Titre

Phishing : De la nécessaire analyse des circonstances pour apprécier la négligence grave de l'utilisateur d'un instrument de paiement

Résumé

La Cour de cassation consacre la nécessaire analyse des circonstances ayant entourées l'exécution d'une opération de paiement contestée pour juger de la conscience par l'utilisateur d'avoir fait l'objet d'un phishing et par conséquent de sa négligence grave (Cass. Com., 25 octobre 2017, n°16-11.644, Caisse fédérale du crédit mutuel Nord Europe c./ Madame X…)

Le phishing ou hameçonnage en matière bancaire est le procédé visant à récupérer des données personnelles sur internet avec l'objectif de détourner des fonds. Le moyen utilisé est l'usurpation d'identité, adaptée au support numérique. L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet (celui d'une banque ou d'un marchand en ligne). L'adresse URL du lien comprise dans le courriel est également « masquée » afin de paraître authentique.

Comme le reconnaissait le Médiateur auprès de la Fédération Bancaire Française (FBF) dans son rapport au titre de l'année 2016, les litiges portant sur des fraudes à la carte bancaire ou sur des paiements en ligne restent abondants.

Dans ce contexte une jurisprudence abondante est apparue au regard des conditions nécessaires à la prise en charge du remboursement des opérations de paiement non autorisées par le prestataire de services de paiement.

Deux visions s'affrontent, une première protectrice de l'utilisateur de l'instrument de paiement qui bénéficierait d'une indemnisation de principe et une seconde fondée sur le principe de responsabilité nécessitant une appréciation globale des circonstances dans lesquelles a été exécutée l'opération de paiement contestée.

Il est nécessaire de rappeler que ces contentieux trouvent leur source dans un régime juridique protecteur du client des établissements bancaires. Ainsi, les articles L133-18, L133-19 et L133-23 du Code monétaire et financier précisent qu'en cas d'opérations non autorisées, le prestataire de service rembourse immédiatement le montant de l'opération, sauf agissements frauduleux du consommateur ou s'il n'a pas satisfait intentionnellement ou par négligence grave à l'obligation qui lui incombe de prendre toutes les mesures raisonnables pour préserver la sécurité de ses dispositifs de sécurité personnalisés.

Ainsi, il revient au prestataire de service de prouver, grâce aux informations techniques en sa possession, que les opérations contestées ont été authentifiées, dûment enregistrées et comptabilisées.

La charge de la preuve de la négligence de l'utilisateur est depuis une décision de principe du 18 janvier 2017 appréciée de manière rigoriste.

La Cour de Cassation dans un arrêt rendu le 18 janvier 2017 a considéré que la charge de la preuve de la négligence grave des utilisateurs pèse sur les banques (Cass.com, 18 janvier 2017, n° 15-18.102). Il était ainsi considéré que « *cette preuve ne peut se déduire du seul fait que*

l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés ».

Cette position est critiquable au regard du droit communautaire originel.

Il convient de rappeler que l'article L133-23 du code monétaire et financier résulte de la transposition de l'article 59.2 de la Directive 2007/64/CE du 13 novembre 2007. L'article L133-23, alinéa 2 du code monétaire et financier dispose : *« Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération n'a pas été exécutée correctement, il incombe au prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée d'une déficience technique ou autre ».*

Certes l'article L133-23 précise en son alinéa 2 que *« L'utilisation de l'instrument de paiement telle qu'enregistrée ne suffit pas nécessairement en tant que telle à prouver que l'opération a été autorisée par le payeur ou que celui-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière ».*

S'il résulte effectivement de ces dernières dispositions que l'utilisation de l'instrument de paiement ne suffit pas nécessairement à établir la négligence ou la fraude, il n'en demeure pas moins que, a contrario, l'utilisation de l'instrument de paiement puisse suffire à prouver la négligence grave en fonction des circonstances particulières du litige qu'il appartiendra au juge du fond d'examiner.

En effet si l'on peut concevoir que les banques soient responsables des instruments de paiement qu'elles mettent à la disposition de leur client, il parait indispensable de leur laisser la possibilité de se dégager de toute responsabilité en cas de négligence grave de ces derniers.

Compte tenu de la difficulté de démontrer un manquement, il convient de tenir compte de l'ensemble des circonstances dans lesquelles ont eu lieu les opérations contestées afin d'établir si il y a eu négligence grave.

Cette position est d'ailleurs conforme au considérant 33 de la Directive 2007/64/CE du 13 novembre 2007 qui précise : *« Afin d'évaluer l'éventualité d'une négligence de la part de l'utilisateur, il convient de tenir compte de toutes les circonstances ».*

La position adoptée par la cour de cassation le 18 janvier 2017 est donc en contravention avec ces principes communautaires

Cependant la Cour de Cassation, dans un arrêt rendu le 31 mai 2016, avait déjà fait référence à un faisceau d'indices et donné raison à une cour d'Appel qui avait retenu la négligence grave du porteur d'une carte de paiement : opérations litigieuses effectuées sur une courte période et à de multiples reprises - composition du code confidentiel pour chaque opération - à la suite du dépôt de plainte, aucune infraction pénale n'avait été mise en évidence - aucune anomalie de fonctionnement bancaire n'avait eu lieu – les distributeurs de billets étant équipés de caméras de surveillance, l'utilisateur ne précisait pas si les données filmées avaient été exploitées – l'utilisateur n'établissait pas le fait qu'il n'avait pu effectuer les achats ou retraits contestés car ne se trouvant pas à l'endroit où ils avaient été effectués or ces paiements ayant été effectués sur une courte période il lui était facile d'établir qu'il n'avait pu être présent au DAB ou dans les commerces où sa carte avait été utilisée.

La cour de cassation dans arrêt du 25 octobre 2017 consacre le pouvoir d'appréciation des juges du fond

Il faut voir dans la décision du 25 octobre 2017 (Pourvoi n°16-11.644) Caisse fédérale du crédit mutuel Nord Europe c./ Madame X…) la consécration du pouvoir d'appréciation des juges du fond.

En l'espèce, Madame X …avait reçu deux SMS lui communiquant un code 3D Secure pour deux opérations qu'elle n'avait pas réalisées. Elle a alors immédiatement fait opposition à sa carte bancaire. Plus tard elle reconnaissait avoir répondu à un courriel émanant d'un émetteur se présentant comme SFR, et avoir transmis des informations relatives à sa carte bancaire, à savoir : ses nom, prénom, numéro de carte bancaire, date d'expiration, cryptogramme. Elle a contesté avoir transmis son code confidentiel.

La caisse de crédit mutuel bien que ne contestant pas que le paiement n'avait pas été autorisé a constaté que les opérations contestées avaient été réalisées en utilisant toutes les coordonnées de la carte bancaire et en renseignant le code 3D Secure.

Pour faire droit à la demande de Madame X…. , la juridiction de proximité de Calais a considéré : « Ces éléments bien que communiqués volontairement à X…, doivent être considérés comme ayant été détournés à son insu car ils ont été communiqués à une personne se présentant sous une fausse identité. Il ne peut être reproché à X….de ne pas avoir respecté les dispositions de l'article L.133-16 du code monétaire et financier ; En effet, elle n'a ni communiqué son code confidentiel, ni communiqué le code 3D Secure à 6 chiffres communiqué par SMS ».

La caisse de crédit mutuel a alors formé un pourvoi contre cette décision.

La Cour de Cassation a considéré *« qu'en se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si Mme X…, n'aurait pas pu avoir conscience que le courriel qu'elle avait reçu était frauduleux et si, en conséquence, le fait d'avoir communiqué son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le cryptogramme figurant au verso de la carte, ainsi que des informations relatives à son compte SFR permettant à un tiers de prendre connaissance de son compte 3D Secure ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article L133-16 du code monétaire et financier, la juridiction de proximité a privé, sa décision, de base légale ».*

Il résulte de cette décision que désormais le juge ne pourra donc plus se contenter de constater que l'utilisateur a fait l'objet d'un phishing pour entrer automatiquement en voie de condamnation à l'égard de la banque, il devra au préalable analyser les circonstances de l'espèce pour apprécier si l'utilisateur a pu avoir conscience que l'email litigieux était frauduleux.

Cette jurisprudence laisse à au juge du fond la liberté d'apprécier les circonstances de la fraude au regard du comportement éventuellement négligent de l'utilisateur.

Certes si l'appréciation des circonstances de l'espèce pour conclure à la négligence grave des utilisateurs devrait permettre aux banques d'être plus souvent exonérées de leur responsabilité en matière de paiement non autorisé, il n'en demeure pas moins que l'arrêt rendu le 25 octobre 2017 n'opère pas un renversement de la charge de la preuve de la négligence grave des utilisateurs qui reste supportée par les banques.

En effet si dorénavant les juges devront rechercher si les utilisateurs ont eu conscience d'avoir fait l'objet d'un phishing, il appartiendra toujours aux banques de rapporter la négligence grave si elles veulent être exonérées de toute responsabilité.

Par ailleurs il est à craindre que cette nouvelle jurisprudence, à priori favorable aux banques, n'incite les utilisateurs à ne plus dévoiler les circonstances dans lesquelles les opérations litigieuses ont eu lieu, et notamment à ne plus exposer le contexte dans lequel est intervenu le phishing, dépossédant ainsi les banques de toute possibilité d'établir une négligence grave.

Dans ce nouveau contexte, il conviendra que les juges du fond incitent les utilisateurs à exposer les conditions dans lesquelles les paiements contestés ont eu lieu, en tirant les conséquences de leur silence, en ne condamnant plus automatiquement, dans cette hypothèse, les banques à rembourser les paiements résultant d'opérations non autorisées.