Chronique

Nouveaux moyens de paiement, banque digitale et protection des données

PIERRE STORRER*
Avocat au Barreau
de Paris
Kramer Levin Naftalis
& Frankel LLP

MYRIAM ROUSSILLE
Agrégée des facultés de Droit
Professeur
Université du Mans
IRJS Sorbonne Affaires-Finance

Tempête sur le droit de la lutte contre le financement du terrorisme

Commentaire de Pierre Storrer

1. Plan d'action européen. À peine publiée, déjà dépassée : tel est le sort qui semble réservé à la 4e directive Antiblanchiment[1], tôt rattrapée par l'actualité terroriste. On s'épargnera le débat, sans doute malséant, autour de ces textes, censément généraux (directives, lois), qui sans cesse courent après l'émotion, au risque de ne plus être que de circonstance, c'est-à-dire plus grand-chose. L'état d'urgence est aussi juridique.

Toujours est-il que la Commission européenne a publié, le 2 février 2016 – et dans le sillage d'une précédente[2] –, une communication relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme[3]. L'information principale à retenir de ce texte est l'invitation faite aux États d'avancer au 4e trimestre 2016 au plus tard la date de transposition de la 4e directive (au lieu du 26 juin 2017). Nous retiendrons ensuite l'engagement de la Commission de proposer, d'ici au 2e trimestre 2016 au plus tard, la modification de certains points de la directive, dont nous évoquerons les principaux.

2. Monnaies virtuelles et monnaie électronique. C'est de lutte contre l'anonymat dont il est question, poursuivant ainsi la stigmatisation des monnaies « alternatives » (mais l'argent liquide n'est pas épargné non plus). « *Le point critique à cet égard*, observe la Commission, *n'est pas tant les formes de paiement elles-mêmes que le fait qu'elles puissent être utilisées anonymement* » (p. 4).

La première mesure envisagée est de réglementer les « *plates-formes de change de monnaies virtuelles* », sorte de *shadow banking* moderne[4] : « Les plates-formes de change de monnaies virtuelles peuvent être considérées comme des bureaux de change "électroniques" qui échangent des monnaies virtuelles contre des monnaies à cours forcé. Les fournisseurs de portefeuilles de monnaie virtuelle détiennent des comptes en monnaie virtuelle au nom de leurs clients. Dans le monde des monnaies virtuelles, ils sont l'équivalent d'une banque proposant un compte courant sur lequel peuvent être effectués des dépôts de monnaie à cours forcé. Ils stockent les monnaies virtuelles et autorisent leur transfert vers d'autres portefeuilles de monnaie virtuelle/comptes en monnaie virtuelle » (p. 5)[5]. Aussi

1. Dir. (UE) 2015/849, 20 mai 2015, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Cf. P. Storrer, « Lutte antiblanchiment : le pas de deux du législateur européen », *Revue Banque* n° 786, juill.-août 2015, p. 72.
2. Le programme européen en matière de sécurité, 28 avr. 2015, COM(2015) 185 final.
3. COM(2016) 50 final. On notera que, parallèlement, a été publiée le 2 décembre 2015, une proposition de directive relative à la lutte contre le terrorisme, qui dépasse donc largement la question de son financement.
4. Cf. Livre Vert de la Commission, *Le Système bancaire parallèle*, COM(2012) 102 final, 19 mars 2012.
5. Comp. FAFT Report, *Virtual Currencies, Key Definitions and Potential AML/CFT Risks*, juin 2014.

* Les propos de l'auteur n'engagent que celui-ci.

bien est-il prévu de « rouvrir », en quelque sorte, pas moins de deux directives majeures en cours de transposition : la 4e directive Antiblanchiment, dont le champ d'application serait étendu auxdites plates-formes et à leurs opérations de change de monnaies virtuelles ; la DSP 2 [6] et ses règles en matière d'agrément et de surveillance, faisant donc de ces plates-formes, voire des « *fournisseurs de portefeuilles de monnaie virtuelle* » [7], si l'on comprend bien, de nouveaux prestataires de services de paiement (PSP).

Haro, ensuite, sur les cartes prépayées, et donc sur la monnaie électronique qu'elles stockent, dans la mesure où elles sont manifestement utilisées pour financer anonymement la logistique d'attentats terroristes. Haro dans la mesure où, en France – et ce plan d'action européen a été adopté sous la pression française –, est actuellement débattu le projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (dit projet de loi « Urvoas »), qui entend à la fois plafonner la valeur monétaire maximale des cartes prépayées [8] et obliger leurs émetteurs à recueillir et conserver les informations et données techniques relatives à l'activation, au chargement et à l'utilisation de la monnaie électronique au moyen de telles cartes. Après les fameux «KYC» (*know your customer*) et «KYB» (*know your business*), verra-t-on éclore un «KYT» (*know your technology*) ? Mais ce qui est intéressant dans la proposition européenne c'est que, en contrepoint du danger présenté par les cartes prépayées, est reconnue, peut-être pour la première fois, leur « *valeur sociale* », imposant dès lors une balance des intérêts plutôt qu'une abrupte condamnation : « *Les cartes prépayées permettent à des personnes vulnérables sur le plan économique ou exclues financièrement de disposer d'un moyen de paiement utilisable hors ligne (comme de l'argent liquide) et, surtout, en ligne, pour acheter des biens et des services sur l'internet. Certaines personnes emploient des cartes prépayées pour limiter le risque de fraude lors d'achats sur l'internet, leur exposition étant limitée au montant de monnaie électronique présent sur la carte. Plusieurs États membres ont recours à ces instruments pour verser les prestations sociales. Par ailleurs, certaines personnes considèrent l'anonymat que certaines cartes prépayées confèrent à leur titulaire comme un moyen avantageux de protéger leur vie privée – problématique qui prend de l'ampleur en ce qui concerne les opérations effectuées sur le* web *– bien que l'anonymat ait également été recherché ou utilisé à mauvais escient pour réaliser des actions illégales* » (p. 6). Des modifications de la directive Antiblanchiment seront proposées par la Commission.

3. Des FICOBA nationaux – Un SSFT européen ? On se souvient que le ministre Michel Sapin avait annoncé en mars 2015, puis confirmé en novembre, sa volonté de « *donner un rôle central à FICOBA et y rattacher les comptes de type Nickel* » (les comptes de paiement donc). Cette mesure devait être effective au 1er janvier 2016, sous l'impulsion de la Direction générale des Finances publiques, gestionnaire de ce fichier. Cela n'est sans doute pas étranger à l'engagement pris par la Commission, dans son plan d'action, de proposer, au prix d'une modification de la 4e directive Antiblanchiment, l'établissement de registres nationaux centralisés des comptes bancaires et des comptes de paiement (ou systèmes électroniques de recherches de données), accessibles aux cellules de renseignement financier (CRF) et autorités compétentes, mais aussi à d'autres et pour d'autres enquêtes.

Et puis ceci, pour terminer [9] : le fameux accord SWIFT ou TFTP (accord entre l'Union européenne et les États-Unis concernant le programme de surveillance du financement du terrorisme) devrait-il être doublé par un équivalent européen, par un Système de surveillance du financement du terrorisme (SSFT) de l'UE ? La Commission l'avait envisagé en son temps pour finalement y renoncer, après que l'analyse d'impact réalisée avait conclu à une menace disproportionnée pour la protection des données à caractère personnel [10]. Voilà un beau sujet de réflexion à l'heure de la prochaine publication du règlement général sur la protection des données ou de celle du « bouclier de protection des données UE-États-Unis » (*EU-US Privacy Shield*). Sujet que le plan d'action sous commentaire semble vouloir rouvrir, ne serait-ce que pour tracer les transactions que l'accord TFTP ne couvre pas, pas moins que les paiements en euros à l'intérieur de l'Union. ■

6. Dir. (UE) 2015/2366, 25 nov. 2015, concernant les services de paiement dans le marché intérieur. Cf. M. Roussille et P. Storrer, « L'économie numérique à l'heure de la DSP 2.0 », *Banque et Droit* n° 165, janv.-févr. 2016, p. 67 ; P. Storrer, « Abécédaire de la DSP 2 », *Revue Banque* n° 793, févr. 2016, p. 76.

7. « *Un fournisseur de portefeuille est une entité qui fournit des moyens (application logicielle ou autre mécanisme/support) de détenir, de stocker et de transférer des* bitcoins *ou toute autre monnaie virtuelle (rapport du GAFI sur les monnaies virtuelles)* » (p. 6).

8. Cependant qu'a déjà été plafonné à 1 000 euros (3 000 euros auparavant) le paiement en espèces ou au moyen de monnaie électronique : CMF, art. D. 112-3, rédac. D. n° 2015-741, 24 juin 2015.

9. On aurait pu évoquer aussi l'invitation à un accès facilité des CRF aux informations et à l'échange de celles-ci entre lesdites CRF.

10. Communication de la Commission, « Un système européen de surveillance du financement du terrorisme », SSFT de l'UE, 27 nov. 2013, COM(2013) 842 final.