Les banques ont-elles une obligation de remboursement en cas de phishing/hameçonnage ?

Le phishing (hameçonnage) est une forme de cybercriminalité dans laquelle la victime est approchée par e-mail, sms, etc. dans lesquels l'escroc se fait passer pour quelqu'un d'autre (une banque, un fournisseur d'énergie, une société de technologie, mais aussi un ami ou un membre de la famille).

Le but est de "pêcher" ("phishing" en anglais) des données sensibles, comme des informations personnelles, des mots de passe, des données de carte bancaire ou de crédit afin d'avoir accès notamment aux comptes de la victime et ainsi lui dérober son argent.

En cas de phishing, la banque est dans l'obligation de rembourser le client victime pour autant que les conditions prévues par le livre VII du Code de droit économique soient réunies.

Les articles VII.41 et suivants du CDE traitent en effet des opérations de paiement non autorisées, c'est-à-dire des opérations de paiement effectuées sans le consentement libre du payeur.

L'article VII.43 du CDE prévoit qu'en cas d'opération de paiement non autorisée, la banque doit rembourser immédiatement au client le montant de l'opération non autorisée. Ce remboursement immédiat doit être effectué dès que la banque a eu connaissance de l'opération ou en a été informée. La loi prévoit que le remboursement doit être effectué au plus tard à la fin du 1er jour ouvrable suivant.

Toutefois, cette obligation de remboursement immédiat ne s'applique pas si la banque a de bonnes raisons de soupçonner une fraude dans le chef du client et si elle communique ces

raisons par écrit au SPF Economie. Le cas échéant, la banque a la possibilité d'effectuer une enquête à ce sujet dans un délai raisonnable, avant de rembourser le client.

En outre, pour que cet article VII.43 soit applicable, et que le client puisse donc obtenir remboursement, il faut que le client informe la banque sans délai après la découverte de la fraude et au plus tard 13 mois après le débit (article VII.38 CDE).

La loi établit une distinction entre les opérations qui ont eu lieu avant et après la notification de la perte, du vol, le détournement ou l'utilisation non autorisée de l'instrument de paiement.

Si l'opération de paiement non autorisée intervient **après** la notification, le client ne supporte aucune conséquence financière, sauf si la banque parvient à démontrer que le client a agi frauduleusement (art. VII.44, §3 CDE).

Si l'opération de paiement non autorisée intervient **avant** la notification, le client ne doit supporter la perte qu'à concurrence d'un montant de 50 € (art. VII.44, §1, al 1 CDE). Toutefois, il ne devra supporter aucune perte financière si :

- La banque n'exige pas une authentification forte du client, à moins qu'il ait agi frauduleusement (art. VII.44, §2 CDE) ;
- La perte, le vol ou le détournement de l'instrument de paiement ne pouvait être détecté par le client avant le paiement, sauf si le client a agi frauduleusement (art. VII.44, §1, al 2 CDE).

Par contre, si le client a subi des pertes à la suite d'opérations de paiement non autorisées du fait d'avoir agi frauduleusement ou de ne pas avoir respecté certaines obligations (art. VII.38 CDE), intentionnellement ou à la suite d'une négligence grave, il doit en supporter toutes les pertes.

Concernant la notion de "négligence grave", la loi prévoit que son appréciation se fait en tenant compte de l'ensemble des circonstances de fait.

De plus, elle prévoit que sont notamment considérés comme négligences graves, les comportements suivants :

- Le fait, pour le payeur, de noter ses données de sécurité personnalisées, telles que son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou document que le payeur conserve ou emporte avec lui avec l'instrument de paiement.

- Le fait pour le payeur de ne pas avoir notifié au prestataire de services de paiement, ou à l'entité désignée par celui-ci, la perte ou le vol de l'instrument de paiement.

La charge de la preuve en matière de fraude, d'intention ou de négligence grave incombe au prestataire de services de paiement.

Les travaux préparatoires de la loi indiquent que l'article VII. 44, §1, alinéa 2 peut être appliqué, par exemple, dans les cas de piratage et d'hameçonnage (phishing).

Selon la doctrine, l'existence ou non d'une négligence grave dans le chef de la victime de la fraude n'est pas pertinente dans l'hypothèse où le payeur ne pouvait pas détecter la fraude au préalable. Cela signifie que lorsque l'article VII.44§1er alinéa 2 CDE s'applique, le payeur ne supportera aucune perte, même s'il a commis une négligence grave.

En matière de jurisprudence, la banque KBC a récemment été condamnée à rembourser des clients victimes de phishing.

Lorsqu'elles sont confrontées à des cas de phishing, les banques essayent d'imputer la négligence aux clients. S'il peut être démontré que le client aurait pu se rendre compte de la fraude, alors la banque n'a pas à rembourser les sommes perdues. C'est ce qu'à tenter la banque KBC dans deux dossiers mais les juges ne l'ont pas suivie et l'ont condamnée à rembourser 32.000 € à des clients victimes de fraude en ligne. Cela crée un précédent juridique pour les pertes d'argent en cas de fraudes dit d'hameçonnage.