

Les services bancaires électroniques et la sécurité

Par Volkan Dulger du Cabinet d'avocats Dulger

10 Juin 2009

Les services bancaires électroniques est un secteur émergent en Turquie en raison des faibles coûts d'exploitation qui s'y attachent.

En plus des distributeurs de billets de banques électroniques et des transactions par téléphone, le secteur bancaire propose maintenant ses services par le biais d'Internet à travers une large gamme de services bancaires à faibles coûts. De nombreux investissements ont été réalisés dans ce domaine récemment. En plus des transactions destinées aux clients particuliers, la technologie d'information est également utilisée pour des affaires interbancaires comme pour le système électronique de liquidation des chèques et le système de débit direct. D'où un profond changement dans la structure du secteur bancaire due au fait qu'aucune banque traditionnelle ne peut survivre sans adopter une stratégie pour Internet.

De nos jours, les banques turques sont conscientes du fait mentionné précédemment et offrent une large gamme de services appelés « Services bancaires en ligne » de la part de leurs branches Internet. Comme les banques disposent de leurs propres sites Internet, les clients peuvent gérer leurs transactions. Il s'agira par exemple des opérations avec cartes de crédit, des virements de compte à compte, des dépôts de demandes de crédit, de l'ouverture d'un nouveau compte bancaire... en pratique, la banque conclut un contrat avec ses clients dans le cadre des dispositions bancaires générales et fournissent un mot de passe pour accéder au système. Avec toutes ces options à portée de clic, les clients privilégient ce moyen et utilisent leurs cartes de crédit pour les transactions en ligne. Ce qui améliore le rendement et l'efficacité de la banque en ligne. Il est donc nécessaire d'examiner les mesures de sécurité prévues pour éradiquer les risques de fraude dans le cadre des services bancaires électroniques.

Pour fournir plus de sécurité pour les services bancaires sur Internet, certains programmes appelés SSL (Secure Socket Layer) and SET (Secure Electronic Transactions) ont été développés. Ces programmes sont largement utilisés en Turquie par la plupart des banques. Chaque partie, dans le cadre du commerce électronique, ne peut voir le numéro de la carte de l'autre. Ces programmes chiffrent chaque donnée entre le client (porteur de la carte), la société et la banque. De plus, personne ne peut décoder les mots de passe ou n'importe quelle autre donnée. Un autre système consiste à octroyer l'e-carte bancaire (carte virtuelle). Elle ne comporte aucune limite et par son utilisation, le client ne fait qu'autoriser la banque à retirer la somme de son compte.

Alors que les banques bénéficient de la technologie afin de mieux protéger leurs systèmes et pour prévenir toute interférence illégale, la législation actuellement en vigueur leur impose des responsabilités et obligations. D'abord, les banques ont l'obligation d'informer leurs clients des nouveaux systèmes technologiques qu'elle utilise et des risques existants. La banque doit aussi assister ses clients dans la protection de la sécurité de leurs comptes. A ce propos et à titre d'exemple, chaque fois que l'on accède au site internet de la banque, cette dernière annonce la dernière transaction opérée avec la carte bancaire en précisant sa date ainsi que d'autres détails

avant toute nouvelle autre transaction. De plus, les clients doivent être informés des dépenses excédant leurs limites ou les ordres donnés à partir d'adresses IP différentes de celle fréquemment utilisée. L'autre obligation des banques consiste à prendre des mesures concernant la fiabilité du système et la prévention des erreurs de données. Si jamais une erreur survient, c'est la banque qui devra réparer le dommage éventuel.

En raison de la survenance d'un nombre important de problèmes du fait de l'usage des cartes de crédit, le Code des banques et Cartes de crédit N°5464 est entré en vigueur le 23 février 2006. La 8^e clause prévoit que les éditeurs de cartes bancaires ont l'obligation de mettre en œuvre un système garantissant une utilisation sécurisée des cartes et de prendre les mesures pertinentes pour classer les notifications, plaintes et réclamations. En plus de cette disposition, l'article 15 dispose qu'à la fin de chaque usage d'une carte de crédit, le détenteur de la carte devra recevoir un reçu faisant preuve de l'achat effectué. Les banques devront quant à elles, confirmer au vendeur le paiement du prix.

Un autre problème concernant la banque en ligne concerne le transfert d'argent des comptes de dépôt des clients vers d'autres comptes par des tiers qui décodent les mots de passe. Ces activités frauduleuses sont la plupart du temps effectuées par des programmes espions répandus sur Internet. Les banques sont fréquemment confrontées à des cas où les comptes bancaires de leurs clients sont vidés par le biais d'une intervention illégale. Dans ce cas, les banques cherchent à se protéger en prétendant qu'elles ne sont pas responsables de ces transactions illégales à travers des clauses de non responsabilité incluses dans le contrat qu'elles ont conclu avec leur client. Cependant, la Cour d'Appel a jugé que les banques sont aussi responsables de prendre toutes les mesures nécessaires pour fournir une protection suffisante du client face à ces intrusions via Internet.

De plus de la législation en vigueur concernant les transactions bancaires, l'interprétation par les tribunaux de ces législations ou de toute faille possible incluse dans ces législations se fait généralement en faveur du client, dans le but de lui fournir une protection suffisante du moment qu'il est plus vulnérable que la banque. Cela ne veut pas pour autant dire que les détenteurs des cartes bancaires n'ont aucune responsabilité vis-à-vis de leurs transactions bancaires électroniques. En effet, un détenteur d'un compte de dépôt est également responsable de protéger son compte.

Dans une affaire récente devant la Cour d'Appel, le compte bancaire internet du demandeur a été victime de plusieurs tentatives de déchiffrement par un inconnu et l'argent présent sur le compte a été transféré vers un autre par seize transactions différentes. Le défendeur (la banque) reproche à son client d'être négligent, de ne pas utiliser le clavier virtuel et de ne pas protéger son ordinateur personnel. La Cour d'Appel a retenu la négligence du demandeur qui n'obéissait pas aux mesures de sécurité appliquées par la banque. Selon l'arrêt, les banques sont responsables des légères négligences découlant du non respect de l'obligation de sécurité en tant que des institutions de confiance. La base de cette appréciation repose sur la « théorie de confiance » prévue par l'article 2 du Code civil turque. Toutefois, il est injuste de ne retenir que la seule responsabilité des banques pour cette intervention illégale sur le système informatique du client alors qu'il ne s'agit pas d'un domaine contrôlé par les banques (Cour d'Appel M.2006/7341, D.22/06/2006). Il existe d'autres décisions qui retiennent la responsabilité des clients qui ne prennent pas suffisamment soin des outils de sécurité de leurs ordinateurs comme les mots de passe qui sont fréquemment fournis pour les services bancaires en ligne. Dans une affaire, la Cour d'Appel avait retenu que la banque n'était

pas responsable pour le dommage subi par un client dont le mot de passe a été déchiffré parce qu'il ne protégeait pas suffisamment son ordinateur (Cour d'Appel M.2003/7705, D.12/09/2003).

En effet, malgré les décisions mentionnées ci-dessus, il n'est pas toujours facile de déterminer de qui émane la faille de sécurité. Le manque de jurisprudence dans ce domaine est un autre problème pour les praticiens pour interpréter cette question. Cependant, en lisant entre les lignes des interprétations de la Cour d'Appel, nous pourrions affirmer qu'en cas d'une intervention illégale sur un compte bancaire, la fourniture de preuve est un premier pas important pour la protection des droits du client dans le but de prouver qu'il a entrepris toutes les mesures nécessaires pour assurer la sécurité de son système informatique. La Cour d'appel considère en effet que les ordinateurs des clients réclamant une compensation doivent être équipés d'un logiciel anti virus pour les protéger des intrusions extérieures.

Pour plus d'informations à propos de ce sujet, veuillez contacter Volkan Dulger du Cabinet d'avocats Dulger par téléphone (+90 212 217 82 98), par fax (+90 212 217 79 34) ou par e-mail (Volkan.dulger@dulger.av.tr).