; le compte destiné « exclusivement » à de telles opérations (cf. CMF, art. L. 522-4, I). Objet mystérieux mais aussi évanescant, si l'on veut bien considérer que le compte de paiement est, par nature, un « compte de flux », et même le « compte d'un jour », après quoi les fonds devront être cantonnés<sup>11</sup>. L'accès au compte de paiement ira-t-il jusqu'au compte de cantonnement (mais ne s'est-il pas déjà transformé en compte de dépôt<sup>12</sup>?) ?

Concerne-t-il aussi le compte de monnaie électronique dont on peut considérer qu'il est un compte spécifique de paiement<sup>13</sup>? Voilà quelques questions qui demeurent en suspens.

Quelques interrogations qui prépareraient, pourquoi pas, l'avènement de ce que l'on nomme aujourd'hui volontiers la « néo-banque » pour désigner, une fois les facilités incantatoires passées (on vous épargnera l'« uberisation » de la banque), une autre façon de faire de la banque, et pourquoi pas de faire de la « banque sans compte », comme il existe des « comptes sans banque ». On ne croit pas qu'il faille prêter tout cela à la DSP2 (on lui prête beaucoup), mais elle y prend certainement sa part.

#### **4. Le compte de paiement, mais seulement le compte de paiement.**

C'est toujours la même chose : mais puis-je aussi avoir accès à compte de dépôt, d'épargne, sur livret, etc. ? Revenons à la seule liste dont nous disposons, celle dressée par l'Arrêté du 29 juillet 2009 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 : « Au sens du présent arrêté, le terme : "compte de paiement" désigne les comptes de dépôt à vue, les comptes ouverts par les établissements de paiement conformément à l'article L. 522-4 du même Code et tout autre compte tel que défini à l'article L. 314-1 du même Code, ouverts par des personnes physiques n'agissant pas pour des besoins professionnels » (art. 1<sup>er</sup>, al. 1<sup>er</sup>).

Si bien que les PSIC, en particulier, n'auront pas accès aux « comptes soumis à une réglementation particulière, notamment les comptes sur livret, les comptes à terme et les comptes d'instruments financiers et les comptes espèces qui leur sont spécifiquement associés » (art. 1<sup>er</sup>, al. 2).

8. Règl. (UE) 2016/679, 27 avr. 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 (règlement général sur la protection des données), art. 201.

9. Cf. Rev. ACPR n° 21, janv.-févr. 2015, Retour sur la directive comptes de paiement, p. 17.

10. On se reportera avec intérêt au Livre vert de la Commission européenne du 10 décembre 2015, De meilleurs produits, un plus large choix et davantage d'opportunités pour les consommateurs et les entreprises, COM(2015) 630 final.

11. Cf. P. Storrer, Brèves remarques sur le compte de paiement, Revue Banque n° 788, oct. 2015, p. 87.

12. Comp. Arr. 27 oct. 2015 relatif à la mise en œuvre de la garantie des dépôts, au plafond d'indemnisation et aux modalités d'application de l'article L. 312-4-1 du Code monétaire et financier, art. 5, I, 1°.

13. Cf. Règl. (UE) 2015/751, 29 avr. 2015, relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, art. 22 : « "compte de paiement" : 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 ».

## ■ II. L'ACCÈS AU COMPTE

### 1. LES PRESTATAIRES DE SERVICES DE PAIEMENT GESTIONNAIRES DE COMPTE

**5. PSPGC.** Nous désignerons les prestataires de services de paiement gestionnaires de compte (*account servicing payment service provider*) par l'acronyme PSPGC. Il va sans dire que l'expression était absente de la DSP, qui ne traitait, indistinctement, que des prestataires de services de paiement (PSP), peu important que lesdits services fussent adossés ou non à un compte. Pour reprendre un bon mot du Professeur Didier R. Martin (qui n'en ait pas avare), on aurait comme « engrossé » les PSP, qui tantôt enfantent des PSPGC, des PSIP ou des PSIC<sup>14</sup>...

Qu'est-ce qu'un PSPGC ? La définition donnée par la DSP2 – on pouvait s'y attendre – est décevante : « un prestataire de services de paiement qui fournit et gère un compte de paiement pour un payeur » (art. 4, 17). Il faut alors se tourner vers la directive Compte de paiement déjà évoquée. On y déniche ceci : « les services liés au compte de paiement [sont] tous les services liés à l'ouverture, à la gestion et à la clôture d'un compte de paiement, y compris les services de paiement [...] » (art. 2, 6. Adde, art. 17, 1).

On y ajoute que les PSPGC sont ceux qui, généralement, délivrent « les données de sécurité personnalisées utilisées pour garantir l'authentification du client, par l'utilisateur de services de paiement ou par le prestataire de services d'initiation de paiement » (cons. 30).

**6. Selon que vous gérez ou non des comptes.** Les PSP sont donc désormais distribués en deux catégories : ceux qui gèrent le compte du payeur ou du bénéficiaire, d'un côté, les PSP sans compte, de l'autre. Deux catégories qui se mêlent à une troisième<sup>15</sup> : les prestataires de services

techniques, avec lesquels flirtent les PSIP et PSIC, si l'on en croit l'article 3, j de la DSP2, excluant de son champ d'application 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 ».

Il est difficile d'en dire davantage sur les PSPGC. La raison est simple : ils n'existent qu'en contrepoint des nouveaux prestataires sans compte (on les nommerait volontiers « orphelins » mais, on va le voir, ils ne le sont pas tant que cela), dont la réglementation dessine en creux les obligations (surtout) et les droits (un peu) des premiers.

### 2. LES PRESTATAIRES SANS COMPTE

**7. Sans compte, ni fonds, mais bien des PSP.** Il serait plus exact de les nommer « prestataires de services non gestionnaires du compte du payeur (ou de l'utilisateur) », mais avouons que cela serait bien lourd. Nous préférons donc l'expression de « prestataires sans compte », ce qui ne veut pas dire qu'ils n'en tiennent pas par ailleurs, mais qu'ils ne gèrent pas, au moment considéré, celui du payeur (ou de l'utilisateur) qui les autorise à y avoir accès.

Prestataires sans compte mais, aussi, sans fonds, car il leur est expressément interdit d'entrer en possession des fonds de leurs clients (cons. 31 et 35). De sorte que, logiquement (c'est une charge considérable en moins), l'article 9 de la

DSP2 les dispense de l'obligation de détenir des fonds propres<sup>16</sup> et, bien sûr, de les protéger (art. 10).

Cela étant, nos PSP sans compte ni fonds ne sont plus considérés comme des « PSP tiers » (on aime encore bien les nommer *Third Party Providers* ou *TPP*, de même qu'il est toujours plus clinquant d'évoquer la PSD2, les PISP pour *Payment Initiation Service Providers* ou les AISP pour *account information service providers*), ainsi que les avaient qualifiés à l'origine la proposition de DSP2<sup>17</sup>, regroupant sous cette dénomination les PSP exerçant « les services fondés sur l'accès aux comptes de paiement fournis par un prestataire de services de paiement qui n'est pas le prestataire de services de paiement gestionnaire du compte, sous la forme de : (a) services d'initiation de paiement ; (b) services d'information sur les comptes » (Annexe 1, pt 7). Petits ou para-PSP, sans doute, mais PSP à part entière faut-il néanmoins retenir.

#### 2.1. Les règles communes

**8. Droit transitoire.** Un principe remarquable de continuité du marché est énoncé au considérant 33 de la DSP2, ainsi traduit aux pts 5 et 6 de l'article 115 :

– « les États membres n'interdisent pas aux personnes morales qui ont, avant le 12 janvier 2016, exercé sur leur territoire des activités de prestataires de services d'initiation de paiement et de prestataires de services d'information sur les comptes au sens de la présente directive à continuer d'exercer les mêmes activités sur leur territoire au cours de la période transitoire visée aux paragraphes 2 et 4 conformément au cadre réglementaire actuellement en vigueur » ;

– « les États membres veillent à ce que, jusqu'à ce que chacun des prestataires de services de paiement gestionnaires de comptes se conforme aux normes techniques de réglementation visées au paragraphe 4, les prestataires de services de paiement gestionnaires de comptes ne puissent abuser de leur non-conformité pour bloquer ou entraver l'utilisation de services d'initiation de paiement et de services d'informa-

14. Cf. D. R. Martin, *Que sont les notions devenues*, Dalloz 2014, p. 164.

15. On pourrait y ajouter encore la catégorie des « PSP intermédiaires » des règlements antiblanchiment, par exemple le dernier (règlement (UE) du 20 mai

2015 sur les informations accompagnant les transferts de fonds, applicable au 26 juin 2017), qui les définit comme les PSP qui ne sont ni les PSP du donneur d'ordre ou du bénéficiaire et qui reçoivent et transmettent un transfert de fonds pour le compte du PSP du donneur d'ordres ou du bénéficiaire ou d'un autre PSP intermédiaire.

16. Mais pas d'une assurance de responsabilité civile professionnelle.

17. COM(2013) 547 final, 24 juill. 2013. Cf. P. Storrer, « De la DME à la DSP2 : le nouvel horizon des paiements », *Banque et Droit* n° 152, nov.-déc. 2013, p. 8.

tion sur les comptes pour les comptes dont ils sont gestionnaires ».

**9. Droit d'accès.** Où le titulaire du compte prime sur son gestionnaire : « Il est nécessaire de définir un cadre juridique clair fixant des conditions dans lesquelles les prestataires de services d'initiation de paiement et les prestataires de services d'information sur les comptes peuvent fournir leurs services avec le consentement du titulaire du compte sans être obligés par le prestataire de services de paiement gestionnaire du compte d'appliquer un modèle commercial donné, qu'il repose sur un accès direct ou indirect, pour la prestation de ces types de services » (cons. 93). L'ACPR résume cela assez bien : « La création de ces nouveaux services a conduit le législateur européen à créer un droit, des utilisateurs, d'accès aux comptes de paiement tenus par les PSP gestionnaires de comptes lorsque ces comptes sont accessibles par voie électronique. Ce droit d'accès concerne les PSIP et les PSIC, mais également les PSP émetteurs d'instruments de paiement liés à une carte »<sup>18</sup>.

Ce faisant, l'enjeu majeur de la réglementation des PSIP et PSIC se concentre sur les règles relatives à l'accès au compte de paiement et à ses données. Celles-ci sont, pour l'essentiel, au nombre de deux : (i) est garanti au payeur ou à l'utilisateur le droit de s'adresser à un PSIP ou à un PSIC dès lors que son compte de paiement est accessible en ligne (art. 66, 1 et 67, 1) et (ii) la fourniture du service d'initiation de paiement ou d'information sur les comptes n'est pas subordonnée à l'existence de relations contractuelles entre PSPIP ou PSIC et PSPGC. Cela est à l'évidence tout à fait remarquable : les relations du payeur (ou de l'utilisateur) avec ses différents PSP demeurent bilatérales, parallèles, points de contrats entre les prestataires, le client les tient à sa main.

L'accès au compte de paiement n'est cependant pas sans limite, comme en dispose le point 5 de l'article 68 de la DSP2 : « Un prestataire de services de paiement gestionnaire du compte peut refuser à un prestataire de services d'information sur les comptes ou à un prestataire de services d'initia-

tion de paiement l'accès à un compte de paiement pour des raisons objectivement motivées et documentées liées à un accès non autorisé ou frauduleux au compte de paiement de la part dudit prestataire de services d'information sur les comptes ou dudit prestataire de services d'initiation de paiement, y compris l'initiation non autorisée ou frauduleuse d'une opération de paiement. Dans ces cas, le prestataire de services de paiement gestionnaire du compte informe le payeur, de la manière convenue, du refus d'accès au compte de paiement et des raisons de ce refus. Cette information est, si possible, donnée au payeur avant que l'accès ne soit refusé et au plus tard immédiatement après ce refus, à moins que le fait de fournir cette information ne soit pas acceptable pour des raisons de sécurité objectivement justifiées ou soit interdit en vertu d'une autre disposition du droit de l'Union ou de droit national pertinente »<sup>19</sup>.

**10. Assurance.** Agréés (PSIP) ou enregistrés (PSIC), les uns et les autres doivent disposer, comme préalable à leur agrément ou à leur enregistrement, d'une assurance de responsabilité civile professionnelle couvrant les territoires où ils proposent des services ou une autre garantie comparable contre l'engagement de leur responsabilité (art. 5, 2 et 3). Le montant minimal de cette assurance ou autre garantie devra être fixé par l'ABE au plus le 13 janvier 2017.

**11. Authentification forte.** La question est évidemment centrale mais ne concerne pas seulement les PSIP et PSIC puisque tout PSP, indistinctement, est sommé d'appliquer l'authentification forte du client<sup>20</sup> dès

lors que le payeur i) accède à son compte de paiement en ligne, ii) initie une opération de paiement électronique et iii) exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse (art. 97, 1). À quoi s'ajoutent les obligations, en matière de paiement à distance, d'établir un « lien dynamique » entre l'opération, le montant et le bénéficiaire donnés (art. 97, 2) ainsi que de prendre des mesures de sécurité adéquates afin de protéger la confidentialité et l'intégrité des mesures de sécurité personnalisées des utilisateurs (art. 97, 3).

Si bien que :

– les paragraphes 2 et 3 ci-dessus s'appliquent aux PSIP ;

– les paragraphes 1 et 3 s'appliquent aux PSIC ;

– et PSIP comme PSIC bénéficient du droit de se fonder sur les procédures d'authentification prévues par les PSPGC à l'intention de leurs utilisateurs.

On note que la question de l'authentification forte fait l'objet d'un Discussion Paper de l'EBA, dont traite M. Geoffroy Goffinet dans le présent hors-série).

**12. Agent, passeport européen, LCB-FT.** PSIP et PSIP pourront-ils recourir à des agents afin d'exercer, pour leur compte, les activités pour lesquels ils sont agréés ? Rien ne semble l'interdire et la définition de l'agent par l'article 4, 38 de la DSP2 est suffisamment large (« agent », une personne physique ou morale qui agit pour le compte d'un établissement de paiement pour la fourniture des services de paiement ») pour le permettre, de même que l'article 19, qui traite du recours à des agents, à des succursales ou à des entités vers lesquelles des activités sont externalisées, ne distingue pas selon la qualité du PSP.

« Tout établissement de paiement agréé souhaitant fournir des services de paiement pour la première fois dans un État membre autre que son État membre d'origine, en vertu du droit d'établissement ou de la liberté de prestation de services, communique les informations suivantes aux autorités compétentes de son État membre d'origine [...] » dispose l'article 28 de

19. Le point 6 ajoutant que, dans ce cas, « le prestataire de services de paiement gestionnaire du compte notifie immédiatement à l'autorité compétente l'incident concernant le prestataire de services d'information sur les comptes ou le prestataire de services d'initiation de paiement. La notification contient les informations pertinentes relatives à l'incident et les raisons justifiant les mesures prises. L'autorité compétente évalue l'incident et prend au besoin des mesures appropriées. »

20. Définie comme « une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession" (quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification. »

18. Revue ACPR n° 26, janv.-févr. 2016, p. 9.

la DSP2. L'emploi du participe passé « agréé » devrait-il exclure du jeu du passeport européen<sup>21</sup> les PSIC qui, on le verra, ne sont qu'« enregistrés » ? Ce serait sans doute lecture trop littérale du texte, d'autant que le considérant 48 est sans ambiguïté : « Les prestataires de services d'information sur les comptes devraient pouvoir fournir leurs services sur une base transfrontalière et bénéficieront des règles en matière de « passeport ». »

Une question à laquelle nous n'avons pas de réponse : par définition, les PSIP et PSIC vont aller « taper » dans des comptes dont leurs clients sont titulaires et dont en relation d'affaires avec leur PSPGC, tenus à ce titre de les connaître. Des obligations particulières de KYC pèseront-elles sur nos prestataires sans compte ? Et bien, un début de réponse peut être trouvé dans les orientations finales de l'Autorité bancaire européenne (ABE) sur la sécurité des paiements sur internet du 19 décembre 2014, dont une note de bas de page nous livre ceci : « Les PSP ne sont pas tenus d'appliquer une procédure distincte d'identification du client pour les services de paiement sur internet, à condition qu'une telle identification du client ait déjà été réalisée, par exemple pour d'autres services existants relatifs aux paiements ou pour l'ouverture d'un compte » (p. 12, note 11).

## 2.2. Les PSIP

**13. Notion.** La définition du service d'initiation de paiement<sup>22</sup> – désormais service 7 aux termes de l'annexe I de la directive – trouve son siège à l'article 4, 15 de 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 ».

Rapidement entrevue, l'initiation de paiement s'apparente à un paiement direct en ligne de compte à compte par virement : « 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 plateforme 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 » (DSP2, cons. 27) L'intérêt pour le commerce en ligne est grand puisque le PSIP assurera au bénéficiaire que le paiement a été initié, si bien que ce dernier sera incité à livrer les biens ou fournir les services sans retard injustifié (cons. 29). Paiement direct de compte à compte : il va sans dire que le paiement par carte à distance s'en trouverait désintermédié, préparant sans doute par-là l'ère de l'instant payment ou instant Sepa Credit Transfer.

De là que la prestation d'initiation de paiement paraît davantage un service offert au bénéficiaire qu'au payeur. Ce que paraît confirmer la lecture des orientations finales de l'ABE sur la sécurité des paiements sur internet, qui, sous le vocable malheureux d'« intégrateurs de paiement »<sup>23</sup>, exposent que ceux-ci « fournissent au bénéficiaire (c'est-à-dire le commerçant en ligne) une interface normalisée avec les services d'initiation de paiement fournis par un PSP » (p. 5).

**14. Perturbation.** L'initiation de paiement crée une perturbation certaine dans notre classification tripartite des opérations de paiement (cf. CMF, art. L. 133-3, II). Sont-elles ordonnées :

- par le payeur, qui donne un ordre de paiement à son PSP ? Il s'agit là d'une opération de virement ;
- par le payeur, qui donne un ordre de paiement par l'intermédiaire du bénéficiaire ? Nous sommes en présence d'un paiement par carte ;
- par le bénéficiaire, qui donne un ordre de paiement au PSP du payeur, fondé sur le consentement du payeur au bénéficiaire ? C'est de virement dont il est question<sup>24</sup>.

Mais où rangera-t-on l'initiation de paiement ? Elle semble certes déclencher une opération de virement, mais son client serait le bénéficiaire...

Perturbations (nécessaires) liées aussi à la vie des opérations de paiement. On en relèvera deux en particulier :

- autorisation d'une opération de paiement : par principe, une opération de paiement est réputée autorisée si le payeur a consenti à son exécution. Mais, aux termes de la DSP2, « le consentement à l'exécution d'une opération de paiement peut aussi être donné par l'intermédiaire du bénéficiaire ou de prestataire de services d'initiation de paiement » (art. 64, 2) ;
- preuve de l'authentification et de l'exécution : « 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 en relation avec le service de paiement qu'il doit assurer » (art. 72, 1, al. 2).

**15. Agrément.** À la différence notable des PSIC (seulement enregistrés), les PSIP devront être agréés aux termes d'une procédure qui, sauf certains points (fonds propres, etc.), ne les traite pas différemment, sauf dans l'exigence d'une assurance de responsabilité civile professionnelle. Ni plus, ni moins<sup>25</sup>, donc, mais, ce faisant, les PSIP seront soumis à des contraintes d'agrément « de droit commun » sensiblement plus lourdes que celles qui prévalent sous l'empire de la DSP<sup>26</sup>.

Par ailleurs, entre le montant minimal de 20 000 euros (service 6 de transmission de fonds) et maximal de 125 000 euros (services 1 à 5), les PSIP devront disposer d'un capital initial de 50 000 euros (art. 7).

21. Remarquons en passant que le terme « passeport » n'apparaissait pas dans la DSP mais fait son entrée dans la DSP2, aux considérants 41 et 48.

22. On trouvera souvent dans les textes anglais l'acronyme PIS pour Payment Initiation Services

23. ABE qui précise au n° 10 de son document que « les intégrateurs de paiement proposant des services d'initiation de paiement sont considérés soit comme acquéreurs de services de paiement sur internet (et donc comme PSP) soit comme fournisseurs externes de services techniques aux systèmes concernés ou aux PSP ».

24. Dont la définition, absente de la DSP, figure désormais à l'article 4, 24 de la DSP2 : « un service de paiement fourni par le prestataire de services de paiement qui détient le compte de paiement du payeur et consistant à créditer, sur la base d'une instruction du payeur, le compte de paiement d'un bénéficiaire par une

opération ou une série d'opérations de paiement réalisées à partir du compte de paiement du payeur ».

25. Notons qu'il n'y aura pas de « petits PSIP » (ni d'ailleurs de « petits PSIC »), comme il y a de « petits EP » (ou de « petits EME ») sous plafond de 3 millions d'euros (art. 32).

26. En ce sens, P. Storrer, « Abécédaire de la DSP2 », précité, v° Agrément.

**16. Règles relatives à l'accès au compte de paiement.** On les trouve détaillées à l'article 66 de la DSP2. Il ne sert à rien de tenter de les paraphraser.

La mise en œuvre du service d'initiation de paiement suppose, du côté de son prestataire, qu'il :

– ne détienne à aucun moment les fonds du payeur en liaison avec la fourniture dudit service ;

– veille à ce que les données de sécurité personnalisées de l'utilisateur de services de paiement ne soient pas accessibles à d'autres parties que l'utilisateur et l'émetteur desdites données et veille à transmettre celles-ci au moyen de canaux sûrs et efficaces ;

– veille à ce que toute autre information relative à l'utilisateur de services de paiement, obtenue lors de la fourniture de services d'initiation de paiement, ne soit communiquée qu'au bénéficiaire et uniquement avec le consentement explicite de l'utilisateur de services de paiement ;

– chaque fois qu'un paiement est initié, s'identifie auprès du PSPGC et communique avec lui, le payeur et le bénéficiaire de manière sécurisée, conformément à l'article 98, 1, d de la directive ;

– ne stocke pas de données de paiement sensibles concernant l'utilisateur de services de paiement ;

– ne demande pas à l'utilisateur de services de paiement des données autres que celles nécessaires pour fournir le service d'initiation de paiement ;

– n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par le payeur ;

– ne modifie pas le montant, le bénéficiaire ou tout autre caractéristique de l'opération (art. 66, 3).

De son côté, le PSPGC :

– communique de manière sécurisée avec les prestataires de services d'initiation de paiement, conformément à l'article 98, 1, d précité ;

– immédiatement après avoir reçu l'ordre de paiement d'un PSIP, fournit à celui-ci, ou met à sa disposition, toutes les informations sur l'initiation de l'opération de paiement et toutes les informations auxquelles il a lui-même accès concernant l'exécution de l'opération de paiement ;

– traite les ordres de paiement transmis grâce aux services d'un PSIP sans aucune discrimination, autre que fondée sur des raisons objectives, en termes de délai, de priorité ou de frais par rapport aux ordres de paiement transmis directement par le payeur (art. 66, 4).

Le lien entre les premiers (PSIP) et les seconds (PSPGC) passe par le consentement explicite à l'exécution d'un paiement donné par le payeur, en vertu duquel ces derniers exécutent les actions prévues ci-dessus afin de garantir le droit du payeur de recourir à un service d'initiation de paiement (art. 66, 2).

**17. Responsabilité.** Le coup est rude pour les PSPGC (on ajouterait « installés ») : ils sont bien responsables en première ligne, quand bien même un PSIP se serait glissé dans l'opération de paiement : « Afin de garantir un niveau élevé de protection des consommateurs, le payeur devrait toujours être en droit d'adresser sa demande de remboursement à son prestataire de services de paiement gestionnaire du compte, même lorsqu'un prestataire de services d'initiation de paiement intervient dans l'opération de paiement. Cette disposition est sans préjudice de la répartition des responsabilités entre les prestataires de services de paiement » (cons. 74).

De sorte que, opération de paiement non autorisée, non exécutée ou mal exécutée, le principe est le même : le payeur s'adresse en priorité à son PSPGC qui le rembourse. Après quoi, si le PSIP est responsable du dysfonctionnement de paiement, il indemnise immédiatement le PSPGC, à sa demande, pour les pertes subies ou les sommes payées en raison du remboursement du payeur.

Sachant que, dans tous les cas de figure, c'est au PSIP de prouver que l'opération de paiement a été authentifiée et dûment enregistrée et traitée sans déficience (art. 73 et 90). À relire ces textes, il n'est pas certain qu'ils soient scandaleux.

### **2.3. Un PSP atypique : l'émetteur d'instruments de paiement liés à une carte**

**18. De la confirmation de la disponibilité des fonds.** La DSP2 fait le constat que les établissements de crédit demeurent la principale

porte d'entrée des consommateurs pour obtenir des instruments de paiement. De là que l'émission d'un instrument de paiement lié à une carte par un PSP autre que celui qui gère le compte du client renforcerait la concurrence, ce qui nous amène sur le terrain de la confirmation de la disponibilité des fonds. Partant, « le prestataire de services qui émet l'instrument de paiement lié à une carte, en particulier des cartes de débit, pourrait mieux gérer et réduire son risque de crédit s'il obtient du prestataire de services de paiement gestionnaire du compte confirmation de la disponibilité de fonds sur le compte du client » (cons. 67)<sup>27</sup>. Il convient de se référer au règlement (UE) 2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte (règlement « CMI ») afin de savoir qu'un instrument de paiement lié à une carte est « tout instrument de paiement, y compris une carte, un téléphone mobile, un ordinateur ou tout autre dispositif technologique doté de l'application de paiement adéquate, qui permet au payeur d'initier une opération de paiement liée à une carte qui n'est ni un virement ni un prélèvement au sens de l'article 2 du règlement (UE) n° 260/2012 » (art. 2, 20).

Une disposition propre de la DSP2, l'article 65, est consacrée à ces acteurs que l'on nomme parfois *card-based payment instrument issuers*. En substance, et à certaines conditions, « un prestataire de services de paiement gestionnaire du compte, à la demande d'un prestataire de services de paiement qui émet des instruments de paiement liés à une carte, confirme immédiatement si le montant nécessaire à l'exécution d'une opération de paiement liée à une carte est disponible sur le compte de paiement du payeur ».

Le régime de la confirmation de la disponibilité des fonds (duquel sont soustraites les cartes qui stockent de la monnaie électronique) est intéressant à plus d'un titre :

– c'est à son PSPGC, et non au prestataire « tiers », que le payeur donne son consentement ;

<sup>27</sup>. Étant ajouté que « dans le même temps, cette confirmation ne devrait pas permettre au prestataire de services de paiement gestionnaire du compte de bloquer des fonds sur le compte de paiement du payeur ».

– la confirmation de la disponibilité des fonds prend la forme d'un simple « oui » ou « non », mais pas d'un relevé de compte, étant ajoutée qu'elle ne peut être ni stockée ni utilisée à d'autres fins que l'exécution d'une opération de paiement : en somme, ce n'est pas une information sur le compte au sens du nouveau service 8 ;  
– la confirmation ne permet pas au PSPGC de bloquer des fonds sur le compte du payeur.

#### 2.4. Les PSIC

##### 19. Quand la DSP2 sort de son lit.

La formule paraîtra curieuse. Elle entend signifier que non, décidément non, les PSIC ne sont pas des PSP, ne « font » pas du paiement et se retrouvent ainsi dans un texte qui ne devrait pas être le leur.

Le considérant 28 de la DSP2 y voit d'ailleurs des services « complémentaires » : « [...] à la faveur des progrès technologiques, de nombreux services complémentaires ont également fait leur apparition ces dernières années, tels que les services d'information sur les comptes. Ces services fournissent à l'utilisateur de services de paiement des informations agrégées en ligne concernant un ou plusieurs comptes de paiement qu'il détient auprès d'un ou de plusieurs autres prestataires de services de paiement et sont accessibles via des interfaces en ligne du prestataire de services de paiement gestionnaire du compte. L'utilisateur de services de paiement est donc en mesure d'avoir immédiatement une vue d'ensemble de sa situation financière à un moment donné ». En somme, l'information sur les comptes est bien un service d'assistance à gestion de ses finances personnelles, un PMF (personal finance management), mais certainement pas un service de paiement. Mais peu importe après tout, puisque le législateur européen a choisi, au prix de quelques contorsions, de le faire tel : « Ces services devraient également être régis par la présente directive, afin d'assurer aux consommateurs une protection adéquate en ce qui concerne les paiements qu'ils effectuent et les données relatives au compte ainsi qu'une sécurité juridique quant au statut des prestataires de services d'information sur les comptes. »

Si bien que constitue le service 8 d'information sur les comptes (account information service ou AIS) le « 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 » (art. 4, 16).

**20. Statut dérogatoire.** La première dérogation, on l'a dit, et non des moindres, est que le PSIC sera le seul des PSP à ne pas devoir disposer de capital initial (article 7 a contrario) ni à être agréé mais enregistré, sans que l'on sache bien, pour l'heure, en quoi consistera cet enregistrement, ni si l'ABE a le projet d'édicter des règles de second niveau en la matière.

Ce que l'on sait, en revanche, c'est que « compte tenu de la nature particulière de l'activité exercée et des risques liés à la prestation de services d'information sur les comptes, il convient de prévoir un régime prudentiel spécifique pour les prestataires de services d'information sur les comptes » ; partant, qu'un article 33 de la DSP2 prévoit le régime d'exemption suivant au profit des PSIC :

- ils sont exemptés de l'essentiel de l'application de la procédure (d'agrément) et des conditions communes aux EP (art. 33, 1) ;
- ils sont traités comme des EP... à ceci près que, sauf quelques dispositions, les titres III (Transparence des conditions et exigences en matière d'information régissant les services de paiement) et IV (Droit et obligations liés à la prestation et à l'utilisation de services de paiement) de la DSP2 ne leur sont pas applicables (art. 33, 2).

Des PSP, certes, mais d'un genre bien particulier (d'aucuns seraient tentés d'y accoler « parasite »), de ceux qui « gravitent » autour du paiement plutôt qu'ils n'y participent directement.

**21. Règles relatives l'accès aux données de comptes de paiement.** On les trouve détaillées à l'article 67 de la DSP2. Nous les reprenons comme nous l'avons fait plus haut concernant les PSIP.

Le PSIC :

- fournit des services uniquement sur la base du consentement explicite de l'utilisateur de services de paiement ;
- veille à ce que les données de sécurité personnalisées de l'utilisateur de

services de paiement ne soient pas accessibles à d'autres parties que l'utilisateur et l'émetteur desdites données et veille, lorsqu'il transmet celles-ci, à utiliser des canaux sûrs et efficaces ;

- pour chaque session de communication, il s'identifie auprès du ou des PSPGC de l'utilisateur de services de paiement et communique avec celui-ci ou ceux-ci et l'utilisateur de services de paiement de manière sécurisée, conformément à l'article 98, 1, d de la directive ;

- accède uniquement aux informations provenant des comptes de paiement désignés et des opérations de paiement associées ;

- ne demande pas de données de paiement sensibles liées à des comptes de paiement ;

- 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 (art. 67, 2).

De son côté, concernant les comptes de paiement, le PSPGC :

- communique de manière sécurisée avec les prestataires de services d'information sur les comptes, conformément à l'article 98, 1, d précité ;
- traite les demandes de données transmises grâce aux services d'un PSIC sans aucune discrimination autre que fondée sur des raisons objectives (art. 67, 3).

## III. LES DONNÉES DE COMPTE

**22. Des différentes catégories de données dans la DSP2.** Les données nécessaires à l'activité de paiement sont au nombre de deux. Se présentent d'une part les « données d'accès » (ou d'« authentification »), i. e. les « données de sécurité personnalisées » : « données personnalisées fournies à un utilisateur de services de paiement par le prestataire de services de paiement à des fins d'authentification » (art. 4, 31), l'utilisateur étant invité à prendre « toute mesure raisonnable pour préserver la sécurité de ses données de sécurité person-

nalisées » (art. 69, 2).

Sont d'autre part envisagées, de manière inédite, les « données dangereuses » : « données de paiement sensibles », des données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude », étant précisé de manière tout à fait remarquable que, « 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 » (art. 4, 32).

Inédite est encore la place faite aux données sensibles de paiement dans le dossier d'agrément d'EP, qui doit réserver « une description du processus en place pour enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles et garder la trace de ces accès » (art. 5, g).

**23. Accès aux comptes de paiement, et ensuite ?** Accéder au compte pour initier une opération de paiement, soit ; s'y introduire pour en récupérer des informations, même sans pouvoir mouvoir des fonds, est déjà plus dangereux dès lors que, vite, très vite, les données de paiement primeront le paiement lui-même.

Or il manque cruellement, dans la DSP2, une définition des « données de compte », c'est-à-dire des données qu'il sera intéressant de recueillir, de traiter... voire de monnayer. Seules les données de paiement sensibles font pour l'heure l'objet d'une pale définition (données susceptibles de fraude) et, on l'a d'ores et déjà vu, de deux règles protectrices minimales : le PSIP ne stocke pas de données de paiement sensibles concernant l'utilisateur de paiement (art. 66, 3, e) ; le PSIC ne demande pas de données de paiement sensibles liées à des comptes de paiement (art. 67, 2, e).

Et ensuite ?

**24. La bataille des données.** Il n'est peut-être pas excessif d'avancer que la « bataille des données de paiement » (ou de données de compte de paiement ou des données de transaction ; plus chic, la « bataille des data ») est (re)lancée par la promotion du service d'information sur les comptes. Il n'est pas certain que la DSP2 en

ait pris (toute) la mesure.

Il y a bien, à l'article 94,2, une timide avancée par rapport à la DSP (art. 79), qui double l'exigence de finalité du traitement des données à caractère personnel (lutte contre la fraude), par le recueil du consentement : « Les prestataires de services de paiement n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement explicite de l'utilisateur de services de paiement. »

Il y a surtout, c'est le bon moment, la nécessité impérieuse de lire la DSP2, en parallèle de cet autre grand texte contemporain : le règlement (UE) 2016/679 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 (règlement général sur la protection des données). Cela tombe assez bien : DSP2 et règlement général seront applicables à quelques mois d'intervalle, 13 janvier 2018 pour l'un, 25 mai 2018 pour l'autre.

**25. Le consentement au recueil des données de compte.** Mon compte et mes données sont à moi : nous croyons que la bataille des données ne sera pas (tout à fait) perdue pour le consommateur qu'au prix d'une contractualisation minutieuse avec les PSIP et, surtout, les PSIC, responsables de traitement ; qu'au prix de l'invention d'un nouveau genre de contrat-cadre de services de paiement d'initiation et d'information, qui ne devra plus être que d'adhésion mais bien le résultat d'un consentement au sens du règlement général sur la protection des données : « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (art. 4, 11)<sup>28</sup>.

Consentement que l'utilisateur de services de paiement devrait pou-

voir retirer à tout moment et aussi facilement qu'il l'a donné (art. 7, 3), tout en pouvant faire valoir, auprès de son responsable de traitement PSIP ou PSIC sous certaines conditions, son droit à l'effacement ou à l'oubli (art. 17).

**26. Et tout l'arsenal du règlement général dur la protection des données.** Ce n'est point le lieu de dérouler l'ensemble des mesures qu'offre ou offrirait le règlement afin de sécuriser les nouveaux services d'initiation de paiement et, surtout (mis on peut penser qu'ils iront souvent ensemble, et seront même redoutables ensemble), et d'information sur les comptes.

Sinon pour avancer, au moins, que la protection des données « dès la conception » (*data protection by design*) sera sans doute bien adaptée à notre matière (art. 25). Ou que la nouvelle procédure de l'analyse d'impact se révélerait particulièrement adaptée, sachant que « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel » (art. 35, 1).

Par un communiqué du 1<sup>er</sup> juin 2016, l'ACPR annonçait la création d'un Pôle FinTech Innovation. Et si un pôle commun était créé avec la CNIL ? ■

<sup>28</sup>. Comp. art. 6, 1, a : « Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques [...] ».