Les innovations dans les paiements

Avec la numérisation des modes de travail et de consommation, le secteur des paiements devient de plus en plus innovant et attractif. De nombreux acteurs ont investi ce domaine en pleine mutation ces dernières années. Voici quelques informations pour mieux comprendre leurs activités et connaître vos droits en tant qu'utilisateurs.

Foire aux questions : les innovations dans les paiements

Consulter la FAQ

Crypto-actifs et stablecoins : de quoi parle-t-on ?

Ces dernières années ont vu l'apparition de méthodes de paiement dites « alternatives », qui présentent la spécificité de permettre d'effectuer des transactions libellées dans des unités autres qu'en monnaie ayant cours légal. Parmi eux, les cryptoactifs ne constituent pas des moyens de paiement au sens légal.

Un cryptoactif est un actif numérique (ou digital), créé grâce à l'utilisation de technologies de cryptographie. Ils sont nommés ainsi car ils s'apparentent à des actifs financiers et sont créés et utilisés via des technologies de cryptage. Les cryptoactifs sont parfois appelés abusivement cryptomonnaies mais ne doivent pas être confondus avec une monnaie.

Il existe plusieurs types de cryptoactifs. Les cryptoactifs de première génération, tels que le Bitcoin et l'Ethéréum, n'ont pas de cours légal ni de valeur intrinsèque. Ils constituent donc des actifs spéculatifs et très risqués. Depuis, des projets de « *stablecoins* » (tels que le projet DIEM) essayent de dépasser ces limites en ayant pour ambition d'avoir une valeur plus stable. Pour cela, leur cours serait lié à celui d'un actif de référence (l'or, l'euro, le dollar, un groupe de monnaies, etc.) afin d'ancrer leur évolution à l'économie réelle et de moins fluctuer, d'où leur nom. Les *stablecoins* peuvent être vus comme une deuxième génération de cryptoactifs.

Crypto-actifs et stablecoins : ces services sont-ils réglementés ?

En l'absence de réglementation internationale des services sur cryptoactifs, plusieurs initiatives ont été lancées ces dernières années dans différents États. La France figure au premier rang des juridictions ayant apporté très rapidement des réponses à ses acteurs. La loi PACTE (loi no 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises) a instauré le statut de prestataire de services sur actifs numériques (PSAN) qui couvre les activités suivantes : conservation d'actifs numériques pour le compte de

tiers, achat/vente d'actifs numériques contre une monnaie ayant cours légal (ou contre d'autres actifs numériques), exploitation d'une plateforme de négociation d'actifs numériques, réception et transmission d'ordres pour le compte de tiers, gestion de portefeuille pour le compte de tiers – ainsi que d'autres services complémentaires (conseil, prise ferme, placement garanti et placement non garanti). La conservation d'actifs numériques pour le compte de tiers et l'achat/vente d'actifs numériques contre une monnaie ayant cours légal doivent faire l'objet d'un enregistrement obligatoire auprès de l'Autorité des marchés financiers (AMF). Les PSAN qui le souhaitent peuvent également solliciter un agrément optionnel auprès de cette institution.

Pour apporter une solution européenne à ces questions, la Commission européenne a publié en 2020 un projet de règlement dédié aux marchés sur cryptoactifs (MiCA), qui introduit un régime pilote pour les infrastructures de marché qui souhaitent négocier et régler des opérations sur instruments financiers sous forme de cryptoactifs.

Les BigTechs : de quoi parle-t-on ?

Le terme « Big Techs » désigne les entreprises qui dominent le secteur des technologies de l'information et de la communication. Parmi ces sociétés, l'on compte les GAFAM américaines (en référence à Google, Apple, Facebook, Amazon et Microsoft), mais également les entreprises chinoises connues sous l'acronymes BATX (Baidu, Alibaba, Tencent et Xiaomi).

Bien que présentes sur un large spectre d'activités allant du e-commerce aux équipements électroniques, ces sociétés investissent de manière croissante les services financiers. Elles capitalisent en effet sur les données recueillies dans le cadre de leurs activités, et profitent de leur positionnement d'interface pour offrir notamment des services de paiement à leurs clients. A l'heure actuelle, leur principal segment d'activité dans la sphère du paiement concerne les portefeuilles électroniques ou *wallets*.

Qu'est-ce qu'un portefeuille électronique ou wallet ?

Les portefeuilles électroniques (*digital wallets*) permettent de confier à un tiers de confiance les informations de la carte de paiement ou les coordonnées bancaires.

Aujourd'hui, la plupart des grands e-commerçants proposent l'enregistrement des coordonnées de la carte de paiement afin de faciliter les paiements par leurs clients, ce qui revient à constituer autant de *wallets* dits commerçants (non liés à l'émetteur de la carte). De plus, les géants du numérique ont profité de l'accroissement de l'utilisation des smartphones pour proposer le même modèle de portefeuille électronique pour les paiements dits « de proximité », c'est-à-dire dans les commerces physiques sur un terminal de paiement électronique. Ces applications proposent de dématérialiser la carte de paiement afin de la stocker sur un téléphone portable, et ainsi transformer le smartphone en carte de paiement. Les cartes sont « tokenisées » : le numéro de la carte est transformé en *token*, la liste des correspondances entre numéros de cartes de paiement et *tokens* étant conservée par un prestataire de services. Ce *token* est enregistré dans un environnement sécurisé du smartphone physique (*secure element*) ou logiciel (*host card emulation*). Grâce à ces dispositifs de sécurité, il est plus difficile d'utiliser la carte de paiement à l'insu de l'utilisateur. Outre la tokenisation, les portefeuilles électroniques sur mobile reposent sur le développement du « sans contact »

pour les paiements par carte et l'équipement des smartphones avec la technologie NFC (*Near Field Communication*).

D'autres applications de paiement mobile se sont développées à l'initiative de nouveaux acteurs ou des banques commerciales. Ces applications proposent généralement un portefeuille électronique et une solution de paiement entre particuliers. Cette dernière s'appuie sur le numéro de téléphone des utilisateurs en remplacement des coordonnées bancaires pour les virements (*proxies*). Si plusieurs solutions de ce type rencontrent un succès modéré en France (Paylib, Lydia, etc.), elles peuvent être très largement adoptées par les utilisateurs. En Suède, la solution Swish est utilisée par 70 % des citoyens du pays. Aux Pays-Bas, la solution iDEAL est utilisée par 10 millions de personnes. Les solutions Blik (Pologne) et Bizum (Espagne) rencontrent également un fort succès.

Qu'est-ce que le RTP ?

Le *Request-to-pay* (RTP) consiste en un service de messagerie permettant de transmettre une créance accompagnée d'une demande de paiement, et de recueillir l'accord (ou non) du débiteur, sur la base duquel le paiement pourra ensuite être initié le cas échéant. Il s'inscrit dans l'évolution du paysage des paiements des dernières années : développement de l'usage des paiements SEPA, économie numérique, dématérialisation de la chaîne de facturation-paiement.

Qui peut proposer le service RTP ?

Le RTP n'étant pas un service de paiement, sa fourniture n'est pas réservée aux prestataires de services de paiement agréés auprès des autorités de supervision. Afin de s'assurer de la fiabilité des prestataires, ces derniers doivent cependant être homologués et respecter les règles définies par le Conseil européen des paiements (European Payments Council – EPC).

Les changements introduits par la DSP2

La deuxième directive européenne sur les services de paiement (DSP2), en vigueur dans l'Union européenne depuis le 13 janvier 2018, comporte un ensemble de dispositions règlementaires visant à encadrer la prestation de services de paiements et renforcer la sécurité des paiements à l'échelle européenne.

Foire aux questions : les changements introduits par la DSP2

Consulter la FAQ

Les agrégateurs de comptes : de quoi parle-t-on ?

Les agrégateurs de comptes mettent à la disposition de leurs clients une interface offrant une vision consolidée de leurs compte(s) de paiement détenus dans un ou de plusieurs établissements. Les agrégateurs de comptes bénéficient d'un cadre juridique depuis la deuxième directive sur les services de paiement [lien vers la directive]. Ils reçoivent notamment un agrément de l'Autorité de contrôle prudentiel et de résolution (ACPR) pour pouvoir exercer leurs activités, qui sont par ailleurs soumises au contrôle de l'Autorité.

Agrégateurs de comptes : ces services sont-ils réellement sécurisés ?

Oui. La DSP2 impose à ces établissements de prendre des mesures de sécurité pour garantir la protection des données personnelles des utilisateurs. L'ACPR ne délivre des agréments que lorsque les agrégateurs apportent toutes les garanties de sécurité. Elle est aidée dans cette tâche par les services de la Banque de France en charge de la surveillance des moyens de paiements scripturaux qui réalisent un bilan sur la sécurité des infrastructures techniques de ces établissements.

Agrégateurs de comptes : le prestataire a-t-il toujours accès à mes données après que j'ai résilié ses services ?

La DSP2 et le règlement délégué relatif à l'authentification forte prévoient que l'utilisateur doit procéder à une authentification forte au moins tous les 90 jours pour que l'agrégateur puisse accéder à ses données de comptes de paiement. En France, pour la clientèle de particuliers, de nombreux établissements accordent aux agrégateurs de comptes ce délai de 90 jours et n'imposent pas d'authentification plus fréquente.

Ainsi, au-delà de 90 jours, si vous n'avez pas renouvelé votre authentification, le prestataire ne peut plus accéder à vos données de comptes.

En outre, à tout moment, vous pouvez résilier le service auprès du prestataire. Ce dernier est alors tenu par la réglementation de ne plus accéder à vos données de comptes.

Enfin, en cas de suspicion d'accès non autorisé, l'utilisateur peut demander à son établissement teneur de compte de révoquer les droits du prestataire.

Les initiateurs de paiement : de quoi parle-t-on ?

Les initiateurs de paiement permettent aux utilisateurs d'effectuer des paiements sans passer par leur espace de banque en ligne grâce à l'interface fournie par les initiateurs et sans avoir à remplir les coordonnées du bénéficiaire. Ils permettent notamment de réaliser un paiement sur Internet auprès d'un commerçant. La DSP2 a donné un cadre juridique aux initiateurs de paiement qui reçoivent un agrément de l'ACPR.

Un initiateur de paiement peut-il conserver mes données pour effectuer de nouveaux paiements ?

La réglementation interdit aux initiateurs de paiement de conserver les données de paiement sensibles concernant l'utilisateur. Une authentification est par ailleurs nécessaire à chaque fois qu'un paiement est réalisé. Si un initiateur conservait de telles données, il s'exposerait à des sanctions de la part de l'ACPR.

Qu'est-ce que l'authentification forte et à quoi sert-elle ?

L'authentification forte implique la confirmation d'au moins deux facteurs d'authentification de catégories différentes parmi les trois catégories suivantes :

1. la possession (une clé, un téléphone portable, etc.)
2. la connaissance (un mot de passe)
3. l'inhérence (une empreinte digitale)

Dans une grande majorité des cas, l'authentification forte implique l'ouverture de l'application mobile de banque en ligne de l'utilisateur et la saisie d'un mot de passe (ou le contrôle de l'empreinte digitale) sur un téléphone préalablement enregistré par l'établissement teneur de compte. Cette méthode remplace l'envoi d'un SMS sur le téléphone portable, qui ne remplit qu'un seul des deux critères s'il n'est pas associé à la confirmation d'un mot de passe.

L'authentification forte permet de renforcer significativement la sécurité pour la connexion à votre espace de banque en ligne et pour l'émission de paiements. Un utilisateur malveillant ne pourrait accéder à l'espace d'un autre utilisateur avec le seul mot de passe. Lors d'un paiement par carte sur Internet, la saisie des informations de la carte de paiement n'est pas suffisante pour effectuer la transaction. L'authentification forte prévue par la DSP2 est plus sécurisée que le seul SMS car il n'est pas impossible d'intercepter les SMS de confirmation de paiement envoyés par les établissements teneurs de comptes (technique du *SIM Swapping*).

Pour aller plus loin

- Le mandat de la Banque de France en matière de surveillance des moyens de paiement scripturaux
- Présentation du Comité national des moyens de paiement (CNMP)
- La stratégie nationale des moyens de paiement