COUR DE CASSATION, CHAMBRE COMMERCIALE, 24 NOVEMBRE 2021, N°20-13.767

MOTS CLEFS : banque – spam – données personnelles – paiement – email – opérations frauduleuses – hameçonnage

Cet arrêt s'inscrit dans une tendance jurisprudentielle qui vient souvent considérer que la communication de données personnelles par le client d'une banque, sous la forme d'informations relatives aux cartes bancaires, constitue une négligence grave. L'établissement bancaire doit toutefois prouver cette négligence, notamment en démontrant que le client n'a pas agi comme une personne raisonnablement avertie en répondant à un courriel d'hameçonnage.

FAITS : Un individu reçoit un courriel qu'il pense venir de sa banque, et qui le conduit à communiquer sur un site internet son numéro de carte bancaire, la date d'expiration et le cryptogramme. A la suite de cette action, il constate trois opérations frauduleuses de paiement effectuées grâce à cette carte bancaire. L'individu se retourne alors contre son établissement bancaire, qui refuse de rembourser les opérations en invoquant une négligence grave.

PROCEDURE : Le client assigne sa banque en paiement devant le Tribunal d'instance de Lens. Les juges du fond condamnent alors la banque à rembourser le client du montant des opérations frauduleuses, assorti des intérêts au taux légal. La banque forme alors un pourvoi en cassation, en s'appuyant sur un moyen unique tiré de la négligence grave de son client.

PROBLEME DE DROIT : Le client d'une banque ayant communiqué des données personnelles sous la forme d'informations de carte bancaire suite à un mail suspect, peut-il obtenir le remboursement des opérations frauduleuses subséquentes à sa banque ?

SOLUTION : La Cour de Cassation infirme la décision du Tribunal d'instance de Lens, en considérant que les juges n'ont pas recherché si le client avait pris les mesures raisonnables pour préserver la sécurité de ces informations de carte bancaire, et en conséquence si la communication de ces informations ne constituait pas une négligence grave au sens du code monétaire et financier.

SOURCES :

KILGUS (N.), « *Phishing* et négligence grave du porteur d'une carte bancaire : les liaisons imposées », *Dalloz IP/IT*, n°07-08, 2018, p. 440
LEGEAIS (D.), « Hameçonnage », *RTD Com*, n°02, 2018, p. 436
« Fraude à la carte bancaire, que faire », *cybermalveillance.gouv.fr,* publié le 3 décembre 2020, consulté le 12 janvier 2022
Cour de Cassation, chambre commerciale, 18 janvier 2017, n°15-18.102
Cour de Cassation, chambre commerciale, 25 octobre 2017, n°16-11.644
Cour de Cassation, chambre commerciale, 28 mars 2018, n°16-20.018

NOTE :

Un débat sur la qualification de négligence grave

En refusant de rechercher si le défendeur aurait pu avoir conscience que le courriel reçu était frauduleux, les juges de première instance font une mauvaise application des articles L.133-16 et L.133-17 du Code monétaire et financier dans leur version antérieure à 2017.

En effet, le premier article prévoit que l'utilisateur des services de paiement, ici le client, doit prendre toutes les mesures raisonnables pour préserver la sécurité de ses instruments de paiement. C'est par exemple le fait de ne pas conserver son code de carte bancaire au même endroit que cette dernière.

Le second article dispose ensuite que le client supportera les pertes occasionnées par des opérations frauduleuses s'il s'agit notamment d'une négligence grave de sa part. Pour ce dernier point, la charge de la preuve pèse sur l'établissement émetteur de l'instrument de paiement. En l'absence de cette démonstration, notamment la preuve d'un courrier frauduleux, la banque sera tenue de rembourser son client (Com, 18 janvier 2017).

Ici, la Cour de cassation considère que les juges du fond auraient dû rechercher si le comportement du client était constitutif d'une négligence grave, et s'il était donc évitable.

L'appréciation de la Cour confirme ici une suite d'arrêts similaires. Notamment, dans un arrêt du 28 mars 2018, les juges de la Cour de Cassation considèrent 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 ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage* ».

Les affaires étant similaires, il est possible de considérer qu'en l'espèce le client a également fait preuve d'une négligence grave. En effet, celui-ci a communiqué les données confidentielles de sa carte bancaire, alors que de nombreux indices permettaient de dire que le courriel reçu était une tentative d'escroquerie.

En l'espèce, l'adresse mail utilisée n'est pas une adresse générique. De plus, l'objet du mail contenait le terme « spam ». Par ailleurs, le message était truffé de fautes d'orthographe. Tout ces éléments sont des indices qu'une personne raisonnablement avertie devrait pouvoir repérer afin d'éviter les escroqueries de ce type.

Un arrêt illustrant la nécessité de former les particuliers à la cybersécurité

Cet arrêt peut sembler sévère notamment à l'encontre des personnes âgées, utilisatrices occasionnelles de l'informatique et qui sont donc plus vulnérables à ce type d'escroquerie nommé l'hameçonnage (ou *phishing*). Cette décision met en lumière la nécessité de pédagogie et de formation des clients ou simples particuliers face aux risques de la cybercriminalité.

C'est notamment pour éviter ces contentieux que de nombreuses entreprises rappellent régulièrement à leurs clients qu'elles ne leur demanderont jamais leurs données confidentielles par mail, et ce malgré la précision sur l'indifférence de la fourniture d'une information sur l'hameçonnage (arrêt de 2018 notamment). Par ailleurs, le site *cybermalveillance.gouv.fr* offre des explications et des conseils aux particuliers contre les risques en ligne, notamment concernant la fraude à la carte bancaire.

Myriam AUTRAND
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2022

ARRET :

1. Selon le jugement attaqué (tribunal d'instance de Lens, 17 décembre 2019), rendu en dernier ressort, M. [W], titulaire d'un compte dans les livres de la société Caisse de crédit mutuel de [Localité 4] (la banque) a contesté trois opérations de paiement effectuées frauduleusement sur ce compte à la suite de sa réponse à un courriel, reçu le 27 décembre 2017, l'ayant conduit à communiquer sur le site internet proposé le numéro de sa carte bancaire avec sa date d'expiration, le code de vérification, et lui en a demandé le remboursement.

2. La banque lui ayant opposé un refus, estimant qu'il avait commis une négligence grave en communiquant ses données personnelles en réponse à un courriel suspect, M. [W] l'a assignée en paiement.

Sur le moyen, pris en sa première branche

Enoncé du moyen

3. La banque fait grief au jugement de la condamner à payer à M. [W] la somme de 2 593 euros, assortie des intérêts au taux légal à compter du 8 novembre 2018, date de la mise en demeure, et de rejeter ses demandes, alors « 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 ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement averti de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage ; qu'en l'espèce, la banque faisait valoir que le courriel du 27 décembre 2017, produit aux débats par M. [W], auquel ce dernier avait admis avoir répondu en communiquant son numéro de carte bancaire, le pictogramme et son numéro de téléphone, comportait des indices qui permettaient à un utilisateur normalement averti de douter de sa provenance, dans la mesure où l'adresse de l'expéditeur de ce courriel était "[Courriel 1] (illisible)[Courriel 1]", que son objet était intitulé "***SPAM*** vous écrit", et que le message de ce courriel, qui indiquait "lors de votre dernier achat, vous été [sic] averti par un message vous informant de l'obligation d'adhérer à la nouvelle réglementation concernant la fiabilité des achats par CB sur internet et la mise en place d'un arrêt pour vos futurs achats. Or, nous n'avons pas à ce jour d'adhésion de votre part et nous sommes au regret de vous informer que vous pouvez plus [sic] utiliser votre carte sur internet", en invitant le destinataire à cliquer sur un lien avec de communiquer ses données personnelles, comportait des fautes de syntaxe et d'orthographe, et ne correspondait pas à la situation de M. [W] qui ne pouvait ignorer que lors de son dernier achat sur internet, il n'avait reçu aucun avertissement quant à un risque de blocage de sa carte pour effectuer des paiements à distance ; que, pour néanmoins faire droit à la demande de M. [W] de remboursement des opérations de paiement réalisées sur son compte le lendemain de sa réponse à ce courriel frauduleux, le tribunal d'instance, après avoir constaté que M. [W] avait admis avoir fourni ses identifiants en réponse à ce courriel, a retenu que la banque "ne rapporte pas la preuve de ce que M. [W] a fourni en pleine connaissance de cause ces éléments et que celui-ci aurait encore failli à son devoir de vigilance, en n'ayant pas vérifié l'origine de l'email litigieux ou qu'il ait manqué à ses obligations contractuelles", que M. [W] avait immédiatement fait opposition dès qu'il avait été informé des débits frauduleux effectués sur son compte, que la banque ne démontrait pas avoir alerté M. [W] sur les risques d'hameçonnage, et enfin, que le client de la banque avait raisonnablement pu s'inquiéter d'un message l'informant que s'il ne procédait pas à cette demande d'adhésion en ligne, rapidement, il perdrait alors l'usage de sa carte bancaire sur internet ; qu'en statuant de la sorte, sans rechercher, ainsi qu'elle y était invitée, si le courriel d'hameçonnage

auquel M. [W] avait reconnu avoir répondu en communiquant les données confidentielles de sa carte bancaire ne comportait pas des indices permettant à un utilisateur normalement averti de douter de sa provenance, de sorte qu'en y répondant, M. [W] avait commis une négligence grave exonérant la banque de son obligation de remboursement, le tribunal d'instance a privé sa décision de base légale au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier dans leur version applicable en la cause. »

Réponse de la Cour

Vu les articles L. 133-16 et L. 133-19 du code monétaire et financier dans leur rédaction antérieure à celle issue de l'ordonnance n° 2017-1252 du 9 août 2017 :

4. Il résulte du premier de ces textes que l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et du second que le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17.

5. Pour condamner la banque à payer à M. [W] la somme de 2 593 euros en remboursement des paiements non autorisés effectués sur son compte, le jugement retient que, s'il est établi que ce dernier a fourni ses identifiants permettant l'accès à son compte en ligne après avoir reçu un courriel frauduleux, la banque ne démontre pas qu'il a fourni ces informations en pleine connaissance de cause et qu'il aurait failli à son devoir de vigilance dès lors qu'il n'avait pas à vérifier l'origine du message et qu'il a pu raisonnablement s'inquiéter à la réception d'un courriel l'informant que, s'il ne procédait pas rapidement à l'adhésion en ligne, il perdrait l'usage de sa carte bancaire sur internet.

6. En se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si M. [W] n'aurait pas pu avoir conscience que le courriel qu'il avait reçu le 27 décembre 2017 était frauduleux et si, en conséquence, le fait d'avoir communiqué ses données personnelles ne caractérisait pas un manquement par négligence grave à ses obligations mentionnées à l'article L. 133-16 du code monétaire et financier, le tribunal d'instance n'a pas donné de base légale à sa décision.

PAR CES MOTIFS, et sans qu'il y ait lieu de statuer sur l'autre grief, la Cour :

CASSE ET ANNULE, en toutes ses dispositions, le jugement rendu le 17 décembre 2019, entre les parties, par le tribunal d'instance de Lens ;