

# Chapitre 7

## Le paiement électronique

par HERVÉ JACQUEMIN<sup>1</sup>

|                           |   |
|---------------------------|---|
| Plan                      |   |
| Section 1 <sup>re</sup> . | Introduction  |
| Section 2.                | Application de la loi sur les services de paiement aux principales formes de paiements électroniques            |
|                           | § 1 <sup>er</sup> . Panorama des principales formes de paiements électroniques                                  |
|                           | § 2. Champ d'application matériel   |
|                           | § 3. Champ d'application personnel  |
|                           | § 4. Champ d'application dans l'espace  |
| Section 3.                | Transparence et loyauté des relations contractuelles et des opérations de paiement nouées dans ce cadre         |
|                           | § 1 <sup>er</sup> . Opération de paiement isolée  |
|                           | § 2. Opérations de paiement couvertes par un contrat-cadre  |
| Section 4.                | Sécurité des opérations de paiement et partage de responsabilité en cas d'opérations de paiement non autorisées |
|                           | § 1 <sup>er</sup> . Mesures préventives   |
|                           | § 2. Mesures curatives  |
|                           | I. Partage de responsabilité entre le prestataire de service de paiement et le payeur                           |
|                           | II. Partage de responsabilité entre le prestataire de service de paiement et le commerçant                      |
| Section 5.                | Sanctions du non-respect des règles prescrites par la loi   |

### *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.
- 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.

1. Chargé d'enseignement à l'Université de Namur; Chargé de cours invité à l'UCL; avocat au barreau de Bruxelles (Liedekerke, Wolters, Waelbroeck, Kirkpatrick).

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.

STEENNOT, R., «Girale en elektronische betalingen», *NjW*, 2010, pp. 518 et s.

STEENNOT, R. et BAES, T., «Wet op betalingsdiensten: bescherming of overbescherming?», *B.F.R.*, 2010, pp. 208 et s.

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

## SECTION 1<sup>re</sup>. INTRODUCTION

- 1.1 En droit civil, le paiement peut être entendu comme «l'exécution volontaire, en nature, de l'obligation telle qu'elle est née initialement, quel[s] qu'en soit[en]t la source»<sup>1</sup> ou l'objet.

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<sup>2</sup> 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 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, mais également quand les parties sont en présence physique l'une de l'autre et que le payeur utilise 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 soumis à la loi du 10 décembre 2009 relative aux services de paiement<sup>3</sup> (ci-après, «LSP»). Celle-ci figure parmi

---

1. P. VAN OMMESLAGHE, «Le paiement : rapport introductif», in *Les aspects juridiques du paiement*, *Rev. dr. U.L.B.*, 1993, pp. 10-11, n° 4. Voir aussi H. DE PAGE, *Traité élémentaire de droit civil belge*, t. III, 3<sup>e</sup> éd., Bruxelles, Bruylant, 1967, p. 391, n° 394 («le paiement est l'exécution par le débiteur, telle qu'elle doit être, de l'obligation à laquelle il est soumis. C'est l'accomplissement de son obligation. Payer, c'est s'exécuter ; c'est effectuer la prestation à laquelle on s'est obligé, quel que soit par ailleurs l'objet de cette prestation (donner, faire, ne pas faire)»); S. STIJNS, D. VAN GERVEN et P. WÉRY, «Chronique de jurisprudence – Les obligations. Le régime général de l'obligation (1985-1995)», *J.T.*, 1999, p. 835, n° 42; H. JACQUEMIN, «Notion de paiement et conséquences sur le plan probatoire», *Obligations. Traité théorique et pratique*, Waterloo, Kluwer, 2009, V.1.1. – p. 2.

2. 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.

3. *M.B.*, 15 janv. 2010. Pour un commentaire de cette loi, voir J. FELD, *op. cit.*, pp. 63 et s.; R. STEENNOT, «Girale en elektronische betalingen», *NjW*, 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.

les textes adoptés par le législateur belge pour transposer la directive 2007/64/CE sur les services de paiement<sup>1</sup>.

Avant le 1<sup>er</sup> avril 2010, date d'entrée en vigueur de la LSP, 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<sup>2</sup> (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)<sup>3</sup>. Ces textes sont désormais abrogés<sup>4</sup>.

Ils trouvaient également 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<sup>5</sup>. Quant à l'article 83*novies* de la LPCC, il a été adopté<sup>6</sup> en vue de mettre le droit belge en conformité avec la directive 2002/65/CE sur les services financiers à distance<sup>7</sup>.

- 1.3 La directive 2007/64/CE sur les services de paiement a pour but de garantir le bon fonctionnement du marché unique de services de paiement, de manière à réaliser le marché intérieur<sup>8</sup>. Dans cette perspective, une grande importance est attachée à la confiance des utilisateurs et à la saine concurrence entre les prestataires. S'agissant précisément des paiements en ligne, réalisés en exécution d'un contrat conclu à distance, ces questions possèdent 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.

1. Directive 2007/64/CE du Parlement européen et du Conseil du 13 nov. 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.*, n° L 319 du 5 déc. 2007. Cette directive est également transposée par la loi du 21 déc. 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 janv. 2010, et la loi du 22 déc. 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 déc. 2009 relative aux services de paiement, *M.B.*, 19 janv. 2010.
2. *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 JACQUEMYS, «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.
3. *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).
4. Art. 77 de la LSP.
5. *J.O.*, n° L 208 du 2 août 1997.
6. 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.
7. Art. 8 de la directive 2002/65/CE du Parlement européen et du Conseil du 23 sept. 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, *J.O.*, n° L 265 du 9 oct. 2002.
8. Voir notamment le considérant n° 1 de la directive.

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 d'abord 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<sup>1</sup>. 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<sup>2</sup>. 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<sup>3</sup> même si, accessoirement, d'autres exigences sont également prescrites.

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 et le payeur est consacré par la loi. Celui-ci 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.

Les dispositions de la LSP s'appliquent à tous les utilisateurs de services de paiement mais, s'agissant des obligations d'information et de transparence (visées par le titre II de la loi), on observe que seuls les consommateurs<sup>4</sup> sont considérés comme étant *a priori* en position de faiblesse<sup>5</sup>. Lorsque l'utilisateur de services de paiement n'est pas un consommateur, les parties sont en effet autorisées à déroger conventionnellement aux dispositions du titre II de la loi<sup>6</sup>. Pour ce qui est de la sécurité des opérations de paiement (régie principalement par le titre III), une analyse plus nuancée s'impose dans la mesure où, même lorsque l'utilisateur n'est pas un consommateur, les dérogations conventionnelles restent interdites dans certaines hypothèses<sup>7</sup>. Aussi veillerons-nous à indiquer, le moment venu, si la règle est impérative, voire d'ordre public, ou simplement supplétive.

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

1. 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.

2. *Ibid.*, pp. 70 et s.

3. Voir le considérant n° 18 de la directive sur les services de paiement.

4. La notion de « consommateur » est définie à l'art. 2, 23°, de la LSP.

5. Voir à cet égard le considérant n° 20 de la directive sur les services de paiement : « les consommateurs et les entreprises ne se trouvent pas dans la même situation, ils ne requièrent pas un niveau de protection identique. Alors qu'il importe de garantir les droits des consommateurs au moyen de dispositions auxquelles il ne peut être dérogé par contrat, il est judicieux de laisser les entreprises et les organisations en décider autrement ».

6. Art. 27 de la LSP.

7. Art. 55 de la LSP.

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 la LSP. Pour cette raison, nous ne nous penchons pas sur les règles spécifiquement applicables à la monnaie électronique<sup>1</sup> ou sur les autres lois adoptées en vue de transposer la directive 2007/64/CE sur les services de paiement<sup>2</sup>.

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 la LSP, 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 (titre II de la loi), d'autre part, sur les droits et obligations liés à la prestation et à l'utilisation de services de paiement (titre III de la loi). 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<sup>3</sup>. 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 pénales, civiles ou administratives susceptibles d'être prononcées en cas de méconnaissance des règles précitées sont présentées (section 5).

1. Voir spéc. la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, *M.B.*, 19 avril 1993, dans laquelle a été transposée la directive 2000/46/CE du Parlement européen et du Conseil du 18 sept. 2000 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, *J.O.*, n° L 275 du 27 oct. 2000. On note que ces règles devront être corrigées à brève échéance pour transposer la directive 2009/110/CE du Parlement européen et du Conseil du 16 sept. 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE, *J.O.*, n° L 267 du 10 oct. 2009.

2. Voir les réf. citées *supra*, n° 102, note 1.

3. 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 (art. 38 et s.); les ordres de paiement (art. 40 et s.); le délai d'exécution et la date valeur (art. 44 et s.) ou la protection des données (art. 58). Sur ces questions, voir not. les références citées *supra*, n° 102, note 3.

## SECTION 2. APPLICATION DE LA LOI SUR LES SERVICES DE PAIEMENT AUX PRINCIPALES FORMES DE PAIEMENTS ÉLECTRONIQUES

- 2.1 Après avoir dressé un rapide panorama des principales formes de paiements électroniques (§ 1<sup>er</sup>), nous déterminons si celles-ci entrent dans le champ d'application de la loi, circonscrit *ratione materiae* (§ 2), *ratione personae* (§ 3) et *ratione loci* (§ 4).

Cette analyse nous permettra d'introduire les concepts-clés utilisés – et, pour la plupart, définis – dans la LSP<sup>1</sup>.

### § 1<sup>er</sup>. Panorama des principales formes de paiements électroniques

- 2.2 En première approximation, lorsque l'on recense les moyens de paiement généralement proposés aux utilisateurs, une distinction peut être faite entre les paiements par carte (de crédit, de débit ou rechargeable), les virements entre comptes et le paiement en espèces. D'autres moyens de paiement plus spécifiques pourraient également être mentionnés, à titre complémentaire, tels que les chèques ou les lettres de change.

Eu égard à l'objet de la présente étude – les paiements *électroniques* –, cette liste doit, d'une part, être réduite, d'autre part, être affinée en vue d'être complétée<sup>2</sup>.

1. Et, pour la plupart, définis à l'article 2 de la loi.

2. D'un point de vue juridique, le souci de systématisation de la doctrine a naturellement conduit celle-ci à établir des typologies permettant de classer les différentes formes de paiement. On distingue ainsi le paiement par carte (de crédit, de débit ou prépayée), le m-paiement et le paiement sur internet, auxquels on ajoute également la monnaie électronique (C. ALTER, *op. cit.*, pp. 104 et s.; J. FELD, *op. cit.*, pp. 69 et s.). Si l'aperçu qui en résulte est intéressant d'un point de vue pédagogique, il n'est pas à l'abri des redondances : les paiements par carte figurent parmi les paiements sur internet (en particulier lorsque l'on utilise sa carte de crédit) et rien n'empêche d'accéder à l'internet depuis son appareil mobile (smartphone, tablette, etc.) pour ensuite y effectuer des paiements (et il devrait alors être question de m-paiement). Les frontières entre les différentes catégories de moyens de paiement peuvent ainsi se révéler incertaines et mouvantes. Puisque l'exercice de qualification n'a de sens qu'à l'aune des catégories légales et des règles propres à chacune d'elles, nous tâcherons de présenter les moyens de paiement sous cet angle, par référence à la terminologie utilisée par la LSP. Pour une présentation des moyens de paiement et du rôle des intervenants, voir aussi Ph. BELLENS, « Aspects généraux du paiement électronique par carte bancaire », in *Aspects juridiques du paiement électronique – Juridische aspecten van de elektronische betaling*, vol. 1, Bruxelles, Kluwer, 2004, pp. 21 et s.

2.3 Les paiements en espèce peuvent en effet être écartés, de même que les chèques<sup>1</sup> ou les lettres de change au format papier. On note d'ailleurs que ces hypothèses sont clairement exclues du champ d'application matériel de la LSP<sup>2</sup> (à ce sujet, voir aussi *infra*, n° 2.12).

2.4 D'un autre côté, eu égard aux possibilités offertes par les technologies de l'information et de la communication, la distinction entre les paiements par carte et les virements entre comptes doit nécessairement être affinée, voire élargie, de manière à révéler les caractéristiques spécifiques des nouveaux moyens de paiement, généralement innovants, qui pourraient justifier l'implémentation de règles spécifiques.

A ce stade, et suivant la terminologie employée dans la loi, l'objectif est donc d'examiner les «instruments de paiement»<sup>3</sup> permettant à un «utilisateur de services de paiements»<sup>4</sup> – un «payeur»<sup>5</sup> ou un «bénéficiaire»<sup>6</sup> – d'initier un «ordre de paiement»<sup>7</sup>.

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 de commerce électronique, tandis que le paiement s'effectue en ligne. Avec les possibilités désormais offertes par les appareils mobiles (de type *smartphone* ou tablette), qui connaissent un succès croissant, il

1. S'agissant du chèque, il est indiqué, à l'occasion d'une question parlementaire posée au Sénat en 2002, que cet instrument ne représentait plus que 5 % des paiements scripturaux en 2000 (contre 8 % en 1997). Conformément aux statistiques de l'A.B.B., on constate également une diminution de 65 % des chèques interbancaires pour la période allant de janvier à octobre 2002. Ce phénomène s'explique notamment par «l'arrivée de l'euro qui a grandement facilité les paiements, mais aussi par la décision de la société Europay de supprimer la commercialisation du produit spécifique que constituait le chèque garanti. Un règlement propre à l'émission et au paiement de ces chèques en déterminait le cadre. En effet, le chèque n'est pas un instrument de paiement garanti en soi. Europay International a décidé de supprimer dans tous les pays son système de garantie à partir du 1<sup>er</sup> janvier 2002, afin entre autres de favoriser le paiement électronique. Il s'agit dès lors d'une décision commerciale justifiée également par le fait que le chèque était de moins en moins utilisé. D'autres institutions offraient également des systèmes de garanties liés au chèque, comme La Poste par exemple. Cette dernière a décidé de supprimer cette garantie à partir du 1<sup>er</sup> janvier 2003» (Question n° 2518 de M. STEVERLYNCK au ministre de la Justice du 12 nov. 2002, *Doc. parl.*, Sénat, sess. ord. 2002-2003, *Bull. Q.R.*, 2-69).

2. Voir l'art. 4, 7°, a) et b), de la LSP.

3. Au sens de la LSP, 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. 2, 10°, de la LSP). Outre les cartes de paiement, sont également visées les procédures de vérification (code PIN, digipass, etc.) permettant à l'utilisateur de donner au prestataire l'instruction d'exécuter une opération de paiement (voir le commentaire des art. du projet de loi relatif aux services de paiement, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/001, p. 15, ci-après, «commentaire des art.»).

4. 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. 2, 3°, de la LSP). A ce sujet, voir aussi *infra*, n° 2.13).

5. 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. 2, 4°, de la LSP).

6. 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. 2, 5°, de la LSP).

7. 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. 2, 7°, de la LSP).

est aussi possible de réaliser le paiement au moyen de ces dispositifs, sans nécessairement utiliser de carte de paiement. Autrement dit, sans même que le contrat se forme à distance, le paiement peut intervenir en ligne.

Nous distinguons les paiements par carte, les virements entre comptes bancaires ainsi que les nouveaux instruments de paiements, tels que les porte-monnaie virtuels ou les *m-payments* (*infra*, n<sup>os</sup> 2.5-2.7).

2.5 S'agissant des paiements par carte, on distingue traditionnellement les cartes rechargeables (la carte Proton, p. ex.), les cartes de débit (Maestro, p. ex.) et les cartes de crédit (Visa ou MasterCard, p. ex.), suivant que 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'un commerçant (on parle de paiement POS – *Point of Sale*). Dans ce cas, sous réserve des cartes rechargeables pour lesquelles cette exigence n'est généralement pas requise, l'«authentification» du payeur est garantie par l'introduction du code PIN sur le terminal du commerçant<sup>1</sup>. La combinaison de la carte et du code PIN du payeur, d'une part, le terminal du commerçant, d'autre part, constituent les «dispositifs de sécurité personnalisés»<sup>2</sup> fournis par le prestataire de service de paiement à l'utilisateur (respectivement le payeur ou le bénéficiaire du service de paiement).

On observe qu'à côté des cartes de paiement classiques, émises par les institutions bancaires traditionnelles, des cartes de paiement comptabilisant les titres-repas électroniques<sup>3</sup> sont à présent disponibles sur le marché<sup>4</sup>.

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 est généralement utilisée. Plus précisément, et sauf exception, c'est moins le support physique (bande magnétique ou puce électronique) que les données qui 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 procédure ne permet donc pas de garantir que le paiement est effectué par le véritable titulaire de la carte – l'exigence d'authentification n'est donc pas satisfaite – ce qui, on le verra, peut donner lieu à l'application d'un régime juridique différencié. Aussi constate-t-on parfois que, pour échapper à ces règles, des procédures complémentaires sont mises en place en vue d'assurer un niveau d'authentification supérieur (sur ce point, voir *infra*, n<sup>o</sup> 4.12).

1. L'«authentification» est «une procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité personnalisés» (art. 2, 11<sup>o</sup>, de la LSP).
2. 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. 2, 24<sup>o</sup>, de la LSP).
3. Art. 183 à 185 de la loi du 30 déc. 2009 portant des dispositions diverses (*M.B.*, 31 déc. 2009); A.R. du 12 oct. 2010 fixant les conditions d'agrément et la procédure d'agrément pour les éditeurs de titres-repas sous forme électronique, exécutant les articles 183 à 185 de la loi du 30 déc. 2009 portant des dispositions diverses (*M.B.*, 23 nov. 2010); art. 19bis de l'arrêté royal pris en exécution de la loi du 27 juin 1969 révisant l'arrêté-loi du 28 déc. 1944 concernant la sécurité sociale des travailleurs (*M.B.*, 5 déc. 1969), tel qu'amendé par l'A.R. du 12 oct. 2010 modifiant l'article 19bis de l'arrêté royal du 28 nov. 1969 pris en exécution de la loi du 27 juin 1969 révisant l'arrêté-loi du 28 déc. 1944 concernant la sécurité sociale des travailleurs, *M.B.*, 23 nov. 2010.
4. Voir par exemple la carte émise par Monizze ou par Sodexo. On considère cependant que cette hypothèse n'est pas couverte par la LSP.



On note qu'à l'issue d'une commande sur un site de commerce électronique, l'acheteur peut également être renvoyé directement vers son application d'*internet banking*, à travers laquelle il est invité à exécuter le paiement. Dans ce cas, le niveau d'authentification est élevé puisqu'il est soumis aux procédures établies dans ce cadre (à ce sujet, voir *infra*, n° XX à compléter).

- 2.6 Quant aux virements 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*, accessible depuis un ordinateur personnel. On note que, dans ces hypothèses, la carte de paiement peut figurer parmi les éléments du dispositif de sécurité personnalisé utilisé par le payeur pour s'authentifier. Dans le cadre des applications d'*internet banking*, par exemple, l'accès aux données ou la réalisation des opérations peut être subordonnée à l'introduction d'un code de sécurité généré par un lecteur de la carte.

Plus récemment, compte tenu des progrès technologiques des appareils mobiles (de type *smartphone* ou tablette), nombreux d'entre eux permettent d'accéder à l'internet dans de bonnes conditions et des applications de *m-banking* (ou *mobile banking*) sont désormais offertes par la plupart des institutions bancaires. Pour permettre l'authentification de l'utilisateur, le dispositif de sécurité personnalisé peut résider dans la combinaison de l'appareil mobile et d'un code PIN (sans recours à une carte de paiement, par conséquent, mais moyennant p. ex. l'envoi d'un SMS contenant un code de sécurité unique, à associer à un login et un mot de passe).

- 2.7 Le développement croissant des technologies de l'information et de la communication et l'encadrement légal de la monnaie électronique ont également permis l'apparition d'autres moyens de paiement, tels que des porte-monnaie électroniques ou virtuels. Les unités de monnaie électronique peuvent être stockées sur la carte à puce de l'utilisateur (comme pour la carte Proton, p. ex.), dans la mémoire de son ordinateur ou de son appareil mobile, voire en ligne. Dès l'instant où le porte-monnaie a été crédité en suffisance (par virement bancaire ou par carte de crédit), l'utilisateur peut effectuer des paiements: il peut ainsi acquitter le solde de ses achats sur les sites de commerce électronique qui acceptent ce moyen de paiement<sup>1</sup>. 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 de sons.

Enfin, pour certains types de paiement, généralement de faible montant – on parle de micro-paiements – 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

1. Voir par exemple les services proposés par PayPal ou Mondex.

coût du SMS mais également celui du bien ou du service acquis de cette manière (sonnerie de téléphone portable, place de parking, etc.).

- 2.8 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»<sup>1</sup>.

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<sup>2</sup> (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.

### § 2. Champ d'application matériel

- 2.9 *Ratione materiae*, la loi s'applique aux «services de paiement». L'expression est définie à l'article 2, 1<sup>o</sup>, de la LSP, qui énumère les sept catégories de services offerts en vente dans le cadre d'une activité professionnelle et susceptibles de répondre à la notion.

Sont notamment visées «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»<sup>3</sup>, y compris lorsque les fonds sont couverts par un contrat de crédit<sup>4</sup>, l'émission et/ou l'acquisition d'instruments de paiement<sup>5</sup>, voire encore les transmissions de fonds<sup>6</sup>.

- 2.10 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 de la LSP.

---

1. 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. 2, 15<sup>o</sup>, de la LSP).

2. C'est par exemple le cas de PayFair, MasterCard ou AtosWorldline.

3. Art. 2, 1<sup>o</sup>, c), de la LSP.

4. Art. 2, 1<sup>o</sup>, d), de la LSP. Le «contrat de crédit» est défini à l'art. 2, 28<sup>o</sup>, de la LSP.

5. Art. 2, 1<sup>o</sup>, e). L'«instrument de paiement» est défini à l'art. 2, 10<sup>o</sup>, de la LSP. Outre les cartes de paiement, sont également visées les procédures de vérification (code PIN, digipass, etc.) permettant à l'utilisateur de donner au prestataire l'instruction d'exécuter une opération de paiement (commentaires des art., *op. cit.*, p. 15).

6. Art. 2, 1<sup>o</sup>, f), de la LSP. La «transmission de fonds» est définie à l'art. 2, 14<sup>o</sup>, de la LSP.

2.11 S'agissant des contenus numériques (film, musique, *software*, sonnerie, etc.) qui, contre paiement, peuvent être exécutés en ligne ou doivent faire l'objet d'un téléchargement, avec un ordinateur ou un téléphone portable, une nuance s'impose<sup>1</sup>.

Peut être considérée comme un service de paiement «l'exécution d'opérations de paiement, lorsque le consentement du payeur à une opération de paiement est donné au moyen de tout dispositif de télécommunication, numérique ou informatique et que le paiement est adressé à l'opérateur du système ou du réseau de télécommunication ou informatique, agissant uniquement en qualité d'*intermédiaire* entre l'utilisateur de services de paiement et le fournisseur de biens ou services»<sup>2</sup>. Ainsi, lorsque l'exploitant – l'opérateur de téléphonie mobile auquel un SMS surtaxé est envoyé, par exemple – ajoute une valeur intrinsèque à ces contenus (une sonnerie de GSM, p. ex.) sous la forme d'un système de recherche ou les fournit directement, il n'agit pas uniquement en qualité d'*intermédiaire*<sup>3</sup>.

Par contre, l'opérateur du système ou du réseau de communication qui reçoit le paiement ne sort pas de son rôle d'*intermédiaire* lorsque le produit est fourni par un autre prestataire que lui<sup>4</sup>. Tel est, par exemple, le cas si un ticket de parking est payé à une entreprise moyennant l'envoi d'un SMS surtaxé.

Par ailleurs, si le téléphone portable est seulement utilisé en tant qu'instrument d'authentification pour réaliser un paiement de son compte de paiement (*m-banking*), aucun paiement n'est transféré à l'exploitant fournissant le service de téléphonie et l'opération ne constitue pas un service de paiement à son égard.

2.12 Il convient de noter que de nombreuses opérations de paiement sont exclues du domaine d'application de la loi conformément à l'article 4.

Il s'agit notamment des paiements en espèces<sup>5</sup>; des opérations fondées sur divers documents au format papier<sup>6</sup> (chèque, titre de service ou un chèque de

1. En effet, la directive sur les services de paiement n'a pas pour but de réglementer la fourniture de tels contenus (voir le considérant n° 6 de la directive sur les services de paiement). Sur les règles applicables à ces contenus, indépendamment des questions de paiement, voir M. DEMOULIN, *Droit des contrats à distance et du commerce électronique*, Bruxelles, Kluwer, 2010, pp. 7 et s., n°s 8 et s.; H. JACQUEMIN, «Les nouvelles règles applicables aux contrats à distance et l'incidence des technologies de l'information et de la communication sur certaines pratiques du marché», in *La protection du consommateur après les lois du 6 avril 2010*, Louvain-la-Neuve, Anthemis, 2010, pp. 63 et s.

2. Art. 2, 1<sup>o</sup>, g), de la LSP. Nous soulignons. Voir aussi l'art. 4, 12<sup>o</sup>, de la LSP, qui exclut de son champ d'application «les opérations de paiement exécutées au moyen d'un appareil de télécommunication numérique ou informatique, lorsque les biens ou les services achetés sont livrés et doivent être utilisés au moyen d'un appareil de télécommunication numérique ou informatique, à condition que l'opérateur du système de télécommunication, numérique ou informatique n'agisse pas uniquement en qualité d'*intermédiaire* entre l'utilisateur de services de paiement et le fournisseur des biens ou services» (nous soulignons). Cette disposition semble le pendant négatif de l'article 2, 1<sup>o</sup>, g), à cette différence près que l'exigence soulignée – la livraison et l'utilisation du bien ou du service au moyen d'un appareil de télécommunication numérique ou informatique – ne figure pas dans cette dernière disposition.

3. Voir le commentaire des articles, pp. 10-11.

4. *Ibid.*, p. 11 et p. 29.

5. Art. 4, 1<sup>o</sup>, de la LSP.

6. A ce sujet, il est intéressant de souligner que, dans les travaux préparatoires, le législateur se demande si «les critères retenus par l'Union européenne ne vont pas mener à un décalage injustifié sur le plan du contenu même des instruments de paiement selon qu'ils sont basés sur un support papier ou électronique» (commentaire des art., *op. cit.*, p. 27). La question mérite d'être posée et il conviendrait, pour y répondre, d'analyser les caractéristiques de ces instruments à la lumière des objectifs poursuivis par les règles adoptées.

voyage)<sup>1</sup> 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<sup>2</sup>.

De même, les services fondés sur des instruments de paiement susceptibles d'être chargés ou déchargés de monnaie électronique mais sans accès à un compte de paiement ne sont pas soumis à la LSP lorsqu'ils ne peuvent être utilisés, «pour l'acquisition de biens ou de services, que dans les locaux utilisés par l'émetteur ou dans le cadre d'un accord commercial avec l'émetteur, à l'intérieur d'un réseau limité de prestataires de services ou pour un éventail limité de biens ou de services»<sup>3</sup>.

### § 3. *Champ d'application personnel*

2.13 *Ratione personae*, les services de paiement sont fournis par un «prestataire de services de paiement»<sup>4</sup> à un «utilisateur de services de paiement».

2.14 Le prestataire de services de paiement<sup>5</sup> doit être un établissement de crédit<sup>6</sup>, un établissement de monnaie électronique<sup>7</sup>, un établissement de paiement<sup>8</sup>, La Poste, la BNB ou la BCE, voire encore les autorités fédérales, régionales ou locales belges<sup>9</sup>.

L'accès et l'exercice de cette activité sont soumis à diverses exigences ressortissant au droit financier et qui ne figurent pas, comme telles, dans la LSP<sup>10</sup>. Tout au plus, celle-ci indique-t-elle que «la personne qui fournit dans le cadre de son activité habituelle ou professionnelle des services de paiement à un utilisateur de services de paiement sans disposer d'un agrément ou d'une autorisation nécessaire reste néanmoins soumise aux dispositions impératives de la présente loi» (art. 2, 2<sup>o</sup>, *in fine*, de la LSP).

2.15 L'utilisateur de services de paiement, quant à lui, peut être un payeur ou un bénéficiaire de services de paiement.

---

1. Art. 4, 7<sup>o</sup>, de la LSP.

2. Art. 4, 10<sup>o</sup>, de la LSP.

3. Art. 4, 11<sup>o</sup>, de la LSP.

4. La notion est définie à l'art. 2, 2<sup>o</sup>, de la LSP.

5. La notion est définie à l'art. 2, 2<sup>o</sup>, de la LSP.

6. Il doit s'agir d'un établissement de crédit établi en Belgique visé à l'article 1<sup>er</sup>, alinéa 2, 1<sup>o</sup> de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit ou d'un établissement de crédit constitué conformément au droit d'un autre Etat membre de l'Espace économique européen auquel s'applique le régime de l'article 66 de la loi précitée. Sont visées les principales institutions bancaires.

7. Sont concernés les établissements de monnaie électronique établis en Belgique visés à l'article 1<sup>er</sup>, alinéa 3, 2<sup>o</sup>, de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit et les établissements de monnaie électronique constitués conformément au droit d'un autre Etat membre de l'Espace économique européen auxquels s'applique le régime de l'article 66bis de la loi précitée. La liste des établissements de monnaie électronique peut être consultée sur le site internet de la FSMA.

8. Sont concernées les personnes morales qui sont habilitées à fournir des services de paiement conformément à la loi du 21 déc. 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. Tel est le cas, par exemple, d'Atos Worldline SA.

9. Encore faut-il qu'elles soient habilitées à cet effet en vertu de la législation qui règle leur mission et/ou leurs statuts et qu'elles n'agissent pas en qualité d'autorité publique.

10. Voir les textes légaux mentionnés aux notes 6-8.

Le cas échéant, l'un ou l'autre peut être considéré comme un consommateur (au sens de l'art. 2, 23<sup>o</sup>, de la LSP) et bénéficiaire de l'application des dispositions protectrices de la loi sans dérogation conventionnelle possible.

Conformément à la directive sur les services de paiement<sup>1</sup>, les Etats membres pouvaient traiter les micro-entreprises<sup>2</sup> 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<sup>3</sup>.

#### § 4. *Champ d'application dans l'espace*

2.16 L'article 3 de la loi circonscrit son champ d'application dans l'espace, ce qui était nécessaire eu égard au caractère transfrontière des services de paiement, favorisé par l'avènement de la société de l'information.

Conformément au § 1<sup>er</sup> de cette disposition, «la présente loi est applicable aux services de paiement, dans la mesure où tant le prestataire de services de paiement du payeur que celui du bénéficiaire, ou l'unique prestataire de services de paiement intervenant dans l'opération de paiement, sont situés dans l'Union européenne<sup>4</sup> et les services de paiement sont offerts en vente en Belgique».

Des exceptions sont cependant prévues: pour l'application des articles 48 et 61, il suffit en effet que le prestataire de services de paiement du payeur ou du bénéficiaire soit situé en Belgique; pour l'application des articles 36 et 37, seul le prestataire de services de paiement doit être situé en Belgique<sup>5</sup>.

Il est également requis que les services de paiement soient fournis en euros ou dans la devise d'un Etat membre en dehors de la zone euro<sup>6</sup>.

1. Voir le considérant n<sup>o</sup> 20.

2. Telles que définies par la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro-, petites et moyennes entreprises, *J.O.*, n<sup>o</sup> L 124 du 20 mai 2003.

3. A ce propos, voir le commentaire des articles, *op. cit.*, p. 13 et p. 33.

4. Sont assimilés aux Etats membres de l'Union européenne les Etats parties à l'accord de l'Espace économique européen (art. 3, § 1<sup>er</sup>, al. 4, de la LSP).

5. Art. 3, § 1<sup>er</sup>, al. 2, de la LSP. Le cas échéant, la liste de ces dispositions peut être étendue par arrêté royal délibéré en Conseil des ministres (art. 3, § 1<sup>er</sup>, al. 3).

6. Art. 3, § 2, de la LSP. Cette disposition ajoute que «les articles 36 et 37 sont toutefois applicables aux services de paiement quelles que soient les devises utilisées».

## 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<sup>1</sup>.

On songe à la loi du 12 juin 1991 relative au crédit à la consommation ou, conformément à la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur<sup>2</sup> (ci-après, LPMC), aux règles applicables aux contrats à distance portant sur des services financiers (art. 49 et s. de la LPMC). Des obligations d'information, assorties d'exigences de forme, sont en effet imposées par ces dispositions.

Le législateur veille à leur articulation<sup>3</sup> et, conformément à l'article 24 de la LSP, les informations visées aux articles 8, 9, 13 et 14 de cette même loi remplacent (et priment donc) les informations visées à l'article 50, § 1<sup>er</sup>, de la LPMC<sup>4</sup>, à l'exception du 2<sup>o</sup>, c) à g), 3<sup>o</sup>, a), d) et e) et 4<sup>o</sup>, b).

3.3 La LSP distingue selon que l'opération de paiement est couverte par un contrat-cadre<sup>5</sup> ou, dans le cas contraire, constitue une opération de paiement isolée<sup>6</sup>.

---

1. Voir en ce sens l'art. 5, al. 2, de la LSP. Voir ég. le considérant n<sup>o</sup> 22 de la directive sur les services de paiement.

2. *M.B.*, 12 avril 2010. Depuis le 12 mai 2010, date de son entrée en vigueur, cette loi abroge et remplace la loi du 14 juill. 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur (ci-après, LPCC).

3. Suivant le considérant n<sup>o</sup> 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 ».

4. L'art. 24 de la LSP fait référence aux dispositions de la LPCC mais, conformément à l'art. 139, § 1<sup>er</sup>, de la LPMC, « les dispositions légales non contraires à la présente loi, qui font référence à des dispositions de la loi du 14 juill. 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, sont présumées faire référence aux dispositions équivalentes de la présente loi ». Aussi ne mentionnons-nous que lesdites dispositions équivalentes.

5. La notion est définie à l'art. 2, 16<sup>o</sup>, de la LSP.

6. A ce sujet, voir J. FELD, *op. cit.*, pp. 99 et s.; C. ALTER, *op. cit.*, pp. 123 et s.; R. STEENNOT, « Precontractuele informatieverplichtingen als beschermingstechniek bij de bescherming van de zwakkere partij in he financieel recht », in *La protection du consommateur en droit financier*, Cahiers AEDBF n<sup>o</sup> 25, Limal, Anthemis, 2012, pp. 107 et s.

§ 1<sup>er</sup>. Opération de paiement isolée

- 3.4 S'il s'agit d'une *opération de paiement isolée*<sup>1</sup> 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<sup>2</sup>, ainsi que, le cas échéant, les informations et les conditions visées à l'article 14.  
Après l'ordre de paiement ou la transaction de paiement, 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)<sup>3</sup>.
- 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 accessible, ce qui requiert de la part de ce dernier une démarche active pour en prendre connaissance<sup>4</sup>. Il lui est cependant permis de demander qu'elles lui soient fournies, sur support papier ou sur un autre support durable<sup>5</sup>. 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, celui-ci est autorisé à y satisfaire immédiatement après l'opération de paiement<sup>6</sup>.
- 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 spécialement adaptés soit à l'environnement traditionnel (le support papier), soit à l'environnement numérique (le support durable).  
Le support durable est ainsi défini comme «tout instrument permettant à l'utilisateur de services de paiement 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» (art. 2, 22<sup>o</sup>, de la LSP).

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»*)» (commentaire des art., *op. cit.*, p. 34).

2. Art. 9 de la LSP.

3. Art. 10 de la LSP.

4. Art. 8, § 1<sup>er</sup>, al. 1<sup>er</sup>, de la LSP. Sur la distinction entre la mise à disposition d'informations et leur fourniture, voir le considérant n° 27 de la directive ou le commentaire des articles, *op. cit.*, pp. 31-32.

5. Art. 8, § 1<sup>er</sup>, al. 2, de la LSP.

6. Art. 8, § 2, de la LSP.

Il ressort de cette définition que le support durable doit remplir trois fonctions<sup>1</sup>. On peut d'abord estimer que le support durable vise à assurer la pérennité de l'information. L'instrument doit en effet *stocker* les informations de sorte qu'elles puissent être consultées *ultérieurement*<sup>2</sup>. Le support durable doit également préserver l'intégrité de l'information dans la mesure où il doit permettre une reproduction à l'identique de celle-ci. Pour ce faire, il faut que le procédé permette d'éviter, autant que possible, les modifications. Enfin, il doit remplir une fonction de lisibilité, qui résulte de l'utilisation des verbes «consulter» ou «reporter»<sup>3</sup>.

Sont notamment visés, suivant les travaux préparatoires de la LSP, «les CD-ROM, les DVD, et les disques durs d'ordinateurs personnels sur lesquels le courrier électronique peut être stocké, ainsi que les sites internet, à condition que ceux-ci puissent être consultés ultérieurement pendant une période adaptée aux fins pour lesquelles les informations sont destinées et permettant la reproduction à l'identique des informations stockées»<sup>4</sup>. Ils ajoutent qu'«un SMS peut par exemple être assimilé à un e-mail, puisqu'un SMS peut être stocké sur le disque dur interne ou sur la carte SIM du GSM qui peut être assimilée à une disquette ou un CD-ROM».

A l'analyse, les trois fonctions correspondent aux fonctions généralement reconnues à l'écrit : la lisibilité<sup>5</sup>, la pérennité<sup>6</sup> et, même si ce point est discuté en

1. Représentant également ces trois fonctions, voir M. DEMOULIN, «La notion de 'support durable' dans les contrats à distance: une contrefaçon de l'écrit?», *R.E.D.C.*, 2000, p. 364.
2. A bon escient, il est précisé que la pérennité des informations doit être garantie pendant une période adaptée à l'objectif de ces informations. Cet élément donne la mesure du caractère durable et confirme que les fonctions ne doivent pas être remplies de manière absolue. Il existe une gradation dans la pérennité. Pour connaître l'objectif des informations et apprécier la durée minimale requise, il faut se référer aux objectifs poursuivis par les formalités.
3. Pour que l'on puisse consulter les informations ou s'y reporter, il faut nécessairement qu'elles soient lisibles. Par ailleurs, pour être en mesure de consulter les informations, il faut nécessairement que les signes soient intelligibles et accessibles, de sorte que le langage qu'ils expriment puisse être compris.
4. Commentaire des articles, *op. cit.*, p. 19.
5. Y. POULLET, «Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve», in *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Bruxelles, Bruylant, 1996, p. 55, n° 12; E. DAVIO, «Preuve et certification sur Internet», *R.D.C.*, 1997, pp. 663-664; R. STEENNOT, «Juridische problemen in het kader van de elektronische handel», *R.D.C.*, 1999, p. 671, n° 39; D. GOBERT et E. MONTERO, «L'ouverture de la preuve littérale aux écrits sous forme électronique», *J.T.*, 2001, p. 124; P. LECOCQ et B. VANBRABANT, «La preuve du contrat conclu par voie électronique», *Le commerce électronique: un nouveau mode de contracter*, Liège, Ed. du Jeune Barreau, 2001, p. 72, n° 27; B. FRANCOQ et C. FRANCOQ, «Nouveautés en matière de pratiques du commerce», in *Le point sur le droit commercial*, Liège, Formation permanente CUP, 2000, p. 174; M. STORME, «De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van een commentaar bij de nieuwe wetsbepalingen», *R.W.*, 2000-2001, p. 1509, n° 17; B. DE GROOTE, «Het bewijs in de elektronische handel – Enkele bedenkingen», *A.J.T.*, 2000-2001, p. 885, n° 16; L. GUINOTTE, «La signature électronique après les lois du 20 oct. 2000 et du 9 juill. 2001», *J.T.*, 2002, p. 555; D. MOUGENOT, *La preuve*, tiré à part du *Rép. not.*, 3<sup>e</sup> éd., Bruxelles, Larcier, 2002, p. 143, n° 83-1.
6. Cette fonction de pérennité est plus généralement qualifiée d'«exigence de durabilité» (M. FONTAINE, «La preuve des actes juridiques et les techniques nouvelles», Actes du colloque organisé les 12 et 13 mars 1987 à l'U.C.L., pp. 8-9; J. LARRIEU, «Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des écrits sous seing privé? Contribution à l'étude juridique des notions d'écriture et de signature», *Cahier Lamy droit de l'informatique*, 1988, H, pp. 12-13, n° 17; D. MOUGENOT, *La preuve*, *op. cit.*, p. 143, n° 83-1) ou de stabilité (Y. POULLET, *op. cit.*, p. 55, n° 12; E. DAVIO, *op. cit.*, pp. 663-664; R. Steennot, «Juridische problemen in het kader van de elektronische handel», *op. cit.*, p. 671, n° 39; B. FRANCOQ et C. FRANCOQ, *op. cit.*, p. 174; D. GOBERT et E. MONTERO, *op. cit.*, p. 124; P. LECOCQ et B. VANBRABANT, *op. cit.*, p. 72, n° 27; B. DE GROOTE, *op. cit.*, p. 885, n° 16; L. GUINOTTE, *op. cit.*, p. 555; D. MOUGENOT, *La preuve*, *op. cit.*, p. 141, n° 83-1).



doctrine, l'intégrité de l'information<sup>1</sup>. C'est l'une des raisons pour lesquelles l'introduction de ce nouveau concept – dont l'initiative revient au législateur européen<sup>2</sup> – ne nous convainc pas<sup>3</sup>. Il eût été plus simple, en effet, de faire référence à l'écrit.

## § 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<sup>4</sup>.

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 papier ou sur un autre support durable<sup>5</sup>, en temps utile et, en tout cas, avant qu'il ne soit lié par le contrat-cadre ou l'offre<sup>6</sup>.

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<sup>7</sup>.

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

1. Cette fonction ne figure pas expressément dans la définition fonctionnelle de l'article 16, § 2, 1<sup>er</sup> tiret, de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003 (ci-après, LSSI). Ni les travaux préparatoires, ni le texte de cette disposition, ne permettent cependant de considérer que le législateur a souhaité exclure cette fonction. On constate en effet que les travaux préparatoires ne traitent pas de cette fonction (et, *a fortiori*, ne l'écartent pas non plus): voir l'exposé des motifs du projet de loi sur certains aspects juridiques des services de la société de l'information, *Doc. parl.*, Ch. repr., sess. ord. 2002-2003, n° 2100/001, p. 44. Au contraire, dans la mesure où l'information (ou les signes) doit être accessible *pour être consultée ultérieurement*, cela suppose nécessairement qu'avec une efficacité minimale, l'intégrité de l'information ait été préservée. A défaut, la fonction de pérennité perdrait tout effet utile. De même, on peut lire dans l'exposé des motifs de la LSSI que l'écrit « doit [...] présenter une stabilité suffisante, le rendant accessible pour une consultation ultérieure » (exposé des motifs du projet de loi sur certains aspects juridiques des services de la société de l'information, *Doc. parl.*, Ch. repr., sess. ord. 2002-2003 (léq. 50), n° 2100/001, p. 44.). A nos yeux, il faut comprendre l'exigence de stabilité comme visant non seulement la pérennité mais également l'intégrité. Sur la fonction d'intégrité et les controverses à son égard, voir H. JACQUEMIN, *Le formalisme contractuel...*, *op. cit.*, n<sup>os</sup> 79-81, et les réf. citées.
2. Utilisant les concepts de support durable et de support papier, voir l'art. 5, § 1<sup>er</sup>, de la directive 2002/65/CE du Parlement européen et du Conseil du 23 sept. 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, *J.O.*, n° L 271 du 9 oct. 2002, pp. 16-24 et l'art. 13, § 1<sup>er</sup>, a), de la directive 2002/92/CE du Parlement européen et du Conseil du 9 déc. 2002 sur l'intermédiation en assurance, *J.O.*, n° L 9 du 15 janv. 2003, pp. 3-10.
3. Voir H. JACQUEMIN, *Le formalisme contractuel...*, *op. cit.*, n° 300. Sur la notion, voir aussi M. DEMOULIN, « La notion de 'support durable' dans les contrats à distance: une contrefaçon de l'écrit? », *R.E.D.C.*, 2000, pp. 361 et s.
4. Voir le considérant n° 24 de la directive sur les services de paiement.
5. Sur cette notion, voir *supra*, n° 3.7.
6. Art. 13, § 1<sup>er</sup>, de la LSP. Conformément à l'art. 13, § 3, de la LSP, le prestataire peut également « s'acquitter des obligations découlant du § 1<sup>er</sup> en fournissant une copie du projet de contrat-cadre comportant les informations et les conditions définies à l'article 14 ».
7. Art. 13, § 2, de la LSP.

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 communication, les mesures de protection et les mesures correctives, la modification et la résiliation du contrat-cadre<sup>1</sup> ainsi que les recours<sup>2</sup>.

- 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<sup>3</sup>.

Dans l'autre hypothèse, les informations doivent être fournies sans tarder par le prestataire du payeur, après la réception de l'ordre de paiement<sup>4</sup>, et par celui du bénéficiaire, après l'exécution de l'opération de paiement<sup>5</sup>.

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 les informations [...] sont fournies ou mises à disposition périodiquement, au moins une fois par mois, 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»<sup>6</sup>. A cet égard, on peut s'étonner que, par souci de cohérence, le législateur n'ait pas imposé la fourniture ou la mise à disposition des informations sur un support papier ou sur un autre 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, la LSP 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 n'excédant pas 30 euros unitairement ou, soit ont une limite de dépenses de 150 euros, soit stockent des fonds dont le montant n'excède à aucun moment 150 euros» (art. 21 de la LSP). La carte Proton est visée, par exemple.

- 3.12 Des exigences figurant dans le titre III de la loi, traitant des droits et obligations liés à la prestation et à l'utilisation de services de paiement, ont 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<sup>7</sup>. Le délai de

---

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. 16-17 de la LSP.

2. Art. 14 de la LSP.

3. Art. 18 de la LSP.

4. Art. 19 de la LSP.

5. Art. 20 de la LSP.

6. Art. 19, § 2, et 20, § 2, de la LSP.

7. Art. 33 de la LSP.

conservation est de cinq 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»<sup>1</sup> (art. 32, 2<sup>o</sup>, de la LSP).

## 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.

Cette exigence se vérifie avec une acuité renforcée dans l'hypothèse des paiements en ligne. Les risques de fraude et le manque de confiance corrélatif des utilisateurs de services de paiement qui effectuent des transactions à travers les réseaux peuvent en effet constituer un obstacle au développement du commerce électronique. Il s'agit d'ailleurs d'un argument avancé pour expliquer les réticences des internautes au moment de conclure des contrats par ce biais, spécialement lorsqu'ils effectuent un paiement par carte de crédit<sup>2</sup>. Ce moyen de paiement est très répandu sur le net en raison, notamment, de sa simplicité d'utilisation. Corrélativement, il faut cependant admettre que le risque de fraude est accru: les données peuvent être interceptées lors de la transmission; le commerçant peut utiliser frauduleusement les données; enfin, sa base de données (dans laquelle il conserverait les informations bancaires) peut être piratée.

Pourtant, 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), le cadre normatif comporte des mesures préventives et curatives. L'analyse qui suit portera principalement sur le paiement par carte de crédit mais, *mutatis mutandis*, les règles peuvent également s'appliquer aux autres moyens de paiements utilisés sur le net.

1. Comp. aux art. 94, 6<sup>o</sup>, et 98 de la LPMC.

2. Plusieurs décisions de jurisprudence traitent du partage de responsabilité à opérer en cas d'utilisation non autorisée (ou prétendue telle) d'une carte de crédit: voir Bruxelles, 15 mars 2007, *D.C.C.R.*, 2007, p. 45, note J. DEWEZ; Bruxelles, 13 sept. 2005, *D.C.C.R.*, 2006, p. 86; Comm. Bruxelles, 27 nov. 2006, *Dr. Banc. Fin.*, 2006, p. 137. Voir aussi les réf. citées *infra*, n<sup>o</sup> 4.10 et 4.16.

### § 1<sup>er</sup>. 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 dispositifs de sécurité personnalisés 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 31»<sup>1</sup> (art. 32, 1<sup>o</sup>).

Diverses informations que le prestataire doit fournir à l'utilisateur conformément à l'article 14, 5<sup>o</sup>, de la LSP, avant qu'il ne soit lié par un contrat-cadre ou une offre, portent sur ces mesures de protection<sup>2</sup>.

- 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 lui impose ainsi d'«utiliser l'instrument de paiement conformément aux conditions régissant l'émission et l'utilisation de cet instrument de paiement» (art. 31, § 1<sup>er</sup>, 1<sup>o</sup>, de la LSP).

Plus précisément, il doit prendre «toutes les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses dispositifs de sécurité personnalisés»<sup>3</sup> (art. 31, § 2, de la LSP).

### § 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 par l'article 28 de la LSP 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, l'article 31, § 1<sup>er</sup>, 2<sup>o</sup>, de la LSP lui impose d'informer sans délai son prestataire de services de paiement ou l'entité indiquée par celui-ci<sup>4</sup>.

---

1. En lien avec cette exigence, il appartient au prestataire d'assumer «le risque lié à l'envoi au payeur d'un instrument de paiement ou de tout moyen qui en permet l'utilisation, en particulier tout dispositif de sécurité personnalisé de celui-ci» (art. 32, 5<sup>o</sup>, de la LSP).

2. Il s'agit en effet de «la description des risques et des mesures de prudence que l'utilisateur de services de paiement prend pour préserver la sécurité d'un instrument de paiement de même que les modalités de notification au prestataire de service de paiement [...]» (art. 14, 5<sup>o</sup>, a), de la LSP).

3. Les travaux préparatoires précisent à juste titre que «cela ne peut en aucun cas empêcher l'utilisateur de réaliser certaines transactions pour lesquelles il est habituel et même nécessaire de donner le numéro apparent de sa carte de paiement, lequel ne peut être considéré comme un dispositif de sécurité personnalisé (opérations à distance comme p. ex. par internet ou par téléphone)» (commentaire des art., *op. cit.*, pp. 61-62).

4. Sur la procédure de notification, voir aussi les art. 34-35 de la LSP.

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.)<sup>1</sup>.

- 4.5 Un régime de responsabilité spécifique est mis en place par la LSP, 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. Celle-ci concerne spécifiquement la relation entre le payeur et le prestataire de service de paiement (I). Nous analyserons également les conséquences d'une opération de paiement non autorisée dans le chef du commerçant (II).

## I. PARTAGE DE RESPONSABILITÉ ENTRE LE PRESTATAIRE DE SERVICE DE PAIEMENT ET LE PAYEUR

- 4.6 L'article 36 de la LSP 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, complété, le cas échéant, d'intérêts calculés sur la somme. D'autres conséquences financières éventuelles doivent aussi être couvertes<sup>2</sup>.

- 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 ces règles (art. 37-39 de la LSP) sont supplétives lorsque l'utilisateur n'est pas un consommateur<sup>3</sup>.

- 4.8 *Après la notification*, lorsque l'instrument de paiement a été perdu, volé ou détourné, les conséquences financières sont supportées par le prestataire<sup>4</sup>. Au nombre des exigences imposées au prestataire par l'article 32 de la LSP figure en effet l'obligation d'empêcher «toute utilisation de l'instrument de paiement après une notification effectuée en application de l'article 31, § 1<sup>er</sup>, 2<sup>o</sup>» (4<sup>o</sup>).

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

1. Art. 32, 3<sup>o</sup>, de la LSP. La loi ajoute 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).

2. Art. 36, al. 2, de la LSP. Sont notamment visés les frais supportés par le titulaire pour la détermination du dommage indemnissable.

3. Art. 55 de la LSP. Suivant le considérant n<sup>o</sup> 35 de la directive sur les services de paiement, «des dispositions différentes peuvent s'appliquer à des utilisateurs de services de paiement qui ne sont pas des consommateurs, de tels utilisateurs étant généralement plus à même d'apprécier le risque de fraude et de prendre des mesures compensatoires».

4. Art. 37, § 2, de la LSP.

- 4.9 *Avant la notification*, les règles introduites par la loi en vue de partager la responsabilité en cas d'opérations de paiement non autorisées distinguent selon que les pertes subies par le payeur résultent ou non «soit d'un agissement frauduleux de sa part, soit du fait qu'il n'a pas satisfait, intentionnellement ou à la suite d'une négligence grave, à une ou plusieurs des obligations qui lui incombent en vertu de l'article 31».
- 4.10 Si le prestataire établit que tel est le cas<sup>1</sup>, le payeur devra supporter toutes les pertes occasionnées par les opérations de paiement non autorisées<sup>2</sup>. La loi donne des exemples de circonstances pouvant être considérées comme des négligences graves<sup>3</sup>. Sont ainsi mentionnés le fait, pour le payeur, de noter ses dispositifs de sécurité personnalisés, 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» (art. 37, § 3, al. 2, de la LSP). 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<sup>4</sup>.
- Un exemple récent est également fourni par un arrêt rendu par la cour d'appel de Bruxelles le 23 juin 2011<sup>5</sup>. 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».
- 4.11 En l'absence de fraude, d'intention ou de négligence grave, la responsabilité du payeur est plafonnée, avant la notification, à 150 EUR pour «les pertes liées à toute opération de paiement non autorisée consécutive à l'utilisation d'un instrument de paiement perdu ou volé ou, si le payeur n'est pas parvenu à préserver la sécurité de ses dispositifs de sécurité personnalisés, au détourne-

1. C'est en effet sur lui que repose la charge de prouver la fraude, l'intention ou la négligence grave (art. 37, § 3, al. 1<sup>er</sup>, de la LSP).

2. Art. 37, § 1<sup>er</sup>, al. 2, de la LSP.

3. Pour des applications jurisprudentielles, sous l'empire de la LTEF, voir not. Bruxelles, 4 oct. 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.

4. Voir l'art. 37, § 3, *in fine*: «pour l'appréciation de la négligence, le juge tient compte de l'ensemble des circonstances de fait. La production par le fournisseur de services de paiement des enregistrements visés à l'article 35 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».

5. *D.C.C.R.*, 2012, note R. STEENNOT, à paraître. On note que cet arrêt est rendu sur la base de la LTEF.

ment d'un instrument de paiement» (art. 37, § 1<sup>er</sup>, al. 1<sup>er</sup>, de la LSP). L'objectif est d'inciter l'utilisateur à notifier la perte ou le vol dans les meilleurs délais.

Sauf en cas de fraude ou de manquement intentionnel, par le payeur, aux obligations prescrites par l'article 31, une double exception est introduite par la loi en vue de dispenser celui-ci de toute perte occasionnée par une opération de paiement non autorisée<sup>1</sup>. *A contrario*, la double exception s'applique également dans l'hypothèse d'une négligence grave.

4.12 Tel est *d'abord* le cas «si l'instrument de paiement a été utilisé sans présentation physique et sans identification électronique» (art. 37, § 1<sup>er</sup>, al. 3, 1<sup>o</sup>, de la LSP). Cette exception pourra généralement être invoquée en matière de contrats à distance puisque, par définition, la conclusion de ceux-ci doit se faire sans la présence physique et simultanée des parties<sup>2</sup> (par téléphone ou à travers un site internet, p. ex.). L'objectif du législateur est clair: encourager les prestataires de services de paiement à mettre en place des dispositifs suffisamment sécurisés lorsque les parties ne sont pas en présence physique l'une de l'autre lors du paiement<sup>3</sup> (hypothèses dans lesquelles les risques de fraudes sont plus importants). Il est en effet de leur intérêt que leur responsabilité demeure exclue pour les sommes couvertes par la franchise de 150 EUR ou en cas de négligence grave.

Reste à comprendre la notion «d'identification électronique». Les travaux préparatoires de la loi nous enseignent que «l'identification électronique vise le cas où l'instrument est par exemple identifié au moyen d'un lecteur de carte ('smart card reader'). [...] La simple utilisation d'un 'code secret' ou d'une preuve similaire n'est pas suffisante en soi pour engager la responsabilité du payeur-titulaire de la carte»<sup>4</sup>. Avant l'entrée en vigueur de la loi du 10 décembre 2009, cette question était régie par l'article 8 de la LTEF<sup>5</sup>, qui prévoyait une règle similaire. Les travaux préparatoires relatifs à cette disposition évoquaient le recours à un mécanisme de signature électronique<sup>6</sup>. La matière des paiements électroniques est en effet l'une des hypothèses dans lesquelles on peut exploiter utilement les fonctions que les procédés de signature électronique permettent

1. On en revient donc à l'application du principe énoncé à l'article 36 de la LSP.

2. Voir, dans la LPMC, les définitions du «contrat à distance» (art. 2, 21<sup>o</sup>) et de la «technique de communication à distance» (art. 2, 22<sup>o</sup>).

3. A ce sujet, voir les travaux préparatoires de la loi: «si le prestataire de services de paiement fait le choix économique de ne pas utiliser de système de sécurité optimal, il ne peut en reporter les conséquences sur l'utilisateur» (commentaire des art., *op. cit.*, p. 71). A ce propos, on note qu'en pratique, il devient de plus fréquent, en cas de paiement par carte de crédit, qu'il soit demandé d'insérer celle-ci dans un lecteur de carte de manière à générer, après introduction du code PIN de la carte, un code unique de validation. Dans ce cas de figure, on peut considérer que l'exigence de l'identification électronique est respectée.

4. Commentaire des articles, *op. cit.*, p. 71. Il est intéressant de noter que la disposition correspondante du projet de loi était complétée comme suit: «le simple usage d'un code confidentiel ou d'une autre preuve similaire de l'identité n'est pas suffisant pour engager la responsabilité du payeur» (*Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n<sup>o</sup> 2179/001, p. 131). Cette formule a toutefois disparu dans les versions ultérieures, sans véritable explication. Il ne semble toutefois pas que la volonté ait été d'aller à l'encontre de cette considération, à la lumière du commentaire de l'article tiré des travaux préparatoires.

5. Sur cette disposition, voir not. M. DEMOULIN, «Le paiement électronique», in *Obligations – Traités théorique et pratique*, Bruxelles, Kluwer, 2007, V.1.7, p. 26; 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, p. 584, n<sup>o</sup> 40; O. GOFFARD, «'Status quaestionis': risques et responsabilités en cas de transfert électronique de fonds», *R.D.C.*, 2005, pp. 5 et s.

6. *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n<sup>o</sup> 1389/001, p. 36. Il n'est plus fait expressément référence à un procédé de signature électronique dans les travaux préparatoires de la LSP mais celui-ci constitue assurément l'un des moyens auxquels les prestataires peuvent recourir pour atteindre les fonctions attendues.

d'atteindre et qui, par comparaison aux fonctions de la signature manuscrite<sup>1</sup>, tantôt sont différentes, tantôt peuvent être remplies avec une efficacité renforcée<sup>2</sup>. En Belgique, la reconnaissance et les effets juridiques de la signature électronique sont visés, de manière générale, par l'article 1322, alinéa 2, du Code civil<sup>3</sup> et par la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification<sup>4</sup> (ci-après, la loi du 9 juillet 2001)<sup>5</sup>. Suivant l'article 4, § 4, de la loi du 9 juillet 2001, est assimilée de plein droit à une signature manuscrite la «signature électronique avancée», «réalisée sur la base d'un certificat qualifié» et «conçue au moyen d'un dispositif sécurisé de création de signature électronique». Pour la désigner, la doctrine<sup>6</sup>, suivie par le législateur<sup>7</sup>, utilise l'expression de «signature électronique qualifiée». A l'analyse, il apparaît que, suivant les exigences légales, le procédé doit non seulement garantir l'authenticité de l'origine mais également l'identification du signataire<sup>8</sup>, et ce, avec une efficacité accrue<sup>9</sup>. L'article 1322, alinéa 2, du Code civil ne pose pas de telles exigences. Les travaux préparatoires de la loi et les commentaires doctrinaux sont en effet unanimes pour dire que la notion d'imputabilité, à laquelle cette disposition fait référence, couvre les fonctions traditionnellement reconnues à la signature manuscrite: l'identification du signataire – à comprendre comme l'authentification de son identité – et son adhésion au contenu de l'acte<sup>10</sup>. C'est principa-

1. On admet généralement que la signature manuscrite poursuit deux fonctions: identifier le signataire (à comprendre comme authentifier son identité) et marquer son adhésion au contenu de l'acte (voir H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, pp. 99 et s., n<sup>os</sup> 59 et s., et les références citées).
2. A ce propos, voir H. JACQUEMIN, «La signature électronique en droit belge: questions choisies», in *An Information Society for All: A Legal Challenge*, Actes du colloque organisé à l'occasion des 30 ans du CRID, 2012, à paraître.
3. Cet alinéa a été ajouté par l'art. 2 de la loi du 20 oct. 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 déc. 2000.
4. *M.B.*, 29 sept. 2001.
5. Ces textes transposent la directive 1999/93/CE du Parlement européen et du Conseil, du 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, *J.O.*, n<sup>o</sup> L 13 du 19 janv. 2000. Pour une analyse récente de ceux-ci, voir E. MONTERO, «La preuve des actes juridiques privés électroniques en droit belge», *R.L.D.I.*, 2009, pp. 19-26; P. VAN EECKE, «De elektronische handtekening in het recht», *R.D.C.*, 2009, pp. 323-354.
6. E. MONTERO, «Définition et effets juridiques de la signature électronique en droit belge: appréciation critique», *DAOR*, 2002/61-62, p. 14, n<sup>o</sup> 6, note 10.
7. Voir l'art. 2, 3<sup>o</sup>, de la loi du 10 juill. 2006 relative à la procédure par voie électronique, *M.B.*, 7 sept. 2006 ou l'art. 1<sup>er</sup>, 5<sup>o</sup> tiret, de l'arrêté du gouvernement wallon du 12 juill. 2007 pris en application du décret du 14 déc. 2006 relatif à la reconnaissance juridique des formulaires électroniques de la Région wallonne, *M.B.*, 20 août 2007.
8. La signature électronique avancée est en effet définie à l'art. 2, 2<sup>o</sup>, de la loi du 9 juill. 2001, comme «une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de *méthode d'authentification* et satisfaisant aux exigences suivantes:  
être liée uniquement au signataire;  
permettre l'identification du signataire;  
être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;  
être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée» (nous soulignons).
9. Voir les exigences posées par le certificat qualifié (art. 2, 4<sup>o</sup>, de la loi du 9 juill. 2001) et le dispositif sécurisé de création de signature électronique (art. 2, 7<sup>o</sup>, de la loi du 9 juill. 2001).
10. Voir le rapport fait au nom de la Commission de la Justice par B. SOMERS, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000 (lég. 50), n<sup>o</sup> 38/008, p. 30. En doctrine, voir E. MONTERO, «Définition et effets juridiques de la signature électronique en droit belge: appréciation critique», *DAOR*, 2002/61-62, p. 16; P. LECOCQ et B. VANBRABANT, «La preuve du contrat conclu par voie électronique», in *Le commerce électronique: un nouveau mode de contracter*, Liège, Ed. du Jeune Barreau, 2001, p. 114; L. GUINOTTE, «La signature électronique après les lois du 20 oct. 2000 et du 9 juill. 2001», *J.T.*, 2002, p. 558.



lement la signature digitale, basée sur la cryptographie asymétrique<sup>1</sup>, qui répond aux conditions de l'article 4, § 4, de la du 9 juillet 2001 ou de l'article 1322, alinéa 2, du Code civil<sup>2</sup>.

En pratique, les banques proposent des lecteurs de carte ou des *Digipass* qui génèrent un code chiffré nécessaire pour accéder au service en ligne et effectuer des transactions. *A priori*, ces mécanismes permettent à tout le moins d'authentifier l'identité du titulaire et, par conséquent, remplissent la condition relative à l'identification électronique, au sens de la loi. En principe, ces mécanismes devraient en tout cas remplir les exigences prescrites par l'article 1322, alinéa 2, du Code civil.

Il est intéressant de noter que les conditions contractuelles établies par les institutions bancaires (et auxquelles le client consent en ouvrant un compte et en utilisant les services qui y sont associés) contiennent généralement des dispositions relatives à la preuve de certaines opérations, notamment les paiements<sup>3</sup>. Dans le Règlement général des opérations d'une banque, on peut lire que «le Client accepte que les données informatiques/électroniques enregistrées par la Banque font preuve des opérations ainsi que des ordres, avis ou information échangés par voie électronique, quel que soit le support sur lequel ces données sont enregistrées. Pour ces opérations électroniques, la signature électronique du Client remplace la signature manuscrite». Il est ensuite précisé les procédés qui peuvent être considérés comme une signature électronique. Il s'agit notamment de l'introduction d'un code pin, d'un code secret, d'un code d'accès, voire de la combinaison de l'introduction d'une carte bancaire ou de crédit avec un code personnel. S'agissant de la signature, il est permis de se demander si un juge aurait pu décider que ces procédés répondent aux conditions fixées par l'article 1322, alinéa 2, du Code civil. *A priori*, sous

1. Dans ce mécanisme, il y a deux clés: une clé privée, connue uniquement de son titulaire et une clé publique, connue de tous. Les deux clés sont liées et la clé publique est une fonction irréversible de la clé privée. Cette technique permet de garantir l'identification du signataire, la confidentialité et l'intégrité du message. L'internet est un réseau ouvert, dans lequel les intervenants ne se connaissent généralement pas. Pour que chacun puisse avoir la certitude que telle clé publique appartient bien à la personne qui s'en prétend titulaire, l'intervention d'un tiers de confiance était nécessaire. C'est la raison pour laquelle l'activité des prestataires de service de certification est désormais visée par la loi. Sur ce mécanisme, voir D. MOUGENOT, *La preuve*, 3<sup>e</sup> éd., tiré à part du *Rép. not.*, Bruxelles, Larcier, 2002, p. 174, n° 121-2; L. GUINOTTE, *op. cit.*, pp. 555-556; P. LECOCQ et B. VANBRABANT, *op. cit.*, pp. 77-84; M. STORME, «De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetbepalingen», *R.W.*, 2000-2001, pp. 1515-1516.
2. Pour une description des différentes formes de signature électronique (combinaison d'une carte et d'un code secret, signatures biométriques, signatures digitales, etc.), voir D. GOBERT et E. MONTERO, «La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle», *DAOR*, 2000, pp. 19-21; D. MOUGENOT, *La preuve*, *op. cit.*, pp. 169 et s., n° 121.
3. De manière générale, sur les questions de preuve posées par ces opérations, voir J.-P. BUYLE, «La preuve et le coût du paiement», *Les aspects juridiques du paiement*, *Rev. dr. U.L.B.*, 1993, pp. 172 et s.; D. MOUGENOT, *La preuve*, *op. cit.*, pp. 297 et s., n°s 253 et s.; H. JACQUEMIN, «Questions de preuve posées par le paiement», in *Le paiement*, Louvain-la-Neuve, Anthemis, 2009, pp. 194-196, n° 25.

réserve d'un examen approfondi du cas d'espèce, la réponse devrait être positive, spécialement pour la combinaison de la carte et du code personnel<sup>1</sup>.

- 4.13 Dans la *seconde hypothèse* établie à l'article 37, § 1<sup>er</sup>, alinéa 3, le payeur ne supporte aucune perte si «l'instrument de paiement a été copié par un tiers ou a été indûment utilisé pour autant que le payeur était, au moment de l'opération contestée, en possession de l'instrument de paiement». Sont ainsi visés les cas de contrefaçons ou de *hacking*.
- 4.14 On note enfin qu'il existe des exceptions à certaines des règles précitées lorsqu'il s'agit d'instruments de paiement de faible montant<sup>2</sup>.

## II. PARTAGE DE RESPONSABILITÉ ENTRE LE PRESTATAIRE DE SERVICE DE PAIEMENT ET LE COMMERÇANT

- 4.15 Dans l'hypothèse où 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 commerçant, devra finalement supporter cette perte (partant du principe que l'auteur de la fraude n'a pas été identifié).
- 4.16 Un arrêt rendu par la Cour d'appel de Bruxelles le 19 juin 2008 permet d'apporter des éléments de réponse<sup>3</sup>. 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

1. Dans le règlement d'une autre banque, on lit qu'«afin de signer de manière électronique des opérations, en ce compris des contrats, le titulaire de la carte utilise ses moyens de signature, à savoir la carte mise à sa disposition par [la banque] et son code secret de 4 chiffres. [...] Pour toutes ses opérations, le titulaire du compte accepte que la signature électronique du titulaire de la carte – validée par les systèmes informatiques de [la banque] et reconnue comme émanant du titulaire de la carte – remplit les conditions d'identification du titulaire de la carte et d'intégrité du contenu attachées à une signature au sens de l'article 1322, alinéa 2, du Code civil et que l'opération revêtue de cette signature électronique a la même valeur probante qu'une opération écrite signée de manière manuscrite par le titulaire de la carte et engage le titulaire du compte comme tel». On note que la fonction d'adhésion du contenu de l'acte, pourtant dérogée de l'exigence d'imputabilité, n'est pas reprise.

2. Art. 57 de la LSP.

3. Bruxelles, 19 juin 2008, *DAOR*, 2009/90, p. 167, note A. VANDOOALAE GHE, *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.

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».

- 4.17 Le partage de responsabilité entre le prestataire de service de paiement et le commerçant (bénéficiaire du service de paiement) en cas d'opération de paiement non autorisée n'étant pas réglé par la LSP, il convient de s'en remettre aux dispositions contractuelles prévues par les parties.

En général, le prestataire aura pris le soin de faire peser le risque de ces opérations sur le commerçant. A moins que ce dernier dispose d'un pouvoir de négociation suffisant pour imposer conventionnellement un autre partage de responsabilité, il devra généralement supporter les pertes qui en résultent.

Aussi faut-il lui conseiller, en tout cas pour les opérations dépassant un certain montant, de convenir avec son prestataire de services de paiement de la mise en place de dispositifs sécurisés permettant de garantir l'authentification du payeur avec un niveau élevé de certitude, voire de procéder lui-même à des vérifications de l'identité du payeur ou de refuser le paiement par carte de crédit, en exigeant un virement international.

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

- 5.1 En cas d'inobservation des obligations prescrites par la loi, outre une action en cessation<sup>1</sup>, des sanctions civiles, pénales ou administratives sont susceptibles d'être mises en œuvre.
- 5.2 Les *sanctions pénales*<sup>2</sup> consistent principalement en des peines d'amendes, qui oscillent entre 250 et 100.000 EUR<sup>3</sup>. Elles peuvent notamment être prononcées si des exigences d'information ont été méconnues ou si le prestataire a manqué aux obligations qui lui incombent (en matière de sécurité des opérations de paiement, p. ex.).

Le cas échéant, des peines d'emprisonnement sont également envisageables<sup>4</sup>.

Ces infractions<sup>5</sup> sont recherchées et constatées par les officiers de police judiciaire ou par les agents commissionnés par le ministre ayant les Affaires

1. Art. 59 de la LSP.

2. On retrouve des mesures similaires dans la plupart des législations consuméristes, et notamment la LPMC. Pour un examen plus détaillé du régime prévu dans ce cadre, voir L. KERZMANN et H. JACQUEMIN, «Le point sur les sanctions pénales dans la loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur», *D.C.C.R.*, 2011/92, pp. 5-30.

3. Art. 64 de la LSP. Ces montants doivent être augmentés des décimes additionnels (et multipliés par 6).

4. Art. 65 de la LSP.

5. On note qu'aux termes de l'art. 73, § 1<sup>er</sup>, ces agents sont également compétents pour «rechercher et constater les actes qui, sans être punissables, peuvent faire l'objet d'une action en cessation formée à l'initiative du ministre qui a les Affaires économiques dans ses attributions».

économiques dans ses attributions, dont les procès-verbaux font foi jusqu'à preuve du contraire<sup>1</sup>.

Ceux-ci peuvent adresser un avertissement au contrevenant pour le mettre en demeure de cesser l'infraction<sup>2</sup>. Ils peuvent également proposer un règlement transactionnel permettant au contrevenant, moyennant le paiement d'une somme d'argent, d'éteindre l'action publique<sup>3</sup>. S'il n'a pas été donné suite à l'avertissement ou si la proposition de transaction n'a pas été acceptée, le procès-verbal est transmis au procureur du Roi<sup>4</sup>.

5.3 Au niveau *administratif*, l'article 71 de la LSP impose à ces agents commissionnés de communiquer la violation, par un prestataire, des dispositions de la loi, à l'autorité de contrôle qui a accordé l'autorisation d'offrir des services de paiement. Celle-ci examinera «si et dans quelle mesure des sanctions de droit administratif ou d'autres mesures particulières doivent être prises à l'encontre du prestataire de services de paiement et ce, conformément au statut spécifique de celui-ci».

5.4 La méconnaissance des dispositions de la loi peut également être *sanctionnée civilement*. Les mesures sont de trois ordres.

5.5 *Primo*, diverses clauses sont interdites et nulles de plein droit. Il s'agit des dispositions contractuelles par lesquelles «l'utilisateur de services de paiement renonce, même partiellement, au bénéfice des droits prévus par la [...] loi»<sup>5</sup> (art. 61, 1<sup>o</sup>, de la LSP).

Il en va de même des clauses limitatives ou exonératoires de responsabilité, au profit du prestataire de services de paiement<sup>6</sup>.

Enfin, lorsque la charge de la preuve incombe au prestataire conformément à la loi, des dérogations conventionnelles ne peuvent avoir pour effet de renverser celle-ci au préjudice de l'utilisateur de services de paiement<sup>7</sup>.

5.6 *Secundo*, si le prestataire n'a pas fourni à l'utilisateur une «description des risques et des mesures de prudence que l'utilisateur de services de paiement prend pour préserver la sécurité d'un instrument de paiement de même que les modalités de notification au prestataire de services de paiement au regard de l'article 31, § 1<sup>er</sup>, 2<sup>o</sup>» (art. 14, 5<sup>o</sup>, a), de la LSP), ou s'il n'a pas mis en place des dispositifs de sécurité personnalisés (art. 32, 1<sup>o</sup>, de la LSP) ou des moyens appropriés pour notifier les opérations de paiement non autorisées (art. 32, 3<sup>o</sup>, de la LSP), le régime de responsabilité établi à l'article 62 de la LSP s'applique.

Conformément à celui-ci, il est responsable, vis-à-vis de l'utilisateur, des conséquences résultant de l'usage d'un instrument de paiement par un tiers non

1. Art. 72, § 2, de la LSP. Voir aussi l'A.M. du 19 avril 2010 désignant les agents chargés de rechercher et de constater les infractions à la loi du 10 déc. 2009 relative aux services de paiement, *M.B.*, 27 avril 2010. Les pouvoirs dont ils disposent dans l'exercice de leurs fonctions sont énumérés à l'article 72, § 2, de la LSP.

2. Art. 60 de la LSP.

3. Art. 74 de la LSP.

4. Art. 72, § 5, de la LSP.

5. Même si la précision eût été utile, il ne paraît pas discutable que la règle s'applique sous réserve des dispositions auxquelles il est permis de déroger contractuellement.

6. Art. 61, 2<sup>o</sup>, de la LSP.

7. Art. 61, 3<sup>o</sup>, de la LSP.

autorisé. La règle ne s'applique toutefois pas s'il démontre une fraude dans le chef du payeur.

- 5.7 *Tertio*, la méconnaissance de diverses obligations énumérées à l'article 63 de la LSP permet à l'utilisateur de résilier le contrat-cadre sans délai et sans frais ni pénalité<sup>1</sup>.

Il doit le faire par lettre recommandée mise (*sic*) à la poste, 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<sup>2</sup> ou le non-respect, par le prestataire, de son obligation de remboursement immédiat en cas d'opération de paiement non autorisée<sup>3</sup>.

Plusieurs critiques peuvent être adressées à l'encontre de cette mesure<sup>4</sup>.

Pour éviter que la sanction puisse être invoquée plusieurs semaines, voire plusieurs mois après la violation des dispositions concernées, nous aurions préféré que la disposition indique expressément que la résiliation peut être demandée *dans un délai raisonnable* à partir du moment où l'utilisateur a connaissance ou aurait dû avoir connaissance du non-respect de ces obligations.

En outre, si la sanction peut se justifier en l'absence de certaines mentions – concernant par exemple les limites de dépenses pour les opérations de paiement exécutées au travers de l'instrument de paiement<sup>5</sup> – la méconnaissance par le prestataire de ses obligations pourrait être jugée plus accessoire par l'utilisateur, de sorte qu'il souhaite poursuivre les engagements résultant du rapport contractuel. On songe, par exemple, à l'imputation de certains frais, dans les cas visés aux articles 41, § 1<sup>er</sup>, 42, alinéa 5, ou 49, § 2, sans qu'ils aient été convenus dans le contrat-cadre ou lorsqu'ils se révèlent excessifs par rapport aux coûts réels (en violation de l'art. 56, § 1<sup>er</sup>, de la LSP). Si le contrat est maintenu, la réparation du préjudice subi pourrait consister à dispenser l'utilisateur de payer ces frais supplémentaires. Pour autoriser cette sanction (qui pourrait d'ailleurs être mise en œuvre sans l'intervention des cours et tribunaux), une modification législative est souhaitable. A notre estime, l'article 63, de la LSP pourrait être amendé de la manière suivante (nous soulignons les modifications): «en cas de non-respect par le prestataire de services de paiement des obligations qui découlent des articles 13, 14, 2<sup>o</sup> à 6<sup>o</sup>, 15 et 16, 21, 23, alinéa 2, 25, 29, 32, 36, alinéa 1<sup>er</sup>, 38, 39, § 2, 40 et 41, 43, 45 à 48, 50 à 52, 56, 57 et 78, l'utilisateur de services de paiement peut, sans préjudice des sanctions de droit commun, par lettre recommandée [...] à la poste et motivée, résilier sans délai et sans frais ni pénalités le contrat-cadre *dans un délai raisonnable* à partir du moment où il a connaissance ou aurait dû avoir connaissance du non-respect de ces obligations, *ou demander l'application de toute autre mesure permettant de réparer le dommage résultant de l'inobservation de ces obligations*».

1. Pour une mesure similaire, voir, en matière de contrats à distance portant sur des services financiers, l'art. 55, § 2, de la LPMC.

2. Voir not. les art. 13, 14, 2<sup>o</sup> à 6<sup>o</sup>, 15, 23, alinéa 2, ou 25 de la LSP.

3. Art. 36, al. 1<sup>er</sup>, de la LSP.

4. A ce sujet, voir H. Jacquemin, «Les paiements électroniques dans les contrats à distance depuis la loi du 10 déc. 2009», *R.D.T.L.*, 2010/4, pp. 20-21.

5. Art. 14, 2<sup>o</sup>, a), de la LSP.

On s'étonne également que les manquements à certaines obligations d'information ne soient pas visés par l'article 63 et, par voie de conséquence, ne fassent pas l'objet d'une sanction civile spécifique<sup>1</sup>, tel notamment le cas du non-respect de l'article 14, 1<sup>o</sup> et 7<sup>o</sup>, ou des articles 18 à 20 de la LSP.

Enfin, lorsque l'utilisateur de services est un consommateur, la loi prescrit l'établissement d'une procédure extrajudiciaire adaptée de traitement des plaintes, à l'issue de laquelle la décision est rendue par un organisme indépendant<sup>2</sup>.

---

1. Des sanctions civiles pourraient être appliquées conformément à la théorie générale des contrats (à ce propos, voir H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, op. cit., pp. 445 et s., n<sup>os</sup> 326 et s.) mais à divers égards, la protection de l'utilisateur serait assurée avec une efficacité renforcée si la mesure était expressément prévue par la loi (*ibid.*, pp. 502 et s., n<sup>os</sup> 373 et s.).

2. Art. 75 de la LSP.