Références

Cour de cassation
chambre commerciale
Audience publique du mercredi 26 juin 2019
N° de pourvoi: 18-13892
Non publié au bulletin **Rejet**

Mme Mouillard (président), président
Me Haas, SCP Célice, Soltner, Texidor et Périer, avocat(s)

Texte intégral

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

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

Donne acte à la société Caisse de crédit mutuel de Dunkerque Malo du désistement de son pourvoi, en ce qu'il est dirigé contre la Société française de radiotéléphone ;

Sur le moyen unique :

Attendu, selon l'arrêt attaqué (Douai, 1er février 2018), que Mme N..., titulaire d'un compte dans les livres de la société Caisse de crédit mutuel de Dunkerque Malo (la banque), a assigné celle-ci en remboursement d'opérations de paiement du prix d'achats effectués par Internet au moyen du système de paiement « 3D Secure », qu'elle contestait avoir autorisées ;

Attendu que la banque fait grief à l'arrêt de la condamner à rembourser à Mme N... la somme de 7 379,34 euros correspondant aux débits non autorisés sur son compte bancaire, ainsi que la somme de 174,34 euros au titre des frais divers et intérêts prélevés sur son compte et relatifs au découvert relevant de la fraude, alors, selon le moyen :

1°/ 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 la négligence grave s'entend de la carence de l'utilisateur du service de paiement à prendre toute mesure raisonnable pour assurer la confidentialité de ses données personnelles ; qu'en jugeant que la négligence grave de l'utilisateur de services de paiement « confinait au dol et dénotait l'inaptitude de celui-ci dans l'accomplissement de son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés, de sorte que cette négligence grave était d'une importance telle qu'elle rendait impossible le remboursement des sommes débitées à la suite d'opérations de paiement non autorisées par l'utilisateur de services », pour apprécier l'existence d'une négligence grave de la part de Mme N... au regard de cette définition, la cour d'appel a violé les articles L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier ;

2°/ que si, selon l'article L. 133-23 du code monétaire et financier, 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, elle peut suffire à rapporter une telle preuve, en fonction des circonstances particulières du litige qu'il incombe aux juges du fond d'examiner ; que pour condamner la banque à rembourser à Mme N... le montant d'opérations réalisées au débit de son compte bancaire, la cour d'appel, après avoir constaté que la banque rapportait la preuve que les opérations de paiement contestées avaient « été authentifiées, dûment enregistrées et comptabilisées, et qu'elles n'avaient pas été affectées par une défaillance technique ou autre, tel un piratage », a néanmoins considéré que les utilisations successives des données attachées à la carte de Mme N... ne pouvaient suffire à prouver que les opérations litigieuses avaient été autorisées par cette dernière, ou qu'elle n'aurait pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière, et a jugé que la banque, qui se bornait à faire état de l'hypothèse d'un « phishing », était défaillante dans l'administration de la preuve de la négligence grave qu'aurait commise Mme N... ; qu'en statuant de la sorte, quand l'utilisation d'un service de paiement sans

défaillance technique est susceptible de démontrer la commission par l'utilisateur de ce service d'une négligence grave dans la conservation de ses données, ce qu'il lui incombait de rechercher au regard des caractéristiques en matière de sécurité des services de paiement employés, la cour d'appel a violé les articles L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier ;

3°/ 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 l'existence d'une négligence grave doit être appréciée au regard de l'ensemble des circonstances de la cause, et peut être prouvée par tous moyens, en particulier eu égard aux caractéristiques de l'instrument de paiement en termes de fiabilité et de sécurité ; qu'en s'abstenant de rechercher, comme elle y était invitée, si la circonstance que les opérations de paiement litigieuses avaient été effectuées via le système de paiement sécurisé « 3D Secure », nécessitant, outre la fourniture des informations présentes sur la carte du sociétaire (nom, cryptogramme visuel, numéro et date d'expiration de la carte), un code de confirmation adressé sur le téléphone portable de ce dernier, ne permettait de présumer que Mme N... avait été gravement négligente dans la conservation de ses données personnelles, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier ;

4°/ qu'en retenant que l'envoi par la banque d'un courrier le 4 décembre 2014 faisant état de l'éventuelle « utilisation frauduleuse » de la carte bancaire de Mme N... « n'était pas particulièrement cohérente avec la thèse de la banque sur la circonstance, alléguée mais non démontrée par celle-ci, que Mme N... aurait nécessairement et volontairement communiqué ses informations personnelles et confidentielles à un tiers par négligence grave (
) », la cour d'appel, qui s'est fondée sur une circonstance impropre à exclure la négligence grave invoquée par la banque, a violé les articles L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier, ensemble l'article 1134 du code civil, dans sa version applicable en l'espèce ;

5°/ que le principe de l'égalité des armes implique que chaque partie ait la possibilité de faire valoir ses prétentions et moyens dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à son contradicteur ; qu'en jugeant qu'il incombait à la banque de prouver « l'implication à un titre ou à un autre de Mme N... dans les opérations litigieuses pour caractériser sa négligence fautive ou son manquement intentionnel, voire son action frauduleuse », et qu'elle ne pouvait invoquer l'article 6, § 1, de la Convention européenne des droits de l'homme sur la nécessité d'un procès équitable quand le prestataire de service de paiement ne dispose d'aucun autre moyen de preuve effectif pour démontrer la négligence grave qu'aurait commise son client, la cour d'appel a méconnu les exigences de l'article 6, § 1, de la Convention européenne des droits de l'homme, ensemble les articles L. 133-15, L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier, ensemble l'article 1315, devenu 1353, du code civil ;

Mais attendu, en premier lieu, que si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, dans leur rédaction antérieure à celle issue de l'ordonnance n° 2017-1252 du 9 août 2017, il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il incombe, par application des articles L. 133-19, IV, et L. 133-23 dudit code, dans leur rédaction alors applicable, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations ; 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 ; qu'ayant exactement retenu, abstraction faite des motifs, surabondants, critiqués par les première et quatrième branches, que les utilisations successives des données attachées à la carte bancaire de Mme N... ne suffisaient pas, en tant que telles, à prouver que les opérations avaient été autorisées par celle-ci ou qu'elle n'avait pas satisfait intentionnellement ou par négligence grave à ses obligations lui incombant en la matière et que la banque se bornait à évoquer l'hypothèse d'un hameçonnage, sans qu'il soit établi que Mme N... avait transmis à un tiers les données confidentielles attachées à son instrument de paiement, la cour d'appel, qui n'était pas tenue de procéder à la recherche, inopérante, invoquée par la troisième branche, a légalement justifié sa décision ;

Et attendu, en second lieu, qu'en retenant que l'utilisation de l'instrument de paiement ou des données personnelles de Mme N... ne permettait pas de présumer la négligence grave de cette dernière, sans considération du niveau de sécurité offert par les services de paiement en cause, et en excluant ainsi de mettre à la charge de cette utilisatrice la preuve, non moins difficile à rapporter, d'une absence de négligence grave de sa part, la cour d'appel, qui n'a fait qu'appliquer les règles de droit commun relatives à la charge et aux modalités de la preuve, n'a pas placé la banque dans une situation de net désavantage dans la présentation de sa cause par rapport à Mme N... et n'a donc pas méconnu le principe de l'égalité des armes ;

D'où il suit que le moyen, inopérant en ses première et quatrième branches, n'est pas fondé pour le surplus ;

PAR CES MOTIFS :

REJETTE le pourvoi ;

Condamne la société Caisse de crédit mutuel de Dunkerque Malo aux dépens ;

Vu l'article 700 du code de procédure civile, rejette sa demande et la condamne à payer à Mme N... la somme de 3 000 euros ;

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-six juin deux mille dix-neuf. MOYEN ANNEXE au présent arrêt.

Moyen produit par la SCP Célice, Soltner, Texidor et Périer, avocat aux Conseils, pour la Caisse de crédit mutuel de Dunkerque Malo.

Il est fait grief au jugement attaqué D'AVOIR condamné la Caisse de Crédit Mutuel de Dunkerque-Malo à rembourser à Mme B... N... la somme de 7.379,34 € correspondant aux débits non autorisés sur son compte bancaire, ainsi que la somme de 174,34 € au titre des frais divers et intérêts prélevés sur son compte et relatifs au découvert relevant de la fraude ;

AUX MOTIFS QUE « A titre liminaire, la cour constate que si Mme N... produit aux débats une attestation de régularisation de la Caisse du 24 février 2015 indiquant que les incidents survenus sur le compte n° [...] ouvert à son nom ont été régularisés, cette attestation est manifestement relative aux frais d'impayés consécutifs aux opérations litigieuses réalisées sur son compte à partir de sa carte bancaire. La cour relève en effet que des frais d'impayés et des frais divers consécutifs au découvert sur son compte bancaire ont fait l'objet d'une rétrocession à la date comptable du 6 janvier 2015, comme cela résulte du document relatif aux mouvements sur le compte de Mme N... d'août 2014 à janvier 2015 produit au débat par la Caisse. Il s'ensuit que la Caisse, si elle s'est engagée, aux termes du courrier du 24 février 2015, à régulariser les incidents survenus sur le compte de Mme N..., ne s'est pas engagée à lui rembourser, contrairement à ce que celle-ci soutient, les paiements litigieux effectués à partir de son moyen de paiement. 1. Sur la demande en remboursement de Mme N... Si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est à ce prestataire qu'il incombe, par application des articles L. 133-19, IV et L. 133-23 du code monétaire et financier, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations ; 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 utilisées. La négligence grave de l'utilisateur de services de paiement confine au dol et dénote l'inaptitude de celui-ci dans l'accomplissement de son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés, de sorte que cette négligence grave est d'une importance telle qu'elle rend impossible le remboursement des sommes débitées à la suite d'opérations de paiement non autorisées par l'utilisateur de services ; il appartient au prestataire de service d'établir par d'autres éléments extrinsèques la preuve d'une négligence grave imputable à l'utilisateur de services. 1.1. Sur l'existence du détournement Mme N... verse au débat un relevé d'informations bancaires à entête de la Caisse daté du 5 novembre 2014 ; il ressort de ce document que les opérations suivantes ont été réalisées le 20 octobre 2014 à partir de la carte bancaire 0467 5098, étant précisé que la date de valeur est le 21 octobre 2014 : - à "Boulogne Bill", 1 paiement de 30 euros au profit de "Ticket Transfer", - à Paris, 7 paiements de 911 euros au profit de "Free Mobile", - à Madrid, 1 paiement de 922,34 euros au profit de "Red Universal Ma Carte", - à Limoges, 1 paiement de 50 euros au profit de "Topengo". Mme N... produit également deux notices d'information relatives aux usages frauduleux de cartes bancaires et aux dispositions du code monétaire et financier en la matière, aux termes desquelles Mme N... s'est présentée au Commissariat de secteur de Grande-Synthe les 22 octobre et 1er décembre 2014 pour déclarer l'utilisation frauduleuse de sa carte de paiement, d'une carte contrefaite ou des données liées à la carte (numéro, date d'expiration). Dans un courrier du 25 novembre 2014 adressé à Mme N..., la Caisse se réfère au sinistre du 20 octobre 2014 et indique que Mme N... a déclaré l'usage frauduleux de sa carte bancaire sans perte ni vol préalable de cette dernière. Dans un autre courrier du 26 décembre 2014 adressé à Mme N..., la Caisse indique que les opérations de paiement par carte bancaire contestées ont été effectuées sur des sites sécurisés 3DS avant la mise en opposition de la carte bancaire le 21 octobre 2014 à 9h25. La cour relève que sur les notices d'information relatives aux usages frauduleux de cartes bancaires et aux dispositions du code monétaire et financier en la matière, sur les courriers des 25 novembre et 26 décembre 2014, et sur le relevé et informations bancaires à entête de la Caisse daté du 5 novembre 2014, Mme N... est domiciliée à Grande-Synthe, [...]. La Caisse produit au débat un "Dossier Phishing" au nom de Mme N... et daté du 22 avril 2015 ; il résulte de ce dossier : - en premier lieu, un détail des opérations réalisées :

Date
Heure
Montant
Devise
(..)
Réseau
(.)
Enseigne
Localisation
Date règlement

20/10/2014
16:30:31
922,34
EUR2
(...)
Mastercard
(...)
RED UNIVERSAL MARKETIN

MADRID
21/10/2014

20/10/2014
16:27:09
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

20/10/2014
16:39:19
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

20/102014
16:53:47
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

20/10/2014
16:46:27
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

20/10/2014
16:49:17
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

20/10/2014
16:35:54
911
EUR2
(...)
Domestique
(...)

FREE MOBILE
PARIS
21/10/2014

20/10/2014
17:24:14
30
EUR2
(...)
Domestique
(...)
TICKET TRANSFER
BOULOGNE BILLANCOURT
21/10/2014

20/10/2014
16:32:56
911
EUR2
(...)
Domestique
(...)
FREE MOBILE
PARIS
21/10/2014

- en deuxième lieu, l'adresse IP utilisée a été localisée à Paris, étant précisé par la cour que Mme N..., comme cela a été précédemment relevé, est manifestement domiciliée à Grande-Synthe, - en troisième lieu, le numéro utilisé pour recevoir les codes de confirmation est le [...] , soit le numéro de Mme N..., - en quatrième lieu, un transfert d'appel de sa ligne SFR a eu lieu vers un mobile orange dont le numéro est le [...] , - en cinquième lieu, Mme N... a fait opposition sur sa carte bancaire Gold n° [...] le 21 octobre 2014 à 9h25, et le motif d'opposition est le suivant : perte sans code. La Caisse produit aussi au débat une facture SFR du 24 octobre 2014, au nom de Mme N..., domiciliée [...] , dont il apparaît que le 20 octobre 2010, 21 appels ont été enregistrés vers un mobile orange dont le numéro est le [...] ; la cour relève que ces appels ont été effectués entre 16h et 17h30 pour des durées n'excédant pas 1 minute. Il résulte de ces éléments que les données attachées à la carte bancaire Gold n° [...] de Mme N... ont été utilisées pour réaliser les achats suivants via le système 3D Secure : - le 20 octobre 2014, à 16h27'09 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h30'31 pour un montant de 922,34 euros, auprès de l'enseigne "Red Universal Marketin" à Madrid, - le 20 octobre 2014, à 16h32'56 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h35'54 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h39'19 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h46'27 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h49'17 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 16h53'47 pour un montant de 911 euros auprès de l'enseigne "Free Mobile" à Paris, - le 20 octobre 2014, à 17h24'14 pour un montant de 30 euros auprès de l'enseigne "Ticket Transfer" à Boulogne Billancourt ; - le 20 octobre 2014 pour un montant de 50 euros auprès de l'enseigne "Topengo" à Limoges, étant précisé que l'heure de l'opération n'est pas connue au vu des pièces fournies au débat. Il résulte également de ces éléments que les circonstances entourant l'utilisation du système 3D Secure généré à partir de la carte de crédit Gold n° [...] de Mme N... démontrent manifestement que les opérations litigieuses réalisées le 20 octobre 2014 entre 16h27'09 et 171124'14 auprès des enseignes "Free Mobile" et "Red Universal Marketin", outre celle réalisée auprès de l'enseigne "Topengo", ont nécessairement été effectuées à l'insu de Mme N..., par le biais d'un détournement frauduleux par un tiers des données attachées à ses instruments de paiement et des données qui y sont attachées, de sorte que ces opérations doivent être regardées comme n'ayant pas été autorisées par le payeur au sens des dispositions de l'article L. 133-18 du code monétaire et financier. A titre surabondant, la cour observe que la circonstance que Mme N... n'ait pas déposé plainte n'est pas suffisante en soi pour démontrer l'absence de réalité de la fraude ou que les opérations litigieuses réalisées le 20 octobre 2014 n'ont pas été effectuées à son insu. Surabondamment encore, la cour observe que la circonstance que le 20 octobre 2014, 21 appels ont été enregistrés vers un mobile orange dont le numéro est le [...] n'est pas suffisante en soi pour démontrer l'absence de réalité de la fraude ou que les opérations litigieuses réalisées le 20 octobre 2014 n'ont pas été effectuées à l'insu de Mme N.... 1.2. Sur la divulgation des données personnelles par Mine N... En premier lieu, il est établi, à la lecture du "Dossier Phishing" au nom de Mme N..., daté du 22 avril 2015, et du courrier de la Caisse du 26 décembre 2014 adressé à Mme N..., que cette dernière a fait une mise en opposition sur sa carte bancaire Gold n° [...] le 21 octobre 2014 à 9h25, et que le motif d'opposition est le suivant : perte sans code. Il s'ensuit que Mme N... a réagi rapidement au détournement de ses données en faisant opposition à sa carte de crédit dès les lendemains matin des opérations litigieuses, étant rappelé que celles-ci sont datées du 20 octobre 2014. De surcroît, Mme N... s'est présentée les 22 octobre et 1er décembre 2014 au Commissariat de secteur de Grande-Synthe

pour déclarer l'utilisation frauduleuse de sa cal te de paiement, d'une carte contrefaite ou des données liées à la carie (numéro, date d'expiration) tel que cela résulte des deux notices d'information relatives aux usages frauduleux de cartes bancaires et aux dispositions du code monétaire et financier qu'elle produit au débat. En second lieu, les pièces versées au débat montrent que la Caisse rapporte la preuve que les opérations de paiement contestées ont été authentifiées, dûment enregistrées et comptabilisées, et qu'elles n'ont pas été affectées par une défaillance technique ou autre, étant toutefois précisé que les utilisations successives des données attachées à la carte bancaire Gold n° [...] de Mme N... ne suffisent pas en tant que telles à prouver que les opérations ont été autorisées par Mme N... ou qu'elle n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. Dans ses écritures, la Caisse indique que "la société SFR, partie en première instance, n'a jamais confirmé ce renvoi ; indiquant par ailleurs qu'un tel service ne pouvait être mis en place qu'à partir du domicile de l'abonné" ; la Caisse poursuit en précisant que "l'opérateur téléphonique a rappelé que le numéro vers lequel la ligne aurait été réorientée est celui d'un correspondant habituel du foyer" et qu'"au jour de la fraude, il y a eu 21 appels enregistrés vers le numéro [...]". La cour observe, à la lecture du "Dossier Phishing" au nom de Mme N..., daté du 22 avril 2015, que le numéro utilisé pour recevoir les codes de confirmation est le [...] , soit le numéro de Mme N..., et qu'un transfert d'appel de sa ligne SFR a eu lieu vers un mobile orange dont le numéro est le [...] . La cour observe également, au vu de la facture SFR du 24 octobre 2014 au nom de Mme N..., produite au débat par la Caisse, que si le 20 octobre 2010, 21 appels ont été enregistrés vers un mobile orange dont le numéro est le [...] , ces appels ont été effectués entre 16h et 17h30 pour des durées n'excédant pas 1 minute. Ce faisant, la Caisse ne produit au débat aucune autre pièce de nature à démontrer que Mme N... serait à l'origine de ce transfert d'appel, voire même qu'une personne vivant à son domicile, ou qu'un de ses proches, aurait effectué ledit transfert d'appel. Au surplus, la Caisse a adressé le 4 décembre 2014 un courrier à Mme N... avec pour objet "Blocage carte bancaire : présomption d'utilisation frauduleuse", étant relevé que ce courrier précise que "l'examen des dernières opérations effectuées avec votre carte bancaire n° [...] (...) nous conduisent à suspecter une utilisation frauduleuse de cet instrument de paiement". Il en résulte que l'envoi de ce courrier le 4 décembre 2014 relatif à une nouvelle utilisation frauduleuse de l'instrument de paiement de Mme N..., postérieurement à la mise en opposition de la carte bancaire Gold n° [...] le 21 octobre 2014, n'est pas particulièrement cohérent avec la thèse de la Caisse sur la circonstance alléguée mais non démontrée par celle-ci, que Mme N... aurait nécessairement et volontairement communiqué ses informations personnelles et confidentielles à un tiers par négligence grave ou par manquement intentionnel à ses obligations lui incombant en la matière, voire même qu'elle aurait agi frauduleusement. La cour observe encore que, dans ses écritures, la Caisse ne fait qu'évoquer au conditionnel la thèse du "phishing" dont Mme N... aurait été la victime malgré l'information qu'elle fait de cette pratique auprès de ses clients. La Caisse ne peut pas utilement se contenter d'exposer que Mme N... ne donne aucune explication rationnelle sur la survenance des opérations qu'elle conteste, et notamment sur le contexte du détournement ou les circonstances d'utilisation du système 3D Secure, étant rappelé que la Caisse est tenue de prouver, sans que soient méconnues les exigences d'un procès équitable et de la loyauté dans l'administration de la preuve, l'implication à un titre ou à un autre de Mme N... dans les opérations litigieuses pour caractériser sa négligence fautive ou un manquement intentionnel à ses obligations légales ou contractuelles, voire même son action frauduleuse. Au surplus, il n'est nullement établi par la Caisse que Mme N... a transmis à un tiers ses identifiants, son code confidentiel personnel, ses clés confidentielles ou ses coordonnées personnelles. En conséquence, la Caisse est défaillante dans l'établissement du manquement intentionnel ou de la négligence grave allégués à l'encontre de Mme N.... Le jugement sera donc confirmé en ce qu'il a condamné la Caisse à rembourser à Mme N... les sommes prélevées sur son compte à son insu, étant précisé qu'il résulte des pièces produites au débat et de ce qui a été précédemment énoncé que les sommes frauduleusement prélevées s'élèvent à la somme de 7 379,34 euros et non à celle de 7.425 euros comme retenu par le premier juge »

AUX MOTIFS, A LES SUPPOSER ADOPTES, QUE « I) SUR LA RESPONSABILITE DE LA CAISSE DE CREDIT MUTUEL En vertu de l'article L 131-9 du Code Monétaire et Financier, «1) 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 autorisé 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 attachés. 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 ». L'article 1315 du Code Civil énonce, quant à lui, que « Celui qui réclame l'exécution d'une obligation doit la prouver. Réciproquement, celui qui s'en prétend libéré, doit justifier le paiement ou le fait qui a produit l'exécution de l'obligation ». Sur le détournement Il appartient au payeur de prouver en premier lieu le détournement de son instrument de paiement ou des données qui lui sont liées. Cette preuve se fait par tout moyen. En l'espèce, les transactions litigieuses ont été effectuées à partir d'une carte GOLD ouverte au nom de Mme B... N.... La Caisse CREDIT MUTUEL Dunkerque Malo a mis en place la procédure requise pour sécuriser les transactions, dénommée « 3D SECURE » ainsi qu'en atteste la pièce produite au débat sous forme de tableau récapitulatif, notamment l'envoi sur le serveur local de la ligne fixe de Mme N..., dont le numéro d'appel est en l'occurrence [...], du code à 6 chiffres requis pour l'autorisation du paiement. Ainsi la Caisse CREDIT MUTUEL a procédé à la délivrance le 20 octobre 2014 et ce, à 9 reprises, d'un code à 6 chiffres, entre 16h27 et 17h24. Toutefois, Mme N... dément avoir saisi les codes. Au contraire, alertée par l'envoi de ces codes sur son serveur vocal, elle a formé opposition le 21 octobre 2014. A supposer la bonne foi des parties 'se pose néanmoins l'existence d'une fraude réalisée à l'insu de Mme N..., payeur. Cette fraude semble pouvoir s'établir à partir de plusieurs éléments. En effet, le tableau « 3D SECURE » produit par la Caisse CREDIT MUTUEL atteste que les prélèvements se sont faits à un rythme anormalement accéléré, en moyenne trois minutes, entre deux prélèvements, ce qui semble pour le moins difficile à réaliser. De même, il conviendra de relever que 7 prélèvements dont le montant est identique, en l'espèce 911 euros, l'ont

été-par le site www. Mobile.free.fr. Un autre prélèvement de 922,34 euros a été réalisé à partir du site www.rumho.fr. Enfin, un prélèvement du 22 octobre 2014, que Mine N... soutient frauduleux, fait état d'une somme de 50 euros, depuis le site de TOPENGO. Le montant total des sommes prélevées est de 7.425 euros. Il est permis de douter que ce soit Mme N... elle-même qui ait procédé à ces prélèvements, au vu de la nature de ces achats identiques, ainsi que de leur montant, Mme N... ne travaillant qu'à mi-temps et percevant un salaire de 750 euros mensuel. La Caisse CREDIT MUTUEL Dunkerque Malo n'apportant aucun éclaircissement sur ces éléments, il apparaît comme manifeste que les prélèvements se sont faits à l'insu de Mme N... de manière frauduleuse. Sur la négligence de Mine N... La preuve de la négligence repose sur la banque. Les modalités exactes du détournement, c'est-à-dire le dispositif mis en place par le fraudeur pour obtenir les données confidentielles restent inconnues. Alertée par l'envoi à plusieurs reprises des codes, elle a procédé le lendemain au blocage de son compte et de sa carte de paiement. Elle a déposé à deux reprises une main courante au commissariat de GRANDE-SYNTHE. La caisse CREDIT MUTUEL soutient que le jour de la fraude, 21 appels ont été enregistrés vers le numéro [...]. Elle explique que si Mme B... N... n'est pas à l'origine des prélèvements litigieux, dans ce cas, ces nombreux appels ont été réalisés par un proche de Mme B... N..., qui a pu mettre en place le renvoi d'appel à partir de son domicile et vers un correspondant connu et habituel. La Caisse CREDIT MUTUEL relève que ce correspondant sera par ailleurs contacté à 22 autres reprises entre le 27 octobre 2014 et le mois de janvier 2015. Toutefois elle ne démontre pas la preuve que le transfert d'appel a été effectué par un proche de Mme N.... Ainsi, la caisse CREDIT MUTUEL échouant à démontrer la négligence de Mme N..., la responsabilité de cette dernière n'est pas engagée. Les conséquences financières des prélèvements frauduleux auraient dû être supportées par la caisse CREDIT MUTUEL. Ainsi, celle-ci se verra condamnée à rembourser à Mme B... N... la totalité des sommes prélevées sur son compte à son insu, soit la somme de 7.425 euros »

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 la négligence grave s'entend de la carence de l'utilisateur du service de paiement à prendre toute mesure raisonnable pour assurer la confidentialité de ses données personnelles ; qu'en jugeant que la négligence grave de l'utilisateur de services de paiement « confin[ait] au dol et dénot[ait] l'inaptitude de celui-ci dans l'accomplissement de son obligation de préserver la sécurité de ses dispositifs de sécurité personnalisés, de sorte que cette négligence grave [était] d'une importance telle qu'elle [rendait] impossible le remboursement des sommes débitées à la suite d'opérations de paiement non autorisées par l'utilisateur de services », pour apprécier l'existence d'une négligence grave de la part de Mme N... au regard de cette définition, la cour d'appel a violé les articles L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier ;

2°) ALORS QUE si, selon l'article L. 133-23 du code monétaire et financier, 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, elle peut suffire à rapporter une telle preuve, en fonction des circonstances particulières du litige qu'il incombe aux juges du fond d'examiner ; que pour condamner la Caisse de Crédit Mutuel de Dunkerque Malo à rembourser à Mme N... le montant d'opérations réalisées au débit de son compte bancaire, la cour d'appel, après avoir constaté que la banque rapportait la preuve que les opérations de paiement contestées avaient « été authentifiées, dûment enregistrées et comptabilisées, et qu'elles n'[avaient] pas été affectées par une défaillance technique ou autre, tel un piratage » (p. 8, 3ème §), a néanmoins considéré que les utilisations successives des données attachées à la carte de Mme N... ne pouvaient suffire à prouver que les opérations litigieuses avaient été autorisées par cette dernière, ou qu'elle n'aurait pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière, et a jugé que la banque, qui se bornait à faire état de l'hypothèse d'un « phishing », était défaillante dans l'administration de la preuve de la négligence grave qu'aurait commise Mme N... ; qu'en statuant de la sorte, quand l'utilisation d'un service de paiement sans défaillance technique est susceptible de démontrer la commission par l'utilisateur de ce service d'une négligence grave dans la conservation de ses données, ce qu'il lui incombait de rechercher au regard des caractéristiques en matière de sécurité des services de paiement employés, la cour d'appel a violé les articles L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier ;

3°) ALORS, EN OUTRE, 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 l'existence d'une négligence grave doit être appréciée au regard de l'ensemble des circonstances de la cause, et peut être prouvée par tous moyens, en particulier eu égard aux caractéristiques de l'instrument de paiement en termes de fiabilité et de sécurité ; qu'en s'abstenant de rechercher, comme elle y était invitée (conclusions d'appel de la banque, not. p. 3-4) si la circonstance que les opérations de paiement litigieuses avaient été effectuées via le système de paiement sécurisé 3D SECURE, nécessitant, outre la fourniture des informations présentes sur la carte du sociétaire (nom, cryptogramme visuel, numéro et date d'expiration de la carte), un code de confirmation adressé sur le téléphone portable de ce dernier, ne permettait de présumer que Mme N... avait été gravement négligente dans la conservation de ses données personnelles, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier ;

4°) ALORS QU' en retenant que l'envoi par la Caisse de Crédit Mutuel de Dunkerque-Malo d'un courrier le 4 décembre 2014 faisant état de l'éventuelle « utilisation frauduleuse » de la carte bancaire de Mme N... « [n'était] pas particulièrement cohérent[e] avec la thèse de la Caisse sur la circonstance, alléguée mais non démontrée par celle-ci, que Mme N... aurait nécessairement et volontairement communiqué ses informations personnelles et confidentielles à un tiers par négligence grave (
) », la cour d'appel, qui s'est fondée sur une circonstance impropre à exclure la négligence grave invoquée par la banque, a violé les articles L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier, ensemble l'article 1134 du code civil (dans sa version applicable en l'espèce) ;

5°) ALORS, EN OUTRE, QUE le principe de l'égalité des armes implique que chaque partie ait la possibilité de faire valoir ses prétentions et moyens dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à

son contradicteur ; qu'en jugeant qu'il incombait à la Caisse de Crédit Mutuel de Dunkerque-Malo de prouver « l'implication à un titre ou à un autre de Mme N... dans les opérations litigieuses pour caractériser sa négligence fautive ou son manquement intentionnel, voire son action frauduleuse », et qu'elle ne pouvait invoquer l'article 6 paragraphe 1er de la Convention européenne des droits de l'Homme sur la nécessité d'un procès équitable quand le prestataire de service de paiement ne dispose d'aucun autre moyen de preuve effectif pour démontrer la négligence grave qu'aurait commise son client, la cour d'appel a méconnu les exigences de l'article 6 § 1er de la Convention Européenne des Droits de l'Homme, ensemble les articles L. 133-15, L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier, ensemble l'article 1315 du code civil (nouvel article 1353 du code civil).

ECLI:FR:CCASS:2019:CO00552

Analyse

Décision attaquée : Cour d'appel de Douai , du 1 février 2018