Texte intégral

Rejet
ECLI : ECLI:FR:CCASS:2025:CO00321
Formation de diffusion : F B
numéros de diffusion : 321

RÉPUBLIQUE FRANÇAISE

AU NOM DU PEUPLE FRANÇAIS

COMM.

HM

COUR DE CASSATION

_____

Arrêt du 12 juin 2025

Rejet

M. VIGNEAU, président

Arrêt n° 321 F-B

Pourvoi n° W 24-13.777

R É P U B L I Q U E F R A N Ç A I S E

_____

AU NOM DU PEUPLE FRANÇAIS

_____

ARRÊT DE LA COUR DE CASSATION, CHAMBRE COMMERCIALE, FINANCIÈRE ET ÉCONOMIQUE, DU 12 JUIN 2025

La société BNP Paribas, société anonyme, dont le siège est [Adresse 1], a formé le pourvoi n° W 24-13.777 contre l'arrêt rendu le 7 février 2024 par la cour d'appel de Paris (pôle 5, chambre 6), dans le litige l'opposant à la société [H] transports, société à responsabilité limitée, dont le siège est [Adresse 2], défenderesse à la cassation.

La demanderesse invoque, à l'appui de son pourvoi, un moyen de cassation.

Le dossier a été communiqué au procureur général.

Sur le rapport de M. Calloch, conseiller, les observations de la SCP Rocheteau, Uzan-Sarano et Goulet, avocat de la société BNP Paribas, de la SARL Meier-Bourdeau, Lécuyer et associés, avocat de la société [H] transports, et l'avis de Mme Henry, avocat général, après débats en l'audience publique du 29 avril 2025 où étaient présents M. Vigneau, président, M. Calloch, conseiller rapporteur, Mme Schmidt, conseiller doyen, et Mme Sezer, greffier de chambre,

la chambre commerciale, financière et économique de la Cour de cassation, composée des président et conseillers précités, après en avoir délibéré conformément à la loi, a rendu le présent arrêt.

Faits et procédure

1. Selon l'arrêt attaqué (Paris, 7 février 2024), le 23 juillet 2019, Mme [W], salariée de la société [H] transport dirigée par M. [G] [H] (la société) a été contactée téléphoniquement par une personne se présentant comme un technicien de la société BNP Paribas (la banque) lui demandant d'effectuer différentes manipulations à l'aide du système de paiement à distance afin permettre la réinscription d'opérations sur le compte.

2. A la suite de ces manipulations, deux virements ont été exécutés vers des comptes domiciliés en Allemagne pour une somme totale de 98 000 euros.

3. Après avoir déposé une plainte pour escroquerie et soutenant ne pas avoir autorisé ces paiements, la société a assigné la banque en réparation de ses préjudices.

Examen du moyen

Enoncé du moyen

4. La banque fait grief à l'arrêt de la condamner à payer à la société la somme de 98 000 euros au titre du remboursement des fonds, alors :

« 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 appel téléphonique dont la teneur permet à un interlocuteur normalement attentif de douter de sa provenance ; qu'en l'espèce, la cour d'appel a relevé qu'il ressortait de l'audition de [G] [H] que " ([R] [W]) ne s'est pas méfiée de son interlocuteur qui ne lui demandait pas de mot de passe (...) ; qu'elle a renouvelé la création d'une signature électronique, son interlocuteur prétendant que la manœuvre n'avait pas réussi " ; qu'elle a également relevé que l'audition de [R] [W] confirmait qu' " elle s'est connectée avec le boîtier et la carte, mais sans le mot de passe", que "l'escroc lui a alors demandé de se connecter et de se déconnecter à plusieurs reprises, puis de saisir la clef d'accès créée par le boîtier. Prétendant que cela ne fonctionnait pas, il lui a demandé d'essayer avec une autre clef d'accès qu'il lui a communiquée. Il lui a refait manipuler le boîtier à plusieurs reprises en l' 'embrouillant', puis lui a demandé de confirmer que le code qu'il lui indiquait au téléphone s'affichait, ce qui était le cas. Il lui a fait appuyer sur un ou deux boutons du boîtier, lui a demandé d'attendre et de confirmer. [R] [W] pense que c'est ce qui a créé une signature pour les virements" ; qu'en considérant qu' "il n'est pas démontré par la banque que la société [H] Transports ait commis une négligence grave exonérant la société BNP Paribas de son obligation de remboursement", quand il ressortait de ses propres constatations que Mme [W], et partant la société [H] Transports, avait

communiqué les données personnelles de son dispositif de sécurité en réponse à un appel téléphonique dont la teneur permettait à un interlocuteur normalement attentif de douter de sa provenance, la cour d'appel a violé les articles L. 133-16 et L. 133-19 du code monétaire et financier ;

2°/ que les juges du fond ne peuvent statuer par voie de simple affirmation sans viser ni analyser, fût-ce sommairement, les éléments sur lesquels ils fondent leur décision ; qu'en première instance, le tribunal de commerce de Paris avait retenu " que Mme [W] a été contactée par téléphone (mais qu'[H] n'apporte pas la preuve qu'il s'agit du numéro de la hotline de BNP)" ; qu'en affirmant de manière péremptoire que " la circonstance que l'escroc ait pu usurper un numéro de téléphone de la société BNP Paribas (...) était de nature à persuader ([R] [W]) qu'elle était en relation avec un technicien de la banque", sans viser ni analyser, fût-ce sommairement, les éléments de preuve sur lesquels elle se fondait pour juger que l'appel provenait d'un numéro de téléphone attribué à la société BNP Paribas, la cour d'appel a violé l'article 455 du code de procédure civile ;

3°/ que commet une négligence grave l'utilisateur de services de paiement qui omet de prendre toute mesure nécessaire pour préserver la sécurité de ses dispositifs de sécurité personnalisés ; qu'en l'espèce, l'article III des conditions générales de fonctionnement de la Carte Transfert Sécurisé (CTS) stipule que le détenteur d'un code personnel communiqué confidentiellement par la société BNP Paribas doit "tenir son code confidentiel absolument secret et ne le communiquer à quiconque" ; que l'article VII précise que "le Détenteur est responsable de l'utilisation et de la conservation de la Carte et du code confidentiel qui y est associé et de leur utilisation conformément aux présentes conditions de fonctionnement", l'article VIII ajoutant que "le Client est tenu solidairement et indivisément responsable de toutes les conséquences financières résultant de l'utilisation et de la conservation de la Carte par son Détenteur" ; qu'il résultait, en outre du bordereau BNP Net Entreprises (production) que Mme [W], désignée comme mandataire "M3", n'était pas habilitée à valider les "virements domestiques/Sepa" et "virements internationau " (" Choix des services et habilitation des mandataires") ; qu'en affirmant que "les documents contractuels et les guides et exemples d'utilisation du service BNP Net Evolution ne suffisent pas à établir les faits de négligence grave imputés à la société [H] Transports, consistant notamment à avoir

laissé [R] [W] utiliser la Carte Transfert Sécurité de [G] [H]", sans expliquer comment cette dernière avait pu valider les virements litigieux quand seule la Carte Transfert Sécurisé (CTS) de [G] [H] permettait de valider les virements internationaux, la cour d'appel a privé son arrêt de base légale au regard des articles L. 133-16 et L. 133-19 du code monétaire et financier ;

4°/ que commet une négligence grave l'utilisateur de services de paiement qui omet de prendre toute mesure nécessaire pour préserver la sécurité de ses dispositifs de sécurité personnalisés ; qu'en l'espèce, la cour d'appel a relevé qu'il ressortait de l'audition de [G] [H] que "([R] [W]) ne s'est pas méfiée de son interlocuteur qui ne lui demandait pas de mot de passe (...) ; qu'elle a renouvelé la création d'une signature électronique, son interlocuteur prétendant que la manœuvre n'avait pas réussi" ; qu'elle a également relevé que l'audition de [R] [W] confirmait qu'elle s'est connectée avec le boîtier et la carte, mais sans le mot de passe ", que l'escroc lui a alors demandé de se connecter et de se déconnecter à plusieurs reprises, puis de saisir la clef d'accès créée par le boîtier. Prétendant que cela ne fonctionnait pas, il lui a demandé d'essayer avec une autre clef d'accès qu'il lui a communiquée. Il lui a refait manipuler le boîtier à plusieurs reprises en l' 'embrouillant', puis lui a demandé de confirmer que le code qu'il lui indiquait au téléphone s'affichait, ce qui était le cas. Il lui a fait appuyer sur un ou deux boutons du boîtier, lui a demandé d'attendre et de confirmer. [R] [W] pense que c'est ce qui a créé une signature pour les virements " ; qu'il résultait de ces constatations que Mme [W] avait utilisé une CTS permettant de créer une signature pour la validation des virements internationaux, à savoir celle de [G] [H] ; qu'en affirmant, au contraire, qu' "il ne ressort pas de l'enquête de gendarmerie que [R] [W] ait utilisé la Carte Transfert Sécurisé de [G] [H] ", la cour d'appel qui n'a pas tiré les conséquences légales de ses propres constatations, a violé les articles L. 133-16 et L. 133-19 du code monétaire et financier. »

Réponse de la Cour

5. Après avoir exactement énoncé que, dans l'hypothèse d'ordres de paiement non autorisés, il appartient à la banque de fournir les éléments afin de prouver la faute ou la négligence grave commise par sa cliente, l'arrêt, se fondant sur les auditions par les services d'enquête du dirigeant et de l'employée de la société,

retient que la secrétaire de cette société avait reçu un appel téléphonique d'un soi-disant employé de la banque l'avertissant d'une panne informatique qui avait fait disparaitre les écritures du matin, et qu'à la demande de l'escroc, cette employée, après s'être connectée au service de paiement en ligne à l'aide du dispositif de sécurité personnalisé mais sans le mot de passe, avait effectué diverses manipulations afin de reconstituer les écritures sans se méfier de son interlocuteur qui ne lui demandait pas de mot de passe. Il relève que la circonstance que l'escroc ait pu usurper un numéro de téléphone de la banque et annoncer le code qui s'affichait sur l'écran de l'utilisatrice était de nature à persuader celle-ci qu'elle était en relation avec un technicien. Il ajoute que la connaissance par son interlocuteur des opérations réalisées avant l'appel et de leur disparition pouvait la conforter dans la croyance qu'un incident informatique était survenu. Il retient encore que l'historique des opérations versé aux débats par la société révèle que le numéro d'abonné du titulaire de la carte de transfert sécurisé n'était pas attaché à la validation des tiers.

6. De ces constatations et appréciations, la cour d'appel a pu déduire que la société n'avait pas commis de négligence grave dans la conservation et l'utilisation de ses données personnelles de sécurité.

7. Le moyen n'est donc pas fondé.

PAR CES MOTIFS, la Cour :

REJETTE le pourvoi ;

Condamne la société BNP Paribas aux dépens ;

En application de l'article 700 du code de procédure civile, rejette la demande formée par la société BNP Paribas et la condamne à payer à la société [H] transports la somme de 3 000 euros ;

Ainsi fait et jugé par la Cour de cassation, chambre commerciale, financière et économique, et prononcé publiquement le douze juin deux mille vingt-cinq par mise à disposition de l'arrêt au greffe de la Cour, les parties ayant été préalablement avisées dans les conditions prévues au deuxième alinéa de l'article 450 du code de procédure civile.

Décision attaquée : Cour d'appel Paris I6 2024-02-07 (Rejet)