David Jeanneret

Résumé

1 En général, les grands criminels recherchent toujours à pouvoir conserver un certain anonymat lorsqu'ils commettent des crimes. Actuellement, tous les moyens de communication à distance permettent à ces criminels d'agir sur toute la planète et de camoufler leurs opérations illicites. Dans ce contexte, les moyens de paiement à distance constituent une aubaine pour eux. Tous les systèmes de paiement à distance présentent de nombreux avantages non seulement pour un pirate qui désire commettre plusieurs fraudes à la carte de crédit ou de débit, mais aussi pour un criminel qui désire blanchir de l'argent.

2 Dans cet environnement criminel, nous avons voulu savoir si la certification électronique permet de transférer les risques de la banque vers le titulaire du certificat électronique ou vers l'autorité de certification. Dans l'affirmative, la banque n'engagera pas sa responsabilité civile en se servant d'un système de paiement à distance dans la mesure où la banque ne saurait répondre de la perte des moyens d'identification de son client. Dans un second temps, nous avons examiné si les techniques de cryptographie permettraient aux banques d'identifier leur cocontractant et l'ayant droit économique des fonds déposés, sans violer leur obligation de diligence en matière de blanchiment d'argent et sans contrevenir aux recommandations du GAFI[1].

3 Même si les systèmes de paiement à distance avec ou sans utilisation d'une carte[2] génèrent des menaces différentes, nous avons mis en évidence dans cette étude que la certification électronique permet de réduire les risques de fraude, pour autant qu'elle soit accompagnée d'autres mesures de gestion des risques[3]. Grâce à la certification, la banque peut, en principe, transférer le risque sur le titulaire du certificat électronique pour autant qu'elle puisse prouver que la cause du dommage provient du vol de la clé privée, de la signature électronique ou du certificat. Toutefois, il faut préciser que d'une part, il ne s'agit que du risque survenant en raison d'un mauvais management des clés privée et publique et que d'autre part, l'information insuffisante des internautes sur l'utilisation de ces techniques de cryptographie empêche de faire supporter les risques de perte et de vol de la clé privée par la partie la plus faible[4]. Dans cette seconde hypothèse, l'autorité de certification devra en répondre et éventuellement, la banque soit pour son auxiliaire (art. 101 CO), soit pour le choix de son partenaire, qui en tant qu'autorité de certification reconnue, a négligé son devoir d'information (« culpa in eligendo » dans le contrat de mandat).

4 En raison du manque de connaissance technique des utilisateurs, les banques penchent actuellement pour l'utilisation de carte à puce qui intègrent la gestion des clés. Dans cette hypothèse, la gestion de la clé privée comme publique est assumée par l'organisme d'émission ce qui permet à première vue d'éviter de nombreuses fraudes. Toutefois, en se fondant sur l'étude qui évalue l'implémentation de la directive 97/489/CE aux systèmes de

1 Nous vous recommandons de consulter l'article de l'ordonnance de la CFB en matière de lutte contre le blanchiment d'argent (OBA-CFB) ainsi que la „recommandation spéciale VII: virements électroniques" du 14 février 2003, édictée par le GAFI/FATF (htpp://www.fatf-gafi.org)

2 CEN/ISSS Electronic Commerce, Ewallet CWA, Authentication and transaction support-the role of eWallet Main Report–Draft, 16 octobre 2002, p. 5 ss.

3 Cf. Annexe n° 19: IT-Governance.

4 Cf. Recommandation de la CFB relative à l'outsourcing.

paiement à distance[5], il est douteux que les juges suisses ne s'inspirent de ces règles et des critères établis par cette étude, lorsqu'ils devront évaluer un manquement à un devoir d'information des clients.

5 Par conséquent, si les banques ne mettent pas en place un système de gestion préventive et réactive des risques, elles risquent de subir non seulement des pertes financières et de réputation importante, mais aussi de se faire actionner en justice. C'est pourquoi, il est impératif que les banques soient en mesure non seulement éviter de s'engager dans des opérations à risque, mais encore de détecter toute anomalie dans une transaction.

6 Pour réduire la survenance des risques opérationnels, de réputation et juridiques, les banques doivent ainsi combiner plusieurs méthodes de prévention et de détection des risques[6]. Elles doivent non seulement prévenir pour empêcher la commission d'un crime, tel que la fraude informatique, mais aussi réagir adéquatement en cas de survenance d'un risque. Sans une information effective, efficiente et régulièrement mise à jour, l'organe de révision sera bien aviser d'imposer aux banques des provisions pour assurer la survie de l'entreprise. De même, il est indispensable de séparer le « front office » informatique du « back office » informatique. Cette mesure permettra d'éviter un risque de corruption privée des informaticiens de la banque. À côté de ces mesures préventives, les banques doivent implémenter toute une panoplie de mesures réactives. Sans un traçage et une surveillance accrue des risques, il leur sera impossible de fournir la moindre information pertinente sur l'auteur d'un crime à une autorité de poursuite pénale. Si elles ne fixent pas des limites à des soldes tant sur les comptes des commerçants que sur celui des consommateurs, elles courent le risque que des sommes faramineuses soient blanchies au travers des systèmes électroniques de paiement fournis par les exploitants de sites de ventes aux enchères. Enfin, il est indispensable qu'elles mettent en place un système d'analyse statistique des opérations pour détecter non seulement des opérations à risque (« scoring »), mais aussi des opérations suspectes. Pour faciliter le travail des banques, une norme ISO comme BIC[7] (ISO 9364) ou IBAN[8] ou IBEI[9] devrait être créée pour identifier les autorités de certification accréditée par un État.

7 Enfin, si une banque choisit de nouer des relations d'affaires par voie électronique, elle devra disposer d'une grande base de données et d'un système efficient de stockage des données. En outre, elle devra être en mesure de fournir rapidement toutes les informations disponibles aux autorités de poursuite pénale si elle entend respecter son devoir de diligence. À côté de son engagement à éviter tout entrave de l'action pénale, elle sera aussi bien avisée de former ses auxiliaires pour qu'ils sachent éclaircir l'arrière-plan économique des clients en cas de soupçons. Ceux-ci devront savoir évaluer une transaction suspectes, clarifier la situation avec le client en posant les bonnes questions et sur la base de leur évaluation, agir correctement et conformément aux procédures et processus internes à la banque.

8 De cette façon, soit la transaction suspecte est régulière, soit des doutes persistent sans être suffisant pour fonder un soupçon, soit le conseiller a des soupçons fondés. En général, la banque pourra décider de mettre fin à la relation d'affaires et demander au client de transférer ces fonds dans un autre établissement. En cas de transfert, elle ne doit pas accepter de retrait

---

5 Cf. Annexe n° 6.

6 Comp. Daniel Heller, Die Rolle der Nationalbank in bargeldlosen Zahlungsverkehr", in: Quartelheft der schweizerischen Nationalbank 1/2003.

7 Banking telecommunications messages – bank identifier code (ISO 9364).

8 International bank account number (ISO 13616).

9 International business entity identifier (ISO 13735).

en espèces et dans tous les cas, elle doit veiller à conserver la trace du transfert (« paper trail »). Dans la deuxième hypothèse, la banque doit aviser le Bureau de communication en matière de blanchiment d'argent. Dans le deuxième cas, le conseiller doit avertir le « compliance officer » qui devra examiner la situation, en prenant en compte toutes les informations disponibles sur le client, et remettre un rapport sur les résultats de son enquête au président du conseil d'administration. Tout manquement à cette obligation pourrait avoir non seulement des conséquences pécuniaires en raison de l'amende prononcée, mais aussi pourrait entraîner des problèmes au niveau de l'autorisation d'exercer une activité bancaire.

9 En conclusion, la certification électronique ne permet de réduire que partiellement la responsabilité civile et pénale des banques. Toutefois, en combinant la certification électronique avec des mesures de gestion préventive et réactive des risques, les banques pourront affirmer qu'elles ont la situation en main et qu'en cas de survenance d'un risque, elles seront capable de réduire le dommage qu'elles pourraient subir. Par conséquent, la responsabilité des banques n'est réduite en principe qu'en cas de vol ou de mauvaise administration des clés privé et publique des utilisateurs. Pour le reste, la responsabilité de la banque ne peut être réduite que si elles mettent en place un système de management préventif et réactif des risques.

10 En revanche, si le projet d'art. 14 al. 2^{bis} P-CO entre en vigueur dans sa teneur actuelle et s'il s'agit d'un chèque électronique, l'application des dispositions du droit des papiers-valeurs relatives aux chèques entraînera assurément un traitement différencié des questions de responsabilité. Dans un tel cas, il conviendra d'appliquer l'art. 1132 CO qui met le dommage à la charge de la banque, sauf en cas de faute grave du titulaire du compte. Si le titulaire ne prend pas des mesures pour éviter de se faire voler sa clé privée, il commet assurément une faute grave.