28 mars 2018

Cour de cassation

Pourvoi nº 16-20.018

Chambre commerciale financière et économique - Formation de section

Publié au Bulletin

ECLI:FR:CCASS:2018:CO00346

Titres et sommaires

BANQUE - paiement - instrument de paiement - utilisation frauduleuse par un tiers - responsabilité du titulaire - fraude ou non-respect des obligations - appréciation - eléments à considérer - négligence grave - applications diverses - communication des données personnelles en réponse à un courriel contenant des indices permettant à un utilisateur normalement attentif de douter de sa provenance

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

Texte de la **décision**

Entête

COMM.

LG

COUR DE CASSATION

_____

Audience publique du 28 mars 2018

Cassation

Mme X..., président

Arrêt n° 346 FS-P+B

Pourvoi n° Q 16-20.018

R É P U B L I Q U E F R A N Ç A I S E

_____

AU NOM DU PEUPLE FRANÇAIS

_____

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

Statuant sur le pourvoi formé par la société Caisse de crédit mutuel de Beauvais, société coopérative de crédit, dont le siège est [...], contre l'arrêt rendu le 19 avril 2016 par la cour d'appel d'Amiens (1re chambre civile), dans le litige l'opposant à M. Jean-François Y..., domicilié [...], défendeur à la cassation ;

La demanderesse invoque, à l'appui de son pourvoi, le moyen unique de cassation annexé au présent arrêt ;

Vu la communication faite au procureur général ;

LA COUR, composée conformément à l'article R. 431-5 du code de l'organisation judiciaire, en l'audience publique du 27 février 2018, où étaient présents : Mme X..., président, Mme B..., conseiller référendaire rapporteur, M. Rémery, conseiller doyen, M. Guérin, Mme Vallansan, M. Remeniéras, Mmes Graff-Daudret, Vaissette, Bélaval, conseillers, Mmes Schmidt, Jollec, Brahic-Lambrey, M. Blanc, conseillers référendaires, M. Graveline, greffier de chambre ;

Sur le rapport de Mme B..., conseiller référendaire, les observations de la SCP Célice, Soltner, Texidor et Périer, avocat de la société Caisse de crédit mutuel de Beauvais, de Me Z..., avocat de M. Y..., l'avis de Mme A..., avocat général, et après en avoir délibéré conformément à la loi ;

Exposé du litige

Attendu, selon l'arrêt attaqué, qu'invoquant le caractère frauduleux de paiements par carte bancaire et par virement débités sur deux comptes ouverts à son nom dans les livres de la société Caisse de crédit mutuel de Beauvais (la banque), M. Y... a assigné cette dernière en remboursement de ces sommes ; que la banque s'y est opposée en lui reprochant une négligence grave dans la garde et la conservation de ses données personnelles du dispositif de sécurité de ces instruments de paiement ;

Moyens

Sur le moyen unique, pris en sa cinquième branche :

Attendu que la banque fait grief à l'arrêt de la condamner à payer à M. Y... la somme de 2 731,98 euros au titre des paiements frauduleux par carte bancaire et celle de 4 500 euros au titre du virement litigieux débité de son Livret Bleu alors, selon le moyen, que la circonstance qu'un service de paiement doté d'un dispositif de sécurité ait été utilisé pour des achats sur internet par utilisation, outre des données afférentes à sa carte bancaire, d'un code adressé directement

au client sur son téléphone mobile ou fixe, permettant à l'utilisateur de venir authentifier le paiement au moyen d'une donnée confidentielle ne se trouvant pas sur la carte de paiement proprement dite, fait à tout le moins présumer le défaut de garde des données confidentielles d'instrument de paiement et la négligence grave de son utilisateur dans la préservation de la confidentialité de ses données personnelles ; qu'il appartient dans ces circonstances à l'utilisateur du service de paiement de rapporter par tous moyens la preuve qu'il a respecté son obligation de conserver les données confidentielles permettant l'utilisation du service qui lui a été proposé ; qu'en statuant comme elle l'a fait, sans rechercher, ainsi qu'elle y était invitée, si la circonstance que les débits litigieux aient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à M. Y..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, ne faisait pas présumer la négligence grave de l'utilisateur dans la conservation de ses données personnelles, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

Motivation

Mais attendu que, 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 même code, 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 n'est pas fondé ;

Moyens

Mais sur le moyen, pris en ses deuxième et quatrième branches :

Motivation

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

Attendu que pour statuer comme il fait, l'arrêt, après avoir relevé que M. Y... a été victime d'un hameçonnage, ayant reçu des courriels successifs portant le logo parfaitement imité du Crédit mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même jusqu'à demander à la banque la communication de sa nouvelle carte de clefs personnelle pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté, retient que la banque convient que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message, sont de nature à interpeller le client, ce à quoi n'est pas nécessairement sensible un client non avisé, étant observé que M. Y..., qui ne se connectait quasiment jamais au site internet de la banque, ignorait les alertes de cette dernière sur le hameçonnage, puis en déduit que c'est à son insu que M. Y... a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte et que n'est pas constitutive d'une négligence grave le fait pour un client "normalement" attentif de n'avoir pas perçu les indices propres à faire douter de la provenance des messages reçus ;

Qu'en statuant ainsi, 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, la cour d'appel a violé les textes susvisés ;

Dispositif

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

CASSE ET ANNULE, en toutes ses dispositions, l'arrêt rendu le 19 avril 2016, entre les parties, par la cour d'appel d'Amiens ; remet, en conséquence, la cause et les parties dans l'état où elles se trouvaient avant ledit arrêt et, pour être fait droit, les renvoie devant la cour d'appel de Rouen ;

Condamne M. Y... aux dépens ;

Vu l'article 700 du code de procédure civile, rejette les demandes ;

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

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

Moyens annexés

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 de Beauvais

Il est fait grief à l'arrêt partiellement infirmatif attaqué D'AVOIR condamné la Caisse de Crédit Mutuel de Beauvais à payer à Monsieur Jean-François Y... la somme de 2.731,98 € au titre des paiements frauduleux par carte bancaire, ainsi que la somme 4.500 € au titre du virement litigieux de son Livret Bleu, et une indemnité de procédure de 1.500 €,

AUX MOTIFS PROPRES QU' « II est renvoyé pour un plus ample exposé des faits, prétentions et moyens des parties au jugement entrepris duquel il résulte essentiellement que : - M. Y... est titulaire auprès du Crédit Mutuel en vertu d'un contrat Eurocompte Confort souscrit le 30 novembre 2010, d'un compte-courant et d'un Livret bleu sur lesquels ont été débitées les 13,14 et 18 septembre 2012 les sommes de 2 731,98 € (compte-courant) et 4 500 € (Livret bleu) dont M. Y... a sollicité, amiablement puis judiciairement, le remboursement auprès de sa banque au prétexte qu'ils étaient frauduleux, - le Crédit Mutuel s'y est opposé reprochant à M. Y... une négligence grave dans la garde et la conservation de ses données personnelles. C'est dans ces conditions qu'est intervenu le jugement entrepris qui a estimé au regard de la convention des parties la banque tenue de rembourser les paiements, effectués par carte bancaire faute d'établir que M. Y... avait communiqué les données concernant sa carte bancaire, mais non le virement opéré à partir du Livret bleu, M. Y... ayant reconnu la communication, sans précaution, de ses codes d'accès internet. Sur l'obligation de la banque : * Au titre des paiements par carte bancaire : Le Crédit Mutuel, qui rappelle les dispositions de l'article L 133-9 du code monétaire et financier applicables en l'espèce, se défend de toute obligation de prise en charge dès lors qu'il résulte du

rapport établi par son service des fraudes que les opérations litigieuses étaient sécurisées par le procédé " 3-D SECURE", protocole développé par Visa et Mastercard, qui impose à l'auteur du paiement de fournir en sus des informations usuelles fournies pour tout paiement "classique" (nom, numéro de carte, date de validité, cryptogramme), son identifiant d'accès au site du crédit mutuel, un mot de passe, une carte de clefs personnelle, son adresse mail et son mot de passe de messagerie. Il souligne la négligence grave commise par M. Y... pour avoir communiqué l'ensemble de ses données à la faveur de messages de "phishing" ne provenant manifestement pas du Crédit Mutuel mais d'expéditeurs inconnus, les dispositions de l'article 2.5.2 alinéa 2 des conditions générales de la convention de compte excluant toute obligation de paiement de la banque en cas de faute du client. M. Y... dément le rôle causal de la fourniture de ses codes personnels à la faveur du phishing dont il a été victime dans la mesure où ceux-ci étaient insuffisants pour procéder au paiement par carte bancaire sur internet, celui-ci requérant la communication de son cryptogramme qu'il conteste avoir fourni. Ainsi que le rappelle le Crédit Mutuel, les dispositions légales en la matière sont celles de l'article L 133-19 du code monétaire et financier dont il résulte notamment : - que la responsabilité du payeur (en l'espèce M. Y...) n'est pas engagée si l'opération de paiement a été effectuée en détournant à son insu l'instrument de paiement ou les données qui y sont liées, - que le payeur supporte toutes les pertes occasionnées par les 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 du code monétaire et financier lesquelles obligent notamment l'utilisateur d'un instrument de paiement à prendre toute mesure "raisonnable" pour préserver la sécurité du dispositif de sécurité personnalisé mis à sa disposition et à informer "sans tarder" le prestataire de toute utilisation de l'instrument de paiement sans son autorisation. Ces dispositions posent le principe de la prise en charge par la banque de toute utilisation frauduleuse d'un instrument de paiement mis à disposition du client (ainsi, comme en l'espèce, une carte bancaire) qui serait la conséquence d'une défaillance technique du dispositif de sécurité et/ou qui ne serait pas imputable à une démarche frauduleuse ou une négligence grave du client. L'analyse du Crédit Mutuel repose sur un rapport de ses propres services dont il résulterait en substance d'une part que son système de sécurité 3-D SECURE serait infaillible, d'autre part que M. Y... aurait commis une négligence grave. Aucun rapport d'un expert indépendant ne vient tout d'abord confirmer l'infaillibilité de ce système de sécurité 3-D SECURE et l'impossibilité absolue pour un informaticien de le détourner pour pouvoir utiliser à son insu la carte bancaire d'un client, étant observé que M. Y... prétend n'avoir jamais fourni le cryptogramme situé au dos de sa carte (laquelle est toujours restée en sa possession).Il sera ensuite rappelé que, dès la réception de messages "SMS" l'avisant d'opérations de paiement en cours, M. Y... s'est rapproché de sa banque et, sur ses conseils, a fait opposition, ce qui prouve une attitude "raisonnable" du client. S'agissant de la négligence grave, il ressort des explications et pièces fournies que M. Y... a été victime d'un "phishing" (hameçonnage) qui consiste, pour des tiers non identifiés, à adresser au client d'une banque des mails pouvant laisser croire qu'ils émanent de celle-ci, prétextant une nouvelle réglementation, la mise en oeuvre d'un nouveau système de sécurité (etc...), l'invitant pour ce faire à fournir l'ensemble des données personnelles composant le protocole sécurisé de paiement par carte bancaire, ce qui s'est produit en l'espèce, M. Y... ayant reçu des mails successifs portant le logo parfaitement imité du Crédit Mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même, semble-t-il, jusqu'à solliciter par mail de la banque la communication de sa nouvelle carte de clefs personnelle (élément essentiel du protocole 3-D SECURE) pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté... Le Crédit Mutuel convient que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message (!), sont de nature à interpeller le client, ce à quoi n'est pas nécessairement sensible un client non avisé, étant observé que M. Y... affirme sans être contredit qu'il ne se connectait quasiment jamais au site intemet du Crédit Mutuel (selon lui une fois en deux ans) en sorte qu'il ignorait les alertes du Crédit Mutuel sur le phishing. De ces circonstances la Cour déduit que c'est véritablement à son insu que M. Y... a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte et que n'est pas constitutive d'une négligence grave le fait pour un client "normalement" attentif de n'avoir pas perçu les indices propres à faire douter de la provenance des messages reçus. Le jugement sera, par suite, confirmé en ce qu'il condamne la banque à rembourser à l'intéressé les paiements litigieux. * Au titre du virement : Le phishing dont a été victime M. Y... a permis de même un virement d'une somme de 4 500 € dont, pour les motifs sus exposés, l'intéressé est fondé à solliciter le remboursement. Le jugement sera, par suite, réformé de ce chef et la banque condamnée au remboursement de cette somme. Sur les demandes accessoires : L'équité commande de faire application de l'article 700 du code de procédure civile au profit M. Y... exclusivement de suivant modalités prévues au dispositif » ;

ET AUX MOTIFS, A LES SUPPOSER ADOPTES DES PREMIERS JUGES, QUE « Sur la demande de dommages et intérêts : L'article 1134 du code civil dispose que les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites.

En l'espèce, Monsieur Y... a souscrit un contrat EUROCOMPTE CONFORT auprès de la CAISSE DE CREDIT MUTUEL DE BEAUVAIS le 30 novembre 2010 incluant une ouverture de compte courant, la mise à disposition d'une carte bancaire de paiement et l'accès aux services télématiques de la banque. L'article 2.5.2 alinéa 2 des conditions générales de la convention de compte stipule que s'agissant des opérations non autorisées, sauf faute imputable au client, la banque remboursera immédiatement le client, et le cas échéant, rétablira le compte débité dans la situation dans laquelle il se serait trouvé si l'opération de paiement n'avait pas eu lieu. L'article 10.1 des conditions générales du contrat porteur CB stipule que lorsque le titulaire de la carte CB nie avoir donné son consentement pour réaliser une opération de paiement et/ou de retrait, il appartient à l'émetteur d'apporter la preuve que l'opération a été authentifiée, dûment enregistrée et comptabilisée conformément à l'état de l'art et qu'elle n'a pas été affectée par une déficience technique. L'article 4 des conditions générales CMNE DIRECT stipule que le souscripteur est seul responsable de la garde, de la conservation et de la confidentialité des informations/données qui lui seront communiquées pour se connecter au serveur de la banque ; il est seul responsable de la conservation, de l'utilisation et de la sécurité relative auxdits éléments communiqués par la banque, et le cas échéant, des conséquences de leur divulgation ou de leur utilisation par des tiers, Il est constant que des paiements en ligne sont intervenus les 13 et 14 septembre 2012 par utilisation de la carte bancaire de Monsieur Y... pour un montant cumulé de 2.731,98 euros et qu'un virement de 4.500 euros a été effectué depuis son livret bleu via internet le 17 septembre 2012. Dès le 18 septembre 2012, Monsieur Y... a contesté être l'auteur de ces opérations. Il ressort de ses déclarations lors du dépôt de sa plainte le 19 septembre 2012 que le 20 août 2012, il a reçu un mail de "agence@mail-mail,com" pour fournir des codes d'accès qu'il avait reçu par courrier et qu'il a donc inscrit ses codes d'accès à l'endroit demandé. Les paiements effectués par carte bancaire nécessitant l'utilisation du numéro de la carte bancaire, de sa date d'expiration et du cryptogramme visuel figurant au verso, la CAISSE DE CREDIT MUTUEL DE BEAUVAIS ne saurait s'exonérer de l'application des dispositions précitée, des articles 2.5.2 alinéa 2 des conditions générales de la convention de compte et 10.1 des conditions générales du contrat porteur CB sans démontrer que la divulgation de ces données est le fait de Monsieur Y.... En l'absence d'une telle preuve, il convient de la condamner à rembourser à Monsieur Y... la somme de 2.731,98 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 constitue une négligence grave la fourniture par le client d'un établissement bancaire à un tiers de données confidentielles dont il a contractuellement la charge de la conservation, ayant permis ou facilité l'utilisation d'un service de paiement sécurisé, dès lors qu'aucune défaillance du système de paiement n'est établie ; qu'en l'espèce, il résulte de l'arrêt attaqué (p. 4, 3ème §) que Monsieur Y... « a été victime d'un « phishing » (
) qui consiste, pour des tiers non identifiés, à adresser au client d'une banque des mails pouvant laisser croire qu'ils émanent de celle-ci, prétextant une nouvelle réglementation, la mise en oeuvre d'un nouveau système de sécurité (etc...), l'invitant pour ce faire à fournir l'ensemble des données personnelles composant le protocole sécurisé de paiement par carte bancaire » et qu'en l'espèce, Monsieur Y... « ayant reçu des mails successifs portant le logo parfaitement imité du Crédit Mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même, semble-t-il, jusqu'à solliciter par mail de la banque la communication de sa nouvelle carte de clefs personnelle (élément essentiel du protocole 3-D SECURE) pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté » ; que pour juger néanmoins que Monsieur Y... n'avait pas commis de négligence grave dans la garde de ses données personnelles, la cour d'appel a considéré que seul « un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message (!), [étaient] de nature à interpeller le client » ; qu'en statuant de la sorte, quand il résultait de ses propres constatations que Monsieur Y... avait fourni à un tiers l'ensemble des données personnelles permettant l'utilisation du système de paiement 3D SECURE ainsi que d'effectuer des virements sur internet, ce qui caractérisait une négligence grave dans la conservation de ses données personnelles, la cour d'appel a violé les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

2°) ALORS AU SURPLUS QU' il résulte des énonciations de l'arrêt attaqué que Monsieur Y..., en réponse à des mails indiquant émaner du Crédit Mutuel, avait fourni « l'ensemble des données personnelles composant le protocole sécurisé de paiement par carte bancaire », un tel comportement « montr[ant] sa totale naïveté » (arrêt attaqué, p. 4, 3ème §) ; qu'en jugeant néanmoins que Monsieur Y... n'avait pas commis de négligence grave dans la conservation des données personnelles permettant l'utilisation des systèmes de paiement sécurisés mis à sa disposition par la banque, quand il résultait de ses propres constatations que Monsieur Y... avait fait preuve d'une « totale naïveté » en communiquant l'ensemble de ses données personnelles en réponse à des mails lui demandant de fournir ces informations, la cour

d'appel a derechef violé les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

3°) ALORS QUE l'objet du litige est déterminé par les conclusions respectives des parties ; qu'en l'espèce, la Caisse de Crédit Mutuel de Beauvais faisait valoir que Monsieur Y... avait commis une négligence grave en répondant au mail de « phishing » qu'il avait reçu le 20 août 2012, dans la mesure où « il aurait dû être interpellé par la nature de la demande et le message incohérent qui était délivré » (ses conclusions d'appel, p. 9, avant-dernier §) ; qu'elle soulignait également le caractère incohérent des mails reçus par Monsieur Y... les 6 et 23 mai 2012, en ce qu'ils comportaient des fautes de grammaire (« Vous pouvez plus » au lieu de « Vous ne pouvez plus »), provenaient d'adresses différentes et manifestement fantaisistes, ne mentionnaient pas le nom du destinataire, et faisaient référence à des achats sur internet alors que Monsieur Y... n'avait pas fourni cette information lors du dépôt de sa plainte auprès des services de police (conclusions d'appel du Crédit Mutuel, p. 7 à 9 ; p. 16) ; qu'en retenant que le Crédit Mutuel « conv[enait] que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message (!), [étaient] de nature à interpeller le client », quand l'exposante soulignait au contraire le caractère manifestement frauduleux des mails en cause, la cour d'appel a dénaturé les écritures de l'exposante, violant ainsi les articles 4 et 5 du code de procédure civile ;

4°) ALORS QUE commet une négligence grave dans la conservation de ses données personnelles le client qui les communique en réponse à un mail manifestement frauduleux ; qu'en l'espèce, il résulte des énonciations de l'arrêt attaqué que les mails reçus par Monsieur Y... comportaient des « adresses internet changeantes » et des indices laissant présumer leur origine frauduleuse tels « les fautes d'orthographes du message » ; qu'en jugeant néanmoins que ces éléments n'étaient pas nécessairement de nature à interpeller « un client non avisé », la cour d'appel a méconnu les articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil ;

5°) ALORS EN TOUT ETAT DE CAUSE QUE la circonstance qu'un service de paiement doté d'un dispositif de sécurité ait été utilisé pour des achats sur internet par utilisation, outre des données afférentes à sa carte bancaire, d'un code adressé directement au client sur son téléphone mobile ou fixe, permettant à l'utilisateur de venir authentifier le paiement au moyen d'une donnée confidentielle ne se trouvant pas sur la carte de paiement proprement dite, fait à tout le moins présumer le défaut de garde des données confidentielles d'instrument de paiement et la négligence grave de son utilisateur dans la préservation de la confidentialité de ses données personnelles ; qu'il appartient dans ces circonstances à l'utilisateur du service de paiement de rapporter par tous moyens la preuve qu'il a respecté son obligation de conserver les données confidentielles permettant l'utilisation du service qui lui a été proposé ; qu'en statuant comme elle l'a fait, sans rechercher, ainsi qu'elle y était invitée, si la circonstance que les débits litigieux aient été effectués par le biais d'un service de paiement sécurisé nécessitant la fourniture de données strictement personnelles à Monsieur Y..., et dont ce dernier avait contractuellement la charge d'assurer la conservation et la confidentialité, ne faisait pas présumer la négligence grave de l'utilisateur dans la conservation de ses données personnelles, la cour d'appel a privé sa décision de base légale au regard des articles L. 133-15, L. 133-16 et L. 133-19 du code monétaire et financier, ensemble l'article 1134 du code civil.

Textes **appliqués**

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

Rapprochements de **jurisprudence**

Com., 18 janvier 2017, pourvoi n° 15-18.102, Bull. 2017, IV, n° 6 (rejet).

Com., 25 octobre 2017, pourvoi n° 16-11.644, Bull. 2017, IV, n° 139 (cassation).