Les nouveaux instruments de paiement, avatars de la monnaie fiduciaire : de nouveaux facteurs de risque en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

Par Bruno DALLES
Directeur du Service Tracfin (ministère de l'Action et des Comptes publics)

L'accélération de la révolution digitale et le développement de nouveaux instruments de paiement constituent un défi en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Certains de ces instruments présentent en effet des risques avérés.
La menace terroriste a conduit le législateur français à encadrer en 2016 l'usage de la monnaie électronique, en particulier celui des cartes prépayées. Ce resserrement réglementaire en matière de produits doit s'accompagner d'une responsabilisation des nouveaux acteurs du paiement, appelés à conforter leur culture de conformité.
Or, la capacité des autorités de supervision à contrôler ces acteurs est amoindrie par le passeport européen et le régime de la Libre Prestation de Services. Le manque d'harmonisation internationale en matière d'exigences anti-blanchiment limite l'efficacité du dispositif, tandis que la fiabilité de certains opérateurs implantés en Europe peut être mise en doute.

Les nouveaux instruments de paiement scriptural englobent les prestations de services de paiement [1] en ligne et l'émission de monnaie électronique [2]. Apparus aux États-Unis dans les années 1990, ils se sont développés en Europe à partir de la fin des années 2000 avec l'essor du commerce électronique et l'adaptation à celui-ci des normes européennes[3].

Ces nouveaux services reposent sur deux types de support : d'une part, les serveurs électroniques sans support physique, utilisés par des prestataires de services de paiement de type PayPal ou similaires, qui proposent des plateformes de paiement en ligne et des *wallets* ; et, d'autre part, les supports physiques de monnaie électronique du type cartes de paiement prépayées ou clés USB, voire des coupons comportant un code à transmettre au destinataire du paiement.

Selon leur degré d'anonymat et de traçabilité, ces différents produits présentent des risques avérés au regard de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT).

La menace terroriste a conduit le législateur français à encadrer, en 2016, l'usage de la monnaie électronique, en particulier celui des cartes prépayées. Ce resserrement réglementaire doit s'accompagner d'une responsabilisation des nouveaux acteurs du paiement. Or, la capacité des autorités à contrôler ces acteurs est amoindrie par le passeport européen, tandis que la fiabilité de certains opérateurs implantés en Europe peut être mise en doute.

(1) Voir l'art. L.314-1 et suivants du Code monétaire et financier (CMF).
(2) Voir l'art. L.315-1 et suivants du CMF.
(3) Directive sur la monnaie électronique, dite DME2 (Directive 2009/110/CE), transposée en droit français en janvier 2013 ; Directive sur les Services de Paiement, dite DSP2 (Directive (UE) 2015/2366) en cours de transposition / 4ème directive anti-blanchiment (Directive (UE) 2015/849) transposée en droit français en décembre 2016.

À la suite des attentats de 2015, le législateur français a décidé d'encadrer l'utilisation de la monnaie électronique

Les cartes prépayées anonymes représentent un risque avéré de blanchiment de capitaux et de financement du terrorisme

Les attentats de 2015 en France et en Belgique ont permis une prise de conscience du caractère anonyme de la monnaie électronique comme moyen de paiement et de stockage de fonds. Les cartes prépayées rechargeables en espèces, quand elles ne sont pas réglementées, présentent le même degré d'anonymat et de non-traçabilité que les espèces. Leur dangerosité est aggravée par une portabilité accrue et une mobilité mondiale des flux.

- L'enquête diligentée après les attaques du 13 novembre 2015 à Paris a mis en évidence l'utilisation de cartes prépayées anonymes par les commandos terroristes pour effectuer des achats démarqués ou payer des hébergements dans un total anonymat. Une fois ces cartes identifiées, les enquêteurs ont pu retracer les paiements et certains déplacements de leurs utilisateurs. Ces cartes ont aussi été utilisées pour des préparatifs de départs vers la zone syro-irakienne.

Certains proches en France de djihadistes partis sur zones de conflit ont utilisé des coupons de rechargement payés en espèces, dont ils transmettaient les codes, par SMS, aux terroristes qu'ils soutenaient. Ces derniers alimentaient ainsi des porte-monnaie électroniques servant à payer certains frais, notamment des communications téléphoniques.

- La criminalité crapuleuse utilise des cartes prépayées pour collecter et évacuer des fonds. Tracfin a traité le cas d'un réseau de prostitution exploitant à Paris et en province plusieurs centaines de jeunes femmes originaires d'Europe centrale. Celles-ci viraient leurs gains à trois proxénètes restés au pays en utilisant pour ce faire soit des sociétés de transferts de fonds en espèces, soit des jeux de cartes prépayées liées au même compte de monnaie électronique. Ces jeunes femmes alimentaient le compte en espèces et utilisaient leur carte pour leurs dépenses, tandis que les proxénètes détenaient la carte jumelle avec laquelle ils pouvaient procéder à des retraits d'espèces dans leur pays. Sur plusieurs années, les montants cumulés ont atteint 2,4 millions d'euros.

En 2016, le législateur français a cherché à limiter ce risque

Le législateur français a publié en 2016 plusieurs textes destinés à réglementer l'usage de la monnaie électronique.

- Depuis le 1er janvier 2017, toute opération de paiement en monnaie électronique effectuée en France, par carte ou depuis un serveur, est plafonnée à 3 000 € [4].
- L'utilisation des cartes prépayées a été encadrée par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement [5]. Un décret a défini des plafonds d'utilisation [6] : une carte ne peut être chargée de plus de 10 000 € ; les rechargements en espèces sont limités à 1 000 € par mois ; les retraits ou les remboursements de solde en espèces sont également limités à 1 000 € par mois.

De plus, la loi oblige les établissements de monnaie électronique à conserver durant cinq ans les informations clients relatives à l'activation, au chargement et à l'utilisation de monnaie électronique au moyen d'un support physique [7].

La transposition en droit français de la 4ème directive européenne anti-blanchiment, par l'ordonnance n°2016-1635 du 1er décembre 2016, a permis de réduire l'anonymat de la monnaie électronique.

Désormais, tout support physique de paiement alimenté à partir de moyens de paiement traçables (comptes bancaires nominatifs ouverts dans un pays de l'espace économique européen) nécessite la présentation d'une pièce d'identité dès que le montant du rechargement dépasse 250 € par mois. Les remboursements en espèces sans vérification d'identité ne sont possibles que jusqu'à 100 €.

Tout support physique de paiement alimenté à partir de moyens de paiement non traçables (espèces ou monnaie électronique anonyme) nécessite la présentation d'une pièce d'identité au premier euro et à chaque rechargement. La seule exception concerne les cartes « enseignes » utilisables uniquement en France pour l'achat de biens et de services limités, qui peuvent être rechargées en espèces sans vérification d'identité jusqu'à 250 € par mois [8].

Enfin, pour les services de paiement en ligne, les opérateurs sont dispensés de vérification d'identité uniquement pour les paiements en ligne d'un compte bancaire de l'espace économique européen (EEE) vers un autre compte bancaire de l'EEE, pour des opérations de moins de 250 € et dans la limite d'un montant cumulé de 2 500 €par an [9].

En matière de services de paiement, la réglementation des produits doit se conjuguer à la responsabilisation des acteurs

Depuis le début des années 2000, la France a mis une dizaine d'années pour développer une culture de conformité solide au sein de ses établissements bancaires. Ce chantier est aujourd'hui rouvert auprès des nouveaux acteurs des services de paiement. Ceux-ci, consacrés par la DSP2, n'ont pas la même culture du risque de blanchiment que les établissements bancaires et font même,

(4) Décret n°2016-1985 du 30 décembre 2016 modifiant l'art. D.112-3 du Code monétaire et financier (CMF).
(5) Loi n°2016-731 du 3 juin 2016, dite « loi Urvoas », notamment sa disposition modifiant l'art. L.315-9 du CMF.
(6) Décret n°2016-1742 du 15 décembre 2016, transcrit dans l'art. D.315-2 du CMF.
(7) Art. L.561-12 du CMF. À fin juin 2017, cette disposition devait encore être précisée par décret.
(8) Art. R.561-16 du CMF.
(9) Art. R.561-16-1 du CMF. Les articles R.561-16 et R.561-16-1 du CMF pourraient être prochainement remaniés et le seuil de 250 € abaissé.

Photo © PHOTOPQR/Le PARISIEN/ MAX PPP

Créé en 1990, Tracfin, la cellule française de renseignement financier, est depuis 2006 un service à compétence nationale (8 octobre 2012).

« Tracfin observe que certains établissements implantés au sein de l'Union européenne et comptant des millions d'utilisateurs pourraient être contrôlés par des organisations criminelles. »

pour certains, de la levée des contraintes réglementaires un ressort de leur développement.

Or, comme tout professionnel assujetti au dispositif LCB/FT, les établissements de paiement (EP) et les établissements de monnaie électronique (EME) sont tenus de respecter leurs obligations de vigilance [10]. L'Autorité de Contrôle prudentiel et de Résolution (ACPR) a déjà sanctionné certains établissements, notamment pour non-respect de leurs obligations d'identification client [11].

Ces obligations sont importantes à quatre titres :

- Les prestataires de services de paiement (PSP) viennent se positionner entre le client et sa banque. Le client enregistre les coordonnées de son compte ou de sa carte bancaire auprès d'un PSP, lequel gère les paiements vis-à-vis des tiers. De ce fait, le PSP prive la banque d'une partie des données nécessaires à l'analyse fine des opérations du client. La banque ne voit plus le PSP que comme la seule contrepartie des flux du compte de son client, d'où l'importance que le PSP puisse assurer sa propre vigilance client ;
- Lorsqu'un client utilise plusieurs PSP successivement, les PSP deviennent interdépendants, chacun formant un maillon d'une chaîne. Une plateforme de paiement électronique peut respecter ses obligations LCB/FT, mais proposer à ses clients de charger leur portefeuille (*wallet*) à partir d'autres établissements moins vigilants. Il suffit d'un seul établissement défaillant pour affaiblir tout le dispositif ;
- Les PSP qui utilisent des réseaux d'agents (pour les services de paiement) ou de distributeurs (pour la monnaie électronique) doivent veiller à la conformité de ces opérateurs, qui, n'étant pas des professionnels de la finance, n'ont aucune culture anti-blanchiment. La concurrence entre PSP pourrait les inciter, auprès de leurs agents et distributeurs, à privilégier le développement commercial au détriment du respect des obligations LCB/FT. De ce fait, les agents et les distributeurs multimarques présentent un risque élevé ;
- Enfin, les professionnels doivent être sensibilisés à tous les types de risque. La fraude documentaire et la fraude à l'identité constituent un sérieux vecteur d'affaiblissement des procédures de connaissance client, et ce, même dans le cas de PSP vigilants.

(10) Identifier et vérifier l'identité de leur client (art. L.561-5 du CMF) ; caractériser la relation d'affaire (art. L.561-5-1 du CMF) ; contrôler la cohérence des opérations client pendant toute la durée de la relation (art. L.561-6 du CMF).

(11) Voir procédure n°2014-10 du 16 octobre 2015, et procédure n°2016-05 du 3 mars 2017, disponibles sur le site Internet de l'ACPR, rubrique « Commission des sanctions ».

Le contrôle des prestataires de services de paiement est limité par le passeport européen, alors même que la fiabilité de certains de ces acteurs peut être mise en doute

Le principal levier pour inciter les nouveaux acteurs du paiement à prendre leurs responsabilités en matière de LCB/FT est un dispositif de contrôle et de sanction efficace. Or, celui-ci est altéré par le passeport européen.

Le passeport européen, en instaurant le régime de la libre prestation de services (LPS), prive les superviseurs nationaux d'une partie de leur capacité à agir

- Le passeport européen permet à une entreprise agréée dans un État membre de l'espace économique européen (pays d'origine) d'offrir ses services sur le territoire d'un autre État membre (pays d'accueil) :

a) soit en libre établissement (LE) à partir d'un établissement permanent dans le pays d'accueil – par exemple, une succursale ou une agence – et/ou en ayant recours à des agents ou à des distributeurs ;

b) soit en libre prestation de services (LPS) sans être établi dans le pays d'accueil, en proposant ses services en ligne.

Photo © Nancy PALMIERI/The New York Times-REDUX-REA

Bitbills, la première carte permettant un paiement en bitcoins (cette carte n'est plus produite depuis le 15 mai 2012).

« Il existe à ce jour une vingtaine de sociétés qui commercialisent des cartes "*bitcoin to plastic*". Elles sont immatriculées dans le monde entier. Plusieurs de ces sociétés s'appuient sur le même EME, immatriculé dans un territoire d'Outre-mer rattaché à l'Union européenne ».

- En libre établissement, les organismes financiers sont soumis aux réglementations nationales relatives à la LCB/FT et à la protection de la clientèle. En France, ceux qui ont recours à des agents ou à des distributeurs de monnaie électronique doivent désigner un correspondant permanent, dont la fonction est d'être l'interlocuteur de Tracfin et de l'ACPR [12].

Les autorités de supervision françaises sont compétentes pour contrôler le respect de ces dispositions. L'ACPR contrôle et sanctionne des succursales exerçant en libre établissement et, depuis 2016, elle procède aux contrôles de réseaux d'agents et de distributeurs.

- En revanche, en libre prestation de services, le superviseur national n'est pas compétent pour contrôler les établissements étrangers exerçant sur son territoire. Ceux-ci doivent, en effet, se conformer à la réglementation de leur pays d'origine. En cas de doute, les autorités du pays d'accueil peuvent alerter les autorités du pays d'origine. Celles-ci ne sont pas toujours coopératives, ni même réactives.

En ce sens, la libre prestation de services représente un risque majeur. À la fin 2016, la France comptait 594 établissements de paiement ou de monnaie électronique opérant sur son territoire, dont 54 établissements agréés par l'ACPR, 48 exerçant sous le régime du libre établissement et 492 exerçant sous le régime de la libre prestation de services [13]. Une harmonisation du niveau d'exigence des différents superviseurs de l'espace économique européen (EEE) devient indispensable.

- Le Brexit représente un enjeu important pour l'avenir du dispositif européen de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB/FT). La plupart des établissements agréés au Royaume-Uni et opérant en Europe sous le régime de la LPS seront vraisemblablement contraints d'obtenir un nouvel agrément dans un autre pays de l'Union.

La fiabilité de certains prestataires de paiement implantés en Europe peut être mise en doute

- Tracfin observe que certains établissements implantés au sein de l'Union européenne et comptant des millions d'utilisateurs pourraient être contrôlés par des organisations criminelles. Ils sont souvent agréés au Royaume-Uni, après avoir essuyé des refus dans d'autres pays de l'Union. Ainsi, un établissement est lié à une société connue pour avoir participé à des opérations de fraude au détriment des banques de son pays. D'autres pourraient avoir pour bénéficiaires effectifs des personnes soumises à des sanctions financières de l'Union européenne et/ou connues pour leurs activités criminelles.

(12) Art. L.561-3 VI du CMF.
(13) Chiffres ACPR au 1er janvier 2017.

Tracfin a enquêté sur un réseau d'escroquerie *via* des sites de *trading* de devises (Forex) ou d'options binaires. Les investisseurs particuliers adressaient leurs paiements vers un compte bancaire ouvert en France par un établissement de paiement (EP) agréé dans un pays membre de l'UE. Celui-ci virait les fonds vers un compte étranger ouvert par un établissement de monnaie électronique (EME) agréé dans un autre pays de l'Union. L'EP s'est révélé être le client unique de l'EME, qui était lui-même contrôlé par des escrocs. Les fonds étaient *in fine* virés sur des comptes *offshore* détenus par les gestionnaires des sites. La juxtaposition d'un EP et d'un EME constituait un empilage de flux financiers marquant une volonté d'opacification.

- D'autres EME localisés en dehors de l'Union européenne font de la garantie de l'anonymat un argument commercial central. Depuis deux ans se développent les cartes de paiement en monnaie réelle adossées à des portefeuilles en bitcoins. Ces cartes fonctionnant sur le réseau VISA sont dites « *bitcoin to plastic* ». Les possibilités de rechargement sont élevées, voire illimitées lorsque l'identité du titulaire est vérifiée, Le sérieux des procédures de vérification d'identité n'est cependant pas toujours acquis.

Ces cartes sont utilisées en fin de chaîne par les criminels pour retirer en espèces des profits illicitement acquis en bitcoins, issus de trafics de stupéfiants, d'armes ou de données bancaires vendus sur le *darknet*. Les trafiquants centralisent les bitcoins obtenus sur un portefeuille dédié, auquel est rattachée une carte de paiement en monnaie réelle.

Il existe à ce jour une vingtaine de sociétés qui commercialisent des cartes « *bitcoin to plastic* ». Elles sont immatriculées dans le monde entier. Plusieurs de ces sociétés s'appuient sur le même EME, immatriculé dans un territoire d'Outre-mer rattaché à l'Union européenne.

Ainsi, l'accélération de la révolution digitale et le développement de la monnaie électronique constituent un défi en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Les banques perdent certaines données utiles à l'analyse des opérations client, tandis que la culture de conformité des nouveaux acteurs reste à développer. Le manque d'harmonisation internationale en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (LCB/FT) limite l'efficacité du dispositif. Seuls la poursuite des discussions internationales entre autorités de supervision et le renforcement de la coopération entre cellules nationales de renseignement financier permettront de conforter les avancées permises par les mesures prises par la France en 2016.