

Payment Services Directive (PSD2)

Dans la deuxième version de sa directive concernant les services de paiement (*Payment Services Directive*, en abrégé PSD2), l'UE redéfinit les règles du jeu en matière bancaire et notamment dans le domaine des services de paiement. Entre autres, ce texte oblige les banques de l'UE à instaurer un droit d'accès aux comptes bancaires en faveur de prestataires tiers (*Third Party Providers*, TPP). Ces TPP sont soumis à l'autorisation et à la surveillance d'autorités nationales qui devront être créées à cet effet.

La PSD2 ne s'applique pas en Suisse, où l'on se demande pourtant s'il n'y aurait pas lieu d'introduire une réglementation équivalente. Dans notre pays, les prestataires tiers ont déjà accès aux comptes bancaires et les banques ouvrent les interfaces client lorsque c'est dans l'intérêt mutuel de l'établissement et du client. Toutefois, il n'existe pas encore d'obligation légale à cet égard. La Suisse mise ainsi sur des solutions faisant appel aux mécanismes de marché.

L'Association suisse des banquiers (ASB) rejette toute réglementation analogue à la PSD2 et tout droit d'accès conféré à des tiers par la loi, pour les raisons suivantes:

- Instaurer en Suisse une réglementation analogue à la PSD2 est **inutile** dans la mesure où il n'y a pas lieu d'agir, où la concurrence fonctionne et où les banques proposent d'ores et déjà (indépendamment de la PSD2) de nombreuses solutions innovantes. Une contrainte réglementaire imposant l'ouverture reviendrait à intervenir inutilement sur un marché performant et entraînerait une distorsion de concurrence au détriment des banques.
- Une réglementation analogue à la PSD2 obligerait à créer un **nouveau dispositif étatique de surveillance**, chargé d'autoriser et de surveiller les TPP.
- La question de la **sécurité des données des clients** joue un rôle primordial dans le domaine de la banque électronique. Une sécurité optimale ne peut être garantie que si le client et la banque coopèrent. Il serait dangereux que les pouvoirs publics imposent le droit d'accès, car les principes de sécurité propres aux banques risqueraient de n'être pas intégralement respectés au niveau des interfaces comme des TPP, ce qui pourrait ouvrir des brèches en termes de sécurité.
- Du côté des établissements financiers, il en résulterait des **charges supplémentaires** et un **surcroît de travail** en matière de sécurité et de compliance, dont le client devrait en fin de compte payer le prix.

Une ouverture unilatérale des droits d'accès aux tiers, telle que l'exige la PSD2 au sein de l'UE, constituerait **une expérimentation au détriment des clients des banques, qui compromettrait la sécurité et la protection des données des clients et nécessiterait la mise en place d'un dispositif de surveillance coûteux.**

Qu'est-ce que la PSD2?

La PSD2 vise à créer au sein de l'UE un cadre juridique uniforme pour les prestataires fournissant des services d'initiation de paiement électronique et mobile ainsi que pour ceux fournissant des services d'information sur les comptes. Les Etats membres de l'UE doivent s'y conformer depuis le début de l'année 2018. La PSD2 prévoit d'ouvrir une brèche dans la sécurité des services de paiement. Des prestataires extérieurs au secteur bancaire, les TPP, auraient accès à des données sensibles de clients. Les banques devraient mettre des interfaces d'accès à leur disposition, et ce gratuitement. Ces nouveaux prestataires seraient d'une part les prestataires de services d'initiation de paiement (*Payment Initiation Service Providers*, PISP) et d'autre part les prestataires de services d'information sur les comptes (*Account Information Service Providers*, AISP).

Le diable se cache dans les détails – bientôt une PSD3?

En mars 2018, l'Autorité bancaire européenne (ABE) a édicté des normes techniques réglementaires (*Regulatory Technical Standards*, RTS), qui définissent concrètement les modalités d'une authentification forte des clients et d'une communication sécurisée. Le secteur bancaire européen a jusqu'à septembre 2019 pour mettre en œuvre cette directive de l'ABE: ce décalage par rapport au délai d'application de la PSD2 est source d'insécurité juridique. En outre, même la directive de l'ABE ne résout pas toutes les questions de détail; les travaux de mise en œuvre au sein de l'UE ont laissé de nombreux points en suspens, qui font toujours l'objet de discussions politiques.

De fait, les RTS se bornent à fixer le cadre réglementaire dans lequel doivent s'inscrire les nouvelles interfaces d'open banking, sans prévoir et/ou créer en elles-mêmes une harmonisation de ces interfaces. Le Berlin Group a donc publié en mars 2018 une norme qui vise à permettre une telle harmonisation sur une base volontaire et en est désormais à sa troisième version. Toutefois, même cette version permet encore différentes mises en œuvre. Il demeure enfin que ce sont les autorités de surveillance nationales qui fixent les exigences applicables aux interfaces d'open banking, ce qui est susceptible de générer des écarts entre les pays et, par là même, d'accentuer la fragmentation. Les régulateurs européens ont identifié ce problème parmi d'autres et réfléchissent d'ores et déjà à une PSD3 qui remédierait aux faiblesses de la PSD2.

Une expérimentation économique au détriment de la sécurité et de la protection des données

Indépendamment des difficultés actuelles inhérentes à la PSD2, les clients qui utilisent la banque électronique et mobile ont droit à un haut niveau de sécurité. Or une ouverture des interfaces imposée par les pouvoirs publics recèlerait des risques considérables en matière de sécurité. Par exemple, les prestataires de services d'initiation de paiement disposeraient-ils d'un accès illimité au compte bancaire électronique? Dans ce cas, ils auraient accès à tous les comptes et dépôts bancaires de la relation d'affaires électronique. Cela reviendrait à leur remettre un chèque en blanc et un exemplaire de tous les relevés de compte. Des prestataires tiers connaîtraient ainsi les valeurs patrimoniales du client et pourraient consulter tous ses paiements – loyer, salaire, assurance, caisse maladie, opérateurs de téléphonie, etc. En outre, le client aurait de plus en plus de mal à savoir ce qu'il advient de ses données, où elles sont enregistrées et quels sont ses droits. L'ouverture imposée des droits d'accès aux comptes bancaires entraînerait pour lui des conséquences difficiles à évaluer.

Un dispositif qui rate sa cible

S'il est vrai que la PSD2 va transformer les services de paiement, elle ne servira pas prioritairement les intérêts des start-up européennes ou même suisses, mais fera le jeu des géants mondiaux de la technologie. Eux disposent de plateformes suffisamment vastes pour agréger les données des clients. Par ailleurs, la PSD2 laisse aux banques et aux autorités de surveillance nationales le soin d'harmoniser les interfaces, d'où un risque de fragmentation du marché. Elle rate ainsi sa véritable cible, qui est de faciliter l'accès au marché financier pour les start-up innovantes et de favoriser la mise en place d'un marché unique des services de paiement en Europe.

La tradition suisse de l'investissement librement choisi et orienté vers l'avenir ouvre une autre voie: les banques suisses investissent dans des solutions Fintech et, à cet effet, elles collaborent étroitement avec des start-up et des prestataires de toute nature. Indépendamment de la PSD2, elles développent elles-mêmes – ou avec des partenaires et des entreprises Fintech – des applications innovantes susceptibles d'apporter de la valeur ajoutée à leurs clients.

La Suisse dispose de solutions adaptées au marché et n'a pas besoin de la PSD2

- Les banques peuvent d'ores et déjà ouvrir les interfaces client lorsque c'est dans l'intérêt de l'établissement et du client.
- La Suisse n'est pas tenue d'appliquer la PSD2, ni directement, ni indirectement. En effet, elle n'est membre ni de l'UE, ni de l'EEE, et les accords bilatéraux conclus avec l'UE ne prévoient aucune obligation à cet égard.
- Les banques suisses proposent d'ores et déjà de nombreuses solutions innovantes en matière de paiement et de gestion financière, et ce sans la moindre contrainte réglementaire. Par exemple:
 - Grâce à l'**e-facture**, on peut vérifier et payer dans l'e-banking des factures pré-enregistrées. L'e-facture est très sûre, car son émetteur est authentifié par la banque, ce qui n'est pas le cas de la facture papier.
 - A partir du milieu de l'année 2020, l'établissement et le règlement des factures seront facilités grâce à la **facture QR**, qui intégrera toutes les informations de paiement. Cette innovation assurera une transition optimale entre l'ancien monde des bulletins de versement sous format papier et le nouveau monde numérique.
 - Il existe sur le marché quelques exemples de **partenariats efficaces**, qui misent sur des interfaces sûres et standardisées. Tel est le cas notamment de l'échange de données automatisé entre l'e-banking et les programmes de comptabilité.
 - Citons également la solution **Corporate API de SIX**, qui démarrera courant 2019, ainsi que la solution **Open Banking de Swiss FinTech Innovations**, disponible sur le marché depuis septembre 2018.
 - L'application de paiement **TWINT** permet d'ores et déjà au client d'effectuer, de manière sûre et confortable, des paiements P2P, e-commerce et POS directement par débit de son compte.