bancaire multifonctions personnalisée et qui permet d'effectuer des paiements de faibles montants au débit du compte bancaire associé à cette carte.

3) L'article 63, paragraphe 1, sous b), de la directive 2015/2366 doit être interprété en ce sens que le paiement sans contact d'un montant de faible valeur au moyen de la fonction de communication en champ proche (Near Field Communication) d'une carte bancaire multifonctions personnalisée constitue une utilisation « anonyme » de l'instrument de paiement considéré, au sens de cette disposition dérogatoire.

4) L'article 63, paragraphe 1, sous a), de la directive 2015/2366 doit être interprété en ce sens qu'un prestataire de services de paiement qui entend se prévaloir de la dérogation prévue à cette disposition ne saurait se borner à affirmer qu'il est impossible de bloquer l'instrument de paiement concerné ou d'empêcher la poursuite de l'utilisation de celui-ci, alors que, au regard de l'état objectif des connaissances techniques disponibles, une telle impossibilité ne peut être établie.

Siège : M. J.-C. Bonichot, président de chambre, M. L. Bay Larsen, Mme C. Toader, MM. M. Safjan et N. Jääskinen (rapporteur), juges

Av. gén. : M. M. Campos Sánchez-Bordona

Aff. C-287/19

•
• • •

Comment le consommateur est-il protégé en cas de paiement sans contact (NFC) ?

I. Faits à l'origine du litige et décision de la Cour de justice

L'affaire soumise à la Cour de justice de l'Union européenne oppose une association de protection des consommateurs (VKI) à une banque autrichienne (DenizBank).

Le litige a trait à l'utilisation de cartes bancaires personnalisées munies d'une fonction de paiement sans contact (ou « NFC » pour « *Near Field Communication* »). Avec ce dispositif, il est possible de payer de faibles montants (maximum 25 EUR dans le cas d'espèce), en approchant la carte du terminal de paiement ; le payeur ne doit donc pas insérer sa carte dans le terminal, ni saisir son code pin.

L'utilisation de cette fonction de paiement sans contact est visée par les conditions générales de la banque. En substance, celle-ci s'exonère de toute responsabilité en cas de paiement réalisé au moyen de cette fonction ; le risque de fraude ou d'usage abusif de la carte par un tiers repose donc intégralement sur le titulaire de celle-ci

(qui peut être un consommateur). En outre, il est précisé qu'en cas de perte ou de vol de la carte, la fonction des paiements de faible montant ne peut pas être bloquée. VKI postule l'annulation des clauses litigieuses et, à cette fin, saisit les juridictions autrichiennes.

Cette modalité de paiement sans contact est facile et très pratique pour l'utilisateur ; durant la crise sanitaire, elle était d'ailleurs encouragée, dès lors qu'elle dispensait le client de tout contact physique avec le clavier du terminal de paiement (réduisant ainsi les risques de contamination)[1]. Des fraudes sont toutefois à craindre, puisque le paiement est effectué sans aucune authentification ou validation de la part du payeur.

L'affaire soumise à la Cour de justice est intéressante puisqu'elle permet de clarifier les règles applicables à cette modalité de paiement électronique, très fréquente en pratique, et en augmentation constante[2]. La question se pose en effet de savoir si les règles de protection consacrées par la directive (UE) 2015/2366 sur les services de paiement dans le marché intérieur[3] (ci-après, « DSP 2 »), telle que transposée, pour ce qui concerne la Belgique, dans le livre VII du Code de droit économique, s'appliquent à ce cas de figure.

Saisie d'un pourvoi en révision suite à l'arrêt du tribunal régional supérieur de Vienne (rendu le 20 novembre 2017), la Cour suprême autrichienne décide de poser trois questions préjudicielles à la Cour de justice.

Cette dernière se prononce le 11 novembre 2020[4].

La première question porte sur la présomption d'acceptation d'une modification du contrat-cadre conclu entre le prestataire et l'utilisateur de services de paiement, telle que visée à l'article 52, 6), *littera* a, et à l'article 54 de la DSP 2. Nous n'analysons pas la réponse de la Cour dans la présente contribution, dès lors qu'elle ne concerne pas directement la fonction de paiement sans contact[5].

---

1 Voy. par ex. https://www.febelfin.be/fr/article/payer-sans-contact-avec-votre-carte.

2 Voy. https://www.lalibre.be/economie/mes-finances/le-dessous-des-cartes-pour-les-paiements-sans-contact-609ea7bad8ad5816b417757c. ou https://www.febelfin.be/fr/communique-de-presse/les-belges-passent-massivement-au-paiement-numerique.

3 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, *J.O.*, L 337 du 23 décembre 2015.

4 C.J.U.E., 11 novembre 2020, aff. C-287/19, *DenizBank AG*, EU:C:2020:897 (ci-après, l'arrêt commenté).

5 Sur ce point, la Cour décide que « l'article 52, point 6, sous a), de la directive 2015/2366, lu en combinaison avec l'article 54, paragraphe 1, de celle-ci, doit être interprété en ce sens qu'il régit les informations et les conditions à fournir par un prestataire de services de paiement souhaitant convenir, avec l'utilisateur de ses services, d'une présomption d'acceptation concernant la modification, conformément aux modalités prévues à ces dispositions, du contrat-cadre qu'ils ont conclu, mais qu'il ne fixe pas de restrictions s'agissant de la qualité de l'utilisateur ou du type de clauses contractuelles pouvant faire l'objet d'un tel accord, sans préjudice toutefois, lorsque l'utilisateur a la qualité de consommateur, d'un possible contrôle du caractère abusif de ces clauses au regard des dispositions de la directive 93/13 » (point 66 de l'arrêt).

La deuxième question est subdivisée en deux parties. Elle porte sur la qualification de la fonction de paiement sans contact dont les cartes bancaires sont équipées, au regard des notions-clés de la DSP 2. Il faut en effet déterminer s'il s'agit d'un « instrument de paiement » et, dans l'affirmative, si son utilisation est « anonyme ».

La troisième question a trait au blocage éventuel de la carte – en ce compris la fonction de paiement sans contact – en cas de perte ou de vol de celle-ci.

Après un bref rappel du cadre normatif applicable, nous examinons successivement ces deux dernières questions.

II. Rappel du cadre normatif

A. DSP 2, règlement délégué (UE) 2018/389 et livre VII du CDE

En droit de l'Union, comme indiqué précédemment, la matière est régie par la directive (UE) 2015/2366 sur les services de paiement dans le marché intérieur, dite « DSP 2 ». Cet instrument abroge et remplace la directive 2007/64/CE[6] (« DSP 1 »).

En droit belge, cette directive est principalement transposée dans le livre VII du Code de droit économique[7], tel qu'amendé par la loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique[8]. On observe que, dans le cas qui nous occupe, de nombreuses règles figuraient déjà dans la DSP 1 (et le livre VII, avant sa modification). La doctrine et la jurisprudence rendues dans ce cadre restent donc pertinentes.

On aura aussi égard au règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et

[6] Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, *J.O.*, L 319 du 5 décembre 2007.

[7] La directive est également transposée par la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement, *M.B.*, 26 mars 2018. En l'occurrence, seules les dispositions du livre VII du CDE retiennent notre attention.

[8] *M.B.*, 30 juillet 2018. À ce propos (et sur la DSP 2), voy. G. Hennard, « La loi du 19 juillet 2018 portant modification et insertion de dispositions en matière de services de paiement dans différents livres du Code de droit économique », *Dr. Banc. Fin.,* 2019, pp. 25 et s. ; C. Bourguignon, « L'utilisateur dans la nouvelle loi sur les services de paiement : entre protection et responsabilisation », *Actualités en droit du numérique*, H. Jacquemin et B. Michaux (dir.), Limal, Anthemis, 2019, pp. 153 et s. ; D. Philippe, « La directive 2015/2336 sur les services de paiement (DSP 2) : la révolution digitale en marche », *Actualités en droit commercial et bancaire*, J.-P. Buyle *et al.* (dir.), Bruxelles, Larcier, 2017, pp. 455 et s. ; Th. Bonneau, « La directive sur les services de paiement "2" : révolution ou évolution ? », *J.D.E.*, 2016/6, n° 230, pp. 214 et s.

du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication[9] (ci-après, règlement délégué (UE) 2018/389). Cet instrument fixe en effet les exigences à respecter en matière d'authentification forte du client[10], ainsi que les dérogations possibles, par les prestataires de services de paiement, à cette obligation.

B. Principales obligations prescrites par la DPS 2 et le livre VII du Code de droit économique

La DSP 2 et le livre VII du Code de droit économique imposent diverses obligations d'information aux prestataires de services de paiement, tout en fixant les droits et les obligations des parties, notamment en cas d'opération de paiement non autorisée (comme la perte ou le vol de l'instrument de paiement).

Les principaux acteurs visés par le cadre normatif sont, d'une part, le prestataire de services de paiement[11], d'autre part, l'utilisateur de services de paiement, qui peut être un payeur ou un bénéficiaire[12]. Des règles spécifiques sont instaurées au bénéfice des consommateurs. Plus précisément, les parties peuvent déroger conventionnellement à certaines dispositions de la DSP 2 ou du livre VII, lorsque l'utilisateur de services de paiement n'est pas un consommateur[13]. Sont notamment visées les règles de partage de responsabilité en cas d'opérations de paiement non autorisées. À l'égard des consommateurs, de telles dérogations sont interdites.

L'objectif des textes est de promouvoir l'utilisation de services de paiements sécurisés, faciles et accessibles à tous, en garantissant un niveau élevé de protection au bénéfice des parties impliquées, spécialement les consommateurs. Ces finalités concernent également les paiements de faible valeur et sans contact : toutefois, dans la mesure où les risques sont plus réduits[14] en ce qui les concerne, un régime allégé est mis en place. Le législateur européen considère en effet que « les instruments de paiement relatifs à des montants de faible valeur devraient constituer un moyen simple et bon marché de régler des biens et des services de faible prix et ne devraient pas être soumis à des exigences excessives »[15].

---

[9] *J.O.*, L 69 du 13 mars 2018. Ce règlement est pris sur le fondement de l'article 98 de la DSP 2.

[10] L'authentification forte du client est définie comme « une authentification reposant sur l'utilisation de deux éléments ou plus appartenant aux catégories "connaissance" (quelque chose que seul l'utilisateur connaît), "possession" (quelque chose que seul l'utilisateur possède) et "inhérence" (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification » (art. I.9, 33/16°, du CDE).

[11] Art. I.9, 2°, du CDE.

[12] Art. I.9, 3° et 4°, du CDE.

[13] Voy. l'art. 61 de la DSP 2 et l'art. VII.29 du CDE.

[14] Voy. le cons. 96 de la DSP 2.

[15] Cons. 81 de la DSP 2.

Moyennant le respect de conditions strictes, l'article 63 de la DSP 2[16] permet aux prestataires de services de paiement, à l'instar de DenizBank, de déroger conventionnellement à plusieurs exigences prescrites par les textes en vigueur pour les instruments de paiement relatifs à des montants de faible valeur (dispositions qui, par ailleurs, peuvent présenter un caractère impératif au bénéfice des consommateurs). La dérogation est limitée aux « instruments de paiement qui, conformément au contrat-cadre, concernent uniquement des opérations de paiement individuelles dont le montant n'excède pas 30 EUR ou qui soit ont une limite de dépenses de 150 EUR, soit stockent des fonds dont le montant n'excède à aucun moment 150 EUR ».

Encore faut-il déterminer si les exceptions de l'article 63 de la DSP 2 s'appliquent aux paiements sans contact, ce que VKI contestait en l'espèce (puisqu'elle postulait la nullité des clauses contractuelles litigieuses).

III. Le partage de responsabilité prévu par la loi en cas d'opération de paiement non autorisée s'applique-t-il à l'hypothèse du paiement sans contact ?

A. Partage de responsabilité consacré par la DSP 2 et dérogation conditionnelle possible pour les opérations de paiement de faible montant

La DSP 2 et le livre VII du CDE règlent l'imputabilité de la responsabilité entre le payeur, le bénéficiaire et le prestataire de service de paiement en cas de pertes liées à une opération de paiement non autorisée. Plus précisément, et par dérogation au droit commun, un régime de responsabilité globalement favorable aux payeurs est mis en place.

Les textes applicables font en effet peser sur le prestataire la preuve que l'opération de paiement contestée a été authentifiée[17]. En outre, ils limitent à 50 EUR les pertes subies par le payeur et liées à une opération de paiement non autorisée intervenant avant la notification[18]. Le payeur ne supporte aucune perte financière dans plusieurs hypothèses (notamment lorsqu'une authentification forte du client n'est pas exigée)[19]. Dans ce

[16] Art. VII.31 du CDE. En l'occurrence, seules les deux premières hypothèses de cette disposition, visées sous 1° et 2° (a et b dans la DSP 2) sont analysées. Les autres exigences de la DSP 2 auxquelles il est permis de déroger conformément à l'article 63 ont trait au refus d'un ordre de paiement (art. 79, § 1er, de la DSP 2, auquel renvoie l'art. 63, § 1er, c)) et à son caractère irrévocable (art. 80 de la DSP 2, auquel renvoie l'art. 63, § 1er, d)), ainsi qu'aux délais d'exécution visés aux articles 83 et 84 de la directive (art. 83 et 84 de la DSP 2, auquel renvoie l'art. 63, § 1er, e)). Nous ne les détaillons pas davantage dès lors qu'elles ne sont pas particulièrement pertinentes dans le cas du paiement sans contact.

[17] Art. 72 de la DSP 2 ; art. VII.43 du CDE.

[18] Art. 73 et 74, §§ 1er et 3, de la DSP 2 ; art. VII.44 du CDE.

[19] Art. VII.44, § 1er, al. 2, et §§ 2-3, du CDE.

cas, le payeur sera remboursé par le prestataire de services de paiement qui réclamera ensuite le montant au bénéficiaire de services de paiement (concrètement, l'entreprise ayant vendu le bien ou fourni le service[20]). Inversement, le payeur devra supporter toutes les pertes s'il a agi frauduleusement ou, dans certains cas, s'il a manqué aux obligations qui lui incombent intentionnellement ou à la suite d'une négligence grave.

Si la dérogation de l'article 63, § 1er, b), de la DSP 2 s'applique à la fonction de paiement sans contact, les règles relatives au partage de responsabilité ne doivent pas être observées et le prestataire peut valablement s'exonérer des conséquences financières d'une opération de paiement non autorisée, moyennant une clause *ad hoc* dans ses conditions contractuelles (c'est d'ailleurs ce qui avait été fait par DenizBank dans la présente affaire).

Sur le plan légistique, l'article 63 de la DSP 2 mentionne les autres articles de la directive qui ne s'appliquent pas si les conditions pour bénéficier de la dérogation sont remplies. Curieusement, les dispositions auxquelles il est renvoyé ne sont pas les mêmes dans la DSP 2 et dans le livre VII du Code de droit économique. Ainsi, à l'article VII.31, § 1er, 2°, du CDE, le législateur belge aurait normalement dû viser l'article VII.44, § 1er, alinéa 2, et l'article VII.44, § 3, *quod non*. La directive procède en effet à une harmonisation totale (sauf exception), qui ne laisse aucune marge aux États au moment de la transposition[21].

Pour établir si les dérogations de l'article 63, § 1er, b), peuvent s'appliquer au cas d'espèce, encore faut-il démontrer que la fonction de paiement sans contact est un instrument de paiement (*cfr infra*, point B) et qu'il est utilisé de manière anonyme (*cfr infra*, point C).

On observe que l'article 63, § 2, b), de la DSP ne permet pas de déroger à l'article 74, § 2. Cette disposition règle le partage de responsabilité en l'absence d'authentification forte du payeur. Elle énonce que « lorsque le prestataire de services de paiement du payeur n'exige pas une authentification forte du client, le payeur ne supporte aucune perte financière éventuelle à moins qu'il ait agi frauduleusement. Lorsque le bénéficiaire ou son prestataire de services de paiement n'accepte pas une authentification forte du client, il rembourse le préjudice financier causé au prestataire de services de paiement du payeur ». En cas de paiement sans contact au point de vente, l'article 11 du règlement délégué (UE) 2018/389 permet toutefois aux prestataires de services de paiement de ne pas appliquer d'authentification forte du client dans ce cas de figure, moyennant le respect de plusieurs conditions[22]. Il en résulte que, si les conditions précitées sont

[20] Voy. par ex. Bruxelles, 19 juin 2008, *DAOR*, 2009/90, p. 167, note A. VANDOOLAEGHE, *R.D.C.*, 2010, p. 117, note M. DELIERNEUX et J.-P. BUYLE. Voy. aussi Bruxelles, 10 mars 2009, *Dr. Banc. Fin.*, 2009, p. 173, note R. STEENNOT.

[21] Art. 107 de la DSP 2.

[22] Les conditions sont les suivantes : « a) le montant individuel de l'opération de paiement électronique sans contact ne dépasse pas 50 EUR ; et b) le montant cumulé des précédentes opérations de paiement électronique sans contact initiées par l'intermédiaire d'un instrument de paiement disposant d'une fonctionnalité sans contact, depuis la date de la dernière authentification forte du client, ne dépasse pas

satisfaites, le prestataire devrait pouvoir s'exonérer valablement de sa responsabilité, même en l'absence d'authentification forte du client, et pour une opération de paiement pouvant atteindre 50 EUR.

B. Instrument de paiement ?

Dans la première branche de la deuxième question préjudicielle, la Cour de justice est interrogée sur la question de savoir si la fonction de paiement sans contact dont la carte de paiement est dotée constitue un « instrument de paiement » au sens de la DSP 2.

La notion désigne « tout dispositif personnalisé et/ou ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement et utilisé pour initier un ordre de paiement »[23].

Deux hypothèses principales se dégagent de cette définition : il doit s'agir soit d'un dispositif personnalisé, soit d'un ensemble de procédures.

Comme l'a jugé la Cour dans une précédente affaire, pour répondre à l'exigence de dispositif « personnalisé », « un instrument de paiement doit permettre au prestataire de services de paiement de vérifier que l'ordre de paiement a été initié par un utilisateur habilité à ce faire »[24]. Le paiement sans contact ne constitue donc pas un dispositif personnalisé puisque, par définition, aucune authentification n'est réalisée. Il en irait différemment si le payeur était invité à introduire son code pin, *quod non*.

S'agirait-il alors d'un « ensemble de procédures », sachant que, suivant la jurisprudence de la Cour, l'ensemble en question ne doit pas nécessairement être personnalisé[25] ?

Dans l'arrêt commenté du 11 novembre 2020, la Cour suit l'avocat général et répond par l'affirmative : la fonction de paiement sans contact dont est dotée une carte bancaire multifonctions personnalisée et qui permet d'effectuer des paiements de faible montant au débit du compte bancaire associé à cette carte constitue un ensemble de procédures non personnalisé et, partant, répond à la définition de l'instrument de paiement.

Une carte bancaire peut ainsi être munie de plusieurs fonctionnalités, dissociables les unes des autres sur le plan juridique[26] : en cas de paiement effectué en insérant la carte dans

150 EUR ; ou c) le nombre d'opérations de paiement électronique sans contact consécutives initiées par l'intermédiaire de l'instrument de paiement disposant d'une fonctionnalité sans contact, depuis la dernière authentification forte du client, ne dépasse pas cinq ».

[23] Art. 4, 14), de la DSP 2.

[24] C.J.U.E., 9 avril 2014, aff. C-616/11, *T-Mobile Austria*, EU:C:2014:242, point 33. *Cfr* le point 70 de l'arrêt commenté, qui fait référence à cette jurisprudence.

[25] C.J.U.E., 9 avril 2014, aff. C-616/11, *T-Mobile Austria*, EU:C:2014:242, points 34-35. *Cfr* le point 71 de l'arrêt commenté, qui fait référence à cette jurisprudence

[26] Points 75-77 de l'arrêt commenté.

le terminal et en indiquant le code pin de celle-ci, il s'agit d'un dispositif personnalisé ; par contre, dans l'hypothèse du paiement sans contact, la fonction répondra aux caractéristiques de l'ensemble de procédures non personnalisé. En tout état de cause, dans les deux cas, il s'agira d'un instrument de paiement au sens de la DSP 2.

La Cour de justice insiste sur l'importance de « contribuer à la réalisation des objectifs poursuivis par la directive 2015/2366, car le fait que la fonction NFC soit ainsi directement soumise aux exigences posées par celle-ci favorise non seulement le développement de ce nouveau moyen de paiement dans le cadre d'une concurrence équitable entre les prestataires de services de paiement, mais également la protection des utilisateurs de ces services, en particulier de ceux ayant la qualité de consommateurs, conformément aux orientations données par le préambule de cette directive, et notamment par son considérant 6 » (point 78).

Cette interprétation doit, d'après nous, être approuvée : il convient en effet de privilégier une acception large de la notion d'instrument de paiement, pour s'assurer que le cadre normatif protecteur (et, globalement, plutôt équilibré, dans l'intérêt de tous les acteurs impliqués), soit respecté.

C. Utilisation anonyme ?

Si la Cour décide que la fonction de paiement sans contact peut être considérée comme un instrument de paiement (ce qui est confirmé en l'espèce – *cfr supra*, point B), la Cour suprême autrichienne lui demande, à titre complémentaire, si son utilisation est « anonyme » au sens de l'article 63, § 1er, b), de la DSP 2.

Aux termes de cette disposition, les parties peuvent convenir que « les articles 72 et 73 et l'article 74, paragraphes 1 et 3, ne s'appliquent pas si l'instrument de paiement est utilisé de manière anonyme ou si le prestataire de services de paiement n'est pas en mesure, pour des raisons autres qui sont inhérentes à l'instrument de paiement, d'apporter la preuve qu'une opération de paiement a été autorisée ». Le prestataire de services de paiement pourrait donc déroger aux règles relatives au partage de responsabilité en cas d'opération de paiement non autorisée.

La Cour de justice confirme que le paiement sans contact d'un montant de faible valeur constitue une utilisation anonyme de l'instrument de paiement.

Elle rappelle d'abord que, s'agissant d'une exception, l'hypothèse visée à l'article 63, § 1er, b), est d'interprétation stricte[27].

Suivant la Cour, une distinction doit être faite entre l'identification du titulaire du compte débité (qui résulte de la personnalisation de la carte bancaire) et l'opération de paiement sans contact

[27] Point 84 de l'arrêt commenté.

en tant que telle, pour laquelle la personne ayant procédé au paiement n'est pas identifiée ou authentifiée (et ne peut pas l'être, objectivement)[28]. Il suffit en effet d'être en possession de la carte pour payer sans contact, puisqu'aucun code pin ni signature n'est requis. Le paiement n'est pas subordonné au consentement du titulaire de la carte et, en cas de vol ou de perte de celle-ci, son détenteur pourra sans difficulté procéder à des paiements de faibles montants sans son accord (dans la limite du plafond autorisé). Il s'agit donc d'une utilisation anonyme.

Comme la Cour le relève ensuite, cette interprétation est conforme à l'économie générale de la directive et à l'équilibre que celle-ci instaure entre les parties impliquées[29] : le prestataire de services de paiement, d'une part, l'utilisateur, d'autre part, y compris s'il est consommateur.

Le paiement sans contact est un moyen facile et rapide de payer (outre qu'il est plus hygiénique, puisqu'il dispense de toucher le clavier du terminal pour introduire son code pin). L'absence d'authentification du payeur peut toutefois donner lieu à des fraudes éventuelles de la part de tiers malintentionnés (en cas de vol ou de perte de la carte, par exemple). Aussi la question se pose-t-elle de savoir sur qui devraient reposer les conséquences financières éventuelles de telles fraudes : sur le prestataire de services de paiement, sur le bénéficiaire du paiement ou sur le payeur ?

Dans le régime de la directive, c'est normalement le payeur qui assume la responsabilité d'une opération non autorisée. Cette conséquence nous paraît raisonnable, d'autant qu'elle est assortie de deux limites importantes. D'abord, un plafond est établi, ce qui limite les pertes financières éventuelles. En outre, il est normalement loisible au payeur de désactiver cette fonction[30] (à noter toutefois que, par défaut, elle est généralement installée). Par conséquent, en utilisant la fonction de paiement sans contact, le payeur accepte aussi « d'être éventuellement exposé aux effets des limitations conventionnelles de la responsabilité du prestataire qui sont permises en vertu de cette disposition [i.e., l'article 63, § 1er, b), de la DSP 2] »[31].

IV. L'instrument de paiement muni d'une fonction NFC peut-il être bloqué ?

En règle, l'utilisateur d'un instrument de paiement doit informer sans délai le prestataire en cas de perte, de vol, de détournement, ou de toute utilisation non autorisée[32].

[28] Points 87 à 89 de l'arrêt commenté.
[29] Point 91 de l'arrêt commenté.
[30] Les applications de *mobile banking* permettent en général de gérer les cartes de paiement et, dans ce cadre, de désactiver la fonctionnalité du paiement sans contact.
[31] Point 91 de l'arrêt commenté.
[32] Art. 69, § 1er, b), art. 70, § 1er, c) et d), et art. 74, § 3, de la DSP 2.

Corrélativement, il incombe au prestataire de mettre en place des moyens appropriés pour permettre une telle notification (c'est le système Card Stop, bien connu).

Conformément à l'article 63, § 1er, a), de la DSP 2, les parties peuvent déroger conventionnellement à ces exigences (et décider qu'elles ne seront pas applicables), pour les instruments de paiement relatifs à des montants de faible valeur, « si l'instrument de paiement ne peut pas être bloqué ou si la poursuite de l'utilisation de celui-ci ne peut pas être empêchée ». Cette exigence est logique puisque la notification a pour objectif principal de permettre au prestataire d'empêcher, pour l'avenir, toute utilisation non autorisée de l'instrument de paiement.

La question se pose de savoir si le prestataire de service de paiement peut se borner à affirmer – dans une clause de ses conditions contractuelles, par exemple – qu'il est impossible de bloquer l'instrument de paiement ou d'empêcher la poursuite de son utilisation, sans devoir démontrer que l'assertion est corroborée par l'état de l'art ou d'autres éléments objectifs, de nature technique.

La Cour confirme, logiquement, qu'on ne peut se satisfaire d'une telle déclaration péremptoire : elle décide en effet que le « prestataire doit établir, à charge pour lui d'en rapporter la preuve en cas de litige, que ledit instrument ne permet en aucune manière, pour des raisons techniques, de procéder à son blocage ou de prévenir son utilisation ultérieure. Si la juridiction saisie estime qu'il était matériellement possible de procéder à un tel blocage ou de prévenir une telle utilisation, compte tenu de l'état objectif des connaissances techniques disponibles, mais que le prestataire n'a pas eu recours à ces connaissances, il ne saurait être fait application, au profit de ce dernier, dudit article 63, paragraphe 1, sous a) »[33].

La Cour rappelle, une fois encore, que s'agissant d'une exception à l'application d'autres dispositions de la DSP 2, il faut procéder à une interprétation stricte de l'article 63, § 1er, a)[34].

La Cour procède également à une analyse des risques encourus par chaque acteur et des obligations et responsabilités corrélatives qui leur incombent[35]. Il faut en effet protéger les utilisateurs de services de paiement, en particulier s'ils ont la qualité de consommateurs. Par ailleurs, l'établissement de mesures de sécurité, proportionnées, repose sur les prestataires. Or, se satisfaire d'une affirmation péremptoire en la matière, sans s'assurer qu'elle est conforme à la réalité, pourrait conduire certains prestataires à mettre en place des mesures de faible qualité, ce qui ne sert ni les intérêts des utilisateurs ni le système dans son ensemble (avec des risques systémiques et une perte de confiance généralisée en cas de brèche de sécurité). Elle aurait aussi pour conséquence de faire reposer sur les

[33] Point 98 de l'arrêt commenté.
[34] Point 101 de l'arrêt commenté.
[35] Points 103 et suivants de l'arrêt commenté.

utilisateurs des risques qu'ils peuvent difficilement prévenir et qui ne devraient pas leur incomber, selon une juste allocation des risques.

V. Conclusion

L'arrêt commenté de la Cour de justice de l'Union européenne, rendu le 11 novembre 2020, est intéressant dans la mesure où il clarifie l'interprétation de plusieurs concepts-clés de la DSP 2, qui conditionnent la dérogation à certaines exigences de la directive en cas de paiements sans contact.

L'interprétation ainsi donnée par la Cour confirme que la fonction de paiement sans contact dont sont dotées les cartes bancaires constitue un instrument de paiement, dont l'utilisation est anonyme. Il est donc permis aux parties de déroger conventionnellement aux règles déterminant le partage de responsabilité en cas d'opération de paiement non autorisée. Concrètement, le titulaire de la carte devra supporter les risques d'une fraude éventuelle, étant entendu que des plafonds relativement bas sont établis et qu'il peut normalement désactiver la fonction s'il le souhaite.

Par contre, le prestataire ne peut affirmer de manière péremptoire que le blocage de la fonction est impossible en cas de perte ou de vol. La preuve de cette impossibilité technique lui incombe.

Les règles applicables aux paiements électroniques sont relativement complexes, car la réalité l'est également, spécialement sur le plan technique. Elles ont pour objet de trouver un équilibre entre les intérêts en présence, tout en promouvant l'utilisation de moyens de paiements rapides, faciles et aisément accessibles. Dans cet arrêt, la Cour est soucieuse de préserver cet équilibre, ce dont on peut se réjouir.

Hervé Jacquemin[36]

[36] Professeur à l'Université de Namur (CRIDS, membre du NaDI). Avocat au barreau de Bruxelles.