COUR DE CASSATION – CHAMBRE COMMERCIALE, 06 JUIN 2018, N°16-29.065

MOTS CLEFS : fraude – carte bancaire – phishing – négligence grave – responsabilité

Alerte vigilance ! Les actes de phishing, technique par laquelle un tiers envoie un courriel dans lequel il prend l'apparence d'une société et tente de collecter les coordonnées bancaires des clients, sont de plus en plus courants. Pourtant, au regard de la jurisprudence actuelle, les chances des victimes de se voir rembourser les sommes frauduleusement prélevées tendent à diminuer. L'arrêt du 06 juin 2018 rendu par la chambre commerciale de la cour de cassation en est une illustration.

FAITS : Mme Y a été victime d'un acte de phishing. Quelques années plus tôt, elle a reçu un courriel lui demandant de régler ses factures téléphoniques impayées en soumettant les coordonnées de sa carte bancaire. L'expéditeur du message ayant pris l'apparence de son opérateur de téléphonie, Mme Y a répondu audit courriel en communiquant les informations confidentielles exigées. En réalité, il s'agissait d'un tiers mal intentionné ayant procédé à des virements bancaires frauduleux. En tant que cliente, Mme Y a donc sollicité la caisse du Crédit Mutuel de Fruges pour obtenir le remboursement des sommes prélevées. L'établissement bancaire a rejeté sa demande.

PROCEDURE : Mme Y a assigné la caisse du Crédit Mutuel de Fruges en paiement. Un jugement de première instance a été rendu, puis l'une des parties a interjeté appel. Dans un arrêt du 3 novembre 2016, la cour d'appel de Douai a statué en faveur de Mme Y et a condamné la caisse du Crédit Mutuel de Fruges au remboursement de sa cliente. Elle soutient que dès lors que le courriel reçu était dépourvu d'anomalies grossières et revêtait l'apparence générale de l'authenticité, Mme Y n'avait commis aucune faute de négligence grave à l'égard de l'obligation de l'article L.133-16 du code monétaire et financier. L'établissement bancaire se pourvoit alors en cassation.

PROBLEME DE DROIT : Lors d'un phishing, la réception d'un courriel dépourvu d'anomalies grossières et revêtant l'apparence générale de l'authenticité permet-t-elle d'exclure toute faute de négligence grave de la victime ayant communiqué les informations confidentielles ?

SOLUTION : La haute juridiction répond par la négative. Dans un arrêt du 06 juin 2018, elle casse et annule la décision rendue par les juges d'appel en leur reprochant de ne pas avoir tiré les conséquences légales de leurs constatations. Selon elle, les différents indices relevés par la cour devaient amener à conclure à une faute de négligence grave de la part de Mme Y.

SOURCES :

CAPRIOLI (E), « Fraude à la carte bancaire par hameçonnage : une nouvelle tendance se dessine », mis en ligne le 24 juillet 2018, *www.usine-digitale.fr*

SOSCONSO, « Phishing : ne pas repérer des incohérences, une négligence grave ? », mis en ligne le 03 juillet 2018*, sosconso.blog.lemonde.fr*

NOTE :

L'ordonnance du 15 juillet 2009, consacrée à l'article L.133-16 du code monétaire et financier, soumet l'utilisateur d'un instrument de paiement à une obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées. L'article L.133-19 de ce même code ajoute qu'en cas de manquement à cette obligation, notamment du fait d'une négligence grave, les pertes seront supportées par le payeur. Dans son arrêt du 06 juin 2018 relatif à un acte de phishing, la cour de cassation tente d'apporter de nouveaux éléments sur l'appréciation de cette faute de négligence grave des titulaires de cartes bancaires. Leur décision, en faveur des établissements bancaires, semble témoigner d'une nouvelle prise de position.

Précisions sur l'appréciation de la faute de négligence grave

Depuis quelques mois, la faute de négligence grave à l'obligation de l'article L.133-16 du code monétaire et financier est régulièrement caractérisée par les juges de cassation. En réalité, cette nouvelle tendance résulte d'un arrêt du 28 mars 2018. Dans cette décision, la chambre commerciale affirme que cette faute peut se révéler lorsque le titulaire de la carte bancaire a répondu à un courriel « qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance ». S'agissant de l'arrêt rendu le 06 juin 2018 par la cour de cassation, c'est l'appréciation de ces fameux indices par la cour d'appel qui est remise en cause. Les juges du fond avaient convenablement relevé que Mme Y avait pour habitude de payer ses factures téléphoniques par prélèvement, mais aussi que le courriel reçu par la victime présentait de « sérieuses irrégularités, de nature à faire douter de sa provenance », tels qu'une adresse d'expéditeur et un numéro de contrat inexactes, ainsi qu'une discordance entre les montants réclamés. Cependant, malgré la présence de ces éléments, les juges du fond n'ont pas conclu à une faute de négligence grave de la victime du phishing. Pour la cour de cassation, même si le courriel était dépourvu d'anomalies grossières et revêtait l'apparence de l'authenticité, la cour d'appel aurait dû soutenir que ces différents indices démontraient ce manquement.

Assouplissement de la position des juges à l'égard des établissements bancaire

Auparavant, en présence d'une situation de phishing, les juges optaient régulièrement pour une responsabilité des établissements bancaires. Aujourd'hui, en procédant à une appréciation plus large de la faute de négligence grave, la tendance semble s'inverser. Par un arrêt du 25 octobre 2017, la chambre commerciale est d'abord venue assouplir sa position en affirmant que les juges devaient rechercher si les faits d'espèce ne démontraient pas une faute de négligence grave de la part de la victime du phishing. Dans les décisions du 28 mars 2018 et du 06 juin 2018, les juges de cassation ont tranché en faveur des établissements bancaires. En réalité, en choisissant de sanctionner plus strictement les victimes d'actes de phishing, la jurisprudence semble poursuivre un objectif bien précis : inciter les utilisateurs de carte bancaire à opter pour un comportement plus vigilant vis-à-vis des fraudeurs de l'internet. En effet, les fraudes à la carte bancaire sont de plus en plus fréquentes. Dans certaines situations, le phishing peut être facilement repéré par les individus. Pour condamner les établissements bancaires à rembourser leurs clients, les juges doivent analyser le comportement des victimes vis-à-vis de la situation à laquelle ils ont été confrontés.

Lisa MALLET
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2018

ARRET :

Cass. Soc., 06 juin 2018, n°16-29.065

Sur le moyen unique, pris en ses deuxième et troisième branches :

Vu les articles L. 133-16 et L. 133-19 du code monétaire et financier ;

Attendu que manque, par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés l'utilisateur d'un service de paiement qui communique les données personnelles de ces dispositifs de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance;

Attendu, selon l'arrêt attaqué, que Mme Y..., titulaire d'un compte dans les livres de la Caisse de crédit mutuel de Fruges (la Caisse), a contesté des opérations de paiement effectuées, selon elle, frauduleusement sur ce compte au moyen de sa carte bancaire et demandé à la Caisse de lui en rembourser le montant ; que se heurtant au refus de celle-ci, qui lui reprochait d'avoir commis une faute en communiquant à des tiers des informations confidentielles permettant d'effectuer les opérations contestées, Mme Y... l'a assignée en paiement ;

Attendu que pour condamner la Caisse à rembourser à Mme Y... les sommes prélevées sur son compte, l'arrêt retient que si celle-ci avait communiqué des données confidentielles ayant rendu possibles les prélèvements contestés en répondant à un courriel comportant le logotype de son opérateur de téléphonie, l'utilisatrice de service de paiement n'avait cependant pas commis de négligence grave, dès lors que ce courriel, dépourvu d'anomalies grossières et revêtant l'apparence générale de l'authenticité, avait surpris sa vigilance ;

Qu'en statuant ainsi, après avoir relevé que Mme Y... réglait ses factures de téléphone par prélèvements et non par carte bancaires et qu'un examen attentif du courriel de rappel de paiement révélait de sérieuses irrégularités, de nature à faire douter de sa provenance, telles que l'inexactitude de l'adresse de l'expéditeur et du numéro du contrat mentionné ainsi que la discordance entre les montants réclamés, la cour d'appel, qui n'a pas tiré les conséquences légales de ses constatations, a violé les textes susvisés ;

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur les autres griefs :

CASSE ET ANNULE, sauf en ce que, confirmant de ce chef le jugement déféré, il déclare irrecevables les demandes de Mme Y... dirigées contre la Caisse fédérale de crédit mutuel Nord Europe, l'arrêt rendu le 3 novembre 2016, entre les parties, par la cour d'appel de Douai ; remet, en conséquence, sur les autres points, la cause et les parties dans l'état où elles se trouvaient avant ledit arrêt et, pour être fait droit, les renvoie devant la cour d'appel d'Amiens ;