Références

Cour de cassation
chambre commerciale
Audience publique du mercredi 29 mai 2019
N° de pourvoi: 17-28271
Non publié au bulletin **Rejet**

Mme Mouillard (président), président
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 :

Sur la déchéance du pourvoi, en ce qu'il est formé contre l'arrêt du 12 janvier 2017 :

Vu l'article 978 du code de procédure civile ;

Attendu que, le mémoire en demande ne contenant aucun moyen dirigé contre l'arrêt du 12 janvier 2017, il y a lieu de constater la déchéance du pourvoi en ce qu'il est formé contre cette décision ;

Sur le moyen unique du pourvoi, en ce qu'il est formé contre l'arrêt du 8 juin 2017 :

Attendu, selon l'arrêt attaqué (Douai, 8 juin 2017), que Mme H..., titulaire d'un compte dans les livres de la société Caisse de crédit mutuel du Quesnoy (la banque), a assigné celle-ci en remboursement d'opérations de paiement du prix d'achats effectués par Internet au moyen des systèmes de paiement « Payweb » et « 3D Secure » qu'elle contestait avoir autorisées ;

Attendu que la banque fait grief à l'arrêt de la condamner à payer à Mme H... les sommes de 1 399,96 euros au titre des opérations non autorisées, de 158 euros au titre des frais et intérêts prélevés sur son compte et de 1 000 euros à titre de dommages-intérêts alors, selon le moyen :

1°/ 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 société Caisse de crédit mutuel du Quesnoy à rembourser à Mme H... le montant d'opérations réalisées au débit de son compte bancaire, et à l'indemniser des préjudices qu'elle avait subis, 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'ont pas été affectées par une défaillance technique ou autre », a néanmoins considéré que « les utilisations successives des données attachées à la carte de Mme H... ne suffis[aient] pas en tant que telles à prouver que les opérations ont été autorisées par Mme H... ou qu'elle n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière », et a considéré 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 de Mme H... ; 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 ;

2°/ que la preuve d'un fait juridique peut être rapportée par tout moyen, y compris par présomption ; qu'en s'abstenant de rechercher, comme elle y était invitée, si la circonstance que les opérations de paiement litigieuses avaient été effectuées via les systèmes de paiement sécurisés « payweb » et « 3D secure », lesquels nécessitaient pour fonctionner non seulement que l'utilisateur accède à son espace personnel en renseignant son identifiant et son mot de passe, mais également une clé personnelle figurant sur une carte établie sur support papier et remise par la banque au client, ainsi qu'un code de confirmation adressé sur l'adresse email ou le téléphone portable de ce dernier (s'agissant du système « payweb ») ou d'un code confidentiel temporaire également adressé sur le téléphone du client (en ce qui concerne le système « 3D secure »), ne permettait pas de démontrer que Mme H... avait nécessairement été négligente dans la conservation des données confidentielles permettant l'utilisation de ces systèmes de paiement hautement sécurisés, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-16, L. 133-19, IV, et L. 133-23 du code monétaire et financier ;

Mais attendu que si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, dans leur rédaction issue de l'ordonnance n° 2009-866 du 15 juillet 2009 transposant la directive 2007/64/CE du 13 novembre 2007, 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 même 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 ; que le moyen, qui postule le contraire, n'est pas fondé ;

PAR CES MOTIFS :

CONSTATE la déchéance du pourvoi, en ce qu'il est formé contre l'arrêt du 12 janvier 2017 ;

REJETTE le pourvoi en ce qu'il est formé contre l'arrêt du 8 juin 2017 ;

Condamne la société Caisse de crédit mutuel du Quesnoy aux dépens ;

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

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-neuf mai 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 du Quesnoy

Il est fait grief à l'arrêt infirmatif attaqué D'AVOIR condamné la CAISSE DE CREDIT MUTUEL DU QUESNOY à payer à Madame H... la somme de 1.399,96 € au titre des opérations non autorisées, la somme de 158 € au titre des frais et intérêts prélevés sur son compte pour dépassement de l'autorisation de découvert, et la somme de 1.000 € à titre de dommages et intérêts ;

AUX MOTIFS QUE « 2. Sur la demande en remboursement de Mme H... 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. Sur l'existence du détournement Le document "Gestion monétique et services clients", produit par la Caisse, montre qu'à partir de la carte de crédit n° [...] : - ont été respectivement créées deux cartes "Payweb" le 1er mai 2013 à 6h19 et 52 secondes et 6h38 et 47 secondes pour un montant de 700 euros et de 1 000 euros, - ont été effectuées, le 1er mai 2013 à 00h00, à partir de ces cartes "Payweb" les cinq opérations suivantes pour un montant de : - 519,90 euros auprès de l'enseigne WU [...] dont la localisation se trouve être : [...], - 343,70 euros auprès de l'enseigne www.watchshop.com dont la localisation se trouve être : [...] - 10,03 euros auprès de l'enseigne EZETOP*TOPUP dont la localisation se trouve être ezetop.com, - 10,03 euros auprès de l'enseigne EZETOP*TOPUP dont la localisation se trouve être ezetop.com, -4,36 euros auprès de l'enseigne EZETOP*TOPUP dont la localisation se trouve être ezetop.com, - soit un montant total de 888,02 euros. Au vu des pièces produites au débat, l'adresse IP utilisée pour ces opérations porte le numéro 41.142.187.98. Le document "Gestion monétique et services clients", produit par la Caisse, montre également qu'à partir de la carte de crédit n° [...] : - a été commandé un paiement via le système "3D Secure" le 2 mai 2013 à 7h44 et 37 secondes pour un montant de 519,90 euros ; - a été effectuée, le 2 mai 2013 à 00h00, après cette commande, une opération pour un montant de 519,90 euros auprès de l'enseigne WU [...] dont la localisation se trouve être : [...]. Au vu des pièces produites au débat, l'adresse IP

utilisée pour cette opération porte le numéro 217.108.228.209. Dans le traçage des différentes opérations et interventions figurant dans ce document "Gestion monétique et services clients", l'incident pour ces deux opérations est daté du 1er mai 2013 à 00h00 et l'opposition à la carte bancaire est datée au 2 mai 2013 à 17h21 sous le motif "vol sans code". Il convient également de préciser que le document "Gestion monétique et services clients" montre, qu'à partir de la carte de crédit n° [...], créée suite à la première mise en opposition le 2 mai 2013 : - a été créé une carte "Payweb" le 11 mai 2013 à 3h58 et 41 secondes pour un montant de 1 000 euros ; - a été effectuée, le 11 mai 2013, à partir de cette carte "Payweb" une opération d'un montant de 1,80 euros auprès de l'enseigne OODOC localisé à Paris. Au vu des pièces produites au débat, l'adresse IP utilisée pour cette opération porte le numéro 41.143.110.78. Dans le traçage des différentes opérations et interventions figurant dans ce document "Gestion monétique et services clients", l'incident pour cette opération est daté du 17 mai 2013 à 17h00 et l'opposition à la carte bancaire est datée au 17 mai 2013 à 17h08 sous le motif "vol sans code". Il en résulte : - d'une part, qu'à l'exception de la carte "Payweb" créée le 11 mai 2013 à partir de la carte de crédit n° [...] et utilisée le même jour pour un paiement de 1,80 euros auprès de l'enseigne OODOC à Paris que la Caisse a pris en charge, les cartes "Payweb" créées le 1er mai 2013, à partir de la carte de crédit n° [...], ont permis d'effectuer le Ier mai 2013 à 00h00 trois achats auprès de l'enseigne EZETOP*TOPUP, un achat auprès de l'enseigne www.watchshop.com, et un paiement auprès de la banque Western Union, tandis que la commande d'un paiement via le système "3D Secure", à partir de la carte de crédit n° [...], a permis d'effectuer le 2 mai 2013 à 00h00 un autre paiement auprès de la banque Western Union, - d'autre part, qu'à chaque connexion à la banque à distance, une adresse IP différente a été utilisée. Mme H... conteste être à l'origine de ces paiements en raison notamment de son absence entre le 2 mai 2013 et le 10 mai 2013. Aux termes du relevé bancaire que Mme H... produit au débat, outre le fait que les cinq paiements réalisés le Ier mai 2013 via le système "Payweb" pour un montant total de 888,02 euros ont pour dates de valeurs les 2, 3 et 6 mai 2013 et le fait que le paiement réalisé le 2 mai 2013 via le système "3D Secure" pour un montant de 519,90 euros a pour date de valeur le 6 mai 2013, ont notamment été effectuées les opérations suivantes : - le 27 avril 2013, un paiement en carte bancaire à Senlis pour un montant de 27,60 euros lequel a pour date de valeur le 2 mai 2013, - le 30 avril 2013, un paiement en carte bancaire à Le Quesnoy pour un montant de 31 euros lequel a pour date de valeur le 2 mai 2013, - le 30 avril 2013, un paiement en carte bancaire à Le Quesnoy pour un montant de 64,88 euros lequel a pour date de valeur le 2 mai 2013, - le 2 mai 2013, un retrait "DAB" à Le Quesnoy pour un montant de 50 euros, lequel a pour date de valeur le 2 mai 2013, - le 2 mai 2013, un retrait "DAB" "REF02725A04"pour un montant de 310 euros, lequel a pour date de valeur le 2 mai 2013, - le 2 mai 2013, un paiement en carte bancaire à Le Quesnoy pour un montant de 38,75 euros lequel a pour date de valeur le 3 mai 2013, - le 2 mai 2013, un paiement en carte bancaire à Le Quesnoy pour un montant de 30 euros lequel a pour date de valeur le 6 mai 2013, - le 2 mai 2013, un paiement en carte bancaire à Le Quesnoy pour un montant de 40,15 euros lequel a pour date de valeur le 6 mai 2013, - le 11 mai 2013, un retrait "C.ARGENT [...]" pour un montant de 200 euros, lequel a pour date de valeur le 13 mai 2013. Il s'ensuit que c'est à tort que le premier juge a considéré que des opérations avaient été effectuées à Le Quesnoy le 2 mai 2013 pour 64,88 euros, le 3 mai 2013 pour 38,75 euros et le 6 mai 2013 pour 30 euros et 40,15 euros afin de démontrer que la carte bancaire de Mme H... a été utilisée sur Le Quesnoy alors que Mme H... prétendait être absente ces deux jours, les dates retenues par le premier juge correspondant en réalité aux dates de valeur et non aux dates d'utilisation de la carte bancaire. En l'état de ces énonciations et constatations, les circonstances entourant la création et l'utilisation des cartes "Payweb" et du système "3D Secure" générés à partir de la carte de crédit n° [...] démontrent suffisamment que les opérations litigieuses réalisées le 1er et le 2 mai 2013 ont nécessairement été effectuées à l'insu de Mme H... par le biais d'un détournement frauduleux par un tiers de ses instruments de paiement ou 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 ; il s'ensuit que c'est à tort que le premier juge a considéré qu'il n'était pas établi que les moyens de paiement de Mme H... ont fait l'objet d'un détournement ou d'une fraude. Le jugement attaqué sera donc infirmé en ce qu'il a dit que la preuve d'un détournement et d'une fraude des moyens de paiement d'U... H... n'est pas rapporté. Sur la divulgation des données personnelles par Mme H... En premier lieu, il est établi que : - Mme H... a fait une première mise en opposition de sa carte bancaire le 2 mai 2013 à 17h21 pour un vol sans code, tel que cela résulte du courrier du courrier du 26 juin 2013 du Crédit Mutuel Nord Europe produit au débat par Mme H..., et du document "Gestion monétique et services distants" produit au débat par la Caisse ; - Mme H... s'est présentée le 11 mai 2013 à la brigade de gendarmerie de Le Quesnoy pour déclarer l'utilisation de ses références de carte bancaire, tel que cela résulte de la notice d'information relative aux usages frauduleux de cartes bancaires et aux dispositions du code monétaire et financier en la matière qu'elle produit au débat ; - Mme H... a ouvert un dossier Réclamation / Sinistre Carte le 11 mai 2013. Il s'ensuit que Mme H... a réagi rapidement au détournement de ses données en informant immédiatement la Caisse, ainsi qu'en faisant opposition à sa carte de crédit. 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 de Mme H... ne suffisent pas en tant que telles à prouver que les opérations ont été autorisées par Mme H... ou qu'elle n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. A l'examen des mails reçus par Mme H... les 6 mai 2013 à 4h59, 9 mai 2013 à 4h58, et 10 mai 2013 à 17h39, la cour constate que le logo de la Caisse est absent, que les mails contiennent de nombreuses fautes d'orthographe et qu'ils sont rédigés avec une ponctuation absente et une syntaxe aléatoire ; il s'ensuit à l'évidence que Mme H... a été la destinataire de mails dit de "phishing", lesquels sont destinés à recueillir les coordonnées et les données strictement confidentielles dont le destinataire est le gardien. Force est cependant de constater que ces mails ont été reçus par Mme H... postérieurement aux opérations litigieuses des 1 et 2 mai 2013 ; ils sont donc insuffisants à démontrer le manquement intentionnel ou la négligence grave de Mme H... allégué par la Caisse, étant au surplus remarqué que dans ses écritures, la Caisse ne fait qu'évoquer au conditionnel la thèse du "phishing" dont Mme H... aurait pu être la victime malgré l'information qu'elle fait de cette pratique auprès de ses clients. Il convient encore de préciser que selon le document "Gestion monétique et services clients", produit par la Caisse, une nouvelle création de carte "Payweb" a été effectuée le 11 mai 2013 à 3h58 et 41 secondes pour un montant de 1 000 euros, laquelle a permis un paiement de 1,80 euros auprès de l'enseigne OODOC localisé à Paris ; cette création de carte "Payweb" et ce paiement ont été réalisés alors que Mme H... avait fait opposition auprès de la Caisse le 2 mai 2013 à 17h21 suite aux opérations litigieuses du 1er et 2 mai 2013, de sorte ces opérations datées du 11 mai 2013 ne sont pas particulièrement cohérentes avec la thèse de la banque sur l'implication personnelle de

Mme H... dans les opérations litigieuses des 1er et 2 mai 2013, voire même sur la circonstance que Mme H... aurait nécessairement autorisé les opérations litigieuses ou communiqué ses données personnelles et confidentielles à un tiers par négligence grave ou par manquement intentionnel à ses obligations lui incombant en la matière. Il résulte ensuite des pièces versées au débat que les messages de confirmation ont été adressés sur la boîte mail personnelle de Mme H... dont cette dernière "estime ne pas avoir été trompée par un état de "phishing"" ou soutient que "même si [elle] avait fait l'objet de ce que l'on appelle un "hameçonnage" ou "phishing", il est incontestable que ses données ont été saisies par ruse" ; la circonstance que les codes de confirmation aient été envoyés sur l'adresse mail de Mme H... ne suffit néanmoins pas en tant que tel à prouver que les opérations litigieuses ont nécessairement été autorisées par Mme H... ou que celle-ci n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière. La Caisse ne peut enfin pas utilement se contenter d'exposer que Mme H... ne donne aucune explication rationnelle sur la survenance des opérations qu'elle conteste, et notamment sur le contexte du détournement ou les circonstances de la création de la carte de paiement "payweb", étant rappelé que la Caisse est tenue de prouver l'implication à titre ou à un autre de Mme H... dans les opérations litigieuses pour caractériser sa négligence fautive ou son manquement intentionnel, voire même son action frauduleuse. Au surplus, il n'est nullement établi par la Caisse que Mme H... a transmis à un tiers ses identifiants, son code confidentiel personnel, ses clés confidentielles ou ses coordonnées personnelles. En l'état de ces énonciations et constatations, la Caisse est défaillante dans l'établissement du manquement intentionnel ou de la négligence grave alléguée à l'encontre de Mme H.... Le jugement attaqué sera donc infirmé en ce qu'il a débouté Mme H... de l'ensemble de ses demandes, la Caisse devant être condamnée à payer à Mme H... la somme de 1.399,96 euros au titre des opérations non autorisées. Mme H... sollicite également le remboursement des frais de fonctionnement et agios prélevés sur son compte depuis le mois d'août 2014 à hauteur de la somme de 259,30 euros. A la lecture des relevés bancaires d'août 2014 à mai 2015 que Mme H... verse au débat, la Cour constate que : - des frais de cotisation pour la tenue du compte bancaire "Eurocompte confort" ont été facturés mensuellement à Mme H... pour un montant total de 101,30 euros ; cette somme correspond à l'abonnement "Eurocompte confort", tel que cela ressort des conditions particulières de la convention de compte courant conclue entre Mme H... et la Caisse que cette dernière produit au débat ; - des frais de "commission d'intervention" et des frais "INT/FRAIS TX DEBIT" ont été facturés à Mme H... pour un montant total de 158 euros ; cette somme correspond aux frais et intérêts prélevés sur le compte de Mme H... à raison du dépassement de son découvert autorisé. En conséquence, la Caisse sera condamnée à rembourser à Mme H... les frais et intérêts prélevés sur son compte pour dépassement de l'autorisation de découvert, soit la somme de 158 euros ;

1°) 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 CREDIT MUTUEL DU QUESNOY à rembourser à Madame H... le montant d'opérations réalisées au débit de son compte bancaire, et à l'indemniser des préjudices qu'elle avait subis, 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'ont pas été affectées par une défaillance technique ou autre » (p. 8, 2ème §), a néanmoins considéré que « les utilisations successives des données attachées à la carte de Mme H... ne suffis[aient] pas en tant que telles à prouver que les opérations ont été autorisées par Mme H... ou qu'elle n'a pas satisfait intentionnellement ou par négligence grave aux obligations lui incombant en la matière », et a considéré 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 de Madame H... ; 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 ;

2°) ALORS SUBSIDIAIREMENT QUE la preuve d'un fait juridique peut être rapportée par tout moyen, y compris par présomption ; qu'en s'abstenant de rechercher, comme elle y était invitée, si la circonstance que les opérations de paiement litigieuses avaient été effectuées via les systèmes de paiement sécurisés « payweb » et « 3D SECURE », lesquels nécessitaient pour fonctionner non seulement que l'utilisateur accède à son espace personnel en renseignant son identifiant et son mot de passe, mais également une clef personnelle figurant sur une carte établie sur support papier et remise par la banque au client, ainsi qu'un code de confirmation adressé sur l'adresse email ou le téléphone portable de ce dernier (s'agissant du système payweb) ou d'un code confidentiel temporaire également adressé sur le téléphone du client (en ce qui concerne le système « 3D SECURE »), ne permettait pas de démontrer que Madame H... avait nécessairement été négligente dans la conservation des données confidentielles permettant l'utilisation de ces systèmes de paiement hautement sécurisés, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-16, L. 133-19 IV et L. 133-23 du code monétaire et financier.

ECLI:FR:CCASS:2019:CO00459

Analyse

Décision attaquée : Cour d'appel de Douai , du 8 juin 2017