Le paiement électronique

Jacquemin, Herve

Published in:
Obligations

Publication date:
2022

Document Version
le PDF de l'éditeur

Sous-titre 4
L'EXÉCUTION DE L'OBLIGATION

Table des matières

Chapitre 3
Le paiement électronique

par HERVÉ JACQUEMIN[1]

Plan

Bibliographie sélective

ALTER, C., « Le paiement électronique », in *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, Bruxelles, Bruylant, 2012, pp. 95 et s.

BONNEAU, Th., « La directive sur les services de paiement '2' : révolution ou évolution ? », *J.D.E.*, 2016/6, n° 230, pp. 214 et s.

1. Professeur à l'Université de Namur, directeur du CRIDS (NADI) ; avocat au barreau de Bruxelles.

BOURGUIGNON, C., « 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.

FELD, J., « Le paiement électronique à la lumière de la nouvelle loi sur les services de paiement », in *Le paiement*, Louvain-la-Neuve, Anthemis, 2009, pp. 63 et s.

HENNARD, G., « 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.

JACQUEMIN, H., « Les paiements électroniques dans les contrats à distance depuis la loi du 10 décembre 2009 », *R.D.T.I.*, 2010/41, pp. 5 et s.

PHILIPPE, D., « La directive 2015/2336 sur les services de paiement (DSP2) : la révolution digitale en marche » *Actualités en droit commercial et bancaire*, J.-P. BUYLE *et al.* (dir.), Bruxelles, Éditions Larcier, 2017, pp. 455 et s.

SAD, J., « Les services de paiement », *T.P.D.C.*, tome 5 – *Droit bancaire et financier*, 2016, pp. 229 et s.

STEENNOT, R., « Art. VII.44 Wetboek Economisch Recht », *Financieel recht. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Kluwer, 2018.

X., *Aspects juridiques du paiement électronique – Juridische aspecten van de elektronische betaling*, Bruxelles, Kluwer, 2004, 3 vol.

SECTION 1RE. INTRODUCTION

1.1 Le paiement est défini à l'article 5.194 du Code civil comme l'« acte juridique unilatéral par lequel la prestation due est exécutée de manière volontaire ».

Dans le langage courant, la notion reçoit toutefois une acception plus réduite puisqu'elle vise seulement le versement d'une somme d'argent. Tel est d'ailleurs le sens qui lui est donné dans l'expression « paiement électronique », généralement usitée en pratique.

Quant à l'adjectif « électronique », il ne permet guère de particulariser l'opération[1] dans la mesure où désormais, sous réserve notamment des paiements en espèces, l'informatique ou, plus globalement, les technologies de l'information et de la communication (ou le numérique) sont systématiquement mobilisées.

Le constat se vérifie lorsque le paiement est réalisé par l'intermédiaire d'une application d'*internet banking* ou en exécution d'un contrat conclu à distance, à travers un site web de commerce électronique ou une application mobile transactionnelle, mais également quand les parties sont en présence physique l'une de l'autre et que le payeur utilise son smartphone ou sa carte de débit ou de crédit depuis le terminal d'un commerce traditionnel (POS – *Point of Sale*).

1.2 La plupart des paiements électroniques sont désormais soumis aux dispositions du livre VII du Code de droit économique.

1. Pour une critique de la notion de paiement électronique, voir J. FELD, « Le paiement électronique à la lumière de la nouvelle loi sur les services de paiement », in *Le paiement*, Louvain-la-Neuve, Anthemis, 2009, pp. 67-68.

Avant le 1er avril 2010, la matière était principalement régie par la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds[1] (ci-après, LTEF) et, s'agissant des contrats à distance, par l'article 83*novies* de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection des consommateurs (ci-après, LPCC)[2]. Ces textes trouvaient leur origine dans des initiatives européennes. La LTEF assurait la transposition de la recommandation 97/489/CE de la Commission du 30 juillet 1997 concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire[3]. Quant à l'article 83*novies* de la LPCC, il avait été adopté[4] en vue de mettre le droit belge en conformité avec la Directive n° 2002/65/CE sur les services financiers à distance[5].

Ces textes ont été abrogés et remplacés par les dispositions de la loi du 10 décembre 2009 relative aux services de paiement[6] [7]. Celle-ci avait pour objet de transposer la Directive n° 2007/64/CE sur les services de paiement (ci-après, « DSP 1 »)[8].

A l'occasion de la promulgation progressive du Code de droit économique, les dispositions de la loi du 10 décembre 2009 ont été intégrées dans le livre VII du Code, consacré aux services de paiement et de crédit (ainsi que dans les livres I et XV).

La matière a été réformée en droit de l'Union, en 2015, par la Directive (UE) n° 2015/2366 sur les services de paiement dans le marché intérieur, (ci-après, « DSP 2 »). Cet instrument abroge et remplace la Directive n° 2007/64/CE. En droit belge, cette directive est principalement transposée dans le livre VII du Code de

1. *M.B.*, 17 août 2002. Pour un commentaire de cette loi, voir not. E. WÉRY, *Paiements et monnaie électroniques*, Bruxelles, Larcier, 2007, pp. 82 et s. ; M. DEMOULIN, « Le paiement électronique », in *Obligations – Traité théorique et pratique*, Bruxelles, Kluwer, 2007, V.1.7 ; M. VAN HUFFEL, « Ma carte bancaire est-elle suffisamment européenne ? », *D.C.C.R.*, 2006/70, pp. 3 et s. ; Th. LAMBERT, « La loi du 17 juill. 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds », *R.D.C.*, 2003, pp. 573 et s. ; L. ROLIN JACQUEMYNS, « Régime juridique des paiements électroniques à la lumière de la nouvelle loi sur les opérations effectuées au moyen d'instruments de transfert électronique de fonds », *Ubiquité*, 2003/16, pp. 9 et s. ; R. STEENNOT, « De wet betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen », *B.F.R.*, 2002, pp. 255 et s.
2. *M.B.*, 29 août 1991. On note que cette loi a par la suite été abrogée et remplacée par la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur (*M.B.*, 12 avril 2010, p. 20.803) et la loi du 6 avril 2010 concernant le règlement de certaines procédures dans le cadre de la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur (*M.B.*, 12 avril 2010, p. 20.841).
3. *J.O.*, n° L 208 du 2 août 1997.
4. Art. 17 de la loi du 25 août 2005 visant à transposer certaines dispositions de la directive services financiers à distance et de la directive vie privée et communications électroniques, *M.B.*, 31 août 2005.
5. Art. 8 de la Directive n° 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les Directives n° 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, *J.O.*, n° L 265 du 9 octobre 2002.
6. *M.B.*, 15 janvier 2010. Pour un commentaire de cette loi, voir J. FELD, *op. cit.*, pp. 63 et s. ; R. STEENNOT, « Girale en elektronische betalingen », *N.J.W.*, 2010, pp. 518 et s. ; R. STEENNOT et T. BAES, « Wet op betalingsdiensten : bescherming of overbescherming ? », *B.F.R.*, 2010, pp. 208 et s. ; H. JACQUEMIN, « Les paiements électroniques dans les contrats à distance depuis la loi du 10 décembre 2009 », *R.D.T.I.*, 2010/41, pp. 5 et s. ; C. ALTER, « Le paiement électronique », in *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, Bruxelles, Bruylant, 2012, pp. 95 et s.
7. Art. 77 de la loi du 10 décembre 2009.
8. Directive n° 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 n° 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la Directive n° 97/5/CE, *J.O.*, n° L 319 du 5 décembre 2007. Cette directive était également transposée par la loi du 21 décembre 2009 relative au statut des établissements de paiement, à l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement, *M.B.*, 19 janvier 2010, et la loi du 22 décembre 2009 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers et instaurant l'action en cessation des infractions à la loi du 10 décembre 2009 relative aux services de paiement, *M.B.*, 19 janvier 2010.

droit économique[1], tel que modifié 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[2]. 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) n° 2018/389 de la Commission du 27 novembre 2017 complétant la Directive (UE) n° 2015/2366 du Parlement européen et 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[3] (ci-après, Règlement délégué (UE) n° 2018/389).

1.3 Les Directives n° 2007/64/CE et 2015/2366 sur les services de paiement ont pour but de garantir le bon fonctionnement du marché unique de services de paiement, de manière à réaliser le marché intérieur[4]. Dans cette perspective, une grande importance est attachée à la confiance des utilisateurs et à la saine concurrence entre les prestataires. S'agissant spécifiquement des paiements électroniques, ces questions présentent une acuité certaine. Dans cette hypothèse, il n'est pas rare, en effet, que la méfiance ou les craintes des consommateurs se focalisent sur la sécurité du processus de paiement et son encadrement normatif.

Pour y répondre adéquatement, la directive et la loi belge de transposition introduisent diverses dispositions, qui tiennent compte de la faiblesse supposée des utilisateurs de services de paiement ou des fraudes dont ils peuvent être les victimes.

On suppose en effet qu'ils peuvent souffrir d'un manque de connaissance sur des éléments de fait ou de droit en lien avec l'opération de paiement ou la relation contractuelle qui a pu être nouée dans ce cadre[5]. La faiblesse peut également être liée à la position respective des parties dans le contrat, l'une étant spécialement puissante et l'autre souffrant d'une vulnérabilité particulière[6]. Pour réduire l'asymétrie informationnelle et garantir une relation contractuelle loyale et équilibrée, diverses obligations sont imposées aux parties. Il s'agit essentiellement d'obligations de transparence et d'information même si, accessoirement, d'autres exigences sont également prescrites.

1. 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 C.D.E. retiennent notre attention.
2. *M.B.*, 30 juillet 2018. A ce propos (et sur la DSP 2), voir 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 (DSP2) : la révolution digitale en marche » *Actualités en droit commercial et bancaire*, J.-P. BUYLE *et al.* (dir.), Bruxelles, Éditions 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.
3. *J.O.* L 69 du 13 mars 2018. Ce règlement est pris sur le fondement de l'article 98 de la DSP 2.
4. Voir notamment le considérant n° 1 de la DSP 1 et le considérant n° 5 de la DSP 2.
5. Sur cette faiblesse d'une partie au rapport contractuel, voir H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, pp. 64 et s. ; Id., « Focus sur certains mécanismes de protection du consommateur de services financiers en matière contractuelle », in *La protection du consommateur en droit financier*, Cahiers AEDBF n° 25, Limal, Anthemis, 2012, pp. 126 et s.
6. *Ibid.*, pp. 70 et s.

La faiblesse des utilisateurs tient également aux fraudes dont ils peuvent être les victimes, de la part de tiers, et qui sont susceptibles de donner lieu à des opérations de paiement non autorisées. Pour lutter contre ces risques, un subtil partage de responsabilités entre le prestataire de service de paiement, le payeur et, le cas échéant, le bénéficiaire, est consacré par la loi. Ce partage doit encourager chacune des parties, tenant compte des compétences et des moyens dont elle dispose, à prendre les mesures qui s'imposent pour renforcer la sécurité des opérations de paiement et empêcher les fraudes.

1.4 La matière des paiements électroniques est couverte par de nombreuses dispositions légales ou réglementaires ressortissant au droit des obligations (relation contractuelle entre le prestataire de services de paiements et le payeur ou le bénéficiaire, partage de responsabilité en cas d'opération de paiement non autorisée, etc.) et au droit bancaire et financier (conditions et formalités à remplir pour exercer l'activité de prestataire de service de paiement, émission de monnaie électronique, etc.).

Dans le cadre du présent chapitre, nous nous limitons aux aspects directement liés aux droits des obligations, tels qu'ils sont traités par le livre VII du Code de droit économique. Pour cette raison, nous ne nous penchons pas sur les règles spécifiquement applicables à la monnaie électronique ou sur les autres lois adoptées en vue de transposer la DSP 2.

1.5 Dans un premier temps, nous analysons le champ d'application de la loi, à la lumière des nombreux moyens de paiements électroniques généralement mis à la disposition des utilisateurs (section 2).

Nous nous penchons ensuite sur les règles matérielles établies par le texte. Dans le livre VII du Code de droit économique, elles sont regroupées en deux titres portant, d'une part, sur la transparence des conditions régissant les services de paiement et les exigences en matière d'information (chapitre I/I et chapitre II du titre III), d'autre part, sur les droits et obligations liés à la prestation et à l'utilisation de services de paiement (chapitre III du titre III). Eu égard à l'objet de cette étude, il ne paraît pas utile d'examiner l'ensemble des dispositions contenues dans ces titres, dès lors qu'elles ne sont pas spécifiques au paiement électronique ou consacrent des mécanismes spécifiques au droit bancaire et financier[1]. Sur ce point, nous renvoyons à la littérature spécialisée.

Nous examinons successivement les règles visant à garantir la transparence et la loyauté des services de paiement (section 3), et celles qui concernent la sécurité des opérations de paiement, avec le partage de responsabilité en cas d'opération de paiement non autorisée (section 4).

Enfin, les sanctions susceptibles d'être prononcées en cas de méconnaissance des règles précitées sont présentées (section 5).

1. Est par conséquent exclue de la présente étude l'analyse des dispositions portant notamment sur le remboursement des opérations de paiement initiées par ou via le bénéficiaire ; les ordres de paiement ; le délai d'exécution et la date valeur ou la protection des données.

SECTION 2. APPLICATION DU LIVRE VII DU C.D.E. SUR LES SERVICES DE PAIEMENT AUX PRINCIPALES FORMES DE PAIEMENT ÉLECTRONIQUE

2.1 Après avoir dressé un rapide panorama des principales formes de paiement électroniques (Sous-section 1re), nous déterminons si celles-ci entrent dans le champ d'application des dispositions du livre VII du C.D.E. en matière de services de paiement, circonscrit *ratione materiae* (Sous-section 2), *ratione personae* (Sous-section 3) et *ratione loci* (Sous-section 4).

Cette analyse nous permettra d'introduire les concepts clés utilisés – et, pour la plupart, définis – dans le C.D.E.[1].

SOUS-SECTION 1RE. PANORAMA DES PRINCIPALES FORMES DE PAIEMENTS ÉLECTRONIQUES

2.2 En première approximation, lorsque l'on recensait les moyens de paiement généralement proposés aux utilisateurs, une distinction pouvait être faite entre les paiements par carte (de crédit ou de débit), les virements entre comptes et le paiement en espèces[2]. Depuis de nombreuses années, les utilisateurs peuvent également accéder aux informations ou effectuer des opérations au moyen des systèmes d'*internet banking* ou de *mobile banking*. Avec les progrès technologiques et les possibilités offertes par les smartphones ou les objets connectés (tels que des montres), de nombreuses alternatives sont désormais offertes. Il est en effet possible de payer (ou de recevoir des fonds) en scannant un QR Code, avant de confirmer en utilisant les moyens d'authentification de l'application bancaire (reconnaissance faciale et/ou code pin). De même, pour les paiements sur les sites ou les applications de commerce électronique, des liens sont généralement faits vers le site de la banque de l'utilisateur ou vers un intermédiaire tel que *PayPal* ou *Payconiq by Bancontact*. Globalement, ces mesures permettent de réaliser facilement et rapidement des opérations, tout en conservant, en principe, un niveau élevé de sécurité sur le plan technique.

1. Et, pour la plupart, définis à l'article I.9 du C.D.E.
2. Nous n'examinerons pas davantage l'hypothèse des paiements en espèce, ni celle des paiements par chèque ou lettres de change, dans la mesure où elles sont exclues du champ d'application du livre VII du C.D.E. (art. VII.3, § 1er, 1° et 7°, C.D.E.).

2.3 A ce stade, et suivant la terminologie employée dans la loi, l'objectif est donc d'examiner les « instruments de paiement »[1] permettant à un « utilisateur de services de paiements »[2] – un « payeur »[3] ou un « bénéficiaire »[4] – d'initier un « ordre de paiement »[5].

Dans tous les cas, on suppose donc une relation contractuelle sous-jacente entre le payeur et le bénéficiaire, en vertu de laquelle, par exemple, en échange d'une livraison de bien ou d'une prestation de service, le payeur est tenu de verser une somme d'argent déterminée au bénéficiaire pour éteindre sa dette. On peut imaginer que la convention se forme dans un magasin traditionnel et que le paiement se fasse par le biais d'un terminal mis à la disposition des utilisateurs. La relation contractuelle peut tout aussi bien être nouée par le biais des réseaux, sur un site ou une application de commerce électronique, tandis que le paiement s'effectue en ligne.

2.4 S'agissant des paiements par carte, on distingue traditionnellement les cartes de débit (Maestro, p. ex.) et les cartes de crédit (Visa ou Mastercard, p. ex.), éventuellement rechargeables. Suivant le cas, le compte du titulaire est respectivement débité avant, pendant ou après la transaction.

Ces moyens de paiement peuvent être utilisés pour effectuer des paiements dans le magasin d'une entreprise (on parle de paiement POS – *Point of Sale*). Dans ce cas, sous réserve des paiements sans contact soumis à des conditions spécifiques (*infra*, n° 4.16), l'« authentification » du payeur est garantie par l'introduction du code PIN sur le terminal de l'entreprise[6]. La combinaison de la carte et du code PIN du payeur, d'une part, le terminal de l'entreprise bénéficiaire, d'autre part, constituent les « dispositifs de sécurité personnalisés »[7] fournis par le prestataire de service de paiement à l'utilisateur (respectivement le payeur ou le bénéficiaire du service de paiement).

Lorsque les parties ne sont pas en présence physique l'une de l'autre et que le paiement a lieu à l'occasion d'une conversation téléphonique ou sur l'internet, la carte de crédit peut être utilisée. Plus précisément, et sauf exception, c'est moins le support physique (bande magnétique ou puce électronique) que les données qui

1. Au sens du C.D.E., un « instrument de paiement » est « tout dispositif personnalisé et/ou ensemble de procédures convenu entre l'utilisateur de services de paiement et le prestataire de services de paiement et auquel l'utilisateur de services de paiement a recours pour initier un ordre de paiement » (art. I.9, 10°, C.D.E.).
2. L'« utilisateur de services de paiement » est « la personne physique ou morale qui utilise un service de paiement en qualité de payeur, de bénéficiaire ou les deux » (art. I.9, 3°, C.D.E.).
3. Le « payeur » est « la personne physique ou morale qui est titulaire d'un compte de paiement et qui autorise un ordre de paiement à partir de ce compte de paiement, ou la personne physique ou morale qui, en l'absence de compte de paiement, donne un ordre de paiement » (art. I.9, 4°, C.D.E.).
4. Le « bénéficiaire » est « la personne physique ou morale qui est le destinataire prévu de fonds ayant fait l'objet d'une opération de paiement » (art. I.9, 5°, C.D.E.). Sur la plateforme Justel (ejustice.fgov.be), la définition semble avoir été abrogée par l'article 2, b), de la loi du 2 mai 2019 portant dispositions diverses en matière d'économie. C'est toutefois une erreur, le but du législateur étant d'abroger l'article I.9, 5°, définissant le « système d'accréditation ». Avec des articles numérotés I.9 (l'un pour le livre VII, l'autre pour le livre VIII), on devait malheureusement s'attendre à ce que ce type de difficulté survienne…
5. Un « ordre de paiement » est « toute instruction d'un payeur ou d'un bénéficiaire à son prestataire de services de paiement demandant l'exécution d'une opération de paiement » (art. I.9, 7°, C.D.E.).
6. L'« authentification » est « une procédure permettant au prestataire de services de paiement de vérifier l'identité d'un utilisateur de services de paiement ou la validité de l'utilisation d'un instrument de paiement spécifique, y compris l'utilisation des données de sécurité personnalisées de l'utilisateur de services de paiement » (art. I.9, 11°, C.D.E.).
7. Le « dispositif de sécurité personnalisé » est « tout moyen technique affecté par un prestataire de services de paiement à un utilisateur donné pour l'utilisation d'un instrument de paiement. Ce dispositif propre à l'utilisateur de services de paiement et placé sous sa garde, permet de vérifier l'utilisation d'un instrument de paiement donné et vise à authentifier l'utilisateur » (art. I.9, 23°, C.D.E.).

figurent sur celui-ci qui permet de réaliser l'opération. Il suffit en effet au payeur de communiquer le numéro de la carte, sa date d'expiration, ainsi que le code de sécurité figurant au verso de la carte pour effectuer le paiement. Cette seule procédure ne permet donc pas de garantir que le paiement est effectué par le véritable titulaire de la carte. Désormais, des procédures complémentaires sont généralement mises en place, pour permettre une authentification forte du client (à ce sujet, voir *infra*, n° 4.11). Concrètement, il est invité à introduire sa carte dans un Digipass, pour générer un code de vérification unique, ou est renvoyé vers son application de *mobile banking* pour confirmer l'opération.

2.5 Quant aux virements[1] entre comptes, ils peuvent être initiés par le payeur depuis un automate de type *self banking* disponible dans les locaux de l'agence bancaire, ou par l'intermédiaire d'une application d'*internet banking* ou de *mobile banking* (moyennant, le cas échéant, l'utilisation d'un QR Code). La carte de paiement ou le smartphone, éventuellement combinés à des lecteurs de type Digipass ou à des systèmes d'identification biométriques, peuvent figurer parmi les éléments du dispositif de sécurité personnalisé utilisé par le payeur pour s'authentifier.

2.6 Le développement croissant des technologies de l'information et de la communication et l'encadrement légal de la monnaie électronique[2] ont également permis l'apparition d'autres moyens de paiement, tels que des porte-monnaie électroniques ou virtuels. L'utilisateur peut ainsi acquitter le solde de ses achats sur les sites ou les applications de commerce électronique qui acceptent ce moyen de paiement[3]. Quant au processus d'authentification, il peut résider dans une combinaison classique login-mot de passe, voire recourir à d'autres procédés plus innovants, faisant par exemple appel à un appareil mobile, par l'envoi de SMS ou la mise en place de mécanismes de reconnaissance faciale.

Enfin, pour certains types de paiements, généralement de faible montant – on parle de micropaiements – réalisés au moyen d'un appareil mobile, l'opérateur du système de télécommunication peut être appelé à jouer un rôle actif. Le paiement peut ainsi se faire par l'envoi d'un SMS surtaxé, dont le coût est facturé à l'utilisateur immédiatement (dans le cas d'une carte prépayée, p. ex.) ou ultérieurement dans un délai fixé conventionnellement (dans le cas d'une facture mensuelle, p. ex.). Le prix facturé au payeur comprend non seulement le coût du SMS mais également celui du bien ou du service acquis de cette manière (place de parking, p. ex.).

2.7 L'utilisation des instruments de paiement décrits ci-dessus exige l'intervention de nombreux prestataires fournissant des services de nature financière et/ou technique. Chacun d'eux joue un rôle indispensable au fonctionnement du « système de paiement »[4].

1. Le virement est défini à l'art. I.9, 31°, du C.D.E.
2. La monnaie électronique est définie à l'art. I.9, 26°, du C.D.E.
3. Voir par exemple les services proposés par PayPal.
4. Le système de paiement est « un système permettant de transférer des fonds, régi par des procédures formelles standardisées et des règles communes pour le traitement, la compensation et/ou le règlement d'opérations de paiement » (art. I.9, 15°, C.D.E.).

En matière de paiement par carte, par exemple, figurent respectivement aux côtés du payeur et du bénéficiaire, l'émetteur (« *Issuer* ») et l'acquéreur (« *Acquirer* »). A ceux-ci peuvent également s'ajouter des prestataires qui fournissent le schéma de paiement[1] (*Payment Scheme*) en tant que tel, garantissant l'échange de données de transaction entre les différents intervenants et le respect de « règles du jeu » préalablement fixées (en matière d'authentification des opérations de paiement, p. ex.). Des prestataires peuvent également jouer un rôle plus technique, en offrant uniquement des moyens de communication sécurisés et fiables.

SOUS-SECTION 2. CHAMP D'APPLICATION MATÉRIEL

2.8 *Ratione materiae*, la loi s'applique aux « services de paiement ». L'expression est définie à l'article I.9, 1°, du C.D.E., qui énumère les huit catégories de services offerts en vente dans le cadre d'une activité professionnelle et susceptibles de répondre à la notion.

Sont notamment visés « l'exécution d'opérations de paiement, y compris les transferts de fonds sur un compte de paiement auprès du prestataire de services de paiement de l'utilisateur ou auprès d'un autre prestataire de services de paiement : [...] l'exécution d'opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire ; l'exécution de virements, y compris d'ordres permanents de paiement »[2], y compris lorsque les fonds sont couverts par un contrat de crédit[3], l'émission et/ou l'acquisition d'instruments de paiement[4], les transmissions de fonds[5], voire encore les nouveaux services ajoutés par la DSP 2 (les services d'initiation de paiement et d'information sur les comptes[6]).

2.9 Les paiements par carte de crédit ou de débit, par l'exécution d'un virement *on-line* ou au moyen de monnaie électronique constituent des services de paiement soumis aux dispositions du livre VII du C.D.E.

2.10 Il convient de noter que de nombreuses opérations de paiement sont exclues du domaine d'application de la loi conformément à l'article VII.3 du C.D.E.

Il s'agit notamment des paiements en espèces[7] ; des opérations fondées sur divers documents au format papier (chèque, titre de service ou un chèque de voyage)[8] ou des services fournis par des prestataires de services techniques qui, sans entrer en possession des fonds, peuvent néanmoins intervenir en appui des prestataires de services de paiement, par exemple en offrant des moyens de communication sécurisés et fiables (à l'exception de services d'initiation de paiement et des services d'information sur les comptes)[9].

1. C'est par exemple le cas de MasterCard ou AtosWorldline.
2. Art. I.9, 1°, c), C.D.E.
3. Art. I .9, 1°, d), C.D.E. Le « contrat de crédit » est défini à l'art. 2, 28°, du C.D.E.
4. Art. I.9, 1°, e). L'« instrument de paiement » est défini à l'art. I.9, 10°, du C.D.E.
5. Art. I.9, 1°, f), C.D.E. La « transmission de fonds » est définie à l'art. I.9, 14°, du C.D.E.
6. Art. I.9, 1°, g) et h), C.D.E.
7. Art. VII.3, 1°, C.D.E.
8. Art. VII.3, 7°, C.D.E.
9. Art. VII.3, 10°, C.D.E.

SOUS-SECTION 3. CHAMP D'APPLICATION PERSONNEL

2.11 *Ratione personae*, les services de paiement sont fournis par un « prestataire de services de paiement » à un « utilisateur de services de paiement ».

2.12 Le prestataire de services de paiement[1] doit être un établissement de crédit[2], un établissement de monnaie électronique[3], un établissement de paiement[4], bpost, la BNB ou la BCE, voire encore les autorités fédérales, régionales ou locales belges[5].

L'accès et l'exercice de cette activité sont soumis à diverses exigences prudentielles ressortissant au droit financier et qui ne figurent pas, comme telles, dans le livre VII du C.D.E. Il faut en effet avoir égard, en particulier, aux dispositions de 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, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement.

2.13 L'utilisateur de services de paiement, quant à lui, peut être un payeur[6] ou un bénéficiaire de services de paiement[7].

Le cas échéant, le payeur peut être un consommateur[8]. Eu égard à la faiblesse dont il est supposé souffrir dans les relations avec les entreprises, le législateur a mis en place un régime plus protecteur au bénéfice de celui-ci. Plus précisément, il est interdit de déroger à certaines dispositions de la loi lorsque l'utilisateur est un consommateur (une telle dérogation conventionnelle étant permise si l'utilisateur n'est pas un consommateur). Cela concerne notamment le chapitre 2[9] (informations régissant les opérations de paiement et les contrats-cadres) et certaines dispositions du chapitre 3[10] (droits et obligations liées à la prestation et à l'utilisation des services de paiement).

1. La notion est définie à l'art. I.9, 2°, du C.D.E.
2. Il doit s'agir d'un établissement de crédit visé à l'article 1er, § 3, alinéa 1er de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse. Sont concernées les principales institutions bancaires.
3. Sont concernés les établissements de monnaie électronique tels que visés à l'article 2, 73°, de la loi du 11 mars 2018.
4. Sont concernées les personnes morales qui sont habilitées à fournir des services de paiement conformément à la loi du 11 mars 2018.
5. Encore faut-il qu'elles soient habilitées à cet effet en vertu de la législation qui règle leurs missions et/ou leurs statuts et qu'elles n'agissent pas en qualité d'autorité publique.
6. Le « payeur » est « la personne physique ou morale qui est titulaire d'un compte de paiement et qui autorise un ordre de paiement à partir de ce compte de paiement, ou la personne physique ou morale qui, en l'absence de compte de paiement, donne un ordre de paiement » (art. I.9, 4°, C.D.E.).
7. Le « bénéficiaire » est « la personne physique ou morale qui est le destinataire prévu de fonds ayant fait l'objet d'une opération de paiement » (art. I.9, 5°, C.D.E.). Sur la plateforme Justel (ejustice.fgov.be), la définition semble avoir été abrogée par l'article 2, b), de la loi du 2 mai 2019 portant dispositions diverses en matière d'économie. C'est toutefois une erreur, le but du législateur étant d'abroger l'article I.9, 5°, définissant le « système d'accréditation ». Avec des articles numérotés I.9 (l'un pour le livre VII, l'autre pour le livre VIII), on devait malheureusement s'attendre à ce que ce type de difficulté survienne…
8. Au sens de l'art. I.1, 2°, C.D.E.
9. Art. VII.5 C.D.E.
10. Art. VII.29 C.D.E.

Conformément à la DSP 1[1] et à la DSP 2[2], les Etats membres pouvaient traiter les microentreprises[3] de la même manière que les consommateurs, de sorte que, dans leurs relations avec le prestataire de services de paiement, les dérogations conventionnelles aux dispositions de la loi soient également prohibées. Cette possibilité n'a toutefois pas été retenue par le législateur belge, ce que l'on regrette.

SECTION 3. TRANSPARENCE ET LOYAUTÉ DES RELATIONS CONTRACTUELLES ET DES OPÉRATIONS DE PAIEMENT NOUÉES DANS CE CADRE

3.1 La transparence et la loyauté des opérations de paiement figurent parmi les moyens permettant de renforcer la confiance des utilisateurs et de garantir une saine concurrence entre les prestataires, au bénéfice du marché intérieur des services de paiement.

Ces objectifs sont principalement atteints par la prescription, à charge du prestataire, d'obligations d'information, dont le contenu et le mode d'extériorisation sont précisément définis.

3.2 On note que ces exigences s'ajoutent à celles qui sont requises par ailleurs, dans d'autres dispositions légales ou réglementaires[4].

On songe aux dispositions du livre VII du C.D.E. relatives au crédit ou, conformément au livre VI du C.D.E., aux règles applicables aux contrats à distance portant sur des services financiers (art. VI.54 et s. du C.D.E.). Des obligations d'information, assorties d'exigences de forme, sont en effet imposées par ces dispositions.

Le législateur veille à leur articulation[5] et, conformément à l'article VII.6 du C.D.E., « les informations visées aux VII.14, VII.15, VII.21 et VII.22 remplacent les informations visées à l'article VI.55, § 1er, du Code de droit économique, à l'exception du 2°, c) à g), 3°, a), d) et e), et 4°, b) ».

3.3 Le livre VII distingue selon que l'opération de paiement est couverte par un contrat-cadre[6] ou, dans le cas contraire, constitue une opération de paiement isolée.

1. Voir le considérant n° 20.
2. Voir le considérant n° 53 ainsi que l'art. 38, § 2, et 61, § 3, de la directive.
3. Telles que définies par la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros-, petites et moyennes entreprises, *J.O.*, n° L 124 du 20 mai 2003.
4. Voir en ce sens l'art. 5, al. 2, du C.D.E. Voir ég. le considérant n° 22 de la directive sur les services de paiement.
5. Suivant le considérant n° 22 de la directive, « il y a lieu de préciser [...] le lien entre les exigences d'information précontractuelle figurant dans la présente directive et celles figurant dans la directive 2002/65/CE ».
6. La notion est définie à l'art. I.9, 16°, du C.D.E.

SOUS-SECTION 1RE. OPÉRATIONS DE PAIEMENT ISOLÉES

3.4 S'il s'agit d'une *opération de paiement isolée*[1] qui n'est pas couverte par un contrat-cadre, les exigences sont assez réduites et se limitent aux informations essentielles (l'utilisateur étant généralement présent au moment de l'ordre de paiement).

3.5 Avant que l'utilisateur ne soit lié par un contrat ou une offre de service de paiement isolé, ces informations portent sur l'identifiant unique, les frais ou le délai d'exécution maximal[2], ainsi que, le cas échéant, les informations et les conditions visées à l'article VII.15.

Après l'initiation ou la réception d'un ordre de paiement et après l'exécution de la transaction, elles concernent respectivement les références permettant d'identifier l'opération de paiement et les parties à celle-ci, son montant, les frais, le taux de change éventuel, ainsi que la date (soit la date de réception de l'ordre de paiement, soit la date valeur du crédit)[3].

3.6 Pour ce qui est de l'extériorisation des informations, la loi exige seulement qu'elles soient *mises à la disposition* de l'utilisateur, sous une forme aisément accessible, ce qui requiert de la part de ce dernier une démarche active pour en prendre connaissance[4]. Il lui est cependant permis de demander qu'elles lui soient fournies sur un support durable[5]. Considérant que la conclusion du contrat par un moyen de communication à distance peut empêcher le prestataire de se conformer à ses obligations d'information préalable – lors d'une communication par téléphone par exemple –, celui-ci est autorisé à y satisfaire immédiatement après l'opération de paiement[6].

3.7 Le recours possible aux technologies de l'information est pris en considération par le législateur puisque les formalités à accomplir sont désignées par des termes fonctionnellement neutres – support durable – et susceptibles de viser des procédés propres à l'environnement traditionnel (papier) ou à l'environnement numérique (voir *infra*, n° 3.9).

1. Les travaux préparatoires indiquent les opérations visées : il s'agit notamment d'un « type particulier de pratiques commerciales anglo-saxonnes, comme les transmissions de fonds (« *money remittance* ») et certains modèles de services de paiement de factures (« *bill payment services* ») » (*Doc. parl.*, Chambre, sess. ord. 2017-2018, n° 3131/001, p. 25).
2. Art. VII.15 C.D.E.
3. Art. VII.16-VII.19 C.D.E.
4. Art. VII.14, § 1er, C.D.E.
5. Art. VII.14, § 1er, al. 2, C.D.E.
6. Art. VII.14, § 2, C.D.E.

SOUS-SECTION 2. OPÉRATIONS DE PAIEMENT COUVERTES PAR UN CONTRAT-CADRE

3.8 Les opérations de paiement couvertes par *un contrat-cadre* sont soumises à des obligations d'information nettement plus lourdes. Cette hypothèse est de loin la plus fréquente en pratique, l'utilisateur disposant généralement d'un compte de paiement ou d'un instrument de paiement pour lequel un contrat a été établi[1].

3.9 Elles portent d'abord sur le contrat-cadre en tant que tel puisque, pour garantir un consentement libre et éclairé de l'utilisateur, diverses informations et conditions doivent lui être *fournies* sur un support durable, bien avant qu'il ne soit lié par le contrat-cadre ou l'offre[2].

La notion de support durable est définie à l'article I.1, 15°, du C.D.E., comme « tout instrument permettant à une personne physique ou morale de stocker des informations qui lui sont adressées personnellement d'une manière lui permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées ». Trois fonctions doivent ainsi être préservées : la lisibilité de l'information, l'intégrité du contenu et sa pérennité. Le législateur donne également des exemples de procédés susceptibles d'être utilisés : le papier (dans l'environnement traditionnel), et « un courrier électronique reçu par le destinataire ou un document électronique enregistré sur un dispositif de stockage ou attaché à un courrier électronique reçu par le destinataire » (dans l'environnement électronique).

Dans l'arrêt *Bawag*, rendu le 25 janvier 2017[3], la Cour de justice a précisé la portée de cette double exigence de « fourniture » et de « support durable », dans le contexte spécifique des services de paiement. La question se posait en effet de savoir si le procédé utilisé par un prestataire de services de paiements pour communiquer les informations légalement requises aux utilisateurs[4] – transmission au moyen d'une boîte aux lettres électronique intégrée au site d'*internet banking* du prestataire – était conforme aux règles applicables.

Tout en rappelant les enseignements de ses précédents arrêts, la Cour veille à confirmer que certains sites internet peuvent être qualifiés de « support durable »[5]. Elle précise en effet que « tel est le cas lorsqu'un site Internet permet à l'utilisateur de services de paiement de stocker les informations qui lui sont personnellement adressées d'une manière telle que ces informations puissent être consultées ultérieurement pendant une période adaptée à leur finalité ainsi que reproduites à l'identique. En outre, pour qu'un site Internet puisse être considéré comme étant un 'support durable', au sens de cette disposition, toute possibilité de modification unilatérale de son contenu par le prestataire de services de paiement ou par un autre professionnel auquel la gestion de ce site a été confiée doit être exclue »[6]. Elle

1. Voir le considérant n° 24 de la directive sur les services de paiement.
2. Art. VII.21, § 1er, du C.D.E. Conformément à l'art. VII.21, § 3, du C.D.E., le prestataire peut également « s'acquitter des obligations découlant du paragraphe 1er en fournissant un exemplaire du projet de contrat-cadre comportant les informations et les conditions définies à l'article VII.22 ». Cette disposition précise par ailleurs les informations à fournir « lorsque le contrat-cadre concerne l'ouverture d'un compte de paiement et qu'il est possible qu'un dépassement soit autorisé au consommateur ».
3. C.J.U.E., 25 janvier 2017, *BAWAG PSK Bank*, C-375/15, ECLI:EU:C:2017:38.
4. Voir, en particulier, l'art. 41, § 1er, de la Directive 2007/64/CE, ainsi que l'article 44, § 1er, qui renvoie à cette disposition.
5. C.J.U.E., 25 janvier 2017, *BAWAG PSK Bank*, C-375/15, ECLI:EU:C:2017:38, points 42-43.

ajoute que l'objectif poursuivi est la protection des utilisateurs de services de paiement, parmi lesquels figurent des consommateurs[1]. L'exclusion de toute possibilité de modification unilatérale du contenu doit d'après nous être interprétée raisonnablement, sous peine de refuser la qualification de « support durable » à de très nombreux procédés, pourtant utilisés en pratique. On rappelle par ailleurs que, dans l'environnement « papier » traditionnel, le caractère inaltérable du support est loin d'être absolu.

Concernant l'exigence de « fourniture » des informations, la Cour veille à clairement distinguer cette modalité de transmission des informations, qui requiert du prestataire qu'il « communique activement les informations concernées, sans autre sollicitation de la part de l'utilisateur », de la « mise à disposition » des informations, où il incombe à l'utilisateur de « prendre activement des mesures afin d'obtenir les informations »[2]. En l'espèce, il s'agit d'une boîte aux lettres intégrées au service d'*internet banking*, qui n'est utilisée que pour cette finalité et que le consommateur ne consulte pas de manière systématique et régulière. La Cour veille cependant à préciser que « les informations concernées qui sont transmises par le l'utilisateur de ces services au moyen d'un site Internet de banque en ligne peuvent être considérées comme étant fournies, au sens de l'article 41, paragraphe 1, de la directive 2007/64, si une telle transmission est accompagnée d'un comportement actif de ce prestataire destiné à porter à la connaissance de cet utilisateur l'existence et la disponibilité de ces informations sur ledit site »[3].

Le cas échéant, si le moyen de communication à distance utilisé à la demande de l'utilisateur ne le permet pas, les formalités peuvent être accomplies immédiatement après la conclusion du contrat-cadre[4].

Sur le fond, les informations requises portent sur le prestataire de service de paiement (données d'identification et coordonnées de l'autorité de contrôle prudentiel), l'utilisation d'un service de paiement (la description du service, en ce compris les caractéristiques techniques de l'équipement de communication qui peut être utilisé, l'identifiant unique, le délai d'exécution, etc.), les frais encourus, la

6. C.J.U.E., 25 janvier 2017, *BAWAG PSK Bank*, C-375/15, ECLI:EU:C:2017:38, point 44.

1. Il appartient évidemment à la juridiction de renvoi de s'assurer que cette condition est satisfaite en l'espèce. Tel semble être le cas ici : la Cour indique en effet dans l'exposé des faits que « il ressort de la décision de renvoi que les messages envoyés dans les boîtes électroniques dédiées aux consommateurs qui se trouvent sur le site Internet de banque en ligne *e-banking* y subsistent sans modification et ne sont pas supprimés pendant une période adaptée aux fins de l'information de ces consommateurs, de telle sorte qu'ils peuvent être consultés et reproduits à l'identique par voie électronique ou imprimés. Ces messages peuvent être gérés par les consommateurs et, le cas échéant, effacés par ceux-ci ».
2. C.J.U.E., 25 janvier 2017, *BAWAG PSK Bank*, C-375/15, ECLI:EU:C:2017:38, point 47.
3. C.J.U.E., 25 janvier 2017, *BAWAG PSK Bank*, C-375/15, ECLI:EU:C:2017:38, point 50. A titre d'exemple, la Cour ajoute que « ainsi que l'a relevé en substance M. l'avocat général au point 79 de ses conclusions, peut notamment constituer un tel comportement l'envoi d'une lettre ou d'un courriel à l'adresse habituellement utilisée par l'utilisateur de ces services pour communiquer avec d'autres personnes et dont les parties ont convenu de l'utilisation dans un contrat-cadre conclu entre le prestataire de services de paiement et cet utilisateur. L'adresse ainsi choisie ne saurait, cependant, être celle dédiée audit utilisateur sur le site Internet de banque en ligne géré par le prestataire de services de paiement ou par un autre professionnel auquel la gestion de ce site a été confiée dans la mesure où ledit site, même s'il contient une boîte à lettres électronique, n'est pas utilisé par le même utilisateur aux fins de sa communication habituelle avec d'autres personnes que ce prestataire ».
4. Art. VII.21, § 2, C.D.E.

communication, les mesures de protection et les mesures correctives, la modification et la résiliation du contrat-cadre[1] ainsi que les recours[2].

3.10 Les opérations de paiement individuelles couvertes par un contrat-cadre peuvent (ou doivent, selon le cas) également faire l'objet de mesures d'information, préalablement ou postérieurement à leur exécution.

Dans le premier cas, elles concernent le délai d'exécution maximal ou les frais et ne sont fournies qu'à la demande du payeur[3].

Dans l'autre hypothèse, les informations doivent être fournies sans tarder par le prestataire du payeur, après le débit du compte du payeur ou la réception de l'ordre de paiement[4], et par celui du bénéficiaire, après l'exécution de l'opération de paiement[5].

Les renseignements portent sur les références permettant d'identifier l'opération, son montant, les frais, le taux de change éventuellement appliqué ainsi que la date valeur du débit ou du crédit.

La loi n'exige toutefois pas que l'utilisateur soit informé après chaque opération de paiement : le contrat-cadre peut en effet prévoir une « condition selon laquelle le payeur peut demander que les informations visées au paragraphe 1er sont fournies ou mises à disposition périodiquement, au moins une fois par mois, gratuitement et selon des modalités convenues qui permettent [à l'utilisateur] de stocker les informations et de les reproduire à l'identique, de façon à lui permettre de suivre raisonnablement l'état de ses dépenses »[6]. Ces informations doivent être communiquées suivant les modalités prescrites par l'article VII.21, qui impose la double exigence de « fourniture » sur un « support durable ».

3.11 Il convient de souligner que, lorsque les opérations réalisées au moyen de certains instruments de paiement portent sur des montants limités, le livre VII du C.D.E. réduit sensiblement les obligations d'information dont le prestataire est normalement débiteur dans les hypothèses décrites précédemment, eu égard, principalement, aux risques limités qu'ils présentent.

Il s'agit des instruments de paiement qui, « conformément au contrat-cadre, concernent exclusivement des opérations de paiement dont le montant unitaire n'excède pas 30 euros ou, soit ont une limite de dépenses de 150 euros, soit stockent des fonds dont le montant n'excède à aucun moment 150 euros »[7].

3.12 Des exigences figurant dans le chapitre 3 du livre VII, traitant des droits et obligations liés à la prestation et à l'utilisation de services de paiement, ont

1. On note à ce propos que des obligations tenant à la modification des conditions contractuelles ou à la résiliation du contrat sont prescrites par les art. VII.24-VII.25 du C.D.E. Voir aussi C.J., 11 novembre 2020, aff. C-287/19, *DenizBank AG*, EU:C:2020:897, où 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).
2. Art. VII.22 C.D.E.
3. Art. VII.26 C.D.E.
4. Art. VII.27 C.D.E.
5. Art. VII.28 C.D.E.
6. Art. VII.27, § 2, et VII.28, § 2, C.D.E.
7. Art. VII.9, § 1er, 1°, C.D.E.

également pour effet de garantir la transparence et la loyauté des relations contractuelles. Des obligations d'archivage incombent ainsi au prestataire, qui doit tenir un registre interne des opérations de paiement[1]. Le délai de conservation est d'au moins dix ans. Il prend cours dès l'exécution des opérations et s'applique sans préjudice des autres dispositions légales ou réglementaires encadrant la fourniture de pièces justificatives. En cas de litige, il importe en effet que les données aient été conservées dans de bonnes conditions. Dans le même objectif de protection de l'utilisateur de service de paiement, pour éviter les fournitures non demandées, le prestataire doit s'abstenir « d'envoyer tout instrument de paiement non sollicité, sauf dans le cas où un instrument de paiement déjà donné à l'utilisateur de services de paiement doit être remplacé »[2].

SECTION 4. SÉCURITÉ DES OPÉRATIONS DE PAIEMENT ET PARTAGE DE RESPONSABILITÉ EN CAS D'OPÉRATIONS DE PAIEMENT NON AUTORISÉES

4.1 La sécurité des opérations de paiement ou, plus globalement, des systèmes de paiement, constitue un élément indispensable de son développement.

Au-delà des mesures techniques ou organisationnelles mises en place pour obvier aux risques de fraudes (cryptage des données ou intervention d'un tiers de confiance, par exemple), le cadre normatif comporte des mesures préventives et curatives.

SOUS-SECTION 1RE. MESURES PRÉVENTIVES

4.2 Pour garantir la sécurité des opérations de paiement, la loi impose diverses obligations au prestataire.

Il est ainsi requis qu'« il s'assure que les données de sécurité personnalisées de tout instrument de paiement ne sont pas accessibles à d'autres parties que l'utilisateur de services de paiement autorisé à utiliser cet instrument, sans préjudice des obligations de l'utilisateur de services de paiement visées à l'article VII.38 »[3].

4.3 Parallèlement, l'utilisateur doit également contribuer à la poursuite de cet objectif, eu égard à ses moyens et compétences.

De manière générale, la loi exige ainsi qu'« il utilise l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de cet instrument de paiement, qui doivent être objectives, non discriminatoires et proportionnées »[4].

1. Art. VII.40 C.D.E.
2. Art. VII.39, 2°, C.D.E.
3. Art. VII.39, 1°, C.D.E. En lien avec cette exigence, il appartient au prestataire d'assumer « le risque lié à l'envoi d'un instrument de paiement à l'utilisateur de services de paiement ou de tout moyen qui en permet l'utilisation, en particulier toute donnée de sécurité personnalisée de celui-ci » (art. VII.39, 6°, C.D.E.).
4. Art. VII.38, § 1er, 1°, C.D.E.

Plus précisément, il doit prendre « toutes les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses données de sécurité personnalisées »[1].

Diverses informations que le prestataire doit fournir à l'utilisateur conformément à l'article VII.22, 5°, du C.D.E., avant qu'il ne soit lié par un contrat-cadre ou une offre, portent sur ces mesures de protection[2].

SOUS-SECTION 2. MESURES CURATIVES

4.4 D'un point de vue curatif, la loi comporte des mesures favorables à l'utilisateur, en ce sens que, moyennant certaines conditions, elles le dispensent de supporter tout ou partie des conséquences résultant des opérations de paiement non autorisées. Le principe établi à l'article VII.32, § 1er, du C.D.E. est en effet qu'« une opération de paiement est réputée autorisée si le payeur a donné son consentement à l'exécution de l'ordre de paiement ».

En cas d'opération de paiement non autorisée, la première obligation incombe à l'utilisateur : dès qu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement[3], l'article VII.38, § 1er, 2°, du C.D.E. lui impose d'informer sans délai son prestataire de services de paiement ou l'entité indiquée par celui-ci[4]. Cette notification doit se faire au plus tard dans les treize mois suivant la date de débit ou de crédit[5] (sauf manquement éventuel du prestataire à ses obligations d'information).

Corrélativement, des moyens appropriés doivent être mis à sa disposition par le prestataire pour lui permettre de procéder à cette notification (le système « Card Stop », p. ex.)[6]. 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 ». La question s'est posée de savoir si cette dérogation pouvait être mobilisée dans l'hypothèse des paiements sans contact. Saisie sur question préjudicielle, la Cour de justice a rappelé que s'agissant d'une exception à l'application d'autres dispositions de la DSP 2, il fallait procéder à une interprétation stricte de l'article 63, § 1er, a)[7]. Tout en nuance, elle confirme qu'on ne peut se satisfaire d'une déclaration péremptoire du

1. Art. VII.38, § 2, C.D.E.
2. Il s'agit en effet de « description des mesures de prudence que l'utilisateur de services de paiement prend pour préserver la sécurité d'un instrument de paiement [...] » (art. VII.22, 5°, a), C.D.E.).
3. L'exigence de notification ne s'applique pas lorsque le payeur pense – même à tort – que sa carte a été avalée par un automate (Bruxelles, 14 novembre 2019, *Dr. banc. fin.*, 2020, p. 71, note R. STEENNOT).
4. Sur la procédure de notification, voir aussi les art. VII.41-VII.42 du C.D.E.
5. Voir à cet égard C.J., 2 septembre 2021, aff. C-337/20, *DM et LR contre Caisse régionale de Crédit agricole mutuel (CRCAM) – Alpes-Provence,* ECLI:EU:C:2021:671, où la Cour décide que l'« utilisateur qui n'a pas signalé à son prestataire de services de paiement une opération non autorisée, dans les treize mois du débit de celle-ci, ne peut pas engager la responsabilité de ce prestataire, y compris sur le fondement du droit commun et, partant, ne peut obtenir le remboursement de cette opération non autorisée » (point 36). Quant à la possibilité pour le prestataire de prévoir un délai plus court, voir Bruxelles, 19 avril 2013, *Dr. banc. fin.*, 2013, p. 314, note R. STEENNOT (qui refuse en l'occurrence cette limitation, par application de la LTEF).
6. Art. VII.39, 3° et 4°, du C.D.E. La loi précise que « le prestataire de services de paiement fournit, sur demande, à l'utilisateur de services de paiement, pendant dix-huit mois à compter de la notification, les moyens de prouver qu'il a bien procédé à cette notification ». Il importe en effet qu'outre l'existence de la notification, son moment exact puisse être démontré avec précision (date et heure).
7. Point 101 de l'arrêt commenté.

prestataire de services de paiement, qui indiquerait – 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. La Cour 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) »[1].

4.5 Un régime de responsabilité spécifique est mis en place par le livre VII du C.D.E., de manière à désigner la partie sur laquelle reposent, totalement ou partiellement, les risques encourus à la suite d'une opération de paiement non autorisée. Cela concerne spécifiquement la relation entre le payeur et le prestataire de service de paiement (§ 1er). Nous analyserons également les conséquences d'une opération de paiement non autorisée dans le chef de l'entreprise bénéficiaire du paiement (§ 2), ainsi que l'application des règles de partage de responsabilité en cas de recours à des mécanismes de paiement sans contact (§ 3).

§ 1er. Partage de responsabilité entre le prestataire de service de paiement et le payeur

4.6 L'article VII.43, § 1er, du C.D.E. pose le principe suivant lequel, en cas d'opération de paiement non autorisée, le payeur doit être remboursé immédiatement par son prestataire de services de paiement.

La règle s'applique si, à l'issue d'une vérification *prima facie*, aucune fraude n'a été détectée dans le chef du payeur.

Le *statu quo ante* doit être rétabli, en créditant par exemple le compte du payeur du montant de l'opération de paiement non autorisée. D'autres conséquences financières éventuelles doivent aussi être couvertes[2].

4.7 Ce principe connaît toutefois des tempéraments. Pour les présenter, une distinction doit être faite suivant que les opérations de paiement non autorisées ont été réalisées avant ou après la notification du payeur. Il convient de noter que certaines de ces règles sont supplétives lorsque l'utilisateur n'est pas un consommateur[3].

4.8 *Après la notification*, lorsque l'instrument de paiement a été perdu, volé ou détourné, les conséquences financières sont supportées par le prestataire[4]. Au

1. Point 98 de l'arrêt commenté.
2. Art. VII.43, § 3, C.D.E. Sont notamment visés les frais supportés par le titulaire pour la détermination du dommage indemnisable. Voir aussi l'art. VII.43, § 2, qui règle l'hypothèse dans laquelle l'opération a été initiée par un prestataire de services d'initiation de paiement.
3. Art. VII.29 C.D.E. : « lorsque l'utilisateur de services de paiement n'est pas un consommateur, les parties peuvent décider que les articles VII.30, § 1er, VII.32, § 3, VII.33, VII.42, VII.44, VII.46 et VII.47, VII.50, VII.55/3 à VII.55/7, ne s'appliquent pas, en tout ou partie. Les parties peuvent également convenir d'un délai distinct de celui fixé à l'article VII.41 ».
4. Art. VII.44, § 3, C.D.E.

nombre des exigences imposées au prestataire par l'article VII.39 du C.D.E. figure en effet l'obligation d'empêcher « toute utilisation de l'instrument de paiement après la notification effectuée en application de l'article VII.38, § 1er, 2° » (5°).

Cette règle est toutefois inapplicable s'il est démontré que le payeur a agi frauduleusement (la charge de la preuve incombant au prestataire).

4.9 *Avant la notification*, il convient de distinguer trois hypothèses principales : (i) le payeur doit supporter toutes les conséquences (et donc toutes les pertes financières) de l'opération de paiement non autorisée (*infra*, n° 4.10), (ii) le payeur ne doit supporter aucune perte financière (*infra*, n° 4.11) et (iii) le payeur doit supporter les pertes éventuelles à concurrence de 50 EUR (*infra*, n° 4.12).

4.10 Le payeur devra supporter toutes les pertes occasionnées par les opérations de paiement non autorisées en cas de fraude de sa part ou s'il n'a pas satisfait à tout ou partie des obligations qui lui incombent conformément à l'article VII.38, « intentionnellement ou à la suite d'une négligence grave »[1]. La charge de la preuve de la fraude, du manquement intentionnel ou de la négligence grave du payeur repose sur le prestataire de services de paiement[2].

La loi donne des exemples de circonstances pouvant être considérées comme des négligences graves[3]. Sont ainsi mentionnés « le fait, pour le payeur de noter ses données de sécurité personnalisées, comme son numéro d'identification personnel ou tout autre code, sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement ou sur un objet ou un document conservé ou emporté par le payeur avec l'instrument de paiement, ainsi que le fait de ne pas avoir notifié au prestataire de services de paiement ou à l'entité indiquée par celui-ci, la perte ou le vol, dès qu'il en a eu connaissance conformément à l'article VII.38, § 1er, 2° »[4]. Ces hypothèses ne sont toutefois pas constitutives d'une présomption de négligence grave, celle-ci devant être établie à la lumière des circonstances de l'espèce[5].

Un exemple est également fourni par un arrêt rendu par la Cour d'appel de Bruxelles le 23 juin 2011[6]. Dans cette affaire, deux cartes bancaires (de débit) sont volées dans une chambre d'hôtel en Italie et des opérations de retrait ou de paiement sont réalisées pour un montant de plus de 2.500 EUR. Les titulaires des cartes postulent par conséquent l'intervention de leur banque, qui refuse pourtant de les indemniser, estimant qu'ils auraient commis une négligence grave (en laissant les instruments de paiement sans surveillance dans la chambre d'hôtel et en rendant le numéro d'identification personnel ou le code aisément accessible). La Cour d'appel retient les arguments de la banque et juge que les demandeurs ont commis une négligence grave « en laissant leurs cartes bancaires sans surveillance dans une chambre d'hôtel, qui est un lieu accessible à diverses personnes, dans les circonstances décrites ci-avant ».

1. Art. VII.44, § 1er, al. 4, C.D.E.
2. Art. VII.44, § 4, C.D.E.
3. Pour des applications jurisprudentielles, sous l'empire de la LTEF, voir not. Bruxelles, 4 octobre 2005, *NjW*, 2006, p. 709 ; Bruxelles, 13 sept. 2005, *D.C.C.R.*, 2006, p. 86 ; Comm. Bruxelles, 27 nov. 2006, *Dr. Banc. Fin.*, 2006, p. 137 ; Bruxelles, 20 avril 2012, *R.D.C.*, 2015, p. 191, note R. STEENNOT.
4. Art. VII.44, § 4, al. 2, C.D.E.
5. Voir l'art. VII.44, § 4, *in fine*: « pour l'appréciation de la négligence, le juge tient compte de l'ensemble des circonstances de fait. La production par le prestataire de services de paiement des enregistrements visés à l'article VII.42 et l'utilisation de l'instrument de paiement avec le code connu du seul utilisateur de services de paiement ne constituent pas une présomption suffisante de la négligence de celui-ci. ».
6. *D.C.C.R.*, 2012, p. 120, note R. STEENNOT, *R.D.C.*, 2013, p. 611, note E. JACOBS. On note que cet arrêt est rendu sur la base de la LTEF.

Le remboursement du payeur est aussi refusé dans une affaire jugée par la Cour d'appel d'Anvers le 5 novembre 2020[1]. Le titulaire du compte avait été victime de phishing, et dépouillé de 48 662,13 EUR. La Cour confirme la décision de première instance, qui avait retenu une négligence grave dans son chef. La Cour relève notamment l'adresse email de l'émetteur (visit@pagemdnn.site), l'absence de logo de la banque dans le message ou l'heure tardive de l'envoi (1h47). Contacté par téléphone, la victime avait notamment communiqué son code pin ainsi que les codes d'authentification générés par son digipass. La Cour confirme également que la négligence grave doit s'apprécier *in abstracto* : « la négligence [...] de la victime d'un email de phishing doit être appréciée selon le critère du comportement attendu d'un payeur normalement prudent et diligent, placé dans les mêmes circonstances externes concrètes, sans qu'il puisse être tenu compte des caractéristiques propres du payeur, comme par exemple son âge ».

4.11 Dans plusieurs hypothèses, au contraire, le payeur ne devra supporter aucune perte.

Deux d'entre elles sont listées à l'article VII.44, § 1er, alinéa 2, du C.D.E. Elles visent les cas où « 1° la perte, le vol ou le détournement d'un instrument de paiement ne pouvait être détecté par le payeur avant le paiement, sauf si le payeur a agi frauduleusement, ou 2° la perte est due à des actes ou à une carence d'un salarié, d'un agent ou d'une succursale d'un prestataire de services de paiement ou d'une entité vers laquelle ses activités ont été externalisées ». La première hypothèse est, par exemple, rencontrée lorsque le payeur est victime de *skimming* et que les données de sa carte de paiement sont dérobées par un appareil électronique placé sur un distributeur de billets ou une borne de paiement (pour l'achat d'un ticket de métro par exemple)[2]. Le payeur étant toujours en possession de sa carte, il peut difficilement détecter la fraude dont il a été victime ; pourtant, sa carte a été clonée et sera ultérieurement utilisée pour des opérations de paiement non autorisées (le cas échéant, en combinaison avec le code pin, dont le voleur a pris connaissance au moyen d'une caméra discrètement placée). L'agissement frauduleux du payeur l'empêche logiquement de bénéficier de ce partage de responsabilité favorable.

Conformément à l'article VII.44, § 2, et sauf agissement frauduleux de sa part, le payeur est également dispensé de toute perte financière éventuelle quand son prestataire de service de paiement n'exige pas une authentification forte. Celle-ci désigne « 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 »[3]. Il s'agit, par exemple, de la carte ou d'un smartphone (« possession »), combiné(e) à un code pin

1. Anvers, 5 novembre 2020, *Dr. banc. fin.*, 2021, p. 3, note G. LAGUESSE. Dans le même sens, Civ. Anvers (div. Anvers), 27 novembre 2019, *Dr. banc. fin.*, 2021, p. 7. Comparer Trib. entr. Louvain, 23 mars 2021 (*R.W.*, 2021-22, p. 1246, *R.D.C.*, 2022/2, p. 221, note A. DIERICK), qui juge que la négligence grave n'est pas d'application lorsque l'utilisation non-autorisée de l'instrument de paiement ne pouvait pas être constatée par le payeur avant le paiement (conformément à l'art. VII.44, § 1er, al. 2, 1°, du C.D.E.).
2. Elle a également été appliquée dans le cas du *phishing* : Trib. entr. Louvain, 23 mars 2021, *R.W.*, 2021-22, p. 1246, *R.D.C.*, 2022/2, p. 221, note A. DIERICK.
3. Art. I.9, 33/16°, C.D.E.

(« connaissance ») ou à un procédé de reconnaissance biométrique, lié aux empreintes digitales ou à la reconnaissance faciale, dont sont équipés certains smartphones (« inhérence »). L'objectif du législateur est d'encourager les prestataires (et les bénéficiaires) à utiliser des mécanismes offrant un niveau élevé de sécurité. Sur ce point, on aura égard au Règlement délégué (UE) n° 2018/389 de la Commission du 27 novembre 2017 complétant la Directive (UE) n° 2015/2366 du Parlement européen et 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.

4.12 Dans les autres cas de figure, la responsabilité sera partagée entre le payeur et le prestataire de services de paiement. Le payeur devra en effet supporter les pertes à concurrence de 50 EUR[1]. Cette hypothèse ne devrait donc s'appliquer qu'en dehors de circonstances dans lesquelles le payeur ne supporte aucune perte (*supra*, n° 4.11) ou, au contraire, est tenu d'assumer toute la responsabilité financière de l'opération de paiement non autorisée (*supra*, n° 4.10). Ce sera, par exemple, le cas si le prestataire a mis en place un mécanisme d'authentification forte et que, malgré celui-ci, une opération de paiement non autorisée est survenue.

§ 2. Partage de responsabilité entre le prestataire de service de paiement et le bénéficiaire

4.13 Lorsque le payeur est exonéré de tout ou partie des conséquences financières résultant d'une opération de paiement non autorisée (et devra donc être indemnisé), la question se pose de savoir qui, du prestataire de service de paiement ou du bénéficiaire du paiement, devra finalement supporter cette perte (partant du principe que l'auteur de la fraude n'a pas été identifié).

4.14 Le livre VII du Code de droit économique ne règle pas spécifiquement cette question, sauf dans l'hypothèse où le bénéficiaire ou son prestataire de service de paiement n'accepte pas une authentification forte du client. Dans ce cas, il est en effet prévu que celui-ci doit rembourser le prestataire de services de paiement du payeur du préjudice financier subi[2]. L'objectif est clairement d'encourager les parties à recourir à de tels mécanismes d'authentification forte et, ainsi, réduire les risques de fraude.

Dans les autres hypothèses, il convient de se référer aux dispositions contractuelles applicables aux relations entre les parties, telles qu'interprétées, le cas échéant, par la jurisprudence. En général, le prestataire aura pris le soin de faire peser le risque de ces opérations sur l'entreprise bénéficiaire des opérations de paiement. A moins que celle-ci dispose d'un pouvoir de négociation suffisant pour imposer conventionnellement un autre partage de responsabilité, elle devra généralement supporter les pertes qui en résultent.

1. Art. VII.44, § 1er, al. 1er, C.D.E.
2. Art. VII.44, § 2, al. 2, C.D.E.

4.15 Un arrêt rendu par la Cour d'appel de Bruxelles le 19 juin 2008 permet d'illustrer ce partage des risques, au détriment de l'entreprise bénéficiaire du paiement[1]. Dans cette affaire, une société spécialisée dans la vente de motos et d'accessoires – Good Bike – est victime d'une société de droit anglais qui lui achète par téléphone du matériel pour un montant de près de 52 000 EUR et acquitte la somme au moyen de plusieurs cartes de crédit. Pour chacune des transactions, la société Good Bike avait reçu une « non opposition » de la part de BCC. Il apparaît par la suite que les cartes de crédit avaient été utilisées frauduleusement : aussi, les titulaires de celles-ci sont-ils remboursés. Parallèlement, BCC réclame la somme à la société Good Bike : ses conditions générales l'autorisent en effet à débiter le compte interne du cocontractant en cas de contestation de l'opération par le titulaire de la carte.

La Cour d'appel de Bruxelles donne raison à BCC, jugeant qu'« en ce qui concerne les transactions par Internet, tout commerçant en connaît ou doit en connaître les risques, dès lors qu'il utilise un système de paiement par carte de crédit. Si le commerçant ne veut pas courir un tel risque, il lui suffit de ne pas accepter une commande à distance effectuée au moyen des cartes Visa et Eurocard-Mastercard. Il doit être conscient du risque lié à ce type d'instrument ».

§ 3. Partage de responsabilité en cas de paiement sans contact

4.16 Il est désormais fréquent d'utiliser la fonction de paiement sans contact (« NFC » pour « *Near Field Communication* ») dont sont munies la plupart des cartes de paiement. Avec ce dispositif, il est possible de payer de faibles montants, 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. 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)[2]. Des fraudes sont toutefois à craindre, puisque le paiement est effectué sans aucune authentification ou validation de la part du payeur.

La question se pose de savoir si les règles de protection consacrées dans le livre VII du Code de droit économique (en particulier le partage de responsabilité favorable au payeur), s'appliquent à ce cas de figure.

4.17 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[3] en ce qui les concerne, un régime allégé est mis en place. Le législateur européen considère en effet que « les instruments de

1. 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. Voir aussi Bruxelles, 10 mars 2009, *Dr. Banc. Fin.*, 2009, p. 173, note R. STEENNOT.
2. Voir p. ex. https://www.febelfin.be/fr/article/payer-sans-contact-avec-votre-carte.
3. Voir le considérant 96 de la DSP 2.

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 »[1].

Moyennant le respect de conditions strictes, l'article 63 de la DSP 2[2] permet aux prestataires de services de paiement 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 ».

4.18

Encore faut-il déterminer si les exceptions de l'article 63 de la DSP 2 s'appliquent aux paiements sans contact et sans authentification. La Cour de justice de l'Union européenne s'est prononcée sur cette question, dans un arrêt du 11 novembre 2020[3].

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. Le paiement sans contact ne constitue 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 » (tel que visé par la définition de « l'instrument de paiement »), sachant que, suivant la jurisprudence de la Cour, l'ensemble en question ne doit pas nécessairement être personnalisé[4] ? 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[5] : en cas de paiement effectué en insérant la carte dans 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.

1. Considération 81 de la DSP 2.
2. Art. VII.31 C.D.E. 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, § 1, de la DSP 2, auquel renvoie l'art. 63, § 1, c)) et à son caractère irrévocable (art. 80 de la DSP 2, auquel renvoie l'art. 63, § 1, 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, § 1, e)). Nous ne les détaillons pas davantage dès lors qu'elles ne sont pas particulièrement pertinentes dans le cas du paiement sans contact.
3. C.J., 11 novembre 2020, aff. C-287/19, *DenizBank AG*, EU:C:2020:897. Pour un commentaire de cet arrêt, voir H. JACQUEMIN, « Comment le consommateur est-il protégé en cas de paiement sans contact (NFC) ? », *D.C.C.R.*, 2021, pp. 61 et s. ; R. STEENNOT, « Gebruik van de NFC-technologie zonder geheime code : afzonderlijk betaalinstrument met bijzondere (aasprakelijkheids)regelen in geval van onrechtmatig gebruik », *R.D.C.*, 2021, p. 207.
4. C.J., 9 avril 2014, aff. C-616/11, *T-Mobile Austria*, EU:C:2014:242, points 34-35. Cf. le point 71 de l'arrêt, qui fait référence à cette jurisprudence.
5. Points 75-77 de l'arrêt.

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), 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. La Cour répond également par l'affirmative. 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 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)[1]. 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.

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 en effet 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, il faut toutefois se référer à l'article 11 du Règlement délégué (UE) n° 2018/389, qui permet 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[2]. Il en résulte que, si les conditions précitées sont satisfaites, le prestataire peut valablement s'exonérer de sa responsabilité, même en l'absence d'authentification forte du client, et pour une opération de paiement pouvant atteindre 50 EUR.

SECTION 5. SANCTIONS DU NON-RESPECT DES RÈGLES PRESCRITES PAR LA LOI

5.1 En cas d'inobservation des obligations prescrites par la loi, diverses sanctions sont susceptibles d'être mises en œuvre. Seules les sanctions prévues dans le Code de droit économique sont analysées[3].

1. Points 87 à 89 de l'arrêt commenté.
2. 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 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 ».
3. Le cas échéant, les sanctions figurant dans la loi du 11 mars 2018 pourraient également être mises en œuvre.

5.2 Les agents du SPF Economie relevant de l'Inspection économique sont compétents pour la recherche et la constatation des infractions[1].

Si une infraction est constatée, plusieurs options sont envisageables : avertissement[2], transaction[3], amende administrative[4] ou poursuite pénale proprement dite.

Les sanctions pénales applicables en cas d'infraction aux dispositions du livre VII du Code de droit économique en matière de services de paiement figurent aux articles XV.87 et suivants du C.D.E.

Le non-respect des obligations d'information (*supra*, section 3) ou des règles de partage de responsabilité (*supra*, section 4) est ainsi frappé d'une sanction de niveau 5[5] (correspondant à « une amende pénale allant d'un montant minimum de 250 euros à un montant maximum de 100 000 euros ou de 6 % du chiffre d'affaires annuel total du dernier exercice clôturé précédant l'imposition de l'amende au sujet duquel des données permettant d'établir le chiffre d'affaires annuel sont disponibles, si cela représente un montant plus élevé, et d'un emprisonnement d'un mois à un an ou d'une de ces peines seulement »[6]).

5.3 La méconnaissance des dispositions de la loi peut également être *sanctionnée civilement*.

Si le prestataire n'a pas respecté les obligations qui lui incombent en vertu des articles VII.13, 5°, a) et c)[7], et VII.31, 1° et 3°, il sera responsable « à l'égard de l'utilisateur de services de paiement, de toutes les conséquences résultant de l'usage d'un instrument de paiement par un tiers non autorisé »[8]. La règle ne s'applique toutefois pas s'il démontre une fraude dans le chef du payeur.

Par ailleurs, la méconnaissance de diverses dispositions[9] énumérées à l'article VII.191 du C.D.E. permet à l'utilisateur de résilier le contrat-cadre sans délai et sans frais ni pénalité.

Il doit le faire par lettre motivée en envoi recommandé, à partir du moment où il a connaissance, ou aurait dû avoir connaissance du non-respect de ces obligations. Sont notamment concernés les manquements à certaines exigences d'information ou le non-respect, par le prestataire, de son obligation de remboursement en cas d'opération de paiement non autorisée.

1. Art. XV.2 et s. et XV.17 et s. C.D.E.
2. Art. XV.31 C.D.E.
3. Art. XV.61 C.D.E.
4. Art. XV.60/4 C.D.E.
5. Art. XV.89, 6° et 17°, C.D.E.
6. Art. XV.70 C.D.E.
7. Cette référence à l'article VII.13 est erronée : suite à la modification du livre VII par la loi du 19 juillet 2018, l'article VII.189 aurait dû être modifié pour viser l'article VII.22, 6°, a) et d), du C.D.E.
8. Art. VII.189 C.D.E.
9. Il semble que la liste n'ait pas non plus été actualisée, suite aux modifications apportées par la loi du 19 juillet 2018.