

25 octobre 2017

Cour de cassation

Pourvoi n° 16-11.644

Chambre commerciale financière et économique – Formation de section

Publié au Bulletin

ECLI:FR:CCASS:2017:CO01327

Titres et sommaires

BANQUE - paiement - instrument de paiement - utilisation frauduleuse par un tiers - responsabilité de la banque - appréciation - éléments à considérer - négligence grave du titulaire

Prive sa décision de base légale, au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier, la juridiction de proximité qui, pour condamner une banque à rembourser une somme prélevée sur le compte de son client au titre d'un paiement effectué par internet sans son autorisation, retient que ce dernier a communiqué, certes volontairement mais à la suite d'un hameçonnage, à une personne se présentant sous une fausse identité, les informations relatives à sa carte de paiement, qui ont ainsi été détournées à son insu, sans toutefois divulguer le code confidentiel de la carte, ni le code 3D Sécure, de sorte qu'il ne peut lui être reproché de ne pas avoir respecté les dispositions de l'article L. 133-16 du code monétaire et financier, sans rechercher, au regard des circonstances de l'espèce, si ce client n'aurait pas pu avoir conscience que le courriel, auquel il avait ainsi répondu, était frauduleux et si, en conséquence, le fait d'avoir communiqué son nom, le numéro de sa carte de paiement, la date d'expiration de celle-ci et le cryptogramme figurant à son verso, ainsi que des informations relatives à son compte auprès de son opérateur téléphonique permettant à un tiers de prendre connaissance du code 3D Sécure, ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article précité

Texte de la décision

Entête

COMM.

CH.B

COUR DE CASSATION

Audience publique du 25 octobre 2017

Cassation

Mme X..., président

Arrêt n° 1327 FS-P+B+I

Pourvoi n° N 16-11.644

R É P U B L I Q U E F R A N Ç A I S E

A U N O M D U P E U P L E F R A N Ç A I S

LA COUR DE CASSATION, CHAMBRE COMMERCIALE, FINANCIÈRE ET ÉCONOMIQUE, a rendu l'arrêt suivant :

Statuant sur le pourvoi formé par :

1°/ la Caisse fédérale du crédit mutuel Nord Europe, société coopérative à forme anonyme à capital variable, dont le siège est [...]

2°/ la Caisse de crédit mutuel de Calais, société coopérative de crédit, dont le siège est [...], et ayant un établissement [...]

contre le jugement rendu le 7 décembre 2015 par la juridiction de proximité de Calais, dans le litige les opposant à Mme Caroline Y... , domiciliée [...]

défenderesse à la cassation ;

Les demanderesses invoquent, à l'appui de leur pourvoi, le moyen unique de cassation annexé au présent arrêt ;

Vu la communication faite au procureur général ;

LA COUR, composée conformément à l'article R. 431-5 du code de l'organisation judiciaire, en l'audience publique du 12 septembre 2017, où étaient présents : Mme X..., président, Mme Z..., conseiller référendaire rapporteur, M. Rémy, conseiller doyen, M. Guérin, Mme Vallansan, M. Remeniéras, Mmes Graff-Daudret, Vaissette, Bélaival, Fontaine, conseillers, Mme Schmidt, M. Guerlot, Mmes Jollec, Barbot, Brahic-Lambrey, M. Blanc, conseillers référendaires, Mme Guinamant, avocat général référendaire, M. Graveline, greffier de chambre ;

Sur le rapport de Mme Z..., conseiller référendaire, les observations de la SCP Célice, Soltner, Texidor et Périer, avocat de la Caisse fédérale du crédit mutuel Nord Europe et de la Caisse de crédit mutuel de Calais, l'avis de Mme Guinamant, avocat général référendaire, à la suite duquel le président a demandé à l'avocat s'il souhaitait présenter des observations complémentaires, et après en avoir délibéré conformément à la loi ;

Moyens

Sur le moyen unique, pris en sa deuxième branche :

Motivation

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

Exposé du litige

Attendu, selon le jugement attaqué, rendu en dernier ressort, qu'après avoir reçu, sur son téléphone portable, deux messages lui communiquant un code à six chiffres dénommé "3D Secure", destiné à valider deux paiements par internet qu'elle n'avait pas réalisés, Mme Y... a, le même jour, fait opposition à sa carte bancaire auprès de la Caisse de crédit mutuel de Calais (la Caisse) dans les livres de laquelle était ouvert son compte ; qu'elle lui a ensuite demandé de lui rembourser la somme qui avait été prélevée sur ce compte à ce titre et de réparer son préjudice moral ; que, soutenant que Mme Y... ne contestait pas avoir, en réponse à un courriel se présentant comme émanant de l'opérateur téléphonique SFR, communiqué à son correspondant des informations relatives à son compte chez cet opérateur, permettant à ce dernier de mettre en place un renvoi téléphonique des messages reçus de la Caisse, ainsi que ses nom, numéro de carte de paiement, date d'expiration et cryptogramme figurant au verso de la carte, la Caisse s'est opposée à sa demande au motif qu'elle avait ainsi commis une négligence grave dans la conservation des dispositifs de sécurité personnalisés mis à sa disposition ;

Attendu que, pour condamner la Caisse à payer à Mme Y... la somme de 3 300,28 euros en remboursement de la somme prélevée sur son compte au titre du paiement litigieux et 1 euro à titre de dommages-intérêts, le jugement retient que si cette dernière a communiqué volontairement les informations relatives à sa carte de paiement, celles-ci ont été détournées à son insu, car communiquées à une personne se présentant sous une fausse identité, et qu'elle n'avait communiqué ni son code confidentiel, ni le code 3D Secure, de sorte qu'il ne peut lui être reproché de ne pas avoir respecté les dispositions de l'article L. 133-16 du code monétaire et financier ;

Motivation

Qu'en se déterminant ainsi, sans rechercher, au regard des circonstances de l'espèce, si Mme Y... 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 du code 3D Secure, ne caractérisait pas un manquement, par négligence grave, à ses obligations mentionnées à l'article L. 133-16 du code monétaire et financier, la juridiction de proximité a privé sa décision de base légale ;

Dispositif

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

CASSE ET ANNULE, en toutes ses dispositions, le jugement rendu le 7 décembre 2015, entre les parties, par la juridiction de proximité de Calais ; remet, en conséquence, la cause et les parties dans l'état où elles se trouvaient avant ledit

jugement et, pour être fait droit, les renvoie devant le tribunal d'instance de Dunkerque ;

Condamne Mme Y... aux dépens ;

Vu l'article 700 du code de procédure civile, rejette la demande ;

Dit que sur les diligences du procureur général près la Cour de cassation, le présent arrêt sera transmis pour être transcrit en marge ou à la suite du jugement cassé ;

Ainsi fait et jugé par la Cour de cassation, chambre commerciale, financière et économique, et prononcé par le président en son audience publique du vingt-cinq octobre deux mille dix-sept.

Moyens annexés

MOYEN ANNEXE au présent arrêt.

Moyen produit par la SCP Célice, Soltner, Texidor et Périer, avocat aux Conseils, pour la Caisse fédérale du crédit mutuel Nord Europe et la Caisse de crédit mutuel de Calais.

Il est fait grief au jugement attaqué D'AVOIR condamné la Caisse de crédit mutuel de Calais à payer à Madame Caroline Y... la somme de 3.300,28 €, la somme de 1 € à titre de dommages et intérêts, ainsi que les entiers dépens,

AUX MOTIFS QUE « Aux termes des dispositions de l'article L. 133-23 du code monétaire et financier : "Lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son 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 par une déficience technique ou autre. L'utilisation de l'instrument de paiement telle qu'enregistrée par le prestataire de services de paiement 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". Aux termes des dispositions de l'article L. 133-19 du code monétaire et financier : "I. En cas d'opération de paiement non autorisée consécutive à la perte ou au vol de l'instrument de paiement, le payeur supporte, avant l'information prévue à l'article L. 133-17, les pertes liées à l'utilisation de cet instrument, dans la limite d'un plafond de 150 euros. Toutefois, la responsabilité du payeur n'est pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé. II. La responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées. Elle n'est pas engagée non plus en cas de contrefaçon de l'instrument de paiement si, au moment de l'opération de paiement non autorisée, le payeur était en possession de son instrument. III. Sauf agissement frauduleux de sa part, le payeur ne supporte aucune conséquence financière si le prestataire de services de paiement ne fournit pas de moyens appropriés permettant l'information aux fins de blocage de l'instrument de paiement prévu à l'article L. 133-17. IV. 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" ; Aux termes des dispositions de l'article L. 133-16 du code monétaire et financier : "Dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés. Il utilise l'instrument de paiement conformément aux conditions régissant sa délivrance et son utilisation". Caroline Y... a formé opposition à la carte bancaire le jour du paiement contesté. Elle indique avoir été alertée par la réception de deux SMS lui communiquant un code 3D secure pour deux opérations qu'elle n'a pas réalisées. La caisse de crédit mutuel de Calais ne conteste pas que le paiement n'a pas été autorisé par Caroline Y... Elle fait valoir que cette opération a été réalisée en utilisant toutes les coordonnées de la carte bancaire et en renseignant le code 3D secure. Elle indique que le code à six chiffres, après avoir été envoyé par sms, a été envoyé vocalement sur le téléphone du domicile de Caroline Y...

. Il résulte des pièces produites aux débats et des explications des parties que Caroline Y... a communiqué les informations relatives à sa carte bancaire après avoir reçu d'un émetteur se présentant comme SFR : nom, numéro de carte, date d'expiration, cryptogramme. Elle conteste avoir communiqué son code confidentiel. Ce code confidentiel n'a d'ailleurs pas été utilisé pour réaliser l'opération. Ces éléments bien que communiqués volontairement par Caroline Y... doivent être considérés comme ayant été étant détournés à son insu car ils ont été communiqués à une personne se présentant sous une fausse identité. Il ne peut être reproché à Caroline Y... 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. Si Caroline Y... a pu communiquer des informations relatives à son compte SFR permettant par la suite à un tiers d'opérer un renvoi téléphonique et de prendre connaissance du code 3D SECURE, cela ne peut être assimilé à une négligence de Caroline Y... quant à la préservation de la sécurité de ses dispositifs de sécurité personnalisés. Compte tenu de ces éléments, la caisse de crédit mutuel de CALAIS sera condamnée à rembourser à Caroline Y... la somme de 3.300,28 € et à payer la somme de 1€ à titre de dommages et intérêts. Succombant à l'instance, la caisse de crédit mutuel de Calais sera condamnée aux dépens. Il n'y a pas lieu à condamnation sur le fondement de l'article 700 du code de procédure civile » ;

1°) ALORS QUE l'utilisateur d'un service de paiement qui agit avec une négligence grave est tenu de supporter l'intégralité de la perte subie ; que constitue une négligence grave la fourniture par le client d'un établissement bancaire à un tiers de données confidentielles permettant ou facilitant l'utilisation d'un service de paiement sécurisé ; qu'en l'espèce, il résulte des énonciations du jugement attaqué que Madame Y... , titulaire d'un compte bancaire auprès de la Caisse de crédit mutuel de Calais, avait, en réponse à un courriel émanant d'une personne se présentant comme la société SFR, communiqué son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le numéro du cryptogramme figurant au dos de la carte (jugement attaqué, p. 3, 5ème §) ; que pour dire que Madame Y... n'avait pas commis de négligence grave, et condamner la banque à lui rembourser une somme de 3.300,28 € correspondant à une opération réalisée par le biais du système de paiement 3D SECURE, la juridiction de proximité a retenu que « ces éléments bien que communiqués volontairement par Caroline Y... doivent être considérés comme ayant été étant détournés à son insu car ils ont été communiqués à une personne se présentant sous une fausse identité », et qu'en outre, Madame Y... n'avait communiqué ni le code confidentiel de sa carte, ni le code 3D SECURE à 6 chiffres qui lui avait été adressé par sms pour valider le paiement (jugement, p. 3, 7ème et 8ème §M) ; qu'en statuant de la sorte, quand il résultait de ses propres constatations que Madame Y... avait communiqué à un tiers des données confidentielles relatives à sa carte bancaire, sans lesquelles l'opération litigieuse n'aurait pu être exécutée, ce qui caractérisait une méconnaissance de son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés, le juge de proximité a violé les articles L. 133-15, L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier, ensemble l'article 1134 du code civil ;

2°) ALORS EN TOUT ETAT DE CAUSE QUE la Caisse de crédit mutuel de Calais faisait valoir dans ses conclusions reprises à l'audience que Madame Y... avait commis une négligence grave en répondant à un « mail de phishing » lui demandant de communiquer certaines données confidentielles relatives à sa carte bancaire, dans la mesure où ce courriel ne comportait aucun nom de destinataire ni d'expéditeur, qu'y figurait un numéro de facture erroné et que la mention d'un rejet ou d'un impayé dans ce courriel était nécessairement inexacte puisque le compte de Madame Y... était créditeur (p. 6) ; qu'elle soulignait également que le Crédit Mutuel communiquait très régulièrement et depuis de nombreuses années sur son site internet afin d'alerter ses clients sur les risques de phishing et la nécessité de ne jamais communiquer ses données confidentielles à quiconque, de même que les pouvoirs publics et la gendarmerie nationale (p. 6) ; qu'en s'abstenant de rechercher, au regard de ces éléments de fait, si Madame Y... n'aurait pas dû avoir conscience que le courriel censé émaner de la société SFR auquel elle avait répondu était nécessairement frauduleux et si en conséquence, le fait d'avoir communiqué à son émetteur son nom, son numéro de carte bancaire, la date d'expiration de celle-ci et le numéro du cryptogramme figurant au dos de la carte (jugement attaqué, p. 3, 5ème §), ne caractérisait pas une négligence grave de sa part, la Cour d'appel a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier, ensemble l'article 1134 du code civil ;

3°) ALORS ENCORE QUE la circonstance qu'un service de paiement doté d'un dispositif de sécurité ait été utilisé pour des achats sur internet par utilisation, outre des données afférentes à sa carte bancaire, d'un code adressé directement au client sur son téléphone mobile ou fixe, permettant à l'utilisateur de venir authentifier le paiement au moyen d'une donnée confidentielle ne se trouvant pas sur la carte de paiement proprement dite, fait à tout le moins présumer le

défaut de garde des données confidentielles d'instrument de paiement et la négligence grave de son utilisateur dans la préservation de la confidentialité de ses données personnelles ; qu'il appartient dans ces circonstances à l'utilisateur du service de paiement de rapporter par tous moyens la preuve qu'il a respecté son obligation de conserver les données confidentielles permettant l'utilisation du service qui lui a été proposé ; qu'en statuant comme il l'a fait, sans rechercher, ainsi qu'il y était invité, si la circonstance que le débit litigieux ait été effectué par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à Madame Y... , et dont cette dernière avait contractuellement la charge d'assurer la conservation et la confidentialité, ne faisait pas présumer la négligence grave de l'utilisateur dans la conservation de ses données personnelles, le juge de proximité a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

Textes appliqués

Articles L. 133-16 et L. 133-19 du code monétaire et financier.