L'ABE va devoir préciser dans les deux prochaines années les conditions d'application de la seconde DSP

GEOFFROY GOFFINET
Consumer Protection Unit
European Banking Authority

L'Autorité bancaire européenne (ABE) doit développer dans les deux ans à venir des normes techniques réglementaires (Regulatory Technical Standards) et des orientations (Guidelines) pour préciser les conditions d'application de la Directive. L'objectif est clair : assurer le développement de moyens de paiement innovants et sécurisés au bénéfice des 500 millions de consommateurs européens et de son industrie.

Par l'adoption de normes techniques réglementaires contraignantes et d'orientation, l'ABE garantit un niveau de réglementation et de surveillance prudentielle harmonisé et cohérent dans l'ensemble du secteur bancaire européen.

L'ABE a par ailleurs un rôle prépondérant dans la protection des consommateurs européens, qui se traduit notamment par une promotion de la transparence, de la simplicité et de l'équité sur le marché des produits ou des services financiers.

L'ABE est enfin chargée de surveiller les innovations financières dans l'Union européenne en vue de parvenir à une approche coordonnée du traitement applicable aux activités financières nouvelles ou innovantes.

Dans le domaine des paiements, l'ABE est intervenue en décembre 2013 pour mettre en garde le public européen sur les monnaies virtuelles, en soulignant que ces instruments n'étaient pas soumis à une régulation particulière et qu'ils exposaient, en conséquence, leurs utilisateurs à des risques importants. Elle a ensuite publié un avis aux institutions de l'Union européenne proposant une analyse plus approfondie des bénéfices et risques encourus par les utilisateurs de ces monnaies et fixant les bases pour un encadrement réglementaire, tout en dissuadant les établissements de crédit, les établissements de paiement ainsi que les établissements de monnaie électronique d'acquérir, de détenir ou de vendre des monnaies virtuelles.

Face à l'augmentation de la fraude sur les paiements sur internet, l'ABE a également adopté en décembre 2014 des orientations sur la sécurité de ces paiements, fixant les requis minimaux sécuritaires à mettre en œuvre par les prestataires de services de paiement européens à compter du 1er août 2015 et jusqu'à la mise en œuvre de la seconde Directive des services de paiement (Directive (EU) 2015/2366, DSP2).

Ces orientations, reprenant les recommandations du forum européen European Forum on the Security of Retail Payments (Secure Pay), visent notamment à généraliser la mise en œuvre de l'authentification forte du client lors des paiements sur internet et permettent ainsi de fournir une base réglementaire harmonisée pour des conditions de concurrence équitables entre les prestataires de services de paiement au niveau européen. Un seul bémol : contrairement aux normes techniques réglementaires directement contraignantes, les orientations doivent être intégrées par les autorités compétentes concernées de l'Union européenne dans leurs pratiques de surveillance selon les modalités qu'elles estiment appropriées. Dans ce contexte, les autorités compétentes peuvent décider de ne pas se conformer à ces orientations. Elles doivent alors communiquer à l'ABE les motifs de leur non-respect. Dans le cadre des orientations relatives à la sécurité des paiements sur internet, vingt-trois

autorités compétentes sur vingt-huit de l'UE se sont déclarées conformes, trois partiellement conformes et deux non conformes[1].

Mais le rôle de l'EBA dans le domaine des paiements a particulièrement pris de l'envergure avec l'adoption de la DSP2. Ainsi, depuis son entrée en vigueur le 13 janvier 2016, le compte à rebours a débuté : l'ABE doit développer dans les deux ans à venir pas moins de cinq normes techniques réglementaires (*Regulatory Technical Standards* - RTS) et cinq orientations (*Guidelines* – GL) pour préciser les conditions d'application de la Directive en matière d'harmonisation des pratiques d'autorisation des établissements de paiement, de supervision des prestataires de services de paiement paneuropéens et de protection des consommateurs, de transparence sur les acteurs agréés et exemptés impliquant la création d'un registre européen, et enfin d'harmonisation des exigences de sécurité auxquelles devront répondre les moyens de paiement électroniques de demain (cf. illustration calendrier des mandats de l'ABE dans le cadre de la DSP2).

C'est un programme de travail ambitieux et l'heure est plus que jamais à la consultation et au dialogue avec les acteurs du marché. L'objectif est clair : assurer le développement de moyens de paiement innovants et sécurisés au bénéfice des 500 millions de consommateurs européens et de son industrie.

LES MANDATS CONFIÉS À L'EBA POUR PRÉCISER LES CONDITIONS D'APPLICATION DE LA DSP2

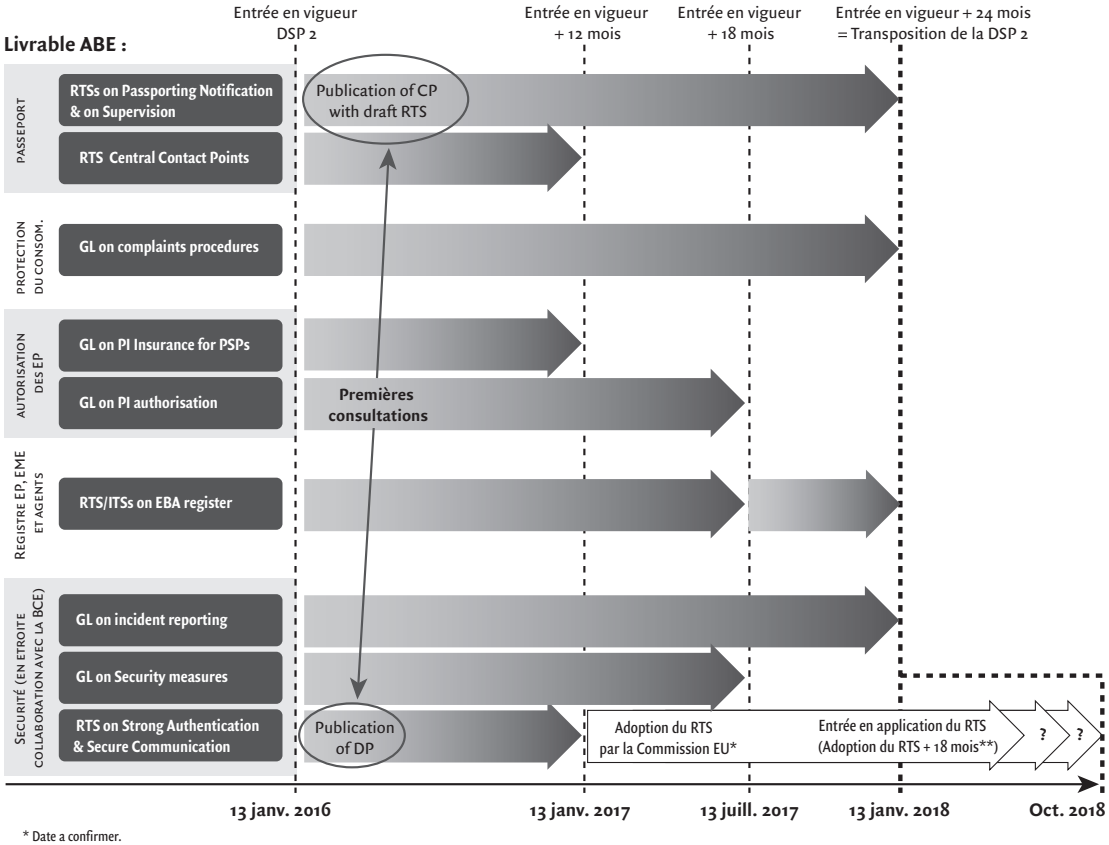
1. Harmoniser les pratiques mises en œuvre par les autorités compétentes en vue d'autoriser les établissements de paiement

À l'instar du régime établi par la Directive sur les services de paiement (Directive (EU) 2007/64/EC), toute institution souhaitant fournir des services de paiement doit, avant de commencer ses activités, obtenir un agrément en tant qu'établissement de paiement auprès des autorités compétentes de l'État membre où son siège statutaire et son administration centrale sont situés et dans lequel l'institution exerce au moins une partie de ses activités.

Pour assurer une égalité de traitement des demandes d'agrément dans l'ensemble de l'Union Européenne, l'article 5.5 de la DSP2 prévoit que l'EBA émette des orientations concernant les informations à fournir aux autorités compétentes dans la demande d'agrément des établissements de paiement. C'est un mandat particulièrement important pour harmoniser les conditions

1. Le tableau de conformité des autorités compétentes au regard de ces orientations est disponible sur le site de l'ABE : https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments/-/regulatory-activity/press-release.

Calendrier des mandats de l'ABE dans le cadre de la DSP2



* Date a confirmer.
** I.e. pas avant sept. 2018.

Source : European Banking Authority.

de délivrance des agréments d'établissement de paiement en Europe. À noter que la DSP2 prévoit qu'en tenant compte, le cas échéant, de l'expérience acquise dans l'application de ces orientations, l'ABE puisse convertir à terme ces orientations en normes techniques réglementaires.

Autre élément crucial pour l'harmonisation des conditions d'exercice des prestataires de services de paiement : l'ABE devra émettre des orientations définissant les critères permettant aux autorités compétentes de déterminer le montant minimal de l'assurance de responsabilité civile professionnelle ou autre garantie comparable que devront détenir les prestataires de services d'information sur les comptes, également dénommés « agrégateurs », et d'initiation de paiement avant d'être autorisés à offrir leurs services. Pour ce faire, l'ABE devra tenir compte du profil de risque de l'établissement, de la nature des autres activités exercées par le prestataire, de la taille de ses activités ainsi que des caractéristiques spécifiques des garanties comparables et les critères de leur mise en œuvre.

Cette assurance ou autre garantie comparable devra permettre aux fournisseurs de ces servies de couvrir, le cas échéant, les risques liés à l'engagement de leur responsabilité vis-à-vis des « banques » (plus précisément des prestataires de services de paiement gestionnaire du compte) ou de l'utilisateur de services de paiement :
– en cas d'un accès non autorisé ou frauduleux aux données des comptes de paiement ou d'une utilisation non autorisée ou frauduleuse de ces données pour les services d'information sur les comptes ;
– en cas de non-exécution, de mauvaise exécution, d'exécution tardive d'une opération de paiement ou d'exécution d'une opération de paiement non autorisée.

Point important à souligner : dans le cas des services d'initiation de paiement, les « banques » seront en charge d'indemniser le payeur en cas d'opération non autorisée, à charge pour elles de se retourner contre le prestataire d'initiation de paiement si ce dernier est fautif, et engager le cas échéant son assurance de responsabilité civile professionnelle ou autre garantie.

Les enjeux des mandats liés à l'autorisation

Harmoniser les pratiques d'autorisation au niveau européen pour assurer des conditions de concurrence équitables entre les prestataires de services de paiement et mettre en place un régime minimum d'assurance de responsabilité civile professionnelle ou autre garantie comparable pour la fourniture de services d'information sur les comptes et d'initiation de paiement.

2. Améliorer et harmoniser les conditions pour permettre aux prestataires de services de paiement d'offrir leurs services au niveau paneuropéen

À l'instar du régime établi par la DSP, 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 via le régime du passeport européen doit y être préalablement autorisé.

Pour ce faire, il doit communiquer un certain nombre d'informations aux autorités compétentes de son État membre d'origine. Ces dernières ainsi que les autorités compétentes de l'État membre d'accueil doivent ensuite coopérer pour autoriser l'établissement de paiement à fournir ses services de paiement en transfrontière, dans le cadre d'un délai précis défini par la DSP2.

Ainsi, dans un délai d'un mois suivant la réception de l'ensemble de ces informations, les autorités compétentes de l'État membre d'origine doivent les analyser et les envoyer aux autorités compétentes de l'État membre d'accueil. Ces dernières ont également un mois pour les évaluer et communiquer le cas échéant aux autorités de l'État membre d'origine tout motif raisonnable de préoccupation en rapport avec la fourniture de services de paiement envisagée par l'établissement de paiement concerné, notamment en ce qui concerne le blanchiment de capitaux ou le financement du terrorisme au sens de la Directive (UE) 2015/849.

Lorsque les autorités compétentes de l'État membre d'origine ne sont pas d'accord avec l'évaluation des autorités compétentes de l'État membre d'accueil, elles communiquent à ces dernières les raisons de leur décision.

En tout état de cause, dans un délai de trois mois suivant la réception des informations de la part des établissements de paiement, les autorités compétentes de l'État membre d'origine communiquent leur décision aux autorités compétentes de l'État membre d'accueil et à l'établissement de paiement.

Pour s'assurer que la coopération entre autorités compétentes fonctionne efficacement, l'ABE s'est vu confier le développement des mandats suivants :
– selon l'article 28(5) de la PSD2, l'ABE est en charge de développer des normes techniques précisant les modalités d'échanges d'informations entre pays d'accueil et pays d'origine lorsqu'un établissement de paiement ou un établissement de monnaie électronique souhaite offrir ses services à l'étranger (notification). L'ABE a déjà lancé une consultation publique[2] sur le projet de normes techniques qui s'est clôturée le 11 mars 2016. L'ABE a reçu sept réponses, qui ont toutes soutenu les objectifs de ces standards. Certaines réponses ont néanmoins soulevé des préoccupations qui ont conduit l'ABE à préciser ou revoir certaines normes techniques. Ces dernières seront finalisées courant 2016 ;
– ces normes seront complétées à terme par d'autres standards techniques relatifs aux échanges d'informations entre autorités pour la supervision des entités agissant en transfrontière, conformément à l'article 29(6) de la PSD2 ;
– conformément à l'article 29(5) de la PSD2, l'EBA devra définir dans le cadre de normes techniques réglementaires les critères permettant de déterminer les circonstances selon lesquelles les États membres d'accueil peuvent exiger des établissements de paiement étrangers exerçant – en vertu du droit d'établissement qu'ils désignent – un point de contact central sur leur territoire afin de faciliter la surveillance des réseaux d'agents. L'EBA devra par ailleurs définir les fonctions de ce point de contact, en particulier pour assurer une bonne communication et une bonne information concernant la conformité de

2. Disponible en ligne sur le site de l'ABE: https://www.eba.europa.eu/.

l'établissement de paiement avec les dispositions prises par l'État membre d'accueil en application des titres III et IV de la PSD2, *i.e.* principalement les mesures relatives à la protection du consommateur. Il est à noter que la quatrième Directive relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (Directive (EU) 2015/849) contient également une option permettant aux États membres d'accueil d'exiger la mise en place d'un point de contact central sur leur territoire aux fins d'assurer la conformité avec les règles relatives au blanchiment d'argent et de financement du terrorisme ;

– conformément à l'article 27 de la DSP2, l'ABE pourra enfin, sur saisine d'une autorité compétente ou de sa propre initiative, prêter assistance aux autorités compétentes pour trouver un accord en cas de différends survenant dans le cadre de la coopération transfrontalière, conformément à ce qui est prévu par le règlement instituant l'ABE (Règlement (UE) No 1093/2010). Ceci signifie concrètement qu'aucun différend entre autorités compétentes ne pourra rester sans réponse.

Les enjeux des mandats liés au passeport européen

Renforcer la coopération entre les autorités compétentes, tant sur les informations échangées que sur la cohérence de l'application et de l'interprétation de la PSD2 lorsqu'un établissement de paiement agréé fournit des services de paiement dans un contexte transfrontière au niveau européen (« passeport »).

3. Préciser les conditions selon lesquelles les consommateurs, y compris les associations de consommateurs, peuvent soumettre des réclamations aux autorités compétentes en cas de violation de la PSD2 par des prestataires de services de paiement

Pour assurer la mise en œuvre de la DSP2, l'article 100(1) de la Directive prévoit que les États membres désignent des autorités compétentes en charge de garantir et de contrôler le respect effectif de cette dernière.

Par ailleurs, l'article 99(1) de la DSP2 requiert la mise en place de procédures permettant aux utilisateurs de services de paiement et aux autres parties intéressées, y compris les associations de consommateurs, de soumettre des réclamations aux autorités compétentes en cas de violation alléguée de la Directive par des prestataires de services de paiement.

Pour assurer des conditions harmonisées pour la soumission de ces réclamations, l'article 100(6) DSP2 confie le soin à l'ABE d'émettre des orientations à l'intention des autorités compétentes au regard des procédures de réclamation permettant aux utilisateurs de services de paiement et aux autres parties intéressées de signaler le cas échéant le non-respect de la présente Directive par des prestataires de services de paiement.

Point à souligner : ce mandat ne couvre donc pas les procédures à mettre en place par les prestataires de services de paiement pour le règlement des réclamations des utilisateurs de services de paiement. À ce titre, l'ABE a déjà émis le 13 juin 2014, conjointement avec l'Autorité Européenne des Marchés Financiers (ESMA), des orientations relatives au traitement des réclamations dans le secteur des valeurs mobilières et le secteur bancaire[3]. Pour autant, l'ABE étudie actuellement l'opportunité de réviser ces orientations à la lumière des nouvelles dispositions de la DSP2, notamment en ce qui concerne l'application de ces orientations aux nouveaux prestataires de services d'initiation de paiement et d'information sur les comptes. Si décidée, cette révision sera menée en parallèle du mandat confié explicitement par l'article 100(6) de la DSP2.

4. Accroître la transparence du fonctionnement des établissements de paiement agréés pour garantir un niveau élevé de protection des consommateurs dans l'ensemble de l'Union

Pour accroître la transparence du fonctionnement des établissements de paiement agréés ou enregistrés auprès des autorités compétentes de l'État membre d'origine, y compris leurs agents, et garantir ainsi un niveau élevé de protection des consommateurs dans l'ensemble de l'Union, la DSP2 prévoit que l'ensemble des autorités compétentes mettent en place un registre public dans lequel sont inscrits les établissements de paiement agréés et leurs agents ainsi que les personnes physiques et morales bénéficiant d'une exemption d'autorisation.

Pour s'assurer que le public a un accès aisé à la liste des entités fournissant des services de paiement, l'article 14 de la DSP2 requiert que l'ABE, à l'instar de ce qui est déjà mis en place pour les établissements de crédit, gère un registre central électronique contenant la liste des entités fournissant des services de paiement au niveau européen.

Point à souligner : le registre de l'ABE n'aura pas de valeur légale, seuls les registres publics des autorités compétentes feront foi. Les autorités compétentes seront responsables de renseigner et mettre à jour les informations figurant dans le registre de l'ABE et l'ABE sera responsable de la présentation correcte de ces informations dans ce dernier.

Pour la mise en place de ce registre, la DSP2 prévoit que l'ABE élabore :

– d'une part, des projets de normes techniques de réglementation fixant les exigences techniques concernant l'établissement, l'exploitation et la gestion du registre électronique central et l'accès aux informations qu'il contient ;

– d'autre part, des projets de normes techniques d'exécution concernant le détail et la structure des informations devant figurer dans le registre.

Les enjeux des mandats liés au registre des établissements de paiement

Rendre public sur internet au niveau européen la liste des établissements de paiement agréés et leurs agents ainsi que les personnes physiques et morales bénéficiant d'une exemption d'autorisation, pour permettre notamment aux utilisateurs de services de paiement de vérifier le statut de son fournisseur de services de paiement.

3. https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-for-complaints-handling-for-the-securities-esma-and-banking-eba-sectors.

5. Renforcer la sécurité des moyens de paiement électronique, notamment pour les paiements sur Internet, et mettre en place un cadre réglementaire favorable à la concurrence entre les acteurs du marché existants et nouveaux tout en garantissant la protection des consommateurs

Alors que la première Directive sur les services de paiement ne comportait aucune disposition en matière de sécurité des paiements, l'augmentation de la fraude sur les paiements sur internet a notamment conduit le législateur à intégrer cet élément dans le cadre de la DSP2. Ainsi, le considérant 95 de la Directive stipule que « la sécurité des paiements électroniques est fondamentale afin d'assurer la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. Tous les services de paiement offerts par voie électronique doivent être effectués de manière sécurisée, en adoptant des technologies capables de garantir l'authentification sûre de l'utilisateur et de réduire, dans la mesure du possible, le risque de fraude ».

Dans ce contexte, la DSP2 apporte un certain nombre d'exigences sécuritaires minimales visant à :
– garantir la protection des consommateurs en imposant la mise en place de l'authentification renforcée des utilisateurs pour les paiements électroniques, notamment les paiements sur internet ;
– promouvoir la concurrence en réglementant les nouveaux services d'information sur les comptes et d'initiation de paiement tout en garantissant aux fournisseurs de ces services un accès aux comptes bancaires dans le cadre d'une communication sécurisée.

Pour ce faire, la DSP2 confie le soin à l'ABE d'émettre des orientations et des projets de normes techniques de réglementation pour assurer la mise en place de mesures de sécurité adéquates pour les paiements électroniques.

Ces mandats incluent :
– des orientations sur les mesures de sécurité devant être mises en œuvre par les prestataires de services de paiement pour la gestion des risques opérationnels et de sécurité (article 95) ;
– des orientations en ce qui concerne : les fournisseurs de services de paiement, sur la classification des incidents majeurs, et sur le contenu, le format et les procédures de notification de tels incidents aux autorités compétentes de l'État membre d'origine ; les autorités compétentes, sur les critères d'évaluation de la pertinence de l'incident et les détails des rapports d'incidents en vue de les partager avec d'autres autorités nationales (article 96) ;
– des normes techniques de réglementation sur l'authentification et la communication (article 98). Dans le cadre de ce dernier mandat, l'ABE doit préciser : les exigences relatives à l'authentification forte du client telle que définie par l'article 2 de la DSP2 ; les dérogations à l'application de l'authentification forte du client ; les mesures de sécurité à mettre en œuvre par les prestataires de services de paiement afin de protéger la confidentialité et l'intégrité des données d'authentification de l'utilisateur de services de paiement ; les standards de communication à mettre en œuvre par les « banques » (prestataires de services de paiement gestionnaires du compte), les prestataires de services d'initiation de paiement, les prestataires de services d'information sur les comptes, les payeurs, les bénéficiaires et les autres prestataires de services de paiement afin d'assurer une communication sécurisée. À noter que la Directive requiert des standards de communication ouverts et communs.

C'est bien entendu un des mandats les plus sensibles de la DSP2 et qui nécessite de trouver un équilibre entre certains objectifs qui peuvent s'avérer parfois contradictoires. L'ABE devra notamment définir des standards établissant un niveau de sécurité élevé tout en maintenant l'efficacité du paiement pour le consommateur ; choisir entre un niveau très détaillé des standards de communication pour éviter la mise en œuvre de solutions très différentes d'un acteur à l'autre ou un niveau moins détaillé permettant de futures innovations dans le domaine…

À ce titre, l'ABE a publié un « *discussion paper* »[4] pour recueillir l'avis de l'ensemble des acteurs concernés sur l'endroit où le curseur doit être placé selon eux. L'ABE a reçu 118 réponses à cette consultation, ce qui en fait la seconde consultation de l'ABE en termes de nombre de réponses reçues. Afin d'assurer une égalité de traitement entre l'ensemble des acteurs, l'EBA communiquera la synthèse des réponses reçues et la façon dont elle a tenu compte de ces retours dans le cadre de la consultation publique qui aura lieu cet été, pour une période de trois mois, sur le projet de normes techniques.

À partir de ces réponses, l'EBA développe actuellement les futurs requis sécuritaires ; un projet devrait être soumis à consultation publique à l'été 2016. À noter que même si les standards techniques doivent être soumis à la Commission d'ici le 13 janvier 2017, ils ne seront applicables réglementairement aux acteurs de marché que 18 mois après leur adoption par la Commission, donc pas avant octobre 2018 au plus tôt si l'on considère que le délai moyen d'adoption d'un projet de normes techniques par la Commission, sous contrôle du Parlement et du Conseil de l'UE, est de trois mois.

Ceci rend donc l'exercice d'autant plus délicat puisque l'ABE écrit actuellement des normes qui ne seront effectives que dans deux ans et demi au plus tôt, alors que le rythme des innovations est particulièrement élevé dans ce secteur. D'autant que c'est la première fois que des exigences de sécurité en matière de paiement seront inscrites dans la loi européenne.

Les enjeux des mandats liés à la sécurité des moyens de paiement électronique

Renforcer la sécurité des paiements électroniques afin d'assurer la protection des utilisateurs et le développement d'un environnement sain pour le commerce électronique. ■

4. Disponible en ligne sur le site de l'ABE: https://www.eba.europa.eu/.