En attendant la DSP2

Le marché unique numérique européen parviendra-t-il à allier sécurité des paiements et accès à l'information

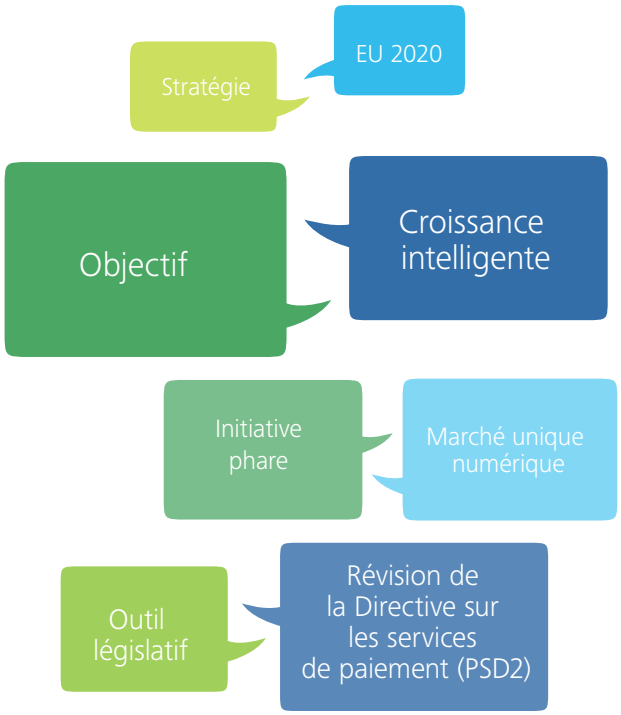
Pascal Martino
Partner
Strategy, Regulatory & Corporate Finance
Deloitte

Charles Delancray
Director
Technology & Enterprise Application
Deloitte

Giulia Bruni Roccia
Analyst
Operations, Excellence & Human Capital
Deloitte

Lorsque Jean-Claude Juncker a été nommé Président de la Commission Européenne (CE), il a élaboré un programme de travail pour la CE sur la période 2014-2019. Ce programme se compose de dix priorités, dont l'une est la mise en place d'un Marché unique du numérique connecté[1], probablement mieux connu du grand public sous le nom de Marché unique numérique[2]. Il s'agit de l'une des trois initiatives phares pour atteindre la croissance intelligente, objectif de la stratégie UE 2020[3].

Figure 1: DSP2 et EU 2020



1 *Commission européenne, 2015. Les commissaires: Jean-Claude Juncker. Disponible à l'adresse suivante: http://ec.europa.eu/commission/2014-2019/president_fr*

2 *Commission européenne, 2015. Agenda numérique pour l'Europe, une initiative Europe 2020: marché unique numérique. Disponible à l'adresse suivante: http://ec.europa.eu/digital-agenda/en/digital-single-market*

3 *Les deux autres objectifs d'UE 2020 sont une "croissance inclusive" et une "croissance durable". Commission européenne, 2012. Europe 2020: initiatives phares. Disponible à l'adresse suivante: http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_fr.htm*

La législation sur le marché des services de paiement, un marché réglementé par la *Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE*, généralement appelée Directive sur les services de paiement (DSP1)[4], est essentielle au développement d'un marché numérique unique dans l'UE.

Cette directive est désormais en cours de révision, le Conseil européen (Conseil), le Parlement européen (PE) et la CE menant des négociations en vue de finaliser la *Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE (DSP2)*[5]. La DSP2 apportera des changements significatifs au marché des services de paiement afin de permettre à l'UE de suivre une évolution technologique aussi rapide qu'inéluctable.

Nous commencerons par une brève synthèse des principales modifications, détaillerons les objectifs qu'elles souhaitent atteindre et présenterons les principaux acteurs, notamment ceux qui seront soumis à la DSP2 et les parties prenantes impliquées dans sa conception. Nous mettrons ensuite l'accent sur deux aspects spécifiques de la directive: la sécurité des paiements et l'accès à l'information, en soulignant leur incompatibilité potentielle. Enfin, nous verrons comment les initiatives de certaines parties prenantes pourraient résoudre cette incompatibilité apparente.

Les institutions européennes sont encore en phase de négociation, ce qui signifie que, pour produire une analyse fiable, il faudra attendre la finalisation de la DSP2 puis sa transposition dans les différents droits nationaux. L'objectif du présent article est donc de soulever des questions, de formuler des réserves et d'envisager ce qui pourrait manquer à la DSP2. En attendant cette finalisation, imaginons que nous appartenons à l'équipe de négociation et confrontons nos points de vue.

Qu'est-ce que la DSP2?

La DSP1 est en place depuis novembre 2007. Depuis cette date, le marché des services de paiement a connu des changements majeurs, qui nécessitent une mise à jour de la législation européenne. Une fois finalisée, la DSP2 modifiera à la fois la portée territoriale des activités de paiement soumises à réglementation, en s'appliquant aux transactions hors devises européennes si le prestataire de services de paiement (PSP) des deux extrémités (payeur ou payé) se trouve dans l'UE, ainsi qu'aux transactions "bancales", où le PSP d'une seule extrémité est situé dans l'UE, quelle que soit la devise. Le périmètre des devises est lui aussi modifié, les exigences de transparence et d'information de la DSP2 s'appliquant indépendamment de la devise. Les dispositions relatives aux droits et obligations des services de paiement s'appliqueront aux transactions en euros ou dans la devise des États membres n'appartenant pas à l'union monétaire[6].

4 *Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32007L0064*

5 *Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

6 *Titre 1, Article 2. Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

Les institutions européennes se sont lancées dans une mission complexe, car leur objectif est de faire coïncider la législation européenne et les législations nationales avec les acteurs et activités du secteur des services de paiement, dont le nombre et la diversité sont en constante augmentation

Les exclusions évoluent également, par exemple en matière d'agents commerciaux, de réseau limité, de télécommunications et de DAB. Les DAB seront notamment retirés de la liste des exemptions afin d'enrayer le développement de DAB indépendants qui facturent des commissions importantes sur les retraits d'argent[7]. L'ensemble des acteurs concernés devra se conformer aux modifications spécifiques des dispositions en matière de transparence, de sécurité, de responsabilité et de protection des consommateurs – frais, commissions, remboursements et gestion des plaintes y compris.

À terme, les objectifs de la DSP2 sont les suivants:

- Poursuivre l'intégration des services de paiement au-delà des frontières nationales pour renforcer l'espace unique de paiements en euros (SEPA)
- À cette fin, vérifier que le cadre législatif est correctement appliqué par les autorités de régulation des États membres, parvenir à la normalisation et l'interopérabilité des services de paiement, leur permettre d'être plus sûrs et plus pratiques numériques et simples d'utilisation
- Inclure un plus grand nombre d'acteurs dans le périmètre réglementaire favorisant par ce biais une course à l'innovation et renforçant la concurrence ainsi que le nombre d'options à disposition des consommateurs
- Améliorer la protection des consommateurs

Bien entendu, la tâche ne sera pas aisée. Les institutions européennes se sont lancées dans une mission complexe, car leur objectif est de faire coïncider la législation européenne et les législations nationales avec les acteurs et activités du secteur des services de paiement, dont le nombre et la diversité sont en constante augmentation. À terme, les institutions européennes s'alignent sur nous. Nous sommes les consommateurs, nous sommes ceux qui, depuis un certain temps déjà, ont clairement cessé de dépendre uniquement des banques traditionnelles. Ce sont nos opérations qui transitent désormais par différents moyens plus tout à fait traditionnels. Mais savons-nous qui sont ces nouveaux acteurs? Connaissons-nous la totalité des services disponibles sur le marché?

7 *Exposé des motifs, Point 5. Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

Figure 2: La DSP2 formule les définitions suivantes

	Definition
Prestataire de services de paiement (PSP)	Un organisme fournissant: • "Des services permettant de verser des espèces" ou d'en retirer d'"un compte de paiement, ainsi que toutes les opérations qu'exige la gestion du compte" • "L'exécution d'opérations de paiement, y compris les transferts de fonds sur un compte de paiement auprès du prestataire de services de paiement de l'utilisateur ou auprès d'un autre prestataire de services de paiement" ainsi que "l'exécution d'opérations de paiement dans le cadre desquelles les fonds sont couverts par une ligne de crédit accordée à un utilisateur de services de paiement". Les deux incluent "les débits directs, y compris les débits directs ponctuels, les opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire, les ordres de virement, y compris les ordres permanents" • "L'émission d'instruments de paiement et/ou l'acquisition d'opérations de paiement" • "La transmission de fonds" • "Des services basés sur l'accès à des comptes de paiement fournis par un prestataire de services de paiement n'étant pas le fournisseur de services de tenue de compte, sous forme du paiement de services d'initiation du paiement et de services d'informations sur le compte"
Prestataire de services de tenue de compte (PSTC)	"Prestataire de services de paiement fournissant et assurant la tenue des comptes de paiement d'un payeur."
Prestataire de Services de Paiement Tiers (PSPT)	"Prestataire de services de paiement n'étant pas le prestataire de services de tenue de compte" et "qui fournit des services d'initiation de paiement et d'information sur les comptes."
Utilisateur de Services de Paiement (USP)	"Personne physique ou morale utilisant un service de paiement en qualité de payeur ou de payé."
Services d'initiation de paiement	"Services de paiement permettant l'accès à un compte de paiement fourni par un prestataire de services de paiement tiers, lorsque le payeur peut être activement impliqué dans l'initiation du paiement ou le logiciel du prestataire de services de paiement tiers, ou lorsque les instruments de paiement peuvent être utilisés par le payeur ou le payé pour transmettre les coordonnées du payeur au prestataire de services de tenue de compte."
Services d'information sur les comptes	"Services de paiement permettant de fournir des informations consolidées et simples d'utilisation à un utilisateur de services de paiement, informations relatives à un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement auprès d'un ou plusieurs prestataires de services de tenue de compte."

Comme pour toutes les directives européennes, la CE, le PE et le Conseil débattent des propositions et les négocient. Ces trois institutions en sont actuellement à la phase de dialogue, et, selon le Conseil européen des paiements, l'approbation du PE est attendue en septembre 2015, avec publication au Journal officiel de l'UE à l'hiver. Les États membres auront ensuite deux ans pour transposer la directive en droit national[8].

Outre ces trois institutions, et compte tenu du sujet de la DSP2, d'autres parties prenantes européennes sont appelées à fournir des recommandations et suggestions d'amendements: c'est le cas de la Banque centrale européenne (BCE) et de l'Autorité bancaire européenne (ABE). Cette dernière est plus spécifiquement chargée d'élaborer les lignes directrices en matière de sécurité qui seront appliquées par les régulateurs nationaux et les acteurs concernés, conformément à la DSP2.[9] La BCE et l'ABE sont particulièrement compétentes sur ce sujet, car elles co-président le Forum européen sur la sécurité des moyens de paiement de détail (Forum SecuRe Pay), une plateforme qui permet à l'ABE et aux États membres du Système européen des banques centrales de développer des connaissances communes sur la sécurité des paiements[10].

Dispositions relatives à la sécurité des paiements et à l'accès à l'information

Afin de fournir aux consommateurs des services pratiques et simples à utiliser au sein d'un marché foisonnant et complexe, l'objectif de la DSP2 est d'assurer un échange d'informations efficace et réglementé entre les acteurs concernés. Parallèlement, les consommateurs doivent être rassurés sur le fait que ces flux d'informations (et le marché des services de paiement de manière plus générale) sont sûrs.
"Ces dernières années, les risques liés à la sécurité des paiements électroniques ont augmenté en raison de la complexité technique croissante de ces paiements, de la progression constante du volume de paiements électroniques à l'échelle mondiale et de l'émergence de nouveaux types de services de paiement. L'existence de services de paiement sûrs et sécurisés étant une condition essentielle au bon fonctionnement du marché des services de paiement, les utilisateurs de services de paiement doivent être correctement protégés contre ces risques[11]."

La DSP2 fusionne souvent les dispositions relatives à la sécurité des paiements et à l'accès à l'information au sens du même article, comme pour signifier qu'ils sont interdépendants, l'un étant l'essence de l'autre. Mais est-ce si facile de supposer que ces deux éléments peuvent appartenir à la même législation? Sont-ils réellement compatibles? Examinons ce que dit la DSP2 et nous verrons peut-être pourquoi ces deux aspects pourraient entrer en conflit.

Afin d'assurer la sécurité des paiements, la DSP2 introduit les concepts d'"authentification" et d'"authentification forte du client". Le concept d'"authentification" désigne *une procédure qui permet au prestataire de services de paiement de vérifier l'identité de l'utilisateur d'un instrument de paiement spécifique, y compris en utilisant des dispositifs de sécurité personnalisés ou en vérifiant les documents d'identité personnalisés."*[12] Le concept d'"authentification forte du client" correspond, lui, à *"une procédure de validation de l'identification d'une personne morale ou physique par le recours à un minimum de deux éléments relevant du domaine de la connaissance, de la possession ou de l'inhérence, étant indépendants, dans le sens où la compromission de l'un ne compromet pas la fiabilité des autres, conçues pour protéger la confidentialité des données d'authentification[13]."*

8 *Boudewijn, G., 2015. DSP2: Almost Final – A State of Play. Conseil européen des paiements, 18 juin 2015 Disponible à l'adresse suivante: http://www.europeanpaymentscouncil.eu/index.cfm/blog/DSP2-almost-final-a-state-of-play/*

9 *Considérant 80, Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

10 *Banque centrale européenne, 2014. Mandate of the European Forum on the Security of Retail Payments. Disponible à l'adresse suivante: https://www.ecb.europa.eu/pub/pdf/other/mandateeuropeanforumsecurityretailpayments201410.en.pdf p.1 et p.2*

11 *Considérant 6, Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

12 *Article 4, Clause 21, Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

13 *Article 4, Clause 22, Proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52013PC0547*

Afin de fournir aux consommateurs des services pratiques et simples à utiliser au sein d'un marché foisonnant et complexe, l'objectif de la DSP2 est d'assurer un échange d'informations efficace et réglementé entre les acteurs concernés

L'Article 87 stipule que les PSP doivent appliquer une authentification forte du client dès qu'un payeur ou un PSPT agissant pour le compte du payeur initie une opération de paiement électronique. Dans ce dernier cas, le PSTC doit alors autoriser le PSPT "*à se fier aux méthodes d'authentification du premier lorsqu'il agit pour le compte de l'USP.*" *Par ailleurs, le PSPT "doit s'authentifier auprès du prestataire de services de tenue de compte du détenteur du compte."*

L'Article 62 indique de son côté que le PSP qui émet une opération doit "*s'assurer que les dispositifs de sécurité personnalisés de l'instrument de paiement ne sont pas accessibles à d'autres parties que l'utilisateur du service de paiement autorisé à utiliser cet instrument de paiement.*" Il précise que le PSP supportera *"le risque lié à l'envoi de l'instrument de paiement au payeur ou l'envoi de ses dispositifs de sécurité personnalisés."*

L'Article 58 doit également être étudié, car il porte sur l'accès aux informations relatives au compte de paiement et leur utilisation par le PSPT:

"Lorsqu'un prestataire de services de paiement tiers a été autorisé par l'utilisateur de services de paiement à fournir des services de paiement, il a les obligations suivantes:

1. Garantir que les dispositifs de sécurité personnalisés de l'utilisateur de services de paiement ne sont pas accessibles aux autres parties
2. S'identifier de manière non équivoque auprès du/des prestataire(s) de services de tenue de compte du détenteur du compte
3. Ne pas stocker de données de paiement ou de données de sécurité personnalisées sensibles sur l'utilisateur de services de paiement

Dispositions relatives à la sécurité des paiements et à l'accès à l'information: une coexistence délicate

Lorsque l'on se penche sur l'approche de la DSP2 en matière de sécurité des paiements et d'accès à l'information, trois grands problèmes apparaissent, trois sources de doute qui pourraient se révéler particulièrement importantes pour le régulateur, le consommateur ou le PSP concerné, le cas échéant.

1

À la lecture de la DSP2, il est relativement clair que le flux d'informations est essentiel au traitement des paiements. Et compte tenu de la diversité des acteurs actifs dans le même domaine, il faut que l'accès à l'information se déroule de manière sécurisée, autorisée et authentifiée. Mais précisément du fait de cette diversité, et parce que les protagonistes traditionnels, "à l'ancienne" et "en retard sur le plan technologique" (les banques) doivent collaborer avec des acteurs plus innovants (notamment les nouveaux PSPT émergents), les plateformes informatiques utilisées pour échanger des informations peuvent varier du tout au tout. Dans certains cas, ces plateformes doivent être construites de A à Z, tandis que dans d'autres, elles sont d'ores et déjà très sophistiquées. Cela se traduit par une faille tout à fait significative dans les procédures. Une étude menée par Finextra et FIS souligne précisément cette lacune:
« *L'un des risques liés au fait d'ouvrir l'accès aux données et fonctionnalités du système central d'une banque est le suivant: si ces systèmes centraux sont anciens et peu flexibles, leurs limites deviennent visibles au-delà du cercle fermé des équipes opérationnelles de la banque. Pire encore, il existe un risque qu'il soit purement et simplement impossible d'accorder un accès sécurisé et fiable en raison de ces lacunes*[14]. »

14 *Finextra, 2015. DSP2 and XS2A – Regulation or Opportunity? Report on a Survey by Finextra and FIS. Disponible à l'adresse suivante: http://www.fisglobal.com/ucmprdpub/groups/public_searchable/documents/webasset/c038915.pdf p.23*

- Pour qui est-ce pertinent? Pour le régulateur, qui doit s'assurer que l'ensemble des acteurs possède des plateformes normalisées et interopérables, mais aussi pour les PSP (même les plus en pointe sur le plan technologique), qui pourraient pâtir du fait de devoir "ralentir" et s'adapter au rythme des acteurs les moins innovants

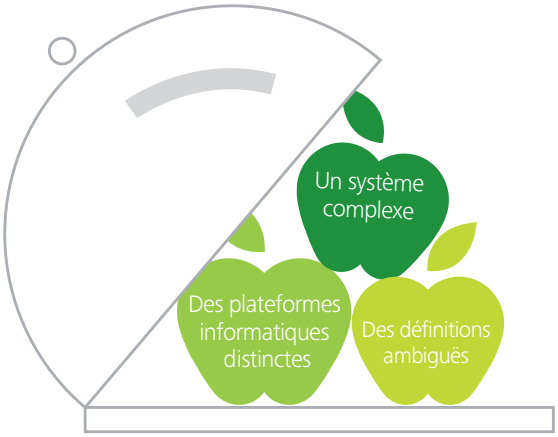
2 Nous comprenons maintenant pourquoi autant d'autorisations sont nécessaires pour accéder à l'information et traiter les paiements, toutes pertinentes pour assurer la sécurité. Mais les différentes parties prenantes (consommateurs, régulateurs et PSP) risquent de se perdre en chemin ; des erreurs peuvent être faites à toutes les étapes et potentiellement ne pas être repérées.

- Pour qui est-ce pertinent? Pour les consommateurs qui, en cas d'incident, pourraient être incapables de remarquer la malversation ni d'utiliser les possibilités de gestion des plaintes offertes par la DSP2 (Articles 88-91). Les PSP sont également concernés, car ils doivent s'assurer que leurs procédures sont parfaitement réglées et conformes aux procédures des autres PSP. Mais aussi les régulateurs, qui devront superviser cette conformité et cette interopérabilité

3 Pourtant, même avec l'octroi de l'ensemble de ces autorisations en matière d'accès à l'information, les nouvelles exigences d'authentification et d'authentification forte du client et les avertissements sur la responsabilité en cas de partage de la mauvaise information avec un acteur non autorisé (Articles 79-83), certains éléments restent flous. Qui définit ce qu'est le "droit" à utiliser un instrument de paiement? (Article 62) Quel est le sens du verbe "stocker" des données de paiement sensibles? (Article 58) À quelle étape du processus de paiement le PSPT doit-il supprimer ces données de paiement sensibles afin de garantir au client que les données ne sont pas "stockées" et détournées? La définition de l'"authentification" indique qu'il s'agit de la procédure qui permet au PSPT d'identifier l'utilisateur du paiement et d'"utiliser" ses coordonnées (Article 4). Quelles sont les activités prévues par ce verbe "utiliser"? Cela inclut-il uniquement le transfert des coordonnées, le simple fait d'entrer les coordonnées pour autoriser le paiement et le traiter? Si c'est le cas, ce n'est pas suffisamment clair, et cela pourrait sans doute également inclure l'activité de "stockage", interdite par l'Article 58.

- Pour qui est-ce pertinent? Pour le régulateur, qui devra superviser la transposition de la directive en droit national et devra être absolument sûr de la signification de chacun des termes, sans laisser de place au doute et aux malentendus

Figure 3: Dispositions relatives à la sécurité des paiements et à l'accès à l'information: une coexistence délicate



Assurer la coexistence entre sécurité des paiements et accès à l'information

Le succès de l'élaboration de toute directive européenne repose sur l'échange d'opinions, de recommandations, d'amendements, chaque partie prenante abordant la question d'une manière différente. Il est particulièrement intéressant d'étudier les positions de la BCE et de l'ABE, car elles se sont largement concentrées sur l'aspect "sécurité".

À la lecture de leurs avis et recommandations, l'on constate que nombreux sont les moyens d'assurer la compatibilité entre sécurité des paiements et accès à l'information.

En janvier 2013, la BCE a formulé des recommandations concernant la sécurité des paiements sur Internet. Puis, en février 2014, elle a formulé un avis sur le projet de législation, en mettant une fois encore l'accent sur les questions de sécurité (pas encore) abordées par la DSP2 et proposé une série d'amendements. La logique de ces documents est la même que celle de la directive: le flux d'informations est essentiel, mais il doit être traité en respectant des étapes spécifiques d'autorisation et d'authentification. Pourtant, les recommandations et l'avis de la BCE passent à côté des lacunes de la DSP2 sur le marché des services de paiement. Les législations encadrant la sécurité des paiements et l'accès à l'information sont une bonne nouvelle. Mais si le consommateur ne sait pas où se trouvent les menaces, comment les contrer, quels types d'informations sur elle/lui sont autorisés à transiter dans le système, il reste un consommateur non protégé et la législation n'est qu'un terrain stérile. Selon la BCE, les PSP pourraient fournir un dispositif de communication sécurisé par le biais duquel ils expliquent aux consommateurs comment signaler des activités potentiellement frauduleuses, comment les PSP réagiront aux plaintes et demandes et comment ils préviendront les consommateurs si ce sont eux qui ont des soupçons[17]. En outre, les PSP pourraient former et sensibiliser les consommateurs pour améliorer leurs connaissances en matière de protection des données, de gestion des données sur différents appareils (ordinateurs, téléphones, etc.) et d'utilisation *"du véritable site de paiement sur Internet du PSP"*[18].

1. Le problème de l'absence de plateformes informatiques normalisées n'est pas soulevé, les recommandations de la BCE préconisant les meilleures pratiques des PSP *"avec un outil unique d'authentification forte du client pour l'ensemble des services de paiement par Internet", car "cela pourrait permettre de faire mieux accepter la solution aux consommateurs et de faciliter une utilisation correcte*[15]», l'authentification forte du client devant être intégrée à *"une interface européenne normalisée d'accès aux comptes de paiement"*[16]. Certes, cela exige plus de travail et plus de législation, mais la mise en place d'un outil unique d'authentification forte du client serait gage de normalisation, d'interopérabilité et d'un moindre risque de doute et/ou d'erreur. La bonne nouvelle, c'est que l'UE possède également les moyens d'instituer et de mettre en place un outil unique, par le biais de l'ABE ou même du Forum SecuRe Pay.

2. La proposition de la BCE sur la sensibilisation des clients et les programmes de formation est très intéressante. Ces programmes devraient résoudre le second problème, celui du manque de compréhension des procédures d'authentification et d'autorisation

3. Enfin, la BCE est également plus précise dans ses définitions, comme le montre son avis sur l'Article 58. L'interdiction de "*stocker les données de paiement sensibles relatives à l'utilisateur des services de paiement"* est précisée:
"obtenues lors de l'accès au compte de paiement des utilisateurs de services de paiement, exception faite des informations destinées à identifier un paiement initié par un prestataire de services de paiement tiers, notamment la référence, l'IBAN du payeur et du payé, le montant de l'opération, les autres références et les informations du système de règlement, sans utiliser ces données pour un

15 *Banque centrale européenne, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Disponible à l'adresse suivante: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf p.10*

16 *Point 2.7, Opinion de la Banque centrale européenne du 5 février 2014 au sujet de la proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf*

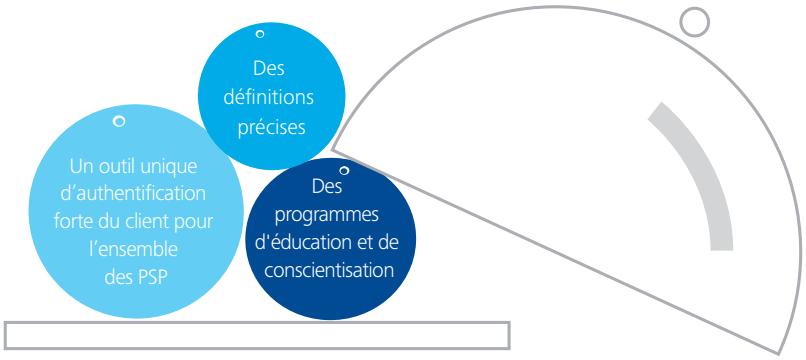
17 *Banque centrale européenne, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Disponible à l'adresse suivante: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf p.13*

18 *Banque centrale européenne, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Disponible à l'adresse suivante: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf p.13*

autre but que celui explicitement formulé par l'utilisateur du service de paiement."[19]

Les recommandations de la BCE ont été utilisées par l'ABE pour élaborer ses Orientations finales sur la sécurité des paiements sur Internet en décembre 2014, en vigueur en août 2015. De fait, l'ABE est une partie prenante particulièrement importante: sur la base de la DSP2, c'est elle qui a la responsabilité de définir les lignes directrices en matière de sécurité et de définir les normes techniques que les États membres devront appliquer dans le sillage des modifications du périmètre et des exigences de la directive.[20] Ces Orientations constituent un travail préparatoire et ne font que définir "des exigences minimales en ce qui concerne la sécurité des paiements sur Internet.[21]» Malheureusement, même en phase préparatoire, des problèmes de mise en place surviennent, car trois des 28 pays ont d'ores et déjà fait part de leur incapacité (ou de leur manque de volonté?) à respecter ces Orientations[22].

Figure 4: Assurer la coexistence de la sécurité des paiements et de l'accès à l'information



Conclusion

Au final, nous constatons que les parties prenantes européennes sont conscientes de l'importance de la sécurité des paiements et de l'accès à l'information (cf la responsabilité dévolue à l'ABE par la DSP2) et nous constatons également que certaines parties prenantes reconnaissent les difficultés liées à la coexistence et la compatibilité entre sécurité des paiements et accès à l'information. Et nous notons, enfin, des propositions de solutions concrètes de la part de ces parties prenantes (Avis de la BCE et propositions ABE/BCE sur les meilleures pratiques). Mais ces solutions seront-elles incluses dans la version finale de la directive ? Comment seront-elles transposées dans les différents droits nationaux, compte tenu de la réticence déjà exprimée par certains États membres à respecter les Orientations ?

Il nous faudra attendre la fin de l'année pour voir comment les choses se déroulent au niveau européen, puis examiner la situation au niveau des États membres dans deux ans. Mais une chose est sûre : avec la DSP2, l'UE tient une véritable opportunité de créer un Marché unique numérique, pour peu que les lacunes soient identifiées et comblées de manière concrète.

19 *Amendement 24, Opinion de la Banque centrale européenne du 5 février 2014 au sujet de la proposition de Directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2013/36/CE ainsi que 2009/110/CE et abrogeant la directive 2007/64/CE. Disponible à l'adresse suivante: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf*

20 *Directive, Considérant 80 ; Article 86, Article 87*

21 *http://www.eba.europa.eu/documents/10180/1004450/EBA_2015_FR+Guidelines+on+Internet+Payments.pdf/5123b322-e410-4574-bab5-dc20c7e5096a*

22 *C'est-à-dire l'Estonie, la Slovaquie et le Royaume-Uni.*
Autorité bancaire européenne, 2015. Compliance Table – Guidelines. Disponible à l'adresse suivante:
https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf