

# L'UE ouvre son marché à de nouveaux prestataires dans le trafic des paiements

Les innovations portées par des acteurs non bancaires sont en passe de révolutionner le trafic des paiements. Les banques traditionnelles s'opposent toutefois à une ouverture régulée du marché. Contrairement à la Suisse, l'UE a pris position en s'ouvrant à d'autres prestataires tout en fixant des règles rigoureuses en matière de sécurité. *Susan Emmenegger*

**Abrégé** La numérisation a permis l'apparition sur le marché des paiements de nouvelles offres et de prestataires non bancaires. La concurrence s'est accrue, de même que les risques d'un accès non autorisé aux comptes de la clientèle. Comment les banques doivent-elles agir face à ces nouveaux acteurs ? Comment la sécurité des comptes peut-elle s'améliorer ? Dans sa seconde directive sur les services de paiement (DSP2), l'UE a fait des choix clairs qui obligent les banques à s'ouvrir aux nouveaux prestataires (les « fintech ») et relèvent les exigences en matière de sécurité pour le traitement des paiements électroniques. En Suisse, les banques s'opposent à ce type de réglementation. À moyen terme, les nouveaux prestataires devront toutefois être soumis à certaines dispositions réglementaires clés. C'est au plus tard à ce moment-là que la question d'une ouverture forcée du marché des paiements aux prestataires du secteur non bancaire se posera de nouveau.

Les innovations technologiques dans le trafic des paiements ont donné lieu à un grand nombre de nouveaux produits et prestataires. Le bitcoin, l'ethereum, le ripple ou d'autres parmi les près de 1500 cryptovalues viennent aussitôt à l'esprit. Elles servent, toutefois, rarement de moyen de paiement, mais plutôt d'instruments de placement. Il existe en revanche des innovations incontournables dans le traitement des paiements traditionnels, telles que la communication en champ proche notamment, utilisée par Apple Pay et l'application suisse de paiements Twint. Au cours des dernières années, les nouvelles technologies ont été largement adoptées, ce qui a modifié en profondeur et accéléré les processus de paiement.

Les entreprises de technologies financières (« fintech ») jouent un rôle décisif dans le développement de ces processus. Elles rompent les chaînes de valeur traditionnelles des banques, tout en se reposant en grande partie sur leur infrastructure pour fournir leurs propres services. Les services de paiement totalement indépendants des banques, tels que le promettent les promoteurs des chaînes de blocs, ne sont en effet pas encore fonctionnels à ce jour.

Le « surf sur l'infrastructure bancaire » pratiqué accentue la problématique de la sécurité et de la protection des données que soulève déjà le traitement électronique des paiements.

Ce dernier implique un risque d'accès non autorisé aux comptes bancaires des clients – notamment par des attaques informatiques.

L'UE a déjà réagi sur ce point. L'apparition de prestataires sans licence bancaire et le risque accru de cyberattaques ont donné lieu à une révision de la première directive sur les services de paiement de 2009. Cette seconde directive (PSD2) est en vigueur depuis début 2018.

## Des services de paiement sans licence bancaire

La nouvelle directive PSD2 prévoit trois catégories de prestataires dans le trafic des paiements tiers autorisés sur le marché : les services d'information sur les comptes, les services d'initiation de paiement et les émetteurs tiers de cartes de paiement. Ces derniers n'existant pas encore sur le marché, le présent article vise essentiellement les deux premières catégories.

Les services d'information sur les comptes tels que Qontis récupèrent toutes les informations concernant un client auprès des différentes banques et lui permettent d'obtenir facilement une vue d'ensemble de sa situation financière. Ils s'ajoutent souvent à d'autres services, tels que des outils de liquidité ou de budgétisation. Les services d'initiation de paiement tels que Klarna (antérieurement Softfort GmbH) proposent une passerelle logi-

cielle entre les commerçants en ligne et les portails web des banques qui permet de simplifier les processus d'achat. Ces deux types de services impliquent que le client du prestataire donne à ce dernier un accès direct en ligne à son compte bancaire, en indiquant son NIP ou son code de transaction sur le portail web du prestataire externe. Ce procédé, appelé « screen scraping », est vulnérable aux attaques informatiques (attaques dites de l'« homme du milieu »).

La Suisse possède également des services d'information sur les comptes et d'initiation de paiement. Leurs utilisateurs supportent toutefois à ce jour l'entière responsabilité d'un éventuel dysfonctionnement, notamment en cas de cyberattaque visant leur compte. Les conditions générales des banques suisses interdisent en effet aux clients de transmettre leurs NIP ou leurs codes de transaction à des tiers.

## L'UE renforce la protection des clients

L'UE a choisi une tout autre approche dans sa directive PSD2, laquelle prévoit une obligation expresse pour les banques d'autoriser les prestataires de paiement tiers à accéder aux comptes des clients qui le souhaitent. Cet accès doit toutefois se faire à travers une interface distincte, le « screen scraping » devant être interdit dans l'UE à l'issue d'une période transitoire. La coopération avec les nouveaux prestataires de paiements devient également obligatoire pour les banques. Les transferts demandés par l'intermédiaire de services d'initiation de paiement doivent ainsi être traités aussi vite et au même coût que s'ils avaient été effectués par la banque elle-même. La directive prévoit que la banque doit coopérer avec le service d'initiation de paiement même lorsqu'elle n'a pas conclu de contrat avec ce dernier. Les banques doivent donc mettre ce service à disposition gratuitement. Le « parasitisme » des prestataires de paiement tiers est ainsi consciemment en-



En Suisse, celui qui utilise les services de paiement non-bancaires est responsable en cas d'attaques de hackers.

couragé par l'UE dans le but de renforcer la concurrence sur le marché des services de paiement. L'ouverture forcée du marché aux prestataires de paiement tiers ne peut toutefois se passer de réglementation. Ils doivent donc être agréés et se conformer à de nombreuses exigences en matière de sécurité et de protection des données.

En Suisse, les prestataires tiers ne sont en revanche pas réglementés. Cela signifie concrètement qu'ils peuvent continuer à procéder par « screen scraping », les clients supportant l'intégralité du risque de dysfonctionnement.

### Accès non autorisé aux comptes bancaires

En matière d'attaques informatiques – risque le plus important à ce jour dans le domaine du trafic de paiements de détail –, l'UE adopte également une approche différente de celle de la Suisse. La directive PSD2 exige ainsi des banques qu'elles procèdent à une « identification forte du client » pour les opérations de paiement électroniques. Cela implique que les moyens de légitimation personnels soient constitués d'au moins deux moyens d'authentification indépendants et qu'il existe un lien dynamique entre l'opération, le montant et le bénéficiaire. Le déclenchement d'une opération de paiement en ligne – via la saisie d'un NIP et d'un code de transaction sur un ordinateur par exemple – ne doit être possible que si un code supplémentaire accompagné de l'indication du destinataire et du montant de la transaction est transmis au client sur un appareil distinct, tel qu'un smartphone. Ce

système permet notamment d'identifier les attaques de l'« homme du milieu ».

Au sein de l'UE, de telles exigences en matière de sécurité sont mises en œuvre non seulement à travers la réglementation, mais également par le biais des règles en matière de responsabilité. Si la banque ne requiert pas d'identification forte du client pour l'initiation d'un paiement électronique, elle est tenue de rembourser les montants indûment soustraits, même en cas de négligence grave du client dans l'usage de ses moyens d'authentification personnels. Ce n'est qu'en cas de fraude volontaire que la banque peut faire supporter le risque d'une transaction non autorisée au client. En outre, l'UE limite à 50 euros le montant du risque à supporter par le client en cas d'identification forte, même en cas de négligence légère de ce dernier. De tels incidents ne devraient toutefois plus survenir après l'introduction des processus d'identification forte. La validation d'un paiement non souhaité malgré l'indication du destinataire et du montant constituerait en effet sans doute un cas de négligence grave.

En Suisse, l'authentification à deux facteurs avec NIP et code de transaction s'est également imposée, mais très peu d'établissements financiers proposent une identification forte du client sur le modèle européen. Les conditions générales des banques suisses prévoient en outre qu'un paiement est considéré comme approuvé dès lors qu'il a été initié par l'utilisation des moyens d'authentification personnels. Le risque d'attaque informatique est donc entièrement supporté par les clients. Le doute subsiste quant à la licéité d'une telle répartition contractuelle des risques du point de vue du droit privé. Elle est toutefois prévue de cette façon dans les conditions générales et les clients victimes de fraudes devraient, dès lors,

porter plainte devant chacune des instances compétentes pour faire valoir leurs droits. Il est certes possible que les banques fassent preuve d'une certaine bonne volonté, notamment en cas d'attaque à grande échelle. Du point de vue des clients, l'espoir d'un tel geste de la part des banques ne constitue toutefois pas une solution durable.

### Des banques suisses opposées à la réglementation

L'UE a réagi aux innovations et à l'augmentation des risques dans le trafic des paiements en prenant des décisions claires dans sa directive PSD2. Cette dernière ouvre le marché à certaines catégories de prestataires en matière de trafic des paiements. En favorisant la concurrence, elle permet en outre à des acteurs tiers de participer à la création de valeur dans ce secteur. La directive fixe par ailleurs des normes élevées en matière de sécurité et étend la protection des clients.

Dans une prise de position de septembre 2017, l'Association suisse des banquiers (ASB) s'est pour sa part prononcée contre l'instauration d'une réglementation équivalente en Suisse. Les critiques formulées visent essentiellement l'obligation d'ouvrir le marché à des concurrents non bancaires. L'ASB estime qu'une telle intervention est inutile dans un marché qui ne pose pas de problème de fonctionnement. Cette ouverture pourrait également poser des problèmes de sécurité, synonymes de coûts supplémentaires devant être reportés sur le client.

La mise en œuvre de la directive PSD2 entraîne effectivement des coûts importants. Elle présente toutefois l'avantage d'inclure les nouveaux prestataires de paiement dans le champ de la réglementation, améliorant ainsi la sécurité des utilisateurs. À moyen terme, ce secteur sera inévitablement soumis à certaines dispositions réglementaires clés. C'est au plus tard à ce moment-là que la question d'une ouverture imposée du marché des paiements aux prestataires externes au secteur bancaire se posera de nouveau.



**Susan Emmenegger**

Professeure de droit privé et de droit bancaire, directrice de l'Institut de droit bancaire de l'université de Berne