RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Légifrance
Le service public de la diffusion du droit

Références

Cour de cassation
chambre commerciale
Audience publique du mercredi 23 octobre 2019
N° de pourvoi: 18-15823
Non publié au bulletin **Rejet**

M. Rémery (conseiller doyen faisant fonction de président), président
SCP Célice, Soltner, Texidor et Périer, SCP de Chaisemartin, Doumic-Seiller, avocat(s)

Texte intégral

REPUBLIQUE FRANCAISE

AU NOM DU PEUPLE FRANCAIS

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

Sur le moyen unique :

Attendu, selon l'arrêt attaqué (Reims, 9 février 2018), que M. et Mme L..., titulaires d'un compte dans les livres de la société Caisse de crédit mutuel de Châlons-en-Champagne (la banque), ont assigné celle-ci en remboursement d'opérations de retrait et d'achats réalisées par Internet au moyen des systèmes "e-retrait" et "Payweb cards" qu'ils contestaient avoir autorisés ;

Attendu que la banque fait grief à l'arrêt de la condamner à payer à M. et Mme L... les sommes de 2 931,56 euros, 37,82 euros et 1 200 euros alors, selon le moyen :

1°/ 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 ; qu'en jugeant, après avoir pourtant retenu qu'il résultait du rapport établi par le service fraudes et affaires spéciales de la banque « que c'est à la suite d'une opération dite de « phishing » résultant elle-même vraisemblablement de la réception par Madame L... d'un SMS frauduleux le 27 octobre 2013 l'invitant à mettre à jour ses coordonnées sur le site de la banque que les données personnelles et confidentielles permettant l'identification des époux L... sur le site de la banque en ligne ont été récupérées par des tiers qui ont à leur [tour] procédé au retrait et aux différents paiements frauduleux » que le fait d'avoir été surpris par une telle manoeuvre ne constituait pas une négligence grave, la cour d'appel a méconnu les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

2°/ que la preuve de la négligence grave commise par l'utilisateur d'un service de paiement peut être rapportée par tout moyen, au regard de l'ensemble des circonstances de l'espèce et en particulier des caractéristiques de l'instrument de paiement utilisé en matière de sécurité ; qu'en affirmant que la banque ne pouvait rapporter la preuve d'une négligence qu'aurait commise l'utilisateur du service de paiement qu'en démontrant que l'instrument de paiement mis en oeuvre était « totalement inviolable », la cour d'appel a encore violé les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

3°/ 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 ; qu'en l'espèce, la cour d'appel a constaté que le système de paiement utilisé pour effectuer les opérations litigieuses était « particulièrement sécurisé », mais a néanmoins considéré, pour condamner la banque à rembourser le montant des débits contestés par les époux L..., que cette dernière

« n'établi[ssait] pas qu'un tel processus serait totalement inviolable et qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte, en ce compris les données figurant sur la carte de code ci-dessus évoquée », quand il lui appartenait de rechercher, ainsi qu'elle y était invitée, si l'utilisation du service de paiement sécurisé payweb et e-retrait ne permettait pas d'établir, ou à tout le moins de présumer, que les époux L... avaient été gravement négligents dans la conservation de leurs données personnelles, la cour d'appel a violé les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

4°/ qu'en exigeant de la banque qu'elle démontre que le service de paiement « payweb » utilisé pour réaliser les opérations litigieuses était « totalement inviolable » et « qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte, en ce compris les données figurant sur la carte de code ci-dessus évoquée », la cour d'appel lui a imposé la démonstration d'une preuve impossible, violant ainsi l'article 1315 du code civil, ensemble l'article 9 du code de procédure civile et le principe d'égalité des armes résultant de l'article 6 § 1 de la Convention européenne des droits de l'homme ;

5°/ que la banque faisait valoir que les opérations de paiement litigieuses avaient été effectuées via le système de paiement sécurisé payweb card et e-retrait, 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 ; qu'en se bornant à retenir que la carte de code à quatre chiffres payweb avait pu se trouver en possession d'un tiers, sans rechercher, ainsi qu'elle y était invitée, si la circonstance que les opérations de paiement litigieuses avaient été effectuées par le biais d'un instrument de paiement nécessitant de disposer simultanément de plusieurs données confidentielles figurant sur des supports différents, dont le client avait légalement comme contractuellement la charge d'assurer la conservation, ne permettait pas de démontrer ou à tout le moins de présumer la négligence grave commise par ce dernier, la cour d'appel n'a pas donné de base légale à sa décision au regard des articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

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 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, en ses deuxième, troisième et cinquième branches, postule le contraire, manque en droit ;

Attendu, en deuxième lieu, qu'il ne résulte d'aucune constatation de l'arrêt que le message d'hameçonnage du 27 octobre 2013, en réponse auquel, à supposer ce fait établi, Mme L... aurait communiqué des données personnelles liées à son instrument de paiement, ait contenu des indices permettant à un utilisateur normalement attentif de douter de sa provenance ;

Et attendu, enfin, que la cour d'appel n'a pas exigé de la banque qu'elle démontre que le système de paiement "Payweb" serait totalement inviolable et qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte mais s'est bornée à retenir qu'en l'absence d'une telle démonstration, il appartenait à la banque d'établir, par d'autres moyens, la négligence grave qu'elle imputait à sa cliente ;

D'où il suit que le moyen n'est pas fondé ;

PAR CES MOTIFS :

REJETTE le pourvoi ;

Condamne la société Caisse de crédit mutuel Châlons-en-Champagne aux dépens ;

Vu l'article 700 du code de procédure civile, rejette sa demande et la condamne à payer à M. et Mme L... la somme globale 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-trois octobre deux mille dix-neuf, et signé par lui, Mme Vaissette, conseiller qui en a délibéré, en remplacement de M. Guerlot, conseiller référendaire rapporteur, empêché, et Mme Labat, greffier de chambre, qui a assisté au prononcé de l'arrêt.
MOYEN ANNEXE au présent arrêt

Moyen produit par la SCP Célice, Soltner, Texidor et Périer, avocat aux Conseils, pour la société Caisse de crédit mutuel Châlons-en-Champagne

Il est fait grief à l'arrêt attaqué D'AVOIR condamné la Caisse de Crédit Mutuel de Chalons en Champagne à payer à Monsieur et à Madame L... les sommes de 2.931,56 € en remboursement des opérations frauduleuses survenues le 27 octobre 2013 sur leur compte bancaire, outre celle de 37,82 € en remboursement du prélèvement sur leur compte, à la

date du 2 avril 2014, d'agios du même montant calculés sur le découvert provoqué par lesdites opérations, et la somme de 1.200 € à titre de dommages et intérêts ;

AUX MOTIFS PROPRES QUE « Les époux L... font valoir à titre liminaire que les conditions générales dont ils ont eu connaissance ne mentionnent pas la possibilité d'avoir accès aux services Payweb Card et E-Retrait. Toutefois, la banque produit en pièce numéro un une convention dite « formule clé » signée de l'un et l'autre des époux L... le 9 février 2010 reconnaissant avoir reçu en temps utile les conditions générales n° 17.03.1507/09 contenant les conditions générales de banque et les conditions générales de produits et services. Ce document, produit en pièce numéro deux par la banque, fait apparaître au titre des conditions générales CMNE Direct la possibilité d'avoir accès aux services Payweb Card. La contestation soulevée à ce titre par les époux L... ne peut donc être retenue par la cour. Il résulte des dispositions du code monétaire et financier relatives aux instruments de paiement dotés d'un dispositif de sécurité personnalisé et notamment de l'article L. 133-19 : - que la responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à son insu, l'instrument de paiement ou les données qui lui sont liées, - que le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sapait ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133-17. Les articles L. 133-16 et L. 133-17 imposent à l'utilisateur du service une obligation de prendre « toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées » ainsi qu'une obligation d'information de la banque « lorsqu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement ou des données qui lui sont liées », et ceci « aux fins de blocage de l'instrument ». Par ailleurs, l'article L. 133-23 du code monétaire et financier dispose :« 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. Le prestataire de services de paiement, y compris, le cas échéant, le prestataire de services de paiement fournissant un service d'initiation de paiement, fournit des éléments afin de prouver la fraude ou la négligence grave commise par l'utilisateur de services de paiement. ». Contrairement à ce que soutient la banque dans ses conclusions, les dispositions de l'alinéa deux de cet article n'instituent aucune présomption ni aucun renversement de la charge de la preuve en faveur du prestataire de services de paiement lorsque l'opération de paiement a été enregistrée comme en l'espèce sans défaillance technique. La banque dans ses conclusions décrit avec précision le processus de création d'une Payweb Card qu'elle qualifie de hautement sécurisé, la création de la carte virtuelle nécessitant en premier lieu l'accès aux services de banque à distance par la saisie d'un identifiant et d'un mot de passe personnels puis l'obtention d'un numéro virtuel obtenu après la saisie d'une clé personnelle se trouvant sur une carte de code remise au client par la banque et dont il est le gardien et doit assurer la confidentialité, le processus se terminant par l'envoi d'un code de confirmation par mail ou par SMS devant être renseigné dans un certain délai. Elle fait valoir à ce titre que pour aboutit à la création de cette carte; l'utilisateur doit connaître l'identifiant de connexion au site en ligne de la banque, le mot de passe correspondant et se trouver en possession de la carte de clé personnelle contenant 64 codes outre la possession du téléphone portable ou de l'adresse e-mail du titulaire du compte. S'il est exact que ce processus est particulièrement sécurisé, et s'il est exact également que, comme l'établit la banque, les paiements litigieux sont intervenus conformément au processus ainsi sécurisé (pièce numéro 3,14 et 15 produite par la banque), elle n'établit pas qu'un tel processus serait totalement inviolable et qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte, en ce compris les données figurant sur la carte de codes ci-dessus évoquée. Dans ces conditions, il ne saurait être retenu à défaut de tout autre élément que le titulaire du compte aurait manqué à l'obligation de conservation et d'utilisation prudente de l'instrument de paiement qui lui est imposée par l'article L. 133-16 du code monétaire et financier. En l'espèce, il apparaît à la lecture même du rapport établi par le service « fraude et affaires spéciales » du Crédit mutuel produit en pièce numéro trois par la banque que c'est à la suite d'une opération dite de « phishing » résultant elle-même vraisemblablement de la réception par Madame L... d'un SMS frauduleux le 27 octobre 2013 l'invitant à mettre à jour ses coordonnées sur le site de la banque que les données personnelles et confidentielles permettant l'identification des époux L... sur le site de la banque en ligne ont été récupéré par des tiers qui ont à leur procédé au retrait et aux différents paiements frauduleux. Le détail de l'opération est décrit dans le rapport du service fraudé affaire spéciales de la banque. Comme l'indique ce rapport, en transmettant un code de confirmation frauduleux reçue par SMS et en l'utilisant vraisemblablement sur un site se présentant frauduleusement comme celui de la banque, Madame L... a pensé valider ses coordonnées personnelles sur le véritable site de l'organisme bancaire. Il n'est d'ailleurs pas impossible que, comme le suggèrent les époux L..., la réponse aux SMS frauduleux ait été apportée par un tiers ayant eu accès à la carte de code confidentiel, éventuellement parmi leur entourage, dans le cadre d'une opération concertée avec l'expéditeur du SMS. En toute hypothèse, à supposer que la réponse aux SMS l'invitant à modifier ses coordonnées émane de Madame L..., le fait d'avoir était surpris par une telle manoeuvre ne constitue pas à lui seul la négligence grave requise par l'article L. 133-23 du code monétaire et financier. Quant à la carte de code à quatre chiffres qui sécurise plus spécialement suivant la banque les opérations de type Payweb Card et E Retrait, elle peut s'être trouvée en possession d'un tiers, notamment dans l'entourage des époux L..., sans qu'une négligence grave puisse de ce seul fait être mise à leur charge pas plus qu'un manquement à l'obligation de conservation et d'utilisation prudente des instruments de paiement i reposée par l'article L. 133-16 du code monétaire et financier. Dans la lettre de leur conseil en date du 8 décembre 2014, les époux L... Lisaient savoir à la banque que deux adresses IP à l'origine, l'une du prélèvement du 27 octobre, l'autre des débits datés du 27 octobre provenaient d'Angleterre et du Maroc. La banque, dans son courrier en réponse, n'a pas contesté ces éléments. Enfin, la banque, au regard même de l'éventualité d'une opération de phishing dont elle n'a pu avoir connaissance que sur la foi des informations données par les époux L... eux-mêmes, ne saurait utilement soutenir que l'application des dispositions ci-dessus rappelées, qui met à sa charge la preuve d'une négligence grave de son client, serait excessive, la mettrait dans l'impossibilité de s'exonérer de sa responsabilité et serait ainsi contraire aux principes du procès équitable. Compte tenu de l'ensemble de ces éléments, la banque ne rapporte pas la

preuve d'agissements frauduleux ou d'une négligence grave imputable aux époux Dintrich.Il serait inéquitable que les époux L... conservent à leur charge le montant des frais irrépétibles engagés pour les besoins de la présente instance. La banque sera condamnée à lui payer la somme de 2.000 € en application de l'article 700 du code de procédure civile »

ET AUX MOTIFS, A LES SUPPOSER ADOPTES, QU' « A titre liminaire, il convient de mettre hors de cause la Fédération du CREDIT MUTUEL NORD EUROPE, le rapport contractuel étant uniquement entre Mr et Mme S... L... et la CAISSE DE CREDIT MUTUEL DE CHALONS EN CHAMPAGNE ayant un établissement à SAINT MEMMIE. Sur les demandes de remboursement des sommes débitées le 23 octobre 2013 et des agios prélevés L'article L. 133-18 du code monétaire et financier dispose : « En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu ». L'article L. 133-23 du code monétaire et financier indique : « 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 ». En l'espèce, le CREDIT MUTUEL indique que le processus de création d'une carte payweb ou d'un e-retrait est hautement sécurisé puisqu'il implique pour l'utilisateur de renseigner plusieurs données, à savoir : son identifiant, son mot de passe strictement personnel, une clef personnelle qui est un code à 4 chiffres présent sur une carte de clefs personnelles de 64 codes remise sur un support papier au sociétaire qui permet de générer un numéro virtuel. Dès que le sociétaire valide l'opération, un code de confirmation lui est envoyé par mail ou par sms. Ce code doit être renseigné dans un certain délai pour permettre la réalisation de l'opération. Le relevé de compte produit par Mr et Mme L... mentionne qu'un e-retrait de 500 € est intervenu le 27 octobre 2013 et que des débits pour un montant chacun de 607,89 € ont été effectués le 29 octobre 2013. Il ressort d'un courrier officiel daté du 8 décembre 2014 du conseil de Mr et Mme L... au conseil du CREDIT MUTUEL que l'e-retrait du 27 octobre 2013 a été effectué d'une adresse IP en Angleterre et que les quatre opérations de paiement ont été effectuées d'une adresse IP provenant du Maroc, ce qui établit que Mr et Mme L... ne peuvent en être les auteurs. Le rapport de faits établi par le service Fraudes et affaires spéciales du CREDIT MUTUEL indique que ces opérations ont été effectuées le 27 octobre 2013 après que la modification du numéro de téléphone et de l'adresse mails ait été réalisée via l'accès de la banque à distance ce même jour à 11 heures. Cependant, ne figurent pas sur le rapport, les étapes de déroulement de cette modification, notamment par une demande de modification du titulaire du compte, puis l'envoi au titulaire du compte d'un code de validation et le renseignement de ce code par l'utilisateur. Ainsi, il n'est pas démontré que Mme L... aurait validé la demande de changement des coordonnées téléphoniques et d'adresse de messagerie envoyée par sms le 27 octobre 2013 sur son téléphone portable. Le rapport du service Fraudes et affaire spéciales du CREDIT MUTUEL ne fait pas non plus apparaître le processus d'obtention d'un numéro virtuel pour chaque opération litigieuse, et notamment le renseignement de la carte de clé personnelle par l'utilisateur pour chacune d'elles. Ainsi, le CREDIT MUTUEL ne démontre pas que les opérations en question, en ce compris la modification des données téléphoniques et messagerie électronique, ont été authentifiées et n'ont pas été affectées par une déficience du système sécurisé. Par conséquent, la CAISSE DE CREDIT MUTUEL DE CHALONS EN CHAMPAGNE doit être condamnée à payer à Mr et Mme S... L... la somme de 2931,56 €
en remboursement des opérations frauduleuses survenues le 27 octobre 2013 sur leur compte bancaire, outre celle de 37,82 € en remboursement du prélèvement sur leur compte, à la date du 2 avril 2014, d'agios du même montant calculés sur le découvert provoqué par lesdites opérations. Sur la demande de dommages et intérêts Le refus de la CAISSE DE CREDIT MUTUEL DE CHALONS EN CHAMPAGNE de procéder au remboursement des sommes débitées frauduleusement sur le compte de Mr et Mme L... leur a causé un préjudice moral et financier. Compte tenu de la somme importante prélevée et de son ancienneté, il convient de condamner la CAISSE DE CREDIT MUTUEL DE CHALONS EN CHAMPAGNE à leur verser une somme de 1200 €. Sur la capitalisation des intérêts Les intérêts afférents aux condamnations n'ayant pas couru depuis plus d'une année, il convient de débouter Mr et Mme L... de leur demande de capitalisation fondée sur l'ancien article 1154 du code civil. Sur la demande de publication du jugement La nature du litige ne justifie pas que soit ordonnée la publication du présent jugement et les demandeurs seront déboutés de cette demande non fondée. Sur les demandes accessoires La CAISSE DE CREDIT MUTUEL DE CHALONS EN CHAMPAGNE, partie succombante, sera condamnée aux dépens. Par ailleurs, il est équitable de la condamner à payer à Mr et Mme L... une indemnité de 2000 au titre des frais irrépétibles. Enfin, la nature et l'ancienneté du litige justifie le prononcé de l'exécution provisoire »

1°) 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 attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage ; qu'en jugeant, après avoir pourtant retenu qu'il résultait du rapport établi par le service fraudes et affaires spéciales du CREDIT MUTUEL « que c'est à la suite d'une opération dite de « phishing » résultant elle-même vraisemblablement de la réception par Madame L... d'un SMS frauduleux le 27 octobre 2013 l'invitant à mettre à jour ses coordonnées sur le site de la banque que les données personnelles et confidentielles permettant l'identification des époux L... sur le site de la banque en ligne ont été récupérées par des tiers qui ont à leur [tour] procédé au retrait et aux différents paiements frauduleux » que le fait d'avoir été surpris par une telle manoeuvre ne constituait pas une négligence grave, la cour d'appel a méconnu les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

2°) ALORS ENCORE QUE la preuve de la négligence grave commise par l'utilisateur d'un service de paiement peut être rapportée par tout moyen, au regard de l'ensemble des circonstances de l'espèce et en particulier des caractéristiques de l'instrument de paiement utilisé en matière de sécurité ; qu'en affirmant que la banque ne pouvait rapporter la preuve d'une négligence qu'aurait commise l'utilisateur du service de paiement qu'en démontrant que l'instrument de paiement

mis en oeuvre était « totalement inviolable », la cour d'appel a encore violé les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

3°) 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 ; qu'en l'espèce, la cour d'appel a constaté (arrêt, p. 4, 2ème §) que le système de paiement utilisé pour effectuer les opérations litigieuses était « particulièrement sécurisé », mais a néanmoins considéré, pour condamner la banque à rembourser le montant des débits contestés par les époux L..., que cette dernière « n'établi[ssait] pas qu'un tel processus serait totalement inviolable et qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte, en ce compris les données figurant sur la carte de code ci-dessus évoquée », quand il lui appartenait de rechercher, ainsi qu'elle y était invitée, si l'utilisation du service de paiement sécurisé payweb et e-retrait ne permettait pas d'établir, ou à tout le moins de présumer, que les époux L... avaient été gravement négligents dans la conservation de leurs données personnelles, la cour d'appel a violé les articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier ;

4°) ALORS QU' en exigeant de la Caisse de Crédit Mutuel qu'elle démontre que le service de paiement « payweb » utilisé pour réaliser les opérations litigieuses était « totalement inviolable » et « qu'il ne serait pas possible à un tiers, par une opération frauduleuse, de récupérer les données personnelles et confidentielles du titulaire du compte, en ce compris les données figurant sur la carte de code ci-dessus évoquée », la cour d'appel a imposé à l'exposante la démonstration d'une preuve impossible, violant ainsi l'article 1315 du code civil, ensemble l'article 9 du code de procédure civile et le principe d'égalité des armes résultant de l'article 6 § 1 de la Convention européenne des droits de l'Homme ;

5°) ALORS, EN OUTRE, QUE la Caisse de Crédit Mutuel faisait valoir (ses conclusions d'appel, not. p. 3 à 6 ; p. 11 à 14) que les opérations de paiement litigieuses avaient été effectuées via le système de paiement sécurisé payweb card et e-retrait, 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 ; qu'en se bornant à retenir que la carte de code à quatre chiffres payweb avait pu se trouver en possession d'un tiers, sans rechercher, ainsi qu'elle y était invitée, si la circonstance que les opérations de paiement litigieuses avaient été effectuées par le biais d'un instrument de paiement nécessitant de disposer simultanément de plusieurs données confidentielles figurant sur des supports différents, dont le client avait légalement comme contractuellement la charge d'assurer la conservation, ne permettait pas de démontrer ou à tout le moins de présumer la négligence grave commise par ce dernier, la cour d'appel n'a pas donné de base légale à sa décision au regard des articles L. 133-16, L. 133-19 et L. 133-23 du code monétaire et financier.

ECLI:FR:CCASS:2019:CO00788

Analyse

Décision attaquée : Cour d'appel de Reims , du 9 février 2018