## Protection des données personnelles

# Exploitation des données de paiement par les établissements financiers : point de vue juridique rapide

**PIERRE STORRER**
Avocat à la Cour
FERAL-SCHUHL/ SAINTE-MARIE

La question de l'exploitation *marketing* des données de paiement par les banques est d'actualité. Il y a cependant un pas entre son opportunité commerciale et sa légitimité juridique…

L'exploitation des informations et données portées par les paiements est un sujet d'importance ; il mériterait une étude approfondie, ne serait-ce que sous l'angle de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT). Où l'on s'apercevrait que le droit de la LCB-FT ne s'articule pas bien avec le droit de la protection des données personnelles. Où l'on se féliciterait, néanmoins, que la proposition de « quatrième directive Antiblanchiment », adoptée par la Commission européenne le 5 février 2013, suggère d'introduire, dans la directive, des dispositions visant à clarifier l'interaction entre les exigences relatives, d'une part, à la LCB-FT et, d'autre part, à la protection des données. Car, ici, la logique est renversée : la question n'est plus celle d'une « opportunité » *marketing* d'exploitation des données de paiement, mais de l'obligation, pour les établissements financiers, de connaître leurs clients (le fameux *Know your Client* – KYC).

### La légitimité des traitements automatisés de données de paiement

Alors, jusqu'où les banques (et autres PSP) peuvent-elles aller dans l'exploitation des données de paiement ? Et peuvent-elles même y songer ? On sait que la CNIL reconnaît la « *légitimité* » des « *traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects* » (c'est l'intitulé de sa norme simplifiée 48, révisée le 21 juin 2012), parmi lesquelles figurent les « *données relatives aux moyens de paiement* » (relevé d'identité postale ou bancaire, numéro de chèque, numéro de carte bancaire, date de fin de validité de la carte bancaire) ou les « *données relatives à la transaction* » (numéro de la transaction, détail de l'achat, de l'abonnement, du bien ou du service souscrit). Seulement, les établissements bancaires ou assimilés (ainsi que les entreprises d'assurances, de santé ou d'éducation) sont expressément exclus du bénéfice de cette norme simplifiée.

### L'obstacle du secret professionnel ?

Par suite, les PSP peuvent-ils envisager d'exploiter à des fins *marketing*, notamment en les communiquant à des tiers, les données de paiement qu'ils collectent ? On leur oppose immédiatement le secret professionnel, auquel ils sont légalement tenus, établissements de crédit (art. L. 511-33 CMF) comme, depuis la transposition de la DME 2 par la loi du 28 janvier 2013, dans des termes communs, établissements de paiement (art. L. 522-19 CMF) et établissements de monnaie électronique (art. L. 526-35 CMF). Certes, mais les uns et les autres « *peuvent communiquer des informations couvertes par le secret professionnel au cas par cas et uniquement lorsque les personnes concernées leur ont expressément permis de le faire* », disposition commune aux trois articles précités. Car « *le secret professionnel du banquier est de simple protection de son client de sorte que celui-ci peut y renoncer* » (Cass. com. 11 avr. 1995, *Bull. civ.* IV, n° 121) ; car « *le client d'une banque peut toujours renoncer à la protection du secret bancaire à condition d'y consentir librement et de manière expresse au vu d'une information complète lui permettant de prendre sa décision de manière éclairée* » (CE 30 déc. 2009, n° 306173, *Rec. Lebon*).

Alors ? La révision européenne en cours de la protection des données à caractère personnel gagnerait sans doute à se pencher davantage sur la question sensible de l'exploitation des données (sensibles) de paiement… ■