Le paiement électronique à la lumière de la nouvelle loi sur les services de paiement

Feld, Julie

Published in:
Le paiement

Publication date:
2009

Document Version
le PDF de l'éditeur

LE PAIEMENT ÉLECTRONIQUE À LA LUMIÈRE DE LA NOUVELLE LOI SUR LES SERVICES DE PAIEMENT

Julie FELD
Avocate au barreau de Bruxelles
Chercheuse aux FUNDP

Introduction

1. Le paiement électronique est un concept juridique complexe, une technique obscure, mais une pratique banale.

La présente contribution entend réconcilier nos gestes quotidiens de consommateurs effectuant chaque jour des paiements électroniques avec une analyse juridique des concepts en jeu et des relations que ces paiements supposent.

2. Cet article propose donc, dans un premier temps, de préciser les contours de la notion de paiement électronique. Nous le verrons, sous cette appellation, ce ne sont pas que les paiements au sens strict qui sont visés, mais toutes sortes d'opérations. Il parait également nécessaire de préciser quels sont, et comment fonctionnent, les modes de paiement électronique les plus utilisés aujourd'hui.

3. Une brève description du cadre normatif européen semble également utile dans la mesure où l'on ne peut ignorer que ce sont les instances européennes qui insufflent leurs modifications aux législations nationales. L'objectif du législateur européen est en effet de s'assurer que le paiement électronique s'inscrit dans un cadre européen harmonisé, indispensable au bon développement des échanges transfrontaliers.

Quant au cadre juridique belge, il est en pleine mutation. D'une part, il devra s'adapter à la nouvelle directive concernant l'accès à l'activité des établissements de monnaie électronique qui est en voie de finalisation, mais également, et surtout, à la directive européenne 2007/64/CE concernant les services de paiement dans le marché intérieur[1].

À l'heure de la rédaction de la présente contribution, ce qu'il est commun d'appeler le «paiement électronique» est encore régi par la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert

---

[1] Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE, *J.O.U.E.*, L 319/1, 5 décembre 2007.

électronique de fonds[2]. Toutefois, la transposition en droit belge de la directive sur les services de paiement dans le marché intérieur[3], qui devrait avoir eu lieu avant le 1er novembre 2009, suppose que la loi du 17 juillet 2002 soit intégralement abrogée, et que la matière soit régie par deux nouvelles lois, la loi relative aux services de paiement[4] et la loi 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, ainsi que par les nouvelles dispositions de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

On ne peut donc que recommander au lecteur de se référer aux textes des lois tels qu'ils auront été publiés, et d'être indulgent quant aux éventuelles inexactitudes de cette contribution qui seraient dues à des modifications de texte en fin de processus législatif.

Cette première analyse de la nouvelle réglementation belge ouvrira ainsi la voie à une réflexion qui pourra être nourrie de l'application, par les acteurs visés, des nouvelles dispositions et par l'interprétation qu'en tirera la jurisprudence. On se référera cependant utilement à la loi du 17 juillet 2002 et aux décisions judiciaires préalables à cette nouvelle loi pour en circonscrire au mieux les contours.

4. Dans une troisième partie, nous verrons comment s'articulent les relations entre les différents intervenants à l'opération de paiement électronique et les responsabilités qui en découlent.

Chapitre I
Le paiement électronique et ses modalités

5. Dans ce premier chapitre, nous nous pencherons sur la signification du concept de paiement électronique, cette expression prêtant à confusion. Afin d'inscrire la présente contribution dans une réalité tangible, et pour permettre au lecteur de bien saisir la portée des concepts présentés, nous dresserons un bref tableau des modes de paiement électronique les plus usités.

2 Loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, *M.B.*, 17 août 2002.

3 Ci-dessous la « SPD », acronyme généralement utilisé pour Paiement Services Directive.

4 Projet de loi relatif aux services de paiement, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, pp. 167 et s.

Section 1
La notion de paiement électronique

6. Dès le jour où un acheteur a pu payer le bien ou le service qu'il souhaitait acquérir autrement que par la remise d'une somme d'argent fiduciaire, ou par de la monnaie scripturale, il a utilisé des moyens de paiement qui furent, au départ, partiellement automatisés ou électroniques, pour devenir aujourd'hui entièrement électroniques, voire dématérialisés, d'où l'expression de « paiement électronique ».

Il faut le souligner d'emblée, la notion de « paiement électronique » est impropre. Elle sera aussi bientôt obsolète.

7. La notion de paiement électronique est tout d'abord impropre parce que, dans son acception commune, elle ne vise pas le paiement au sens juridique du terme.

Dans les années 80, au vu du développement des systèmes électroniques de paiement, la commission européenne a décidé, après avoir pris plusieurs recommandations en la matière[5], de mettre l'accent sur un système garantissant aux utilisateurs une confiance dans les moyens de paiement électronique mis à leur disposition, et dans leur utilisation. Elle a donc adopté une recommandation relative aux opérations effectuées au moyen d'instruments de paiement électronique en date du 30 juillet 1997[6]. L'article 11 de cette recommandation invitait les États membres à prendre les mesures nécessaires afin de mettre les émetteurs d'instruments de paiement électronique en conformité avec les dispositions qu'elle contient. C'est ainsi que, malgré l'absence de toute force juridiquement contraignante, la Belgique a décidé de mettre en œuvre les lignes directrices de la commission en adoptant une loi et a ainsi, assez fidèlement, transposé les dispositions de cette recommandation dans l'ordre juridique interne.

Toutefois, si le titre de cette recommandation visait « les opérations effectuées au moyen d'instruments de paiement électronique », le législateur belge a souligné[7], à juste titre, que cet intitulé limitait par lui-même le champ d'application de ce texte aux seuls paiements. Or, il convenait d'inclure dans le champ d'application de la loi les paiements qui éteignent des obligations, mais également les libéralités et les transferts de fonds effectués par une personne entre

5 Voir n°s 48 et s.

6 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, *J.O.C.E.*, n° L 208, 2 août 1997.

7 Loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 1389/001, p. 6.

ses différents comptes. Le titre de la loi du 17 juillet 2002 (ci-après la « LTEF ») vise donc les « instruments de *transfert* électronique » et non pas les « instruments de *paiement* électronique ». Cette différence entre le titre de la loi et celui de la recommandation n'est donc pas purement formelle, mais bien sémantique.

Ainsi donc, depuis 2002, les règles en la matière visent tout type d'opérations et non pas seulement le paiement.

Cette conception large de la notion de paiement est d'ailleurs confirmée par la SPD et le sera vraisemblablement par sa loi de transposition. L'annexe de cette directive définit en effet les services de paiement comme étant des services relatifs à la gestion de comptes bancaires (versements et retraits de fonds), au transfert et à la transmission de fonds, à l'émission et l'acquisition d'instruments de paiement.

Il est donc clair que le paiement électronique ne se résume pas au paiement d'une somme d'argent.

8. L'expression « paiement électronique » risque toutefois, à très court terme, d'être considérée comme obsolète.

Force est en effet de constater que la notion de paiement électronique, et même celle de transfert électronique, ne ressortent nulle part du texte de la SPD et du projet de loi sur les services de paiement.

Il est vrai que l'objectif de la directive est de couvrir l'ensemble des paiements, en ce compris les paiements électroniques. Est-ce à dire qu'à l'heure actuelle plus aucun texte juridique ne réglerait la problématique des paiements électroniques ? Formellement oui. Mais à considérer le champ d'application de la SPD et du projet de loi de transposition[8] qui excluent les « opérations de paiement exclusivement effectuées en espèces et allant directement du payeur au bénéficiaire, sans l'intervention d'un intermédiaire », ainsi que les opérations fondées sur des chèques, traites, lettres de change et autres[9], et au vu des situations de fait que ces textes tendent à régir, il est évident que les nouveaux cadres juridiques s'appliquent certes aux « services de paiement » de manière générale, mais que cette notion recouvre principalement les anciens « transferts électroniques ».

8 Dans la suite du texte, on entendra par l'acronyme « LSP », le projet de loi relatif aux services de paiement.

9 Article 3, a) et g) de la SPD et article 4, 7° de la LSP.

Section 2
Les différents modes de paiement électronique

9. Le paiement électronique est aujourd'hui la norme. Il est utilisé pour l'achat de biens matériels dans un environnement tangible où les parties sont, ou non, en présence l'une de l'autre et pour l'achat, dans un environnement virtuel, de biens matériels ou dématérialisés, comme par exemple l'achat de musique sur internet.

10. À défaut d'indications dans la LSP, il est utile, pour saisir ce que recouvre l'expression « paiement électronique », de s'en référer aux dispositions de la LTEF.

En filigrane de son article 2, la LTEF postule que les opérations de transfert électronique de fonds sont les opérations réalisées au moyen d'un instrument de transfert électronique de fonds. Un instrument de transfert électronique de fonds est quant à lui « tout moyen permettant d'effectuer par voie entièrement ou partiellement électronique » une opération de transferts de fonds, un retrait ou un dépôt d'argent liquide, l'accès à distance à un compte ainsi que le chargement et le déchargement d'un instrument rechargeable.

11. Il nous semble exact de dire qu'un paiement sera qualifié d'électronique soit fonction du moyen utilisé pour sa réalisation, soit en fonction de l'espace où il est exécuté.

Ce premier critère, tiré de la LTEF, vise tout paiement fait par un procédé qui implique un traitement électronique, comme les paiements faits par carte de banque, par le biais de monnaie électronique, ou au moyen d'un téléphone portable, ainsi que les opérations qui s'exécutent à partir de terminaux situés dans des points de vente[10], à partir de distributeurs automatiques[11], d'un téléphone (*phone banking*), d'un ordinateur (*home banking* ou *computer banking*), ou à partir d'un dispositif mis en place par l'émetteur, de type *self-banking*[12].

Selon le second critère, tout paiement fait sur un réseau, tel internet ou un réseau de télécommunication numérique ou informatique sera également électronique.

Aussi peut-on dire qu'un paiement sera électronique parce qu'il répond à l'un seulement de ces critères, comme ce sera le cas des virements effectués sur internet ou des paiements par carte POS, ou aux deux critères à la fois comme

10 Généralement désignés sous l'appellation POS pour « *Point of Sale* ».

11 Généralement désignés sous l'appellation ATM pour « *Automated Teller Machine* ».

12 Projet de loi relatif aux opérations effectuées au moyen d'instruments de transfert électronique de fonds, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 1389/001, p. 8.

pour les paiements par carte effectués sur internet ou via un téléphone portable, ou pour les paiements faits sur internet via un téléphone mobile, ou via un ordinateur qui est relié à internet grâce à une connexion mobile.

La présentation ici faite n'a donc pas pour objet de créer des distinctions entre les différents modes de paiement électronique, mais uniquement d'en dresser un bref tableau, tout en gardant à l'esprit qu'il est impossible d'en faire un inventaire statique tant ce domaine est sujet aux évolutions technologiques.

Il faut toutefois faire remarquer que les règles juridiques qui s'appliquent au paiement électronique ne diffèrent pas selon la technologie choisie.

§ 1. Le paiement par carte

12. Que la transaction ait lieu dans le point de vente en présence des deux parties, ou à distance – par téléphone, par correspondance ou par internet – l'acheteur pourra payer les biens ou les services acquis par carte de paiement[13]. Cet instrument de paiement électronique est ainsi utilisable tant dans les environnements tangibles que dans le monde virtuel.

Les études au sujet des cartes de paiement sont nombreuses et nous ne nous y attarderons donc que peu[14].

Notons qu'il existe trois types de paiement électronique par carte qui se différencient selon que le compte du titulaire de la carte sera débité avant, pendant ou après la transaction[15]. Dans le premier cas, on sera face à une carte rechargeable, dans le second, face à une carte de débit, et dans le dernier cas, on aura à faire à une carte de crédit.

[13] L'article 2, § 5° de la LTEF définit la carte comme « tout instrument de transfert électronique de fonds dont les fonctions sont supportées par une carte ».

[14] Sur la carte de crédit voir entre autres: J.-P. Buyle et M. Delierneux, « Paiement par carte de crédit: nature juridique, preuve et répartition des risques », *R.D.C.*, 2000, p. 696; M. Schauss et X. Thunis, *Aspects juridiques du paiement par carte*, Cahiers du C.R.I.D., Gand, Story-Scientia, 1988, p. 46; J.-P. Buyle et O. Poelmans, « Description des moyens de paiement en réseau ouvert », in *Internet face au droit*, Gand, Story-Scientia, 1997, pp. 88 et s.; J.P. Buyle, « Le paiement électronique », *J.T.*, 2001, p. 131; P. Kileste, « Le titulaire d'une carte de crédit est-il engagé par déclaration unilatérale de volonté? », *R.D.C.*, 1986, p. 495; G.-A. Dal et I. Corbisier, « Les instruments de paiement et de crédit (chronique) », *J.T.*, 1990, p. 440, n° 77; R. Steenoot, *Elektronisch betalingsverkeer. Een toepassing van de Klassieke principes*, Intersentia, 2002, p. 160; P.-P. Lemyre, « Le paiement électronique », in *Le Guide juridique du commerçant électronique*, sous la dir. de E. Labbé, D. Poulin, F. Jacquot et J.-F. Bourque, Montréal, Ed. Thémis, p. 146. Fr. de Clippele et O. Goffard, « 'Go Digital': Het vertrouwen in de e-handel en de juridische kwalificatie van de elektronische betalingsmechanismen – Toetsing van het beginsel van de rechtszekerheid in het rechtsgebied van elektronische betaling aan de hand van de nationale en Europese rechtsbronnen », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, pp. 71-77; Fr. de Clippele et O. Goffard, « Qui va payer? Ou questions quant à la responsabilité de l'émetteur de la carte en cas de transfert électronique de fonds », *J.T.*, 2004, p. 372; Th. Lambert, « La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds », *R.D.C.*, 2003, p. 573.

13. Les paiements au moyen d'une carte de crédit[16] peuvent aussi bien être réalisés *on-line* qu'*off-line*. Lors des paiements *on-line*, une communication directe entre le commerçant et l'institution émettrice de la carte est nécessaire pour l'autorisation de la transaction. Le paiement est alors immédiatement enregistré dans l'ordinateur de l'institution émettrice et le client reçoit une preuve de sa transaction.

Les paiements *off-line* sont eux utilisés par les commerçants qui ne reçoivent qu'un nombre limité de paiements par carte. Au-delà d'un certain montant, le commerçant contactera l'émetteur pour la réalisation du transfert des divers paiements enregistrés vers son compte.

14. La carte de débit peut être utilisée pour effectuer des paiements POS, pour retirer de l'argent d'un ATM et pour effectuer des paiements sur internet[17].

Le transfert électronique de fonds par une carte de débit est réalisé au moyen d'une télécommunication *on-line*. C'est ainsi que le débit peut avoir lieu au moment même de la transaction lorsque le titulaire de la carte autorise la transaction en introduisant son code secret.

Cette communication *on-line* offre l'avantage d'une vérification immédiate de la présence de fonds suffisants sur le compte. Ce caractère *on-line* garantit également le statut de la carte, entre autres le fait de savoir si la carte a été bloquée ou pas. Après ces vérifications, le transfert est immédiat et définitif. Le commerçant a donc l'assurance que si une transaction est acceptée par le terminal de paiement, son compte sera crédité du montant de la transaction[18].

15. Le troisième type de carte, celui qui fonctionne selon le mode *pay before*, est la carte rechargeable ou carte à puce. Selon la LTEF, il s'agit d'un instrument de transfert électronique de fonds sur lequel des unités de valeur sont stockées électroniquement[19].

Elle présente deux fonctions principales. D'abord, elle est chargeable et rechargeable. Le titulaire d'une telle carte pourra donc débiter son compte bancaire afin de charger des unités de valeur sur sa carte. D'autre part, elle est déchargeable. Ce déchargement peut se faire soit auprès d'un commerçant dans un but de paiement, soit sur le compte du titulaire ou sur un autre compte pour y

[16] *Parmi les cartes de crédit, une différence peut être faite entre les deffered debet cards et revolving credit cards. Par l'utilisation de la deffered debet card, il est accordé au titulaire de la carte un report de paiement jusqu'à réception de la facture mensuelle. Le titulaire d'une revolving credit card peut étaler les remboursements des montants déboursés.*

[17] *Voir n° 42.*

[18] *F. De Clippele et O. Goffard, « Qui va payer? », op. cit., p. 370.*

[19] Article 2, 2° de la LTEF.

inscrire des unités de valeur stockées sur la carte. Le chargement se fera donc nécessairement par accès au compte, alors que le déchargement pourra se faire via accès au compte, ou sans accès au compte et dans ce cas auprès d'un commerçant[20].

À titre d'exemple, la carte à puce Proton est une carte rechargeable qui enregistre dans sa mémoire de l'argent électronique chargé à partir du compte de son titulaire. À chaque paiement, les unités sont transférées vers le terminal du commerçant qui pourra virer cet argent vers son propre compte[21].

Ce moyen de paiement, qui trouve des applications dans le monde physique et sur internet, est une forme de monnaie électronique.

§ 2. La monnaie électronique

16. Les moyens traditionnels de paiement ont dû s'adapter rapidement aux nouveaux environnements dématérialisés. À travers le monde, et sous l'impulsion d'entreprises privées, différentes monnaies électroniques ont vu le jour.

17. La monnaie électronique est une notion aujourd'hui consacrée par le législateur européen et belge.

Selon la directive 2000/46/CE[22], dite «directive Monnaie Électronique», il s'agit d'«une valeur monétaire représentant une créance sur l'émetteur, qui est stockée sur un support électronique, émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise, acceptée comme moyen de paiement par des entreprises autres que l'émetteur».

L'article 5 de la loi du 25 février 2003[23] a introduit un article 3, § 1er dans la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit[24] qui reprend textuellement cette définition.

La définition européenne sera toutefois amenée à changer sous peu dès l'adoption du projet de directive concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle des ces établissements dans sa version telle qu'adoptée par le parlement européen

0 A. SALAÜN, «Une nouvelle pierre à l'édifice de protection des consommateurs: la loi sur les instruments de transfert électronique de fonds», *J.T.*, 2003, p. 206.

1 *Ibidem.*

2 Directive 2000/46/CE du 18 septembre 2000 du Parlement européen et du Conseil, concernant l'accès à l'activité des institutions de monnaies électroniques et son exercice, ainsi que la surveillance prudentielle de ces instituions, *J.O.C.E.*, L 275/39, 27 octobre 2000.

3 Loi du 25 février 2003 modifiant la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, *M.B*, 7 mars 2003.

4 Loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, *M.B.*, 19 avril 2003.

le 24 avril 2009[25]. Le texte proposé est le suivant: «toute valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement telles que définies à l'article 4, point 5) de la directive 2007/64/CE et qui est acceptée par une personne physique ou morale autre que l'émetteur»[26].

La monnaie électronique ne repose sur aucun support physique. Elle peut être conservée dans des porte-monnaie électroniques qui se trouvent sur des cartes à puce rechargeables (du type carte proton) ou sur le disque dur d'un ordinateur.

18. Au vu des différents systèmes de monnaie électronique proposés, on peut estimer que, pour être considérée telle, la monnaie électronique doit répondre à certains critères[27].

Tout d'abord, la monnaie électronique a pour objet de remplacer l'utilisation de la monnaie fiduciaire par de nouvelles valeurs n'ayant pas cours légal. L'effet libératoire de ces monnaies ne tient donc qu'au cadre contractuel existant entre les vendeurs et les clients utilisateurs[28].

Tout comme pour la monnaie fiduciaire, cette monnaie électronique n'est pas la propriété de la personne qui la détient.

Par ailleurs, il n'y aura réellement monnaie électronique que pour autant que le support (carte à puce ou mémoire d'ordinateur) soit chargé d'unités monétaires cessibles et réutilisables et dont la circulation ne transite pas par un compte bancaire[29].

Enfin, l'usage du support ne doit pas être limité auprès du seul émetteur de cette monnaie électronique[30].

19. Si la monnaie électronique est matérialisée sur une carte, cette carte peut être prépayée (*pre-paid card*) ou multifonctionnelle (*multipurpose card*).

25 Voir la position du Parlement européen arrêtée en première lecture le 24 avril 2009 en vue de l'adoption de la directive 2009/ /CE du Parlement européen et du Conseil concernant 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, disponible sur le site http://www.europarl.europa.eu.

26 Article 4, point 5) de la SPD: «opération de paiement: une action, initiée par le payeur ou le bénéficiaire, consistant à verser, transférer ou retirer des fonds, indépendamment de toute obligation sous-jacente entre le payeur et le bénéficiaire».

27 P.-P. LEMYRE, *op. cit.*, p. 153.

28 Th. LAMBERT, *op. cit.*, p. 99.

29 X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Namur, Presses universitaires de Namur, 1996, n° 58.

30 Ainsi, une carte émise par un magasin, pouvant être rechargée mais ne permettant des achats que dans ce magasin, ne sera pas considérée comme support de monnaie électronique.

Une illustration de ce qu'est la monnaie électronique et de son fonctionnement peut être donnée par la carte «Proton». Proton est une carte multifonctionnelle permettant aux titulaires d'un compte bancaire d'effectuer des paiements de faibles montants pour l'achat de biens ou de services auprès de commerçants équipés du terminal de paiement requis.

En application du système *pay before*[31], le client charge préalablement sa carte Proton d'unités «monétaires» électroniques, débitant ainsi son compte à vue ouvert auprès de l'émetteur de la carte. Il est donc détenteur d'unités électroniques dont il n'est pas titulaire et les fonds correspondants sont rendus indisponibles.

Selon les termes de la définition de la monnaie électronique, les unités électroniques ainsi chargées sur la carte sont des titres de créances à l'égard de l'émetteur. Ces unités constituent, en réalité, un instrument de paiement émis par une banque.

Lorsque la carte est utilisée auprès d'un terminal de paiement, les unités électroniques inscrites sur cette carte sont irrévocablement transférées en faveur du commerçant, impliquant, par là même, un transfert du droit de créance sur l'émetteur – matérialisé dans les unités électroniques – au profit du commerçant bénéficiaire du paiement. Par l'effet de ce transfert, le commerçant sera donc titulaire d'une créance sur l'établissement émetteur jusqu'au crédit de son compte personnel[32].

20. La doctrine analyse le paiement par monnaie électronique comme une dation en paiement ou comme un échange, selon l'objet initial des consentements[33].

§ 3. Le M-paiement

21. Si ces dix dernières années ont vu les interactions sociales et les relations commerciales devenir électroniques (sous forme du courrier électronique, du commerce électronique, du paiement électronique...), il y a fort à gager que les dix suivantes tomberont sous le coup de la mobilité.

Les téléphones portables rivalisant à développer de nouvelles fonctionnalités, ils proposent aujourd'hui toutes sortes d'applications qui permettent à leurs utilisateurs d'être informés en temps réel, d'effectuer des réservations, de conclure

Voir n° 12.

Loi du 25 février 2003 modifiant la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit, Exposé des motifs, *Doc. Parl.*, Ch. repr., sess. ord., 2002-2003, n° 2122/01, pp. 5 et 6.

Sur cette analyse, et son incidence en cas de faillite de l'acheteur, voir J.P. Buyle, *op. cit.*, p. 131.

des contrats[34] et de payer. Le paiement par téléphone portable, ou mobile-paiement, est manifestement un mode de paiement appelé à un avenir prometteur.

22. Le paiement mobile désigne l'utilisation d'un téléphone mobile ou de tout autre dispositif de télécommunication, numérique ou informatique, pour l'émission d'un paiement, que cette émission soit formalisée par un appel téléphonique ou par un SMS[35]. On pourra donc considérer que, dès lors qu'un ordre de paiement part d'un support électronique portable et passe par un réseau de télécommunication ou un réseau informatique, le paiement est mobile.

23. Il existe diverses méthodes de M-paiement[36].

Premièrement, l'opérateur de systèmes ou réseaux de télécommunication ou informatiques[37] peut assurer le paiement au vendeur, et répercuter le coût des biens commandés ou des services prestés par sa facturation. Si l'acheteur a un abonnement de téléphonie qui lui permet de payer ses communications à l'issue de chaque mois, le coût de l'opération sera porté en compte de sa facture mensuelle, alors que si le consommateur dispose d'un compte prépayé, le paiement sera immédiatement débité de son compte prépayé et viendra imputer le volume de communications qu'il a préalablement acheté. Dans ces deux cas, l'opérateur de télécommunication qui agit en tant que prestataire de services de paiement verse, ou reverse, au vendeur une partie du montant facturé selon l'accord conclu préalablement.

Notons que si l'opérateur intervient dans un mode *post-paid*, c'est-à-dire via une facturation postérieure à la fourniture des biens ou services achetés, il agira soit par le biais d'un contrat de *factoring* en son nom et pour son compte à la suite d'une cession de créances de la part du fournisseur des biens ou services, soit en qualité de mandataire de ce fournisseur. Par contre, si le paiement se fait par le débit d'une carte prépayée, l'opérateur à qui le fournisseur a cédé sa créance se paie en prélevant des unités électroniques contenues dans la carte prépayée. Ces unités, qui peuvent donc être échangées contre du temps d'appel ou contre la fourniture des biens ou services peuvent être considérées comme de la monnaie électronique[38].

34 Ce qu'on appelle le Mobile commerce, ou M-commerce.

35 Acronyme de Short Message System.

36 T. Verbiest et E. Wery, «Commerce électronique par téléphonie mobile (m-commerce): un cadre juridique mal défini», *Recueil Dalloz*, 2004, n° 41, pp. 2 et s.

37 Désigné plus loin comme «l'opérateur».

38 J.-P. Degueе, «Le statut légal des établissements de monnaie électronique», in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, p. 21.

Deuxièmement, le paiement peut être fait par un acheteur qui donne ordre à son opérateur de débiter son compte bancaire ou sa ligne de crédit ouverte auprès d'un organisme émetteur de carte de crédit. Dans ces deux cas, l'opérateur de téléphonie mobile doit avoir conclu un accord préalable et global avec l'organisme bancaire de l'acheteur ou avec l'organisme émetteur de sa carte de crédit. En réalité, il faut que le client se soit préalablement enregistré auprès de l'opérateur pour pouvoir utiliser ce service de M-paiement en donnant les informations relatives à sa carte de crédit ou au compte bancaire sur lequel le montant du paiement peut être prélevé. Lorsqu'un paiement est effectué, l'opérateur transmet les détails de la transaction à la banque ou à l'organisme de crédit. Ceux-ci vont alors débiter le compte du client et créditer le montant sur le compte bancaire du vendeur.

Dans ce schéma, par opposition au précédent, aucun montant n'est géré par l'opérateur qui agit comme intermédiaire entre l'acheteur et l'organisme de crédit ou la banque. Le vendeur est payé soit par la banque de l'acheteur, soit par l'émetteur de sa carte de crédit. On le verra, lorsque l'opérateur joue un rôle de simple interface, cela peut avoir des conséquences quant à l'application de la LSP.

Troisièmement, le M-paiement peut faire appel à de la monnaie électronique. Deux applications peuvent ainsi être mises en parallèle avec le porte-monnaie électronique et le porte-monnaie virtuel.

Le paiement peut se faire par prélèvement du montant sur un compte prépayé dédié aux paiements mobiles et qui est géré dans le réseau de l'opérateur. Dans ce cas, l'acheteur s'est enregistré auprès de son opérateur et a alimenté son compte personnel, soit par virement bancaire, soit par carte de crédit, soit par paiement d'un surplus facturé au même moment que les communications. Si le vendeur a adhéré à ce système, il communique les informations utiles au paiement à son acheteur, qui les communique à son tour à l'opérateur. Celui-ci vérifie le solde du montant disponible. Si ce solde est suffisant, il autorisera le paiement et transférera lui-même le montant sur le compte du vendeur éventuellement ouvert auprès de l'opérateur, et débitera le porte-monnaie électronique du client[39]. Selon les cas, le vendeur pourrait réutiliser les valeurs ainsi reçues pour effectuer lui-même d'autres transactions, ou les convertir en valeur fiduciaire.

Le paiement peut également se faire par prélèvement sur un compte prépayé qui est hébergé dans le téléphone mobile du client. Le système est assez semblable à celui décrit ci-dessus, si ce n'est que le client effectuera directement

39 Tunz propose ce type d'application avec l'avantage que le créancier du paiement ne doit pas nécessairement disposer d'un compte auprès de cette compagnie.

le paiement auprès d'un marchand adhérant à ce système en lui envoyant son paiement sans avoir besoin de transiter par un intermédiaire. Sa monnaie électronique est en effet stockée entre ses mains, et non pas sur le réseau de l'opérateur.

§ 4. Les paiements sur internet

24. Internet est passé en quelques années du statut de source universelle d'informations à celui de plateforme mondiale d'opérations commerciales.

Son développement fulgurant et les relations juridiques qui en découlent ont largement modifié les méthodes d'achat en ligne.

Les conventions conclues sur internet mettent aujourd'hui en présence des acteurs souvent situés dans des territoires différents[40]. Ceux-ci seront désireux que la transaction soit rapide et sure, le vendeur voulant s'assurer qu'il recevra bien le paiement alors que l'acheteur voudra être garanti contre tout risque lié à la communication de ses données de paiement en ligne.

Le commerce électronique requiert donc des modes de paiement rapides, sûrs et efficaces.

25. Pour pouvoir évaluer la sécurité d'un paiement sur internet, il faut garder à l'esprit trois critères.

Il faut d'abord s'assurer de la confidentialité des informations transmises sur le réseau, en particulier les informations bancaires. Il convient également de se garantir de l'intégrité du message pour que les parties en présence puissent être assurées que le message transmis par internet n'a pas été modifié. Enfin, il sera nécessaire d'authentifier le donneur d'ordre. Cette authentification garantira au vendeur, et aux prestataires de paiement intervenant dans le processus de paiement, que c'est bien le titulaire du compte qui a passé la commande et qui recevra le bien acheté.

26. Internet donne par lui-même la qualification de « électronique » aux paiements qui y ont lieu. Néanmoins, les types de paiement qui y sont réalisés

40 Quant aux questions liées à la détermination du moment et du lieu de la transaction, voir A. BRUYNEEL, « Le virement », in *La banque dans la vie quotidienne*, Bruxelles, Ed. Jeune Barreau de Bruxelles, 1986, p. 387, n° 25; X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Presses universitaires de Namur, 1996, p. 275; M. DEMOULIN, « La vente à distance: des contrats entre absents au commerce électronique », in *Vente – Commentaire pratique*, Bruxelles, Kluwer, 2007, I.3; M. DEMOULIN et E. MONTERO, « La conclusion des contrats par voie électronique », in *Le processus de formation du contrat – contribution comparative et interdisciplinaire à l'harmonisation du droit européen*, Bruxelles-Paris, Bruylant-LGDJ, 2002, p. 784; P.-P. LEMYRE, *op. cit.*, p. 146.

seront soit électroniques par nature (comme le paiement par carte), soit électroniques par acquis (comme le virement bancaire).

Par ailleurs, les procédés auxquels il est fait appel sont soit des procédés traditionnels adaptés à l'internet (paiement par carte, par virement ou par chèque), soit des procédés conçus en fonction des protocoles, de l'architecture et de la sécurité sur l'internet[41] (cartes prépayées, porte-monnaie virtuel, portefeuille électronique).

Nous analyserons donc comment les procédés de paiement traditionnels ont pu, ou doivent encore, s'adapter aux transactions dématérialisées et comment fonctionnent ces nouveaux moyens de paiement *tailor-made* pour l'internet[42].

A. Le paiement par carte

1. *Le paiement par carte de crédit*

Le paiement par carte de crédit est sûrement le moyen de paiement sur internet le plus répandu à l'heure actuelle. Il nécessite donc que l'on s'y attarde quelque peu.

a. Fonctionnement et risques

27. Au premier abord, le paiement par carte de crédit semble parfaitement adapté au contexte du paiement sur internet puisque ce mécanisme ne nécessite pas la présence physique des parties. Il suffit, pour réaliser la transaction, que le client fournisse les données visibles de sa carte, tels son numéro, sa date d'expiration, et éventuellement un code supplémentaire tout autant visible, afin de procéder au paiement. Le vendeur transmettra alors ces informations à sa banque qui lui confirmera la transaction. Cette façon de procéder est utilisée depuis de nombreuses années dans le cadre de la vente par correspondance et de la vente à distance[43].

28. Toutefois, l'utilisation de la carte de crédit sur internet n'est pas dénuée de risques.

Dans la mesure où les renseignements fournis ne contiennent aucune information spécifique au client, rien ne prouve *a priori* que celui à qui les biens seront livrés est le titulaire réel de la carte utilisée.

41 D. Bounie, « Quelques incidences bancaires et monétaires des systèmes de paiement électronique », *Rev. Eco*, vol. 52, 2001/7, p. 314.

42 D. et R. Mougenot, « Droit des obligations : La preuve », *in Répertoire notarial*, tome IV, 3e édition, Larcier, Bruxelles, n° 259- 6 et s.

43 P.-P. Lemyre, *op. cit.*, p. 150.

D'autre part, en divulguant ses données personnelles, le titulaire de la carte s'expose à l'utilisation frauduleuse de sa carte par le vendeur à qui les données ont été communiquées, ou par un tiers qui les aurait recueillies soit lors de leur transmission au vendeur, soit en pénétrant dans le système informatique du vendeur.

Mêmes risques donc que dans le monde réel, mais accrus par l'anonymat qui règne sur internet et par les possibilités accrues de piratage.

Divers procédés de sécurité ont dès lors été développés pour sécuriser de tels paiements.

b. Les procédés de sécurisation

29. Un paiement par carte, de crédit implique plusieurs niveaux contrôle[44].

Le statut de la carte, pour s'assurer qu'elle n'a pas été bloquée, le contrôle des plafonds financiers et du montant disponible, ainsi que le contrôle de la validité de la carte sont en général vérifiés instantanément si la transaction se fait *on-line*[45].

Par contre, la confidentialité des données bancaires, l'authentification du donneur d'ordre et l'intégrité du message contenant les indications de paiement font parfois défaut.

Aussi, différents modes de sécurisation ont vu le jour et garantissent, plus ou moins, ces différents niveaux de contrôle. Nous présenterons ici les principaux.

Le SSL (Secure Socket Layer)

30. Le protocole SSL est le système de sécurisation des paiements le plus utilisé sur Internet.

Beaucoup de sites de vente par internet offrent à leurs clients la possibilité d'autoriser un paiement en insérant et en confirmant leur numéro de carte et sa date de validité. Dans ce cas, la sécurisation de l'échange des données est attestée par la présence sur l'écran du logo d'un cadenas et par l'adjonction de la lettre S à la formule http (https://...).

Ce protocole permet de crypter les données relatives à une carte de crédit communiquées par son titulaire, via internet, vers le serveur du vendeur. Son avantage principal est donc que les données qui transitent grâce à ce système sont protégées et que la confidentialité de la communication est assurée[46].

44 P. Bellens, « Aspects généraux du paiement électronique par carte bancaire », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, p. 21.

45 Voir n° 13.

46 O. Goffart, « Status quaestionis : risques et responsabilités en cas de transfert électronique de fonds sur internet ou : Des risques encourus par le titulaire et l'émetteur d'un instrument de transfert électronique de fonds, spécialement lorsque l'instrument est utilisé sans présentation physique et sans identification électronique : application au paiement sur Internet », *R.D.C.*, 2005/I, p. 15.

Néanmoins, la clé de chiffrement qui permet de crypter les données bancaires est assez courte et donc aisément cassable, de sorte que la confidentialité des informations communiquées peut être violée.

D'autre part, pour utiliser ce protocole et autoriser le paiement, le client doit seulement insérer les numéros apparents de sa carte de crédit et la date de validité, de sorte qu'il n'y a aucune vérification de son identité. Ce mécanisme ne requiert en effet aucun code d'identification personnelle au titulaire de la carte. L'infrastructure SSL n'est donc pas à même de garantir le vendeur de la bonne identité de celui qui lui communique les informations. Elle ne garantit pas non plus au titulaire de la carte que le destinataire auquel les données vont être communiquées est bien celui auquel il veut les communiquer, comme ce serait le cas dans l'hypothèse d'une tentative de *phishing*[47].

Le SET (Secure Electronic Transaction)

31. Tout comme le SSL, le protocole SET a recours à la cryptographie asymétrique pour répondre aux impératifs de confidentialité et d'intégrité du paiement.

Le SET va toutefois beaucoup plus loin que le SSL car il utilise des certificats et des signatures électroniques afin de garantir l'identité du titulaire de la carte et du vendeur.

Pratiquement, le client n'utilise pas sa carte bancaire mais un certificat qui lui a été délivré et qui est enregistré sur le disque dur de son ordinateur. Il suffit donc pour le client d'activer un logiciel préalablement téléchargé pour s'authentifier avec le certificat et réaliser une transaction[48].

Les données d'identification ainsi certifiées seront envoyées par le client au vendeur qui les communiquera ensuite à sa banque. Celle-ci, ayant reçu les données relatives à l'identité du client, vérifiera la validité de son certificat. Le paiement n'aura lieu qu'après cette vérification.

Le protocole SET est donc basé sur une authentification de toutes les parties. Le commerçant est assuré que le payeur est bien le client, et le client, quant à lui, est assuré que le vendeur est effectivement enregistré comme tel auprès des organismes de cartes de crédit[49].

Ce système assure donc l'irréfutabilité de la transaction. Le commerçant reçoit en effet une autorisation basée sur l'identification du client avant de procéder

47 Voir n° 192.

48 D. Bounie, *op. cit.*, p. 316.

49 P.-P. Lemyre, *op. cit.*, p. 161.

au paiement et il est assuré d'être payé, même en cas de fraude. D'autre part, le client est rassuré par le cryptage de ses données de paiement[50].

Le système 3-D Secure

32. *3-D Secure* est le nom d'une solution de paiement par carte bancaire sur internet qui a pour objectif de réduire la fraude en permettant à l'organisme émetteur de la carte de crédit d'authentifier le porteur de la carte lors de toutes les transactions qu'il ferait avant de les autoriser[51].

Selon ce système, le client s'est préalablement inscrit auprès de son organisme émetteur. Lorsque le client veut ensuite passer une commande sur un site internet, il communique ses données de carte bancaire, numéro et date de validité, mais devra en plus s'authentifier et autoriser la transaction en insérant un code secret qui sera généré par un mécanisme mis en place par son prestataire de services de paiement, par exemple par un *digipass*[52].

Dans le système *3-D Secure*, l'authentification du porteur de la carte par la banque émettrice, au moyen d'un *digipass* ou de tout autre module de sécurité, permet, en plus de garantir la confidentialité de la communication, de s'assurer que le client a été dument authentifié comme titulaire de la carte.

L'infrastructure PKI (Public Key Infrastructure)

33. L'infrastructure PKI permet aux utilisateurs d'un réseau non sécurisé du type d'internet d'échanger des données de manière sécurisée et confidentielle. Pour ce faire, ils ont recours à des autorités de certification. Le fait de faire appel à un prestataire de services de certification – établi selon la loi relative aux signatures électroniques et aux services de certifications[53] – constitue un élément de confiance pour sécuriser la transaction.

L'identification du titulaire de la carte est faite grâce à l'insertion d'un code secret permettant d'initialiser le mécanisme cryptographique. Ensuite l'infras-

50 Selon O. Goffart toutefois, l'identification du titulaire par l'insertion d'un code secret faisant défaut, l'authentification du client n'est pas garantie.

51 P. Bellens, *op. cit.*

52 « Le digipass est un module de sécurité fourni par les banques à leurs clients. Il s'agit d'un mécanisme d'authentification et de signature se présentant sous forme d'une petite calculette équipée d'un écran et d'un clavier, dont la fonction est de générer des codes d'accès utilisables de manière unique, sur base d'une information à valider et d'un code personnel. Chaque digipass contient un identifiant unique, une paire de clés cryptographiques spécifiques ainsi qu'un code secret. Le digipass offre deux grands types de fonctions. La fonction d'authentification et la fonction de signature électronique » : O. Goffart, *op. cit.*, p. 17.

53 Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001, p. 33070.

tructure, composée d'un logiciel, de clés et de certificats électroniques, sera vérifiée électroniquement par une autorité tierce qui apportera l'assurance que les clés et les certificats sont bien originaux et valides[54].

Cette solution permet donc d'assurer l'intégrité du message transmis, de préserver la confidentialité des informations, et d'authentifier les parties.

L'enregistrement sur le site

34. Une solution envisageable pour sécuriser les paiements, sans toutefois avoir recours à des outils techniques, consiste à l'enregistrement du client sur le site.

Lors de sa première visite sur un site internet, l'utilisateur est invité à transmettre son identité et les références de sa carte de crédit – voire davantage encore – par téléphone, fax, courrier ou tout autre procédé de transmission hors ligne. Il reçoit en échange un code qu'il n'aura plus qu'à communiquer lors de la conclusion de chaque transaction.

Ce système évite de faire passer des informations bancaires sur le réseau, mais suppose toutefois une grande confiance dans le destinataire des informations que l'utilisateur ne connait *a priori* pas[55].

Le recours à un intermédiaire

35. Une autre manière de limiter les risques de fraudes vise à faire intervenir, dans la relation de paiement, un intermédiaire auprès duquel l'utilisateur s'enregistre préalablement et qui offrira une garantie de sécurité aux parties[56]. Cette méthode se développe de plus en plus.

Nous avons certes déjà évoqué l'intervention, dans certains procédés, de la banque émettrice, de l'organisme émetteur de cartes de crédit ou d'une autorité de certification. L'intermédiaire peut toutefois être étranger au milieu bancaire et non visé par la loi du 9 juillet 2001.

Concrètement, le titulaire de la carte va transmettre au tiers les références de la carte en le chargeant d'exécuter les instructions de paiement qu'il lui renseignera. Il pourra ensuite librement conclure toutes sortes de transactions et transmettra chaque fois des instructions de paiement cryptées au vendeur, lequel s'adressera à l'intermédiaire en vue de les faire décrypter et exécuter[57].

O. GOFFART, *op. cit.*, p. 15.
J.-P. BUYLE, *op. cit.*, p. 130.
P.-P. LEMYRE, *op. cit.*, p. 146.
P.-P. LEMYRE, *ibidem*, p. 162.

Dans certains cas, le titulaire de la carte donnera à l'intermédiaire un ordre de paiement après l'avoir préalablement autorisé à débiter sa carte de crédit, dans d'autres il mettra à disposition de l'intermédiaire des fonds, que ce dernier gèrera avec son autorisation expresse [58].

Le recueil en ligne des données financières par une société spécialisée crée la confiance entre les parties et lève le risque de piratage informatique. Toutefois, ces intermédiaires ont généralement pour obligation de recueillir en ligne de façon sécurisée les données financières, mais pas de contrôler l'identité de l'acheteur[59].

Les intermédiaires de paiement les plus connus sont aujourd'hui la société belge Ogone, clear2pay ou neosmerchant[60].

2. *Le paiement par carte de débit*

36. Bien que ce soit une pratique moins courante, un client peut, pour effectuer des paiements, utiliser sa carte de débit.

Il peut en effet effectuer des transferts de fonds sur internet en insérant cette carte dans un terminal personnel relié à son ordinateur. Ce terminal se présente sous forme d'un boitier muni d'un clavier et d'un écran. Lors de l'achat en ligne, il devra alors autoriser la transaction en insérant son code PIN sur le clavier.

Ce processus est similaire au paiement dans le monde physique. Par l'insertion de la carte dans le lecteur, la validité de la carte est vérifiée. Le code PIN qu'aura introduit le titulaire de la carte aura en plus permis son authentification[61].

B. Le virement électronique

37. Les applications qui permettent l'exécution des virements électroniques nécessitent soit un ordinateur relié à un réseau sécurisé (système du *Home banking)* soit un dispositif installé par un prestataire (*self-banking).*

Pour effectuer un virement électronique à partir d'un ordinateur personnel, il sera nécessaire que le système de communication par lequel passent les ordres du client vers sa banque soit hautement sécurisé.

Pour garantir l'intégrité de l'ordre transmis, la confidentialité des données et l'identité du donneur d'ordre, la plupart des solutions *E-banking* offertes par les

58 J.-P. BUYLE, *op. cit.*, p. 132.
59 Sauf pour les intermédiaires prestataires de services de certification, comme par exemple dans le PKI.
60 Voir aussi Payline et Globe ID.
61 O. GOFFART, *op. cit.*, p. 18.

établissements bancaires utilisent des infrastructures dans lesquelles la signature digitale du donneur d'ordre sera certifiée.

C. Les chèques virtuels

38. Quant à la transposition du mécanisme du chèque papier au contexte électronique, le consommateur pourra disposer d'un carnet de chèques virtuel qu'il pourra visualiser et remplir *on-line*.

La signature manuscrite du chèque sera remplacée par une signature digitale. Il pourra éventuellement être fait appel à un intermédiaire pour éviter que les informations sensibles ne transitent par le réseau[62] et ne soient communiquées au commerçant lors de la transmission du chèque[63].

Jusqu'à maintenant, ces chèques électroniques ne remportent pas un vif succès auprès des acteurs du commerce électronique.

D. La monnaie électronique

39. On l'a vu, la monnaie électronique est une créance sur un institut d'émission inscrite sur une carte à microprocesseur (porte-monnaie électronique) ou sur un logiciel (porte-monnaie virtuel).

40. En plus de son utilisation pour des transactions hors ligne, le porte-monnaie électronique, chargé d'un certain montant de monnaie électronique, peut servir au paiement de transactions sur internet. La carte sera débitée à chaque opération au moyen d'un terminal installé sur l'ordinateur de l'utilisateur pour créditer le créancier au moyen d'un terminal installé sur son serveur[64].

Si la carte Proton ne requiert aucune signature, aucune certification, pas plus qu'une quelconque identification de l'utilisateur, le système proposé par Internetcash est basé sur une signature digitale. Le système de Mondex offre lui des applications tant dans le monde réel que sur internet et sur téléphones portables[65].

Le porte-monnaie virtuel est, lui, un instrument propre à l'environnement virtuel qui a été développé pour permettre une plus grande facilité dans le commerce électronique[66].

62 P.-P. Lemyre, *op. cit.*, p. 162.

63 D. et R. Mougenot, « Droit des obligations : La preuve », *in Répertoire notarial*, tome IV, 3e édition, Larcier, Bruxelles, p. 318.

64 Du style Czam/PC.

65 http://www.mondex.com. Voir aussi http://www.internetcash.com.

66 D. Bounie, *op. cit.*, pp. 318 et 319.

Par ce procédé, l'acheteur adresse au vendeur des unités de paiement électroniques stockées, non pas sur une carte à puce, mais sur le disque dur de son ordinateur.

L'exemple type de ce genre de systèmes est celui proposé par PayPal. L'acheteur peut charger son compte Paypal par virement bancaire ou par carte de crédit et ne doit alors plus encoder ses données bancaires ou personnelles dans le site du commerçant. Citons également Moneybookers.

Chapitre II
Le cadre légal

Section 1
Le cadre européen[67]

41. Comme il a été précisé dans l'introduction, vu l'influence du législateur européen et sa politique d'harmonisation, on ne peut faire l'économie d'une description de l'évolution du processus législatif à ce niveau.

42. Consciente que la problématique des systèmes de paiement devait être traitée au niveau européen, la Commission a voulu très tôt réglementer, ou en tout cas dessiner, un cadre général pour l'utilisation des cartes de paiement.

Ainsi, en 1987 déjà, elle a pris une communication consacrée spécifiquement aux cartes de paiement, intitulée «Tout atout pour l'Europe, les nouvelles cartes de paiement»[68]. La Commission européenne y insiste sur la dimension communautaire de l'utilisation des cartes de paiement et l'importance de pouvoir les utiliser en dehors de l'État membre où elles ont été émises afin de faciliter l'intégration du marché unique européen.

La même année, la Commission a pris une recommandation portant sur un code européen de bonne conduite en matière de paiement électronique[69].

67 Voir S. de Brouwer, «Un nouveau cadre juridique pour les paiements électroniques dans le marché intérieur», in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, p. 239.

68 Tout atout : Les nouvelles cartes de paiement, Communication de la Commission, COM (86) 754 final, 12 janvier 1987.

69 Recommandation 87/598/CEE de la Commission du 24 décembre 1987 portant sur un code européen de bonne conduite en matière de paiement électronique (Relations entre institutions financières, commerçants-prestataires de services et consommateurs), *J.O.C.E.*, L.365, 24 décembre 1987.

Une seconde recommandation du 17 novembre 1988 concernant les systèmes de paiement, et en particulier les relations entre titulaire et émetteur de cartes[70] propose un régime de répartition des risques entre émetteur et titulaire, et plus spécifiquement une limitation de la responsabilité du titulaire après la notification de la perte, du vol ou de la contrefaçon de sa carte à l'émetteur. C'est là un des principes de base de la législation belge que nous étudierons plus loin.

Une troisième recommandation prise en 1990[71] énonce certains principes et certaines règles en matière d'information à la clientèle et d'efficacité des exécutions des transferts.

43. Par après, vu le développement important des systèmes de paiement, la Commission européenne a décidé de mettre en place un système garantissant plus encore aux utilisateurs une confiance dans les instruments de paiement électroniques mis à leur disposition. La Commission était en effet consciente que le développement de ce mode de paiement devait se faire dans le respect des intérêts de toutes les parties, institutions émettrices, commerçants et utilisateurs. Elle a donc adopté une recommandation relative aux opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire en date du 30 juillet 1997[72].

Cette recommandation entend «contribuer à l'avènement de la société de l'information, en particulier du commerce électronique, en suscitant une plus grande confiance de la clientèle envers ses instruments et leur plus large acceptation par les commerçants»[73]. Concrètement, cette recommandation vise les opérations effectuées à partir d'un instrument de paiement électronique: transferts de fonds, retraits d'argent en liquide, accès au compte, opérations de chargement ou de déchargement d'instruments de monnaie électronique. Elle aborde la question de la transparence des conditions applicables aux opérations, ainsi que les obligations et responsabilités des parties. Cette recommandation a été largement traduite en droit belge par la LTEF.

44. Suite à ces premières initiatives, les autorités européennes ont ensuite adopté d'autres actes juridiques qui ont eu des implications plus concrètes dans

0 Recommandation 88/590/CEE de la Commission du 17 novembre 1988 concernant les systèmes de paiement et en particulier les relations entre titulaire et émetteur de cartes, *J.O.C.E.*, L.317, 24 novembre 1988.

1 Recommandation 90/109/CEE de la Commission du 14 février 1990 concernant la transparence des conditions de banque applicable aux transactions financières transfrontalières, *J.O.C.E.*, L.67, 15 mars 1990.

2 Recommandation 97/489/CE de la Commission du 30 juillet 1997 relative aux opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire, *J.O.C.E.*, L 208/52, 2 août 1997.
Considérant n° 4.

notre droit interne, comme la directive 97/5/CE[74] transposée par la loi belge du 9 janvier 2000 relative aux virements d'argent transfrontaliers[75] ou la directive européenne 97/7/CE modifiée par la directive 2002/65/CE concernant la protection des consommateurs en matière de contrat à distance[76] qui fixe, en son article 8, un régime particulier pour les paiements par carte pour les contrats à distance.

45. Par la suite, la Commission a adopté deux directives relatives à la monnaie électronique[77]. Il existe toutefois une proposition de directive du Parlement et du Conseil concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements qui abrogera l'une de ces deux directives. Cette proposition a été adoptée par le Parlement européen, en première lecture, le 24 avril 2009. Il faudra donc être attentif à l'actualité législative européenne dans les semaines à venir afin d'évaluer précisément les contours de cette future directive.

Enfin, pierre angulaire de la matière et déclencheur de la réforme qui s'annonce, la Commission a adopté en 2007 la directive relative aux services de paiement[78].

Dans la mesure où le projet de loi relatif aux services de paiement est une transposition fidèle de cette directive, hormis son titre II, nous renvoyons ici à l'analyse faite du projet de loi.

Section 2
L'objet de la transposition

46. La législation belge en matière de paiement électronique est le fruit de plusieurs modifications ponctuelles, mais surtout de transpositions, en droit interne, de normes européennes.

74 Directive 97/5/CE du Parlement européen et du Conseil, du 27 janvier 1997, concernant les virements transfrontaliers, *J.O.U.E.*, L. 43, 14 octobre 1997.

75 Loi du 9 janvier 2000 relative aux virements d'argent transfrontaliers, *M.B.*, 9 février 2000.

76 Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrat à distance, *J.O.C.E.*, L.144/9, du 4 juin 1997 et Directive 2000/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les Directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE, *J.O.C.E.*, L. 271/16, du 9 octobre 2002.

77 Directive 2000/28/CE du Parlement européen et du Conseil du 18 septembre 2000 modifiant la directive 2000/12/CE concernant l'accès à l'activité des établissements de crédit et son exercice et la Directive 2000/46/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, *J.O.C.E.*, L. 275/37, 27 octobre 2000.

78 Pour un commentaire précis de la directive: Y. LAUWERS et I. VANWEDDINGEN, « Toepassinggebied Richtlijn betreffende betalingsdiensten in de interne markt », *D.B.F.*, 2008/IV, pp. 312 et s.

D'abord, afin de transposer la directive « contrats à distance », la loi du 25 mai 1999[79] a modifié la loi sur les pratiques du commerce[80] (ci-après la LPCC) par l'actuel article 83*novies* pour reprendre le principe de partage de responsabilités entre l'émetteur et le titulaire d'un instrument de paiement[81].

Ensuite, et malgré l'absence de force juridiquement contraignante, la Belgique a décidé de mettre en œuvre les recommandations de la Commission du 30 juillet 1997 en adoptant la LTEF. Elle a ainsi, assez fidèlement, transposé les dispositions de cette recommandation dans l'ordre juridique interne afin d'assurer un degré élevé de protection des consommateurs dans l'utilisation des instruments de paiement électronique[82].

Enfin, la Belgique est en passe de transposer les dispositions prévues par la SPD.

47. Le législateur belge a décidé d'effectuer cette transposition par trois lois distinctes, chacune faisant application de certaines dispositions de la directive qui étaient suffisamment différentes pour ne pas justifier d'un traitement dans un acte législatif unique.

La LSP vise à transposer le volet relatif aux services de paiement.

Le volet de la directive SPD réglant le statut des institutions de paiement, l'accès à l'activité de prestataire de services de paiement et à l'accès aux systèmes de paiement est intégré dans un second projet de loi[83].

79 Loi du 25 mai 1999 modifiant la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur du 25 mai 1999, *M.B.*, 23 juin 1999, p. 23670.

80 Loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.*, 29 août 1991, p. 18712.

81 Pour un commentaire de cette loi, voir A. Salaün, « Transposition de la directive 'contrat à distance': analyse de la loi belge du 25/5/1999 », *J.T.*, 8 janvier 2000, p. 37.

82 Pour une analyse de cette loi, voy. entre autres: F. De Clippele et O. Goffard, « Qui va payer ? Ou questions quant à la responsabilité de l'émetteur de la carte en cas de transfert électronique de fonds », *J.T.*, 2004, p. 369; M. Demoulin, « Le paiement électronique », in *Obligations: commentaire pratique*, 2007, Vol. 2.; M. Gustin, « La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électroniques de fonds », in X, *Contrats à distance et protection du consommateur*, C.U.P., Bruxelles, Larcier, 2003, vol. n° 64, p. 183; Th. Lambert, « La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds », *R.D.C.*, 2003, p. 573; L. Rolin-Jacquemyns, « Régime juridique des paiements électroniques à la lumière de la nouvelle loi sur les opérations effectuées au moyen d'instruments de transfert électronique de fonds », *Ubiquité*, 2003/16, p. 9; A. Salaün, « Une nouvelle pierre à l'édifice de protection des consommateurs: la loi sur les instruments de transfert électroniques de fonds », *J.T.*, 2003, p. 205; R. Steennot, « De bescherming van de houder van instrument voor de elektronische overmaking van geldmiddelen », *Juristenkrant*, 2002, liv. 54, p. 67; R. Steennot, « Elektronisch betalen: eidelijk een wettelijke regeling! », *N.J.W.*, 2002, p. 82; J. Stuyck et T. Van Dyck, « Wet 17 juli 2002 betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen – Een kritische benadering van het begrippenkader en toepassingsgebied van de wet », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2002, p. 93.

83 Projet de loi relatif 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, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2182/01, pp. 92 et s.

Enfin, il y existe également un projet de loi modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers[84], et instaurant l'action en cessation des infractions à la loi relative aux services de paiement[85]. Ce troisième projet de loi transpose les dispositions finales du titre VI de la SPD.

48. La LSP a pour objectif de gagner la confiance des utilisateurs de services de paiement en leur offrant un haut degré de protection ainsi que des garanties liées à la sécurité, l'efficacité et le coût des paiements.

Dans cette mesure, elle prévoit des obligations dans le chef de chaque partie et un principe de partage des responsabilités entre les différents prestataires et les utilisateurs de services de paiement.

Des règles relatives au consentement et à l'exécution des opérations de paiement, en ce compris les délais d'exécution, sont également prévues, ainsi qu'un régime de plainte et de sanction.

En outre, la LSP vise à coordonner certaines matières jusqu'ici régies par des lois particulières, mais qui ont depuis lors été réglées par la directive. Les règles prévues par ces lois ont donc été intégrées dans la LSP et les lois en question seront par conséquent abrogées. Cela vise la LTEF, la loi du 15 mai 2007 concernant certains services bancaires, la loi du 10 juillet 1997 relative aux dates de valeur des opérations bancaires et la loi du 9 janvier 2000 relative aux virements d'argent et aux paiements transfrontaliers.

Section 3
Le champ d'application de la loi

§ 1. Le champ d'application matériel

A. Le champ d'application matériel général

49. La LSP a vocation à s'appliquer à tous les services de paiement qui sont fournis en euro ou dans la devise d'un État membre de la Communauté européenne en dehors de la zone euro[86], à un utilisateur de services de paiement par un prestataire de services de paiement tel que défini à l'article 2, 2°, sous réserve de ce qui est prévu à l'article 2, 2° *in fine*.

84 Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, *M.B.*, 4 septembre 2002.

85 Projet de loi 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 relatif aux services de paiement, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, 2183/01, pp. 8 et s.

86 Exception faite des prestations visées aux articles 36 et 37 de la LSP.

50. La loi énumère plusieurs types d'opérations qui peuvent être qualifiées de services de paiement.

Cette énumération est une transposition fidèle de celle contenue dans de l'annexe de la SPD à la seule différence que lorsque l'annexe de la directive parle de « *prélèvements, y compris de prélèvements autorisés unitairement* », la loi belge utilise le terme de « *domiciliations* ».

51. Selon la loi, un service de paiement pourra être toute activité professionnelle qui consiste à offrir un service permettant de verser[87] ou de retirer[88] des espèces sur un compte de paiement. Ces retraits et dépôts pourront avoir lieu au guichet, et le service de paiement ne sera alors pas électronique, ou via un distributeur ATM. En plus du dépôt et du retrait, sont également visées les « opérations qu'exige la gestion d'un compte de paiement », comme l'accès à distance en vue contrôler le solde du compte ou le fait de recevoir des extraits de compte[89].

52. Sont également considérées comme service de paiement, l'exécution de domiciliations[90], d'opérations de paiement par carte ou par un dispositif similaire, et l'exécution de virements[91] (en ce compris des ordres permanents de paiement).

Quant aux opérations de paiement, définies à l'article 2, 6° de la loi, les travaux préparatoires[92] en proposent une distinction selon la manière dont elles sont initiées. Cette distinction a tout son intérêt car nous verrons plus loin que les règles applicables peuvent différer selon cette catégorisation.

Aussi, une opération telle qu'un virement, un ordre permanent ou un retrait d'argent auprès d'un ATM est une opération initiée par le payeur. Une opération initiée par le bénéficiaire sera une domiciliation par laquelle le créancier prend l'initiative lui-même de transmettre un ordre de paiement à charge du payeur. Enfin, une opération peut être initiée par le payeur via le bénéficiaire

87 Article 2, 1°, a) de la LSP.

88 Article 2, 1°, b) de la LSP.

89 Cette opération était déjà visée dans la LTEF et plusieurs critiques avaient été émises à son égard. Voir notamment Th. LAMBERT, *op. cit.*, p. 574, n° 2.

90 La domiciliation est définie à l'article 2, 13° comme étant un service de paiement visant à débiter le compte de paiement d'un payeur, lorsqu'une opération de paiement est initiée par le bénéficiaire sur la base du consentement donné par le payeur au bénéficiaire, au prestataire de services de paiement du bénéficiaire ou au propre prestataire de services de paiement du payeur.

91 Les travaux préparatoires précisent que les virements comprennent également les « transferts automatiques d'argent » ou les « ordres permanents ». Voir Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 9.
Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 13.

lorsque, par exemple, le paiement d'un service ou d'un bien se fait par le titulaire d'une carte via le terminal du commerçant.

Ces trois types d'opérations (domiciliations, virements et paiements par carte) peuvent être des transferts de fonds réalisés sur un compte de paiement[93] ou dans le cadre d'un contrat de crédit accordé à l'utilisateur de ces services[94].

Notons que parmi ces opérations, les domiciliations bancaires et les virements ne seront pas nécessairement des opérations de paiement électronique, bien que le transfert de fonds puisse se faire de manière électronique ou non. Par contre, les opérations réalisées par carte seront dans tous les cas considérées comme des opérations de transfert électronique de fonds.

53. Les services liés à l'émission et/ou à l'acquisition d'instruments de paiement[95] sont également des services de paiement.

Dans ce cas, l'émetteur est – en principe – l'institution qui met une carte ou un autre instrument de paiement à disposition. Par contre, l'acquéreur n'est pas le titulaire de la carte, mais bien le prestataire de services de paiement qui se trouve dans la relation contractuelle avec le commerçant et qui lui règlera le paiement des opérations effectuées par des payeurs au moyen d'une carte.

Si l'émission et l'acquisition sont effectuées par le même prestataire, on sera dans un schéma à trois parties[96]. Si par contre, l'émetteur et l'acquéreur sont deux personnes distinctes, on sera dans un schéma de carte à quatre parties[97].

Une remarque doit néanmoins être faite quant à ce concept d'instrument de paiement.

Selon l'article 2, 10° de la nouvelle loi, un instrument de paiement est un dispositif personnalisé et/ou ensemble de procédures convenu entre l'utilisateur d'un service de paiement et le prestataire du service de paiement auquel l'utilisateur a recours pour initier un ordre de paiement.

Les travaux préparatoires précisent qu'il faut entendre par « dispositif personnalisé » les instruments techniques tels que les cartes ou téléphones portables. Les « procédures » sont, elles, des procédures de vérification dont l'utilisateur se servira pour donner des instructions à son prestataire de services, tels des codes d'identification personnel[98], des codes d'autorisation de l'opération[99], des *digipass*, des procédés de login/mot de passe, etc.

93 Article 2, 1°, c) de la LSP.

94 Article 2, 1°, d) de la LSP.

95 Article 2, 1°, e) de la LSP.

96 Ce sera le cas pour les prestataires American Express ou Diners Club.

97 Ce sera le cas avec les prestataires Mastercard et Visa.

98 Ou code PIN (Personal identification number).

99 Ou code TAN (Transaction Authentification number).

Notons toutefois que cette vérification n'a pas toujours lieu par une lecture électronique de l'instrument physique. Le meilleur exemple est celui du paiement par carte de crédit pour lequel une facturette est délivrée, sans lecture électronique, ou encore lorsque le numéro et la date d'échéance de la carte de crédit sont transmis par téléphone[100].

54. Un autre service de paiement visé par la loi est la transmission de fonds. La transmission de fonds est définie à l'article 2, 14° de la LSP. Elle consiste pour un payeur, à transférer une somme à un prestataire de services de paiement, qui transmet le montant à un bénéficiaire ou à un autre prestataire de services de paiement agissant pour le compte du bénéficiaire[101]. La particularité de cette opération est que la réception des fonds se fait dans le seul but de les mettre à disposition ailleurs.

55. Enfin, est également visé comme un service de paiement, le Mobile-paiement.

Selon l'article 2, 1°, g), trois conditions doivent être réunies pour qu'un M-paiement soit considéré comme un service de paiement au sens de la loi.

Tout d'abord, il faut que le consentement du payeur à l'opération de paiement soit donné au moyen d'un dispositif de télécommunication, numérique ou informatique. Dans la pratique, ces services seront effectués au moyen d'un téléphone mobile ou d'un *Smartphone*. Le paiement sera donc, par essence, considéré comme un paiement électronique.

Deuxièmement, il faut que le paiement soit adressé à l'opérateur du système ou du réseau de télécommunication ou informatique.

Si donc un acheteur paie des biens ou services à un fournisseur en utilisant son téléphone portable, mais a recours à son opérateur de télécommunication uniquement pour transmettre l'ordre de paiement, qui sera exécuté à partir de son compte par son organisme bancaire ou par l'émetteur de sa carte de crédit, il n'y a aucun paiement transféré à l'opérateur. On ne sera donc pas face à un service de paiement au sens de la LSP. Par conséquent, le troisième mode de M-paiement décrit au n° 23 ne sera pas soumis aux dispositions de la LSP.

Troisièmement, la LSP, traduisant en cela la volonté du législateur européen, exige que ce service de paiement n'implique l'intervention de l'opérateur de télécommunication qu'en qualité d'intermédiaire.

[100] Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 15.

[101] Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 17.

Dès lors, ce n'est que lorsque l'opérateur n'ajoute aucune valeur intrinsèque aux biens ou services achetés au moyen du dispositif de télécommunication qu'il devrait être considéré comme un prestataire de services de paiement.

Sortent donc de cette notion de service de paiement les activités commerciales consistant, pour un opérateur, à fournir à ses abonnés des biens et des services numériques (tels que des sonneries téléphoniques, de la musique ou des journaux numériques) en plus des services de télécommunication auxquels ils ont souscrits[102].

La loi n'a en effet pas pour but de réglementer les activités commerciales consistant, pour les opérateurs de systèmes ou de réseaux de télécommunication ou informatiques, à fournir des biens et des services numériques.

B. Les exclusions du champ d'application matériel

56. La LSP exclut de son champ d'application quinze types d'opérations.

Ces opérations peuvent être regroupées en six catégories différentes.

57. Sont tout d'abord exclues du champ d'application de la loi, les opérations qui ne nécessitent aucun traitement électronique pour l'exécution du service de paiement[103].

Tel sera le cas des opérations de paiement effectuées exclusivement en espèces entre le payeur et le bénéficiaire ou des activités de change « espèce contre espèces ».

Sont également exclues les opérations de paiement qui pourront être réalisées par voie électronique, mais qui sont initiées au départ d'un document papier[104].

[102] Selon le considérant n° 6 de la SPD : « En outre, il convient de distinguer le cas où des moyens sont offerts par les opérateurs de systèmes ou de réseaux de télécommunication ou informatiques en vue de faciliter l'achat de biens ou de services numériques tels que des sonneries téléphoniques, de la musique ou des journaux sous format numérique venant s'ajouter aux services vocaux traditionnels et à la distribution de ceux-ci vers des appareils numériques. Le contenu de ces biens ou services peut être produit par un tiers ou par l'opérateur même, qui peut leur ajouter une valeur intrinsèque sous la forme de systèmes d'accès, de distribution ou de recherche. Dans ce dernier cas, lorsque les biens ou services sont distribués par un de ces opérateurs ou, pour des raisons techniques, par un tiers, et ne peuvent être utilisés que par le biais d'appareils numériques, tels qu'un téléphone mobile ou un ordinateur, ledit cadre juridique ne devrait pas s'appliquer, étant donné que l'activité de l'opérateur va au-delà d'une simple opération de paiement. Toutefois, il convient que ledit cadre juridique s'applique aux cas où l'opérateur agit seulement en qualité d'intermédiaire permettant simplement l'exécution du paiement à un fournisseur tiers ».

[103] Voir l'article 4, 1°, 3°, 4°, et 6° de la LSP.

[104] Article 4, 7° de la LSP.

58. Conformément à l'article 2, 2°, les services de paiement qui sont exécutés par une personne physique ou morale autre qu'un prestataire au sens de la loi sont exclus de son champ d'application.

Tel est le cas des opérations de paiement exécutées par un agent commercial dans le cadre de son activité habituelle[105], agissant au nom d'un utilisateur. Par contre, l'agent qui agit au nom et pour le compte d'un prestataire de services de paiement effectuera des services qui seront qualifiés au sens de la loi de «services de paiement».

Pour la même raison, les opérations de paiement au sein d'un même groupe, sans l'intervention d'un prestataire, ne tombent pas sous le coup de la loi[106].

De même, tout service de cash-back sort du champ d'application de la loi[107]. Le cash-back a lieu lors d'un paiement effectué au moyen d'un instrument de paiement, dont le montant payé est, à la demande du payeur, plus élevé que celui qui est dû. La différence entre le montant payé et le montant dû est alors remise en argent comptant au payeur par le commerçant, bénéficiaire du paiement effectué.

Enfin, on peut souligner que la prestation de service rendant possible les retraits d'espèces au moyen de distributeurs automatiques de billets indépendants est également exclue du champ d'application[108]. L'exception visée sous ce point concerne uniquement les services fournis par les prestataires de services indépendants, c'est-à-dire ceux qui n'offrent aucun service de paiement au sens de l'article 2,1° ou qui ne sont pas dans une relation contractuelle avec le titulaire de la carte utilisée pour le retrait. Lorsque le fournisseur de distributeurs automatiques de billets est soit émetteur de cartes soit fournisseur d'autres services de paiement, il retombe dans le champ d'application.

59. Les opérations qui sortent de la relation directe entre un prestataire et un utilisateur de services de paiement sont également exclues du champ d'application de la loi[109].

60. La loi exclut de même les opérations de paiement liées aux services d'actifs et de titres, y compris la distribution de dividendes, de revenus ou autres, et les services fournis par des prestataires techniques à l'appui de la fourniture de services de paiement[110].

5 Article 4, 2° de la LSP.
Article 4, 14° de la LSP.
Article 4, 5° de la LSP.
Article 4, 15° de la LSP.
Articles 4, 8° et 4, 13° de la LSP.
Article 4, 9° et 10° de la LSP.

61. Les dispositions de la loi ne s'appliqueront pas non plus aux services de paiement et opérations effectuées à l'aide d'instruments de paiement qui présentent un usage restreint[111].

L'usage restreint est établi, au sens de la loi, lorsque deux conditions sont réunies. La première condition pour que l'on puisse parler d'usage restreint est que l'instrument de paiement ne puisse être utilisé que dans les locaux de l'émetteur de l'instrument[112], à l'intérieur d'un réseau limité de prestataires de services[113], ou encore pour un éventail limité de biens ou de services[114]. Par ailleurs, il faut que cet instrument de paiement ne soit pas lié à un contrat de crédit[115] ou, s'il s'agit d'un instrument rechargeable de type porte-monnaie électronique, qu'aucun accès direct au compte de paiement servant au chargement et au déchargement ne soit possible à l'aide de cet instrument.

62. Enfin, comme cela ressort de la définition même de «services de paiement», la loi exclut de son champ d'application les opérations de M-paiement dans lesquelles l'opérateur n'agit pas uniquement comme intermédiaire. Ce sera le cas lorsque les biens ou services sont fournis par l'opérateur lui-même (par exemple une sonnerie de GSM) ou pour tout autre service de base de «téléphonie mobile», comme un répondeur, un message textuel ou un SMS.

§ 2. Le champ d'application personnel

63. La LSP a défini un champ d'application stricte des personnes physiques ou morales impliquées dans les opérations de services de paiement.

111 Article 4, 11° de la LSP.

112 Par exemple les cartes de magasin (*«storecards»*) qui peuvent uniquement être utilisées pour les paiements dans un magasin spécifique ou les bons cadeaux qui sont distribués par un commerçant individuel pour acquérir des biens uniquement dans son commerce.

113 Par exemple une carte essence qui peut être utilisée auprès d'une chaine de stations-services déterminées ou les cartes de magasin qui peuvent être utilisées pour les paiements dans une chaîne de magasins. Attention, les cartes qui peuvent être utilisées pour les achats auprès de commerçants qui sont sur une liste (par exemple les «bons-cadeaux» pouvant être utilisés dans une vaste liste de participants) ne tombent pas dans l'exemption puisque ces cartes sont spécialement conçues pour un réseau ouvert de fournisseurs, lequel ne pourrait plus être considéré comme «limité».

114 Comme les chèques-repas ou les titres-services.

115 Telle une carte de magasin dont l'utilisation est liée directement ou indirectement à un contrat de crédit, proposée le cas échéant par le vendeur qui est intermédiaire de crédit ou prêteur, comme pour la carte Amex de SN Airlines.

A. Les prestataires de service de paiement

64. Il faut tout d'abord définir celui qui peut être prestataire de services de paiement et qui est, dès lors, susceptible d'offrir en vente les services tels que définis ci-dessus.

65. Selon l'article 2, 2°, le prestataire de service de paiement est toute personne morale qui fournit des services de paiement à un utilisateur de services de paiement et qui répond aux caractéristiques d'un établissement de crédit établi en Belgique[116] (ou constitué conformément au droit d'un autre État membre de l'EEE) ou d'un établissement de monnaie électronique établi en Belgique[117] (ou constitué conformément au droit d'un autre État membre de l'EEE).

Peut également être qualifié de prestataire de services de paiement, un établissement de paiement habilité, conformément à la loi qui devrait être prise en vue de transposer le titre II de la SPD[118].

Enfin, La Poste, la BNB et la BCE, ainsi que les autorités fédérales, régionales et locales belges légalement habilitées, et pour autant qu'elles n'agissent pas en qualité d'autorité monétaire ou d'autorité publique, peuvent être considérées comme des prestataires de services de paiement. Lorsqu'ils exercent leurs tâches publiques, ces organismes n'entrent pas, en principe, dans le champ d'application de la loi. En revanche, lorsqu'ils interviennent sur base commerciale et offrent des services de paiement, ils doivent être considérés comme des prestataires de services de paiement puisqu'ils entrent en concurrence avec d'autres prestataires. Il va de soi que, dans ce cas, ils devront respecter les dispositions de la LSP dans leurs relations avec les utilisateurs.

Il est donc clair que les institutions qui n'offrent pas directement des services de paiement aux utilisateurs, par exemple les institutions intermédiaires mandatées par le prestataire de services de paiement du payeur pour transmettre les opérations de paiement au prestataire du bénéficiaire, ou des prestataires de services techniques, ne pourront être considérées comme des prestataires de services de paiement au sens de la loi.

66. Le champ d'application personnel de la loi va toutefois au-delà des prestataires tels que définis ci-dessus.

16 Établissement de crédit tel que visé par l'article 1er, alinéa 2, 1° de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit.

17 Établissement de monnaie électronique tel que visé par l'article 1er, alinéa 3, 2°, de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit.

8 Projet de loi relatif 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.

La loi précise en effet que toute personne morale qui offrirait des services de paiement sans pour autant répondre aux conditions pour être qualifiée tel, sera en tout état de cause soumise à toutes les dispositions impératives de la loi.

Le législateur a bien fait de choisir cette sanction plutôt que l'annulation de toutes les opérations que cette personne morale aurait effectuées. Une telle annulation aurait en effet été préjudiciable aux utilisateurs qui ont, de bonne foi, fait appel à ce prestataire non autorisé.

B. Les utilisateurs de services de paiement

67. L'utilisateur de services de paiement est la « personne physique ou morale qui utilise un service de paiement en qualité de payeur ou de bénéficiaire ou les deux »[119].

Il est donc utile de préciser qu'un payeur est la personne physique ou morale qui soit est titulaire d'un compte de paiement et autorise un ordre de paiement à partir de son compte, soit, en l'absence de compte de paiement, donne un ordre de paiement[120].

Le bénéficiaire, quant à lui, est la personne physique ou morale destinataire des fonds ayant fait l'objet d'une opération de paiement[121].

68. Deux remarques doivent être faites au sujet de ces définitions.

Tout d'abord, il s'avère que la LSP est, par principe, d'application pour tous les utilisateurs, tant les personnes physiques que morales alors que dans la LTEF, la notion de titulaire (d'un instrument électronique) était limitée aux personnes physiques.

De plus, l'utilisateur peut agir tant à des fins privées que professionnelles. Toutefois, il pourra être dérogé à certaines dispositions de la loi si l'utilisateur n'est pas un consommateur. À cet égard, il faut préciser que le consommateur[122] sera la personne physique qui agit dans un but autre que son activité commerciale ou professionnelle[123].

119 Article 2, 3° de la LSP.

120 Article 2, 4° de la LSP.

121 Article 2, 5° de la LSP.

122 Article 2, 28° de la LSP.

123 Quant à la portée des termes « but autre que son activité commerciale ou professionnelle », il semblerait que tant au niveau européen (voir CJCE: Shearson Lehman Hutton, HJEG, C-89/91, Rec. 1993, I-139: « consommateur final non engagé dans des activités commerciales ou professionnelles ») qu'au niveau national (voir article 1, 7° de la LPCC et article 1, 1° de la loi du 12 juin 1991 relative au crédit à la consommation) le service doit être utilisé « exclusivement » à des fins privées et l'utilisateur ne sera pas considéré comme consommateur en cas d'usage mixte, c'est-à-dire si le service est utilisé ou acquis à des fins principalement privées.

§ 3. Le champ d'application territorial

69. L'article 3 de la loi, transposant ainsi l'article 2 de la SPD, détermine les hypothèses d'application de la loi selon des critères de rattachement géographique. Trois critères devront être rencontrés.

70. À la lecture de l'article 3, § 1er, on peut dire que la loi sera applicable quand le prestataire de services de paiement du payeur et le prestataire de service de paiement du bénéficiaire seront tous deux situés dans l'Union européenne ou dans un État membre de l'EEE, ou bien lorsque l'unique prestataire de services de paiement intervenant dans l'opération de paiement est situé dans l'Union européenne ou dans un État membre de l'EEE.

Par exception à cette règle, les articles 48 et 61 seront d'application dès que l'un seulement des deux prestataires (lorsqu'il y en a deux) est établi en Belgique. De même, les articles 36 et 37 seront d'application si le prestataire de services de paiement du payeur est situé en Belgique.

Dans ces cas, la condition d'établissement est donc assouplie à l'un seulement des deux prestataires, mais la loi exige toutefois qu'il soit localisé en Belgique.

71. Deuxièmement, il faut que les services de paiement soient mis à disposition en Belgique. C'est là une application du principe du « droit du pays de destination » et des articles 5(2) ainsi que 37(2) et 42(7) (a) de la Convention de Rome.

Le critère en vertu duquel il peut être déterminé qu'un service de paiement est offert en Belgique devra être examiné *in concreto*. Il faudra établir que le prestataire de services souhaite, directement ou via un intermédiaire, engager une relation contractuelle avec des utilisateurs de services de paiement potentiels en Belgique. Tel sera le cas s'il développe ses activités commerciales en Belgique ou qu'il dirige de telles activités vers, entre autres, la Belgique, par exemple en formalisant ses offres de services par l'intermédiaire d'un site internet « .be ».

72. Enfin, le service de paiement doit, conformément à la directive, être exécuté à l'intérieur de l'Union européenne (« intracommunautaire »)[124].

Notons que la loi du 17 juillet 2002 ne limitait pas les obligations et le régime de responsabilité aux seules opérations intracommunautaires. Selon les travaux préparatoires toutefois, le but de la LSP est de rester applicable aux opérations de paiement non autorisées réalisées avec un instrument de paiement en dehors de l'Union européenne[125].

---

[124] Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 24.

[125] *Ibidem*.

Section 4
Les droits et obligations des intervenants

73. Ayant ainsi pu déterminer le champ d'application de la LSP, on comprend que les services de paiement sont des mécanismes complexes qui impliquent diverses opérations et obligations.

74. Nous analyserons dans cette section les droits et obligations des intervenants à un service de paiement.

Rappelons qu'à côté des parties au paiement – le payeur et le bénéficiaire – ce sont les prestataires de services qui sont parties prenantes au service de paiement. C'est en effet par l'intermédiaire de ces prestataires que le paiement sera exécuté et que le débiteur se libèrera de son obligation principale. C'est principalement sur la relation entre les prestataires et leur contractant, et les rapports juridiques qui en découlent, que la loi se concentre.

La loi énumère un nombre important d'obligations à charge des prestataires. Ils sont tenus d'une obligation d'information et responsables, selon les circonstances, de la bonne exécution des opérations de paiement qui ont été ordonnées et autorisées par le payeur. Des obligations annexes, à charge du payeur et du bénéficiaire sont également prévues par la loi.

§ 1. L'obligation d'information

75. On l'a dit, l'une des préoccupations du législateur européen, lors de l'élaboration de la SPD, mais également lorsqu'il a pris les diverses recommandations préalables mentionnées ci-dessus, a été la protection de l'utilisateur de services de paiement. Plus l'utilisateur est protégé, plus il aura confiance dans les instruments et les services mis à sa disposition, et mieux s'en portera le développement économique et commercial.

Savoir c'est s'armer. L'une des mesures de protection et de sécurité première pour l'utilisateur est de lui assurer les moyens nécessaires pour qu'il sache ce à quoi il s'engage. La transparence des conditions contractuelles qui lui seront applicables est donc primordiale. Par ailleurs, en recevant des informations claires, d'un même niveau élevé, sur les services de paiement auxquels il souhaite souscrire, l'utilisateur pourra réaliser un choix éclairé et comparatif entre les services de différents prestataires et ce, au bénéfice d'une concurrence saine et encadrée au sein de l'Union européenne.

C'est donc pour ces raisons qu'il est mit à charge des prestataires de service de paiement des exigences spécifiques en matière d'informations à fournir aux utilisateurs de services de paiement, qu'ils soient payeurs ou bénéficiaires.

76. Tant dans la LTEF que dans la SPD et dans la LSP, les règles en matière de transparence des conditions contractuelles et les exigences en matière d'informations forment un chapitre à part[126].

Ces règles constituent pourtant une obligation importante, et sévèrement sanctionnée, à charge des prestataires. C'est pourquoi il nous semble plus opportun de les présenter au titre des obligations légales des prestataires.

77. Notons toutefois, avant d'entamer un examen approfondi, que les obligations en matière d'informations énumérées par la loi ne doivent pas porter préjudice à l'application des dispositions particulières en matière d'informations relatives au crédit à la consommation[127]. Il faudra donc garder à l'esprit que la LSP est la *lex generalis* et que la loi relative au crédit à la consommation[128] est la *lex specialis*.

78. À titre de préambule, notons que les informations que la loi énumère sont des informations de base obligatoires.

Par conséquent, les parties ne peuvent y renoncer, sauf si l'utilisateur n'est pas un consommateur[129], et il appartiendra toujours au prestataire de prouver l'accomplissement de son obligation d'information[130].

Pour consacrer ces obligations en principe, la loi précise également que les informations doivent être communiquées gratuitement. Des frais seront toutefois possibles si les parties conviennent d'informations supplémentaires, plus fréquentes ou transmises par d'autres moyens de communication que ceux initialement prévus[131].

A. Le contenu de l'obligation d'information

79. Les informations que doit communiquer le prestataire[132] concerneront tant le contrat de service de paiement lui-même que l'opération de paiement, qu'elle soit qualifiée d'individuelle ou d'isolée. Elles varieront selon le moment où elles doivent être communiquées.

26 Ici le Titre II de la LSP.
27 Article 5, al. 2 de la LSP.
28 Loi du 12 juin 1991 relative au crédit à la consommation, *M.B.*, 9 juillet 1991.
29 Article 27 de la LSP.
30 Article 26 de la LSP.
31 Article 25 de la LSP.
32 Entendez par « prestataire » dans la suite du texte « prestataire de services de paiement ».

1. *Les informations relatives au contrat-cadre*

80. Les contrats-cadres[133], par exemple un contrat de gestion de compte de paiement ou un contrat de mise à disposition et d'utilisation d'un instrument de paiement, et les opérations de paiement qui en découlent sont plus fréquents et d'une importance économique plus grande que les opérations de paiement isolées. Les obligations d'information qui s'y appliquent sont dès lors beaucoup plus globales et plus sévères.

a. Les informations et conditions précontractuelles

81. Avant que l'utilisateur de service ne soit lié par un contrat-cadre ou une offre, son prestataire aura dû lui communiquer, selon les modalités précisées ci-dessous[134], un certain nombre d'informations que la loi répertorie selon sept types.

82. En premier lieu, le prestataire doit communiquer à son futur contractant des informations d'identification le concernant et les coordonnées de l'autorité de contrôle prudentielle par laquelle il est agréé, ainsi que les moyens d'identification au sein de cette autorité[135].

83. Le prestataire devra également fournir à l'utilisateur des informations relatives au service de paiement proposé[136].

Plusieurs types de renseignements permettront à l'utilisateur de se faire une idée correcte de ce service.

Le prestataire devra tout d'abord décrire les principales caractéristiques du service, et si le service est lié à un instrument de paiement, il devra lui décrire cet instrument et lui indiquer ses utilisations possibles[137].

Il devra ainsi lui indiquer les caractéristiques et exigences techniques minimales de l'équipement de communication que l'utilisateur peut utiliser[138], le territoire sur lequel l'instrument peut être utilisé, les supports techniques auxquels l'utilisateur pourra faire appel, la liste des supports agréés, les ordinateurs

133 La définition à l'article 2, 16° de la LSP est « contrat de services de paiement qui régit l'exécution future d'opérations de paiement particulières et successives et peut énoncer les obligations et les conditions liées à l'ouverture d'un compte de paiement ».
134 Voir n^{os} 109 et s.
135 Article 14, 1°, a et b de la LSP.
136 Article 14, 2° de la LSP.
137 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 40.
138 L'utilisateur doit par exemple être informé clairement que lors d'un paiement en ligne sur l'internet ou d'un paiement au moyen de la fonction « wap » sur un téléphone mobile, le paiement ne peut pas être effectué sur certains appareils non compatibles avec l'équipement de communication de l'émetteur

et modems répondant aux exigences techniques et de sécurité fixées par le l'émetteur de l'instrument,...

Il devra également décrire les différentes opérations qui peuvent être effectuées au moyen de l'instrument et, s'il s'agit d'un instrument de paiement rechargeable, la durée de validité et la destination du solde restant à l'issue de cette période de validité.

Le prestataire devra indiquer à l'utilisateur les données précises ou l'identifiant[139] qu'il devra fournir pour l'exécution d'un ordre de paiement et le moment de la réception de l'ordre de paiement ainsi que le délai d'exécution maximal au cours duquel il s'engage à effectuer le service de paiement.

Le prestataire devra aussi indiquer à l'utilisateur la forme et la procédure à suivre pour qu'il puisse donner ou retirer son consentement à l'exécution d'un paiement.

84. Le prestataire doit préciser, avant la conclusion du contrat, les frais payables par l'utilisateur, les taux d'intérêt et les taux de change. Les parties doivent par ailleurs avoir convenu de l'application immédiate, ou non, des modifications des taux de change ou taux d'intérêt[140].

85. En ce qui concerne la communication entre parties[141], il est prévu par la loi que le prestataire informe clairement son contractant des moyens de communication et des exigences techniques qui devront être applicables à l'équipement, des modalités et de la fréquence selon lesquelles les informations seront fournies ou mises à disposition, ainsi que du droit de l'utilisateur de recevoir les informations précontractuelles sur support papier ou autre support durable[142].

86. Le prestataire devra également informer l'utilisateur de mesures de protection et de mesures correctives[143].

Il devra lui indiquer quand et comment lui notifier les opérations de paiement non autorisées ou mal exécutées, lui décrire les principes qui mènent à sa responsabilité lors de l'exécution d'opérations de paiement[144], voire d'opérations de paiement non autorisées[145] et les conditions du remboursement[146].

En outre, s'il est fait usage d'un instrument de paiement, le prestataire doit informer l'utilisateur des risques et des mesures de prudence qu'il doit prendre pour préserver la sécurité de cet instrument ainsi que des modalités de notification de la perte, du vol, du détournement ou de l'utilisation non autorisée de son instrument. L'utilisateur devra par ailleurs être informé de la responsabilité qui lui incombera avant cette notification, ou s'il n'est pas parvenu à préserver la sécurité de son instrument[147]. Les parties peuvent par ailleurs prévoir, au bénéfice du prestataire, la possibilité de bloquer l'instrument de paiement dans certaines conditions qui doivent alors être clairement indiquées.

87. Le prestataire doit fournir des informations concernant le droit applicable au contrat et la juridiction compétente, ainsi que les voies de réclamation et de recours extrajudiciaires ouvertes à l'utilisateur.

88. Enfin, concernant la vie du contrat, il faudra indiquer à l'utilisateur la durée du contrat-cadre, son droit de résiliation et, s'il en est convenu ainsi, le fait que l'utilisateur est réputé avoir accepté toute modification des conditions contractuelles qui lui aurait été proposée, à moins d'avoir notifié son opposition avant la date proposée pour l'entrée en vigueur de cette modification.

b. Les informations à communiquer en cours de contrat

89. À tout moment pendant le contrat, l'utilisateur a le droit de recevoir, sur demande, les termes contractuels et les informations précontractuelles[148].

Il pourra ainsi toujours disposer des informations nécessaires pour comparer les services et les conditions de son prestataire avec ceux d'autres prestataires, et vérifier ses droits et obligations contractuels en cas de litige éventuel.

90. De plus, le prestataire est soumis à une obligation d'information spécifique en cours de contrat.

Selon l'article 30, § 2, si le prestataire est amené à bloquer un instrument de paiement, il doit informer le payeur du blocage de l'instrument de paiement et des raisons qui le justifient avant que l'instrument ne soit bloqué, ou immédiatement après. Des situations préjudiciables pourraient en effet naître du blocage

139 L'identifiant unique est, selon l'article 2, 12° de la LSP la « combinaison de lettres, de chiffres ou de symboles indiquée à l'utilisateur de services de paiement par le prestataire de services de paiement, que l'utilisateur de services de paiement doit fournir pour permettre l'identification certaine de l'autre utilisateur de services de paiement et/ou de son compte de paiement pour une opération de paiement ». L'identifiant unique sera par exemple un numéro de compte, éventuellement sous sa forme internationale (IBAN), qui peut être lié au code d'identification bancaire (BIC) si ce dernier est exigé comme condition d'identification. D'autres moyens sont possibles, pour autant qu'ils soient uniques et qu'ils permettent d'identifier de manière certaine, pour une opération donnée, un bénéficiaire et son compte de paiement.

140 Article 14, 3° de la LSP.

141 Article 14, 4° de la LSP.

142 Voir n° 113.

143 Article 14, 5° de la LSP.

144 Comme prévu aux articles 50 à 52 de la LSP.

145 Comme prévu à l'article 36 de la LSP.

146 Conformément aux articles 38 et 39 de la LSP.

147 Conformément à l'article 37 de la LSP.

148 Article 15 de la LSP.

de la carte pour l'utilisateur, situations qu'il pourra éviter s'il en a été préalablement informé.

Cette obligation d'information joue toutefois sans préjudice de l'article 59, § 3 de la loi relative au crédit à la consommation, et n'est pas requise, dit l'article 30, § 2, « si elle est contrecarrée par des raisons de sécurité objectivement motivées ou interdite en vertu d'une autre législation applicable ».

c. La modification des conditions contractuelles et la résiliation

91. Au cas où les parties en auraient convenu ainsi[149], le prestataire qui souhaite modifier les conditions contractuelles doit rappeler à l'utilisateur qu'il est réputé accepter cette modification s'il n'a pas exprimé son opposition avant la date d'entrée en vigueur proposée, et qu'il a le droit de résilier le contrat-cadre immédiatement et sans frais.

Cette modification du contrat-cadre ou des informations et conditions précontractuelles doit être proposée par le prestataire de services au plus tard deux mois avant la date proposée pour son entrée en vigueur.

Cette disposition est dérogatoire à l'article 32, § 9 de la LPCC selon lequel est réputée abusive, à l'égard du consommateur, une clause « qui autorise le vendeur à rompre ou modifier le contrat unilatéralement sans dédommagement pour le consommateur ». Toutefois, les droits d'opposition et de résiliation *ad nutum* reconnus à l'utilisateur sont sensés le protéger contre toute modification unilatérale, proposée ou imposée, et contrebalancer cette dérogation au droit commun.

Si par contre, par la modification proposée, de nouveaux services s'ajoutent au contrat-cadre initial, par exemple la mise à disposition d'une carte de paiement en combinaison avec le compte de paiement existant, il s'agira alors d'un contrat complémentaire auquel les obligations d'information préalable doivent s'appliquer.

Par dérogation, les modifications des taux d'intérêt ou de change peuvent s'appliquer immédiatement et sans préavis, à condition que le contrat-cadre le prévoie.

92. Afin de faciliter la mobilité des clients, ce qui est un facteur important dans l'effort visant à favoriser la concurrence, il est reconnu à l'utilisateur un droit légal de résiliation. Cette résiliation peut avoir lieu sans frais et avec effet immédiat, sauf si un délai de préavis, d'au maximum un mois, a été convenu.

9 Article 16 de la LSP.

Le prestataire de services de paiement peut lui, uniquement si le contrat-cadre le prévoit expressément, résilier le contrat-cadre conclu pour une durée indéterminée, moyennant un préavis d'au moins deux mois et selon des modalités strictes[150].

En cas de résiliation, l'article 17, § 2 règle la question du remboursement des frais, du solde positif du compte, des intérêts et des frais de gestion.

2. *Les informations relatives à un paiement individuel ou à un paiement isolé*

93. Les opérations de paiement individuelles sont les opérations de paiement qui relèvent du contrat-cadre.

Elles sont donc encadrées par le contrat conclu entre le prestataire et son utilisateur. Si l'utilisateur est certes déjà informé du cadre contractuel général, il n'empêche que, lors de l'exécution d'une opération individuelle, des informations spécifiques à cette opération devront lui être communiquées par les prestataires avant et après la transaction.

94. Les opérations de paiement isolées ne sont, elles, pas couvertes par un contrat-cadre. À la lecture des travaux préparatoires, il apparait que pour que l'on puisse parler d'opération de paiement isolée, il faut de surcroit qu'aucune opération de même nature que l'opération de paiement isolée ne soit ultérieurement convenue entre les parties par un contrat-cadre. Dans la pratique, ces opérations visent notamment les transmissions de fonds et certains modèles de services de paiement de factures.

95. Ces deux types d'opérations ressortent donc de contextes fondamentalement différents, même si elles peuvent être de même nature. Les informations qui doivent être communiquées par les prestataires, dans un cas comme dans l'autre, sont donc fort similaires.

Dans ces deux hypothèses, les informations sont fonction du moment auquel elles doivent être communiquées.

a. Les informations préalables à l'exécution de la transaction de paiement

96. Dans le cas d'un paiement isolé, avant que l'utilisateur ne se soit engagé vis-à-vis du prestataire, celui-ci doit mettre à disposition certaines informations[151].

150 Voir n[os] 111 et s.

151 Article 9 de la LSP.

Ces informations sont relatives, à tout le moins[152], aux données précises que l'utilisateur devra fournir pour l'exécution correcte de son ordre de paiement, au délai d'exécution maximale dans lequel le service de paiement sera fourni, aux frais, éventuellement ventilés et, le cas échéant, au taux de change qui sera appliqué.

97. Dans l'hypothèse d'un paiement individuel, le prestataire doit, à la demande du payeur et préalablement à l'exécution de l'opération, fournir expressément des informations relatives au délai d'exécution maximal et aux frais devant être payés, éventuellement ventilés[153].

98. Les différences entre les informations à communiquer préalablement à une opération de paiement, qu'elle soit individuelle ou isolée, sont donc ténues. Les informations à communiquer avant un paiement individuel le seront à la demande du payeur seulement. En outre, les données nécessaires à la bonne exécution du paiement et le taux de change sont des informations qui auront déjà dû lui être communiquées si son opération s'inscrit dans une relation gérée par un contrat-cadre[154].

b. Les informations subséquentes

99. Le principe de protection des utilisateurs veut que les opérations de paiement soient transparentes pour que le payeur ait une vue claire des frais qui y sont liés.

100. Qu'elles soient relatives à des opérations de paiement isolées ou individuelles, la loi énumère des informations qui doivent être communiquées par le prestataire de service de paiement du payeur au payeur et par le prestataire du bénéficiaire au bénéficiaire.

Ces informations sont fonction du moment de leur communication. Ainsi, le prestataire du payeur devra communiquer certaines informations au payeur immédiatement après avoir reçu l'ordre de paiement lorsqu'il s'agit d'un paiement isolé[155] ou, s'il s'agit d'une opération individuelle, après que le montant du paiement individuel ait été débité de son compte ou après réception de l'ordre de paiement[156].

2 Article 9, § 2 de la LSP.
3 Article 18 de la LSP.
4 Article 14 de la LSP.
5 Article 10, al. 1er de la LSP.
6 Article 19, al. 1er de la LSP.

Quant aux informations à fournir au bénéficiaire, son prestataire devra les lui communiquer immédiatement après l'exécution d'un paiement isolé[157] ou, pour un paiement individuel, simplement après son exécution[158].

101. Ici encore le contenu des informations est quasi similaire pour les paiements isolés et pour les paiements individuels.

Ainsi, il faudra que les prestataires communiquent une référence permettant d'une part au payeur[159] et d'autre part au bénéficiaire[160] d'identifier l'opération et « le cas échéant » les informations relatives au bénéficiaire ou celles relatives au payeur. La loi rajoute, au bénéfice du bénéficiaire, « la communication de toute information transmise avec, ou lors de, l'opération de paiement ».

Dans l'hypothèse d'une opération isolée comme dans celle d'une opération individuelle, le payeur devra être informé du montant de l'opération dans la devise utilisée dans l'ordre de paiement ou, mais pour une opération individuelle seulement, dans la devise dans laquelle son compte sera débité[161]. Cette information devra être donnée au bénéficiaire dans la devise dans laquelle les fonds seront mis à sa disposition ou encore, pour l'opération de paiement individuelle, dans la devise dans laquelle son compte sera crédité[162].

Dans les deux cas, les prestataires devront également indiquer au payeur et au bénéficiaire le montant des frais qui leur sont respectivement imputables, éventuellement ventilés[163]. Pour le paiement individuel, il est en plus prévu que l'intérêt dû par le payeur ou par le bénéficiaire doit être spécifié[164].

Doivent également être communiqués au payeur, qu'on soit face à une opération individuelle ou isolée, le taux de change appliqué par le prestataire du payeur et le montant de l'opération après cette conversion[165]. Le taux appliqué par le prestataire du bénéficiaire, ainsi que le montant de l'opération avant cette conversion, doivent être communiqués au bénéficiaire[166].

Enfin, pour les opérations de paiement isolées, le prestataire de services du payeur lui communiquera la date de réception de l'ordre de paiement et le prestataire du bénéficiaire lui communiquera la date de valeur du crédit[167].

157 Article 11, al. 1er de la LSP.
158 Article 20, al. 1er de la LSP.
159 Articles 10, 1° et 19, 1° de la LSP.
160 Articles 11, 1° et 20, 1° de la LSP
161 Articles 10, 2° et 19, 2° de la LSP.
162 Articles 11, 2° et 20, 2° de la LSP.
163 Articles 10, 3° et 11, 3° de la LSP.
164 Articles 19, 3° et 20, 3° de la LSP.
165 Articles 10, 4° et 19, 4° de la LSP.
166 Articles 11, 4° et 20, 4° de la LSP.
167 Articles 10, 5° et 11, 5° de la LSP.

Lorsque l'opération est dite individuelle, le prestataire du payeur pourra également transmettre à son contractant la date de réception de l'ordre de paiement[168].

3. *Les informations relatives aux opérations de paiement réalisées avec des instruments de paiement de faibles montants*

102. La loi établit un régime dérogatoire aux obligations d'information énumérées ci-dessus pour les instruments de paiement qui ne peuvent être utilisés que pour des opérations de paiement n'excédant pas 30 euros unitairement ou qui, soit ont une limite de dépenses de 150 euros, soit stockent des fonds dont le montant n'excède à aucun moment 150 euros.

Ces instruments, que nous appellerons «instruments de paiement de faibles montants» doivent, selon la SPD[169], constituer des moyens simples et peu onéreux de régler des biens et des services de faible prix. Ils ne peuvent dès lors impliquer, à charge des prestataires, des obligations d'information nécessitant un déploiement de lourds moyens. En outre, les risques que présentent ces instruments de paiement, en particulier prépayés, sont limités. Les exigences d'information qui leur sont applicables ne peuvent donc pas être excessives et doivent être limitées aux informations essentielles en tenant compte des capacités techniques que l'on est en droit d'attendre d'instruments spécialisés dans les paiements de faibles valeurs[170].

103. Ainsi, les informations préalables à la conclusion du contrat-cadre et aux opérations de paiement individuelles sont fortement nuancées. Il suffira en effet au prestataire de fournir au payeur des informations sur les principales caractéristiques du service de paiement, y compris la manière dont l'instrument peut être utilisé, les responsabilités, les frais et lui indiquer l'endroit où les autres informations et conditions préalables sont disponibles.

De plus, et si les parties en conviennent, il peut être prévu un système assoupli au bénéfice du prestataire en cas de modification des clauses contractuelles. Il peut également être prévu une diminution des informations à fournir après l'exécution d'une opération de paiement individuelle. Ce seuil minimal d'informations à communiquer peut encore être abaissé, sur accord des parties, lorsque l'instrument de paiement est utilisé de manière anonyme ou si le prestataire n'est techniquement pas en mesure de les fournir. Toutefois, le prestataire devra toujours permettre au payeur de vérifier le montant des fonds stockés.

[168] Article 19, 5° de la LSP.

[169] Considérant n° 30.

[170] Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 52.

Gardons néanmoins à l'esprit que si l'instrument de paiement est «multifonctionnel» ou «hybride» (carte de paiement avec fonction proton), différents régimes peuvent être applicables simultanément.

B. Les modalités de communication des informations

104. Les modalités de communication des informations sont fonction du contenu et de l'importance de ces informations.

Ainsi, les modalités de communication des informations relatives à une opération de paiement isolée seront moins strictes que les modalités de communication des informations à fournir avant la conclusion d'un contrat-cadre ou celles à communiquer après l'exécution d'une opération de paiement individuelle. En outre, des modalités plus souples sont d'application pour les instruments de paiement de faibles montants.

105. En ce qui concerne le mode de communication, on verra que, selon les cas, l'information doit être communiquée par le prestataire seulement à la demande de l'utilisateur, ou spontanément.

Dans certains cas, le prestataire pourra être tenu de fournir l'information, c'est-à-dire de la communiquer activement, et dans d'autres, il ne sera tenu que de mettre passivement les informations à la disposition de l'utilisateur. Celui-ci devra alors prendre activement des mesures afin d'obtenir les informations, par exemple en adressant une demande explicite à son prestataire, en consultant son compte bancaire en ligne, ou en se procurant lui-même ses extraits de compte.

1. *Les modalités de communication strictes*

106. Les informations précontractuelles, la proposition de modification du contrat ou des informations précontractuelles, la résiliation du contrat par le prestataire, ainsi que les informations qui doivent être communiquées après la réalisation d'une opération de paiement individuelle revêtent une importance telle qu'il ne peut y avoir de doute quant à leur prise de connaissance par l'utilisateur.

107. Dans ces situations, le prestataire doit *fournir* les informations activement.

Cette communication doit se faire sur un support papier ou sur un autre support durable[171].

[171] L'article 2, 22° de la LSP définit le support durable 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

Selon le considérant n° 24 de la SPD, les supports durables sont les extraits imprimés par les automates bancaires, les disquettes, les CD-ROM, les DVD, les disques durs d'ordinateurs personnels sur lesquels le courrier électronique peut être stocké, ainsi que les sites internet à condition qu'ils puissent être consultés ultérieurement pendant une période adaptée aux fins auxquelles les informations sont destinées et qu'ils permettent la reproduction à l'identique des informations stockées[172].

108. Ces informations devront être formulées dans des «termes aisément compréhensibles et sous une forme claire et intelligible, dans la langue de la région linguistique dans lequel le service de paiement est offert ou dans toute autre langue convenue par les parties».

109. Quant au moment de la communication, les modifications au contrat-cadre et l'avis de résiliation doivent parvenir à l'utilisateur au moins deux mois avant l'événement qu'elles annoncent.

Les informations relatives à une opération de paiement individuelle doivent parvenir au payeur «sans tarder» après que son compte ait été débité ou après réception de l'ordre de paiement, et au bénéficiaire, «sans tarder» après l'exécution de l'opération de paiement.

Quant aux informations et conditions précontractuelles, celles-ci doivent être communiquées «en temps utile» avant que l'utilisateur ne soit lié par un contrat ou par une offre. Toutefois, si le contrat-cadre est conclu à distance et que le prestataire ne peut communiquer les informations précontractuelles avant la signature du contrat, il lui sera autorisé de les communiquer immédiatement après la conclusion du contrat-cadre[173].

2. *Les modalités de communication assouplies*

110. Les informations relatives aux opérations de paiement individuelles doivent être communiquées selon les modalités décrites ci-dessus, mais dans des formes assouplies.

111. Premièrement, l'article 18 stipule que les informations relatives au délai d'exécution maximal et aux frais doivent être certes communiquées activement avant la transaction, mais à la demande du payeur seulement.

auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées».

172 Sur la notion de support durable, voir: M. DEMOULIN, «La notion de support durable dans les contrats à distance: une contrefaçon de l'écrit?», *R.E.D.C.*, 4/2000, p. 361.

173 Voir article 83*quinquies*, § 2 de la LPCC.

112. Deuxièmement, les articles 19, § 2 et 20, § 2 ouvrent la possibilité aux parties de convenir, dans le contrat-cadre les liant, que les informations postérieures à l'exécution du paiement peuvent être soit communiquées, soit mises à la disposition de l'utilisateur.

Cette communication ou mise à disposition doit être périodique, et tout au moins mensuelle. La périodicité des relevés doit en effet être suffisante pour permettre à l'utilisateur de suivre raisonnablement l'état de ses dépenses.

Il peut ainsi être convenu que, pour les opérations bancaires via internet, toutes les informations concernant le compte de paiement sont mises à disposition en ligne d'une manière permettant à l'utilisateur de les stocker et de les reproduire à l'identique.

3. *Les modalités de communication faibles*

113. Les informations et conditions précontractuelles qui doivent être communiquées avant un paiement isolé et les informations qui doivent être communiquées après l'ordre de paiement et après la transaction de paiement, répondent à des modalités de communication moins strictes.

114. En effet, ces informations doivent être communiquées passivement et donc uniquement mises à la disposition de l'utilisateur sous une forme aisément accessible. Selon les travaux préparatoires[174], comme le payeur est en général présent lorsqu'il donne un ordre de paiement isolé, il n'est pas nécessaire d'exiger que les informations lui soient fournies sur papier ou un autre support durable. Le prestataire de services peut tout à fait lui communiquer les informations verbalement au guichet ou les rendre aisément accessibles à un endroit apparent de l'établissement, de sorte que l'utilisateur puisse les consulter immédiatement et de manière permanente. Tel sera le cas si les conditions sont affichées sur un panneau d'information dans les locaux du prestataire, ou sur son site internet. Le prestataire devra néanmoins indiquer à l'utilisateur où il peut trouver des informations plus détaillées.

Sur demande de l'utilisateur, toutefois, le prestataire devra lui fournir ces informations et conditions sur un support papier ou sur un autre support durable.

115. Les mêmes exigences en termes de forme et de langue que celles pour les modalités de communication strictes sont d'application.

174 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 35.

116. Enfin, si la communication des informations doit avoir lieu avant que l'utilisateur ne soit engagé, encore le prestataire dispose-t-il, ici aussi, de la dérogation applicable en cas de contrats de services financiers conclus à distance.

4. *Les modalités de communication minimales*

117. La loi prévoit un régime particulier pour les instruments de paiement de faibles montants.

Le contrat-cadre qui règle les droits et obligations des parties en cas d'émission d'un tel instrument ne doit contenir qu'un nombre limité d'informations précontractuelles, le prestataire devant uniquement indiquer au payeur l'endroit où il pourra prendre connaissance des informations et conditions précontractuelles qui ne lui ont pas été activement communiquées.

De plus, si le prestataire souhaite modifier les conditions contractuelles, il ne sera pas tenu des conditions applicables à la procédure stricte.

§ 2. Les obligations spécifiques en cas d'utilisation d'un instrument de paiement

118. Le législateur a établi un traitement propre aux opérations de paiement effectuées au moyen d'un instrument de paiement.

Cette particularité nous appelle à nous y pencher spécifiquement et à analyser les obligations mises à charge des parties.

Notons toutefois que la loi[175] a prévu, tout comme pour l'obligation d'information, une application plus souple de certaines des obligations lorsqu'est utilisé un instrument de paiement de montants faibles.

A. Les obligations de sécurité

119. Le prestataire de services qui a émis au bénéfice de son contractant un instrument de paiement a, par là même, souscrit à des obligations spécifiques liées à cet instrument.

Tout d'abord, le prestataire doit s'assurer que les dispositifs de sécurité personnalisés[176] de l'instrument de paiement ne sont pas accessibles à d'autres qu'à son utilisateur. À cette fin, il devra garantir la confidentialité du numéro d'identification personnel ou de tout autre code d'identification de l'utilisateur. Il devra, entre autres, veiller à prendre les mesures utiles au sein de son entreprise

5 Article 57, § 1er de la LSP.

6 Voir n° 59.

afin de faire respecter cette obligation par son personnel[177] et veiller, lorsqu'il envoie l'instrument de paiement à son contractant, à ce que le code ne soit pas aisément violable par les tiers[178].

Il s'agit là d'une véritable obligation de résultat à charge du prestataire et il sera donc tenu pour entièrement responsable s'il n'a pas respecté cette obligation élémentaire de sécurité[179].

Le contenu et les modalités de cette obligation de sécurité ne sont toutefois pas précisées par la loi et il reviendra au juge d'en donner une appréciation *in concreto*.

120. Par ailleurs, l'utilisateur de l'instrument est également tenu à une obligation de sécurité et de « bonne utilisation ». Ces obligations ressortent de la lecture conjointe des articles 31, § 1er, 1° et § 2.

L'article 31, § 1, 1° stipule que l'utilisateur doit utiliser son instrument conformément aux conditions d'émission et d'utilisation qui lui auront été transmises avant la conclusion de son contrat. Il doit par ailleurs, en vertu du § 2, prendre toutes les mesures raisonnables afin de préserver la sécurité de l'instrument de paiement et de ses dispositifs de sécurité personnalisés.

Cela signifie qu'il doit faire preuve de prudence dans l'utilisation de son instrument. Ainsi, il ne peut noter son code PIN sous une forme aisément reconnaissable sur la carte elle-même ou sur tout objet qui serait conservé avec elle. Il ne doit pas non plus communiquer son numéro d'identification personnel à un tiers. Néanmoins, il peut, afin de réaliser une transaction par internet ou par téléphone, donner le numéro apparent de sa carte de paiement, ou un code d'identification qui s'y trouve inscrit, puisque ces indications ne seront aucunement considérées comme des dispositifs de sécurité personnalisés.

B. Les obligations en cas de blocage de la carte

121. Selon les termes du contrat liant le prestataire à l'utilisateur, il est envisageable que le prestataire se soit réservé le droit de pouvoir bloquer l'instrument de paiement[180].

Il peut agir de la sorte, dit la loi, pour des raisons « objectivement motivées » qui seraient liées à la sécurité de l'instrument, par exemple suite à des problèmes techniques ou de piratage informatique, ou parce qu'il existe des présomptions

177 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 62.

178 Article 32, 1° de la LSP.

179 Article 32, 5° de la LSP.

180 45.000 cartes sont ainsi bloquées par an en Belgique

d'utilisation non autorisée ou frauduleuse, ou encore si l'instrument a été remis dans le cadre d'un contrat de crédit et qu'il existe un risque accru que l'utilisateur soit dans l'incapacité de s'acquitter de ses paiements.

122. S'il procède à ce blocage, le prestataire sera tenu, si possible avant qu'il ait eu lieu ou immédiatement après, d'en informer le payeur et de lui en indiquer les raisons. Cette obligation de motivation peut toutefois être paralysée par toute autre législation applicable ou par des raisons de sécurité.

Dès que les motifs du blocage auront disparu, le prestataire aura l'obligation de débloquer l'instrument ou de le remplacer[181].

C. L'obligation de protection

123. Dans un but de gestion saine et de protection des utilisateurs, il est interdit à un prestataire d'envoyer à son contractant un instrument de paiement qu'il n'aurait pas sollicité. Cette interdiction ne jouit d'aucune dérogation même lorsque l'utilisateur n'est pas un consommateur. La loi va donc plus loin que la simple protection du consommateur et vise à protéger tout utilisateur quel qu'il soit.

Cette obligation de ne pas faire doit être considérée comme une obligation de résultat dont la violation impliquera automatiquement la mise en cause de la responsabilité du prestataire.

124. Elle jouit toutefois d'une exception, de bons sens, lorsque l'instrument envoyé l'est en remplacement d'un instrument échu, perdu ou volé.

D. Les obligations liées à la notification

125. Dès que l'utilisateur a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de son instrument de paiement[182], il doit en informer son prestataire de services[183]. Notons que la LTEF visait la perte, le vol ou l'utilisation non autorisée, et que la nouvelle loi y rajoute l'hypothèse du détournement qui pourra viser le *skimming*[184].

Selon les travaux préparatoires, la perte, le vol, le détournement ou l'utilisation non autorisée visent tant l'instrument de paiement lui-même que les moyens qui en permettent son utilisation, même lorsque l'utilisateur est encore en possession de l'instrument. On peut regretter que le législateur n'ait pas traduit, dans le texte de la loi, cette conception large des événements qu'il convient de notifier au prestataire.

La notification à charge de l'utilisateur doit se faire «sans délai» dès qu'il a connaissance de l'événement. Cette notion de temps est floue, et sera fonction de la lecture qu'aura le juge de la situation de fait[185]. Toutefois, l'utilisateur aura tout intérêt à effectuer cette notification au plus tôt, d'une part parce que le fait de tarder à procéder à cette notification pourra être considéré comme une négligence grave, d'autre part parce que c'est elle qui mettra fin à son obligation de supporter les risques liés à l'événement en question.

C'est en effet au moment où cette notification a lieu que la responsabilité des parties basculera des épaules de l'utilisateur à celles du prestataire.

126. Parce que cette notification, et son moment exact, revêtent donc une importance capitale dans le partage des responsabilités, il incombe au prestataire de fournir à l'utilisateur, titulaire de l'instrument, tous les moyens appropriés aptes à lui permettre de procéder à cette notification[186]. En d'autres termes, il doit mettre à sa disposition un système lui permettant de remplir son obligation de notification 24 heures sur 24 et 7 jours sur 7[187].

Le prestataire doit également fournir à l'utilisateur tous les moyens de prouver qu'il a bien procédé à cette notification et surtout le moment où elle a eu lieu. Ces moyens de preuve relatifs à la notification et à son moment exact ne seront toutefois fournis à l'utilisateur que s'il en fait la demande exprès. On peut supposer que tel sera le cas dans l'hypothèse où naît un litige entre le prestataire et l'utilisateur quant à leur responsabilité respective. On peut alors regretter que cette obligation de collaboration à la charge de la preuve soit limitée à une durée de 18 mois à compter de la notification. On peut en effet imaginer que le prestataire pourrait ne fournir aucune information à l'utilisateur sous prétexte qu'aucune notification n'a été faite depuis 18 mois, ce dont l'utilisateur ne pourra que très difficilement apporter la preuve du contraire puisque seul le prestataire a entre ses mains les moyens de preuve pertinents.

127. Notons que les parties auront pu déroger dans leur contrat-cadre à l'obligation de notification à charge de l'utilisateur et à l'obligation à charge du prestataire de lui fournir les dispositifs nécessaires si l'instrument ne permet le paiement que de faibles montants et si ses caractéristiques techniques ne

181 Article 30, § 2 de la LSP.

182 Voir Bruxelles, 15 mars 2007, *D.C.C.R.*, n° 77, p. 45: la Cour souligne qu'aucune notification n'a été faite par le titulaire d'une carte de crédit qui n'a pourtant été ni volée ni perdue, mais uniquement utilisée à son insu.

183 Article 32, § 1er, 2° de la LSP.

184 Voir n° 191.

185 Voir Bruxelles, 27 mai 2002, *R.D.C.* 2004/2, p. 158: selon la Cour, mais avant l'adoption de la LTEF, la notification un mois après la perte de la carte ne signifie pas la mauvaise foi du titulaire de la carte.

186 Article 32, 3° de la LSP.

187 Du style de «Cardstop».

permettent pas son blocage ou la prévention de son utilisation après que l'utilisateur ait procédé à la notification[188]. Dans ces cas évidemment, les obligations à charge des parties n'auraient pas de sens.

E. La prévention de toute utilisation ultérieure

128. Dès lors que l'utilisateur lui aura notifié le vol, la perte, le détournement ou l'utilisation frauduleuse de son instrument, le prestataire devra empêcher toute utilisation ultérieure de l'instrument[189]. Il s'agit là aussi d'une obligation de résultat. Le prestataire est en effet le seul à pouvoir interrompre l'utilisation de l'instrument.

Il est bien évident que cette obligation vaut pour toute utilisation ultérieure, quelle que soit la manière dont l'instrument sera utilisé par un bénéficiaire. Si, lorsqu'un commerçant utilise une communication *on-line* pour lire une carte de crédit, il est immédiatement informé de l'éventuel blocage de la carte, tel n'est pas le cas s'il utilise une lecture manuelle. Le prestataire est pourtant tenu d'empêcher tout paiement même si l'instrument n'est pas lu de manière électronique[190].

129. Si, comme il été mentionné ci-dessus, les parties ont dérogé pour les instruments de paiement de faibles montants à l'obligation, pour le prestataire, de mettre à disposition de l'utilisateur des moyens aptes à ce qu'il puisse procéder à la notification, il est plus que vraisemblable que les parties auront également dérogé à l'obligation d'empêcher toute utilisation ultérieure de l'instrument.

F. L'obligation d'archivage

130. La loi prévoit que le prestataire de services doit tenir un registre interne des opérations de paiement pendant une période d'au moins cinq ans à compter de l'exécution de l'opération[191].

Un tel délai n'était pas prévu par la SPD. Le législateur belge a toutefois fixé ce délai de conservation par référence à celui prévu à l'article 7, alinéa 3, de la loi sur le blanchiment[192], qui est similaire d'ailleurs à ce qui est prévu à l'article 6, 4° de la LTEF.

188 Article 57, § 1er, 1° de la LSP.
189 Article 32, 4° de la LSP.
190 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 63.
191 Article 33 de la LSP.
92 Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, *M.B.*, 9 février 1993.

§ 3. L'exécution de l'opération de paiement et les obligations qui y sont liées

A. L'obligation de bonne exécution, le consentement et l'irrévocabilité

131. L'opération de paiement ne pourra être exécutée par le prestataire que si elle a été préalablement autorisée par le payeur.

Avant de déterminer quand et comment une opération de paiement doit être exécutée, il faudra en effet savoir *si* elle doit être exécutée. C'est pourquoi nous devons tout d'abord nous pencher sur la notion de consentement.

L'article 28 de la LSP consacre le principe selon lequel une opération n'est réputée autorisée que si le payeur a donné son consentement à l'exécution de l'ordre de paiement à son prestataire. À défaut, elle sera réputée non autorisée.

L'autorisation peut être préalable ou postérieure à l'exécution du paiement[193]. Elle devra être donnée dans la forme et selon la procédure convenues entre le payeur et son prestataire[194].

Lorsque la relation contractuelle entre le payeur et le commerçant suppose que les paiements seront faits par domiciliation, l'autorisation sera basée sur un mandat accordé par le payeur à son prestataire de services, au bénéficiaire, ou au prestataire de services de ce dernier. Ce mandat doit être exprès et faire explicitement référence au contrat sous-jacent, sauf si le payeur n'est pas un consommateur. La domiciliation et le mandat qui y est attaché peuvent être résiliés par chaque partie, à tout moment, par simple notification au cocontractant. Cette résiliation sera opposable à tous les mandataires du payeur dès lors qu'il l'aura notifiée à son créancier ou à son prestataire de service[195].

L'article 28 consacre également le droit, pour le payeur, de retirer son consentement à une opération de paiement. Ce droit prendra cependant fin dès que l'opération passera sous statut d'irrévocabilité.

132. Le principe d'irrévocabilité des ordres initiés par le payeur ou par le bénéficiaire ressort de l'article 42 de la loi.

On peut déduire de la lecture combinée de ses deux premiers paragraphes que, lorsque le paiement est initié par le payeur, l'irrévocabilité naît dès que l'ordre

193 J. Dewez, « Carte de crédit : autorisation de paiement et responsabilités », *D.C.C.R.*, 2007, n° 77, pp. 49 et s. ; Au sujet de l'autorisation préalable, voir Bruxelles, 15 mars 2007, *D.C.C.R.*, n° 77, p. 45 : les faits ont lieu avant l'entrée en vigueur de la LTEF et la cour considère que le fait de remettre à la réception d'un hôtel ses documents d'identité et sa carte de crédit dont l'empreinte a été prise constitue une autorisation globale et préalable du paiement de toutes les dépenses qui seront faites, conformément aux conditions générales de l'émetteur de la carte.
194 Article 28, § 1er et § 2 de la LSP.
195 Article 29, § 4 de la LSP.

aura été reçu par le prestataire du payeur, alors que si le paiement est initié par, ou via, le bénéficiaire, le payeur ne peut plus révoquer son ordre de paiement après que cet ordre ait été transmis ou après que le payeur ait exprimé son consentement à l'opération. Ce principe est évidemment sécurisant pour le commerçant, bénéficiaire d'un paiement. Lorsque ce paiement sera effectué au moyen d'un instrument de paiement, le commerçant aura en effet la certitude que la transaction, une fois autorisée par le client au moyen de l'introduction du code PIN ne pourra plus être révoquée.

En cas de domiciliation ou en cas d'opération de paiement sous « date mémo », le paiement étant mis en suspend, le payeur pourra révoquer son ordre jusqu'au jour ouvrable précédant le jour convenu pour le paiement.

Passé les délais indiqués, les ordres de paiement ne pourront plus être révoqués que si cette possibilité a été prévue contractuellement entre le payeur et son prestataire, qui pourrait alors lui imputer des frais. Lorsque l'ordre est initié par ou via le bénéficiaire, la révocation devra toutefois être agréée par ce dernier. Cette exception ne vaut pas lorsque le payeur a exprimé son consentement au moyen d'un instrument de paiement de faibles montants.

Il peut être dérogé dans le contrat-cadre à ce droit de rétractation prévu au bénéfice de l'utilisateur, mais seulement si celui-ci n'est pas un consommateur.

133. Concernant l'exécution de l'opération de paiement à proprement parler, la LSP met plusieurs obligations à charge du prestataire de services du payeur et du prestataire de services du bénéficiaire, ainsi que d'autres intermédiaires.

L'obligation principale qui constitue la pierre angulaire du système de services de paiement veut que, lorsque le paiement est initié par ordre du payeur, son prestataire exécute l'opération ordonnée[196].

Une obligation de bonne exécution équivalente existe à charge du prestataire du bénéficiaire[197]. Lorsqu'un ordre de paiement est initié par ou via le bénéficiaire, son prestataire doit transmettre cet ordre au prestataire du payeur soit immédiatement[198], soit dans les délais ou à la date convenue[199]. Le prestataire du bénéficiaire doit également veiller à ce que le montant de l'opération soit mis à sa disposition immédiatement après qu'il ait été crédité sur son compte[200].

Enfin, l'article 43 de la LSP met à charge des deux prestataires et de tous leurs intermédiaires l'obligation de transférer le montant total du paiement en s'abstenant de prélever des frais, sauf dans le cas où le bénéficiaire et son prestataire auraient contractuellement prévu une telle possibilité.

Cette obligation se déduit de l'article 50, § 1er de la LSP.
Article 51, § 1er de la LSP.
Article 51, § 1, al. 2 de la LSP.
Article 45, § 3 de la LSP, auquel l'article 51 fait référence comme étant l'article 45, alinéa 4.
Article 51, § 2 et 48, § 1er, al. 2 de la LSP.

B. Les obligations en cas de mauvaise exécution

134. En plus de l'obligation de notification spécifique qui existe à charge du payeur en cas de vol, perte, détournement ou utilisation frauduleuse de son instrument de paiement, tout utilisateur est obligé de signaler sans délai à son prestataire qu'il a constaté une opération de paiement non autorisée ou non correctement exécutée donnant lieu à revendication. Cette notification conditionne ce que l'article 34 nomme la « correction » de l'opération.

Cette notification doit être faite dans des conditions de temps déterminées. Elle doit avoir lieu sans délai à partir de sa prise de connaissance mais en plus, elle doit avoir lieu dans les 13 mois suivant la date de débit ou de crédit[201].

À défaut de notification dans le délai imparti, l'opération sera considérée comme ayant été autorisée et donc correctement exécutée. Il s'agit là, selon la doctrine, d'une consécration légale de la théorie de la ratification tacite en matière d'opérations de paiement[202].

Le fait que ces deux conditions temporelles liées à la notification soient cumulatives ouvre la voie à certaines questions. Que dire en effet si l'utilisateur ne respecte que l'un des deux délais fixés par la loi ?

Si l'utilisateur signale une opération non ou mal exécutée à son prestataire sans délai après en avoir pris connaissance, mais plus de treize mois après sa date, on peut supposer qu'il sera considéré comme forclos et dès lors ne pourra plus demander la correction de l'opération. Néanmoins, l'obligation de notification de l'utilisateur est subsidiaire à l'obligation d'information du prestataire. Aussi, si le prestataire n'a pas fourni ou mis à disposition les informations relatives à cette opération, la correction de l'opération sera toujours possible au bénéfice de l'utilisateur.

Quel sort réserver toutefois à l'utilisateur qui notifie l'erreur dans les treize mois de sa survenance, mais attend un certain temps après en avoir eu connaissance ? Certains pourraient penser que dans cette hypothèse, comme dans la précédente, l'utilisateur qui viole l'une des deux conditions temporelles perd son droit de contester l'opération. Nous penchons néanmoins plutôt pour la thèse selon laquelle l'utilisateur qui tarde à notifier l'opération est présumé

201 Q&A de la commission européenne, question 111: « the payer must notify without undue delay on becoming aware of the unauthorised transactions, and, in any case, within a 13 month period », http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq-2008_11_04_en.pdf

202 G. Hennard, « L'exécution d'opérations de paiement non autorisées et l'inexécution ou l'exécution incorrecte d'opérations de paiement », D.B.F., 2009/I, p. 4.

l'avoir ratifié et donc présumé avoir renoncé à la remettre en cause. Pendant un délai de treize mois, cette présomption ne serait toutefois que non irréfragable et l'utilisateur pourrait la renverser en apportant la preuve du contraire[203]. S'il parvient à rapporter cette preuve, il reviendra alors au prestataire d'établir que l'opération ne peut être remise en cause parce qu'elle aurait été authentifiée, enregistrée et comptabilisée et qu'elle n'aurait été affectée d'aucune déficience technique[204]. Cette thèse est d'ailleurs corroborée par l'absence de toute indication de ce que signifie « bref délai » dans la loi, qui laisse donc grande ouverte la porte à l'interprétation.

135. Lorsqu'un prestataire n'a pas, ou a mal, exécuté un ordre de paiement initié par son contractant – payeur ou bénéficiaire – et quelle que soit la responsabilité qui sera déterminée *in fine*[205] et les obligations qui en résulteraient, le prestataire doit s'efforcer de retrouver la trace de l'opération de paiement et doit notifier à son contractant le résultat de sa recherche.

Si par contre, l'opération de paiement a été mal exécutée parce que l'identifiant fourni par l'utilisateur était inexact, le prestataire doit alors s'efforcer, « dans la mesure du raisonnable », de récupérer les fonds engagés dans l'opération[206].

On notera que la mesure « raisonnable » des efforts à fournir par le prestataire est prévue par la loi uniquement lorsqu'il n'y a pas de doute quant à la responsabilité de l'utilisateur qui a communiqué un identifiant erroné. Y aura-t-il selon les cas un niveau d'exigence différent pour les efforts que doit déployer le prestataire ? On en doute.

C. Les obligations liées au refus d'exécution d'une opération de paiement

136. Aux termes de l'article 41, § 1er, si un prestataire de services refuse d'exécuter un ordre de paiement émanant d'un payeur ou émanant d'un bénéficiaire, ce refus ainsi que, si possible, les motifs de ce refus de même que la procédure à suivre pour corriger toute erreur factuelle l'ayant entraîné, doivent être notifiés à l'utilisateur, sauf si cette obligation de motivation est empêchée par le respect de la loi relative au blanchiment ou par une autre interdiction légale.

On peut toutefois s'étonner que le législateur prévoie que les raisons du refus de l'exécution ne doivent être données que « si cela est possible ».

3 Bruxelles, 4 mars 2004, *D. B. F.*, 2004, liv. 4, 227, et note Fr. STEENNOT.
4 G. HENNARD, *op. cit.*, p. 5.
5 Dans les hypothèses visées aux articles 50, § 3 et 51, § 4.
5 Article 49, § 2 de la LSP.

137. Une exception peut être prévue contractuellement à cette obligation de notification si le payeur utilise un instrument de paiement de faibles montants et que le refus de l'opération ressort clairement du contexte[207]. Tel sera le cas lorsque les fonds stockés sur la carte prépayée ne suffisent pas et que l'exécution de l'opération de paiement a été refusée par le terminal POS.

D. L'obligation de remboursement

138. Par dérogation au principe d'irrévocabilité visé à l'article 42, le prestataire du payeur pourra, dans certains cas, être amené à rembourser le montant d'une opération valablement autorisée par le payeur et qui a déjà été exécutée[208].

Ce remboursement pourra avoir lieu lorsque plusieurs conditions seront réunies. D'abord, il doit s'agir d'un paiement initié par, ou via, le bénéficiaire. Ensuite, il faut que l'autorisation n'indiquait pas le montant exact de l'opération lorsqu'elle a été donnée. Enfin, le montant de l'opération de paiement doit dépasser le montant auquel le payeur pouvait raisonnablement s'attendre, tenant compte du profil de ses dépenses passées, des conditions contractuelles et des circonstances pertinentes de l'affaire. Tel sera le cas, par exemple, lorsqu'un client donne les références de sa carte de crédit lors de la réservation d'un hôtel ou pour la location d'une voiture et que le montant débité est sans commune mesure avec ce qui était annoncé, compte tenu des circonstances de fait[209].

Ce droit au remboursement peut être restreint dans le contrat-cadre selon les modalités prévues à l'article 38, § 3 ou peut être étendu au cas de domiciliations[210].

139. Le remboursement peut être demandé pendant une période de huit semaines à compter de la date à laquelle les fonds ont été débités. Le prestataire doit alors prendre position dans un délai de dix jours ouvrables suivant la réception de la demande[211].

140. Si le remboursement est accordé par le prestataire, celui-ci récupérera les fonds auprès du bénéficiaire. Restera alors ouverte la question de la responsa-

207 Article 57, § 1er, 3° de la LSP.
208 Article 38 de la LSP.
209 Cette hypothèse était visée par l'article 8, § 1er, al. 4 de la LTEF : que « le titulaire ne peut révoquer une instruction qu'il a donnée au moyen de son instrument de transfert électronique de fonds, à l'exception des instructions relatives à des opérations dont le montant n'est pas connu au moment où l'instruction est donnée ». On peut regretter que cette exception ne soit pas reprise dans la nouvelle loi. Certes l'article 38 ouvre au payeur un droit de remboursement, mais conditionné par le dépassement substantiel du montant débité par rapport aux attentes légitimes du payeur.
210 Article 38, § 1er, al. 4 de la LSP.
211 Article 39, § 2 de la LSP.

bilité contractuelle du payeur et du bénéficiaire, et il reviendra au payeur de justifier à l'égard du bénéficiaire la non-exécution de son obligation de paiement[212].

E. L'obligation de sécurité

141. On remarquera qu'aucune obligation générale en matière de sécurisation des réseaux ou des infrastructures informatiques n'est prévue à charge du prestataire, hormis l'obligation de confidentialité des codes d'identification pour les instruments de paiement.

Les travaux préparatoires stipulent toutefois qu'il appartient au prestataire de services de paiement de mettre au point ou d'organiser, au sein de son entreprise, les structures sécurisant les opérations de paiement[213] bien que cette explication ne soit pas en relation avec une quelconque obligation légale claire et explicite[214].

§ 4. Les responsabilités des prestataires

142. S'il est évident que selon le droit commun le prestataire sera responsable du non-respect des obligations que nous avons analysées ci-dessus, la LSP prévoit toutefois un régime structuré de responsabilités propre à deux cas particuliers.

A. En cas d'opérations mal ou non exécutées

143. La SPD insiste sur le fait qu'« un fonctionnement harmonieux et efficient du système de paiement dépend de la confiance que peut avoir l'utilisateur dans le fait que le prestataire de services de paiement va exécuter l'opération de paiement correctement et dans le délai convenu »[215].

Dans cette optique, la LSP fixe la responsabilité du prestataire de services du payeur ou de celui du bénéficiaire, selon que l'ordre de paiement ait été initié par le payeur ou par le bénéficiaire.

12 Voir chapitre III.

13 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 69.

14 Notons toutefois qu'en avril 2009, la Commission Bancaire, Financière et des Assurances a publié une circulaire déterminant les exigences prudentielles en matière de services financiers via internet. Cette circulaire donne une série de recommandations et explique les principales dispositions du cadre réglementaire et prudentiel en vigueur qui s'appliquent spécifiquement à la fourniture de services financiers via internet. Une annexe relative aux saines pratiques en matière de gestion des risques de sécurité des opérations sur internet est également publiée : http://www.cbfa.be/fr/ki/circ/pdf/cbfa_2009_17.pdf.

5 Considérant n° 46.

144. Le nouveau régime mis en place par la LSP diffère de celui de la LTEF. L'ancienne loi prévoyait que le prestataire du payeur ne pouvait, en cas d'exécution incorrecte d'un paiement électronique, se dégager de sa responsabilité en se prévalant d'une faute du prestataire de services du bénéficiaire ou d'un cas de force majeure[216]. Ce principe a été remis en cause dans la directive, et le nouveau système diffèrera donc de ce qui était préalablement prévu.

1. *La responsabilité du prestataire du payeur*

145. L'article 50 de la LSP règle les responsabilités lorsque l'ordre de paiement a été initié par le payeur. Dans ce cas, son prestataire sera en premier lieu responsable de l'exécution correcte du paiement.

Sa responsabilité sera mise en cause en cas, disent les travaux préparatoires, « d'exécution fautive ou incorrecte »[217]. L'exécution incorrecte, et donc fautive selon une expression qui nous parait plus juste, s'apprécie en fonction de plusieurs facteurs. Elle peut porter sur la non-exécution de l'ordre initié, l'exécution tardive, le transfert d'un montant erroné, le transfert à un bénéficiaire erroné, etc. Ces irrégularités peuvent toucher tant le compte du payeur que celui du bénéficiaire. Pour le payeur, il s'agira alors de débits injustifiés, et pour le bénéficiaire, il s'agira de transactions partiellement exécutées, du versement d'un montant incorrect, ou du prélèvement de frais indus[218].

146. L'article 51 vise les cas où l'ordre de paiement est initié par, ou via, le bénéficiaire, par exemple s'il s'agit d'une domiciliation ou si une transaction par carte a lieu dans un point de vente. Dans ce cas, si l'ordre de paiement a été mal ou non exécuté et si, conformément aux articles 51, §§ 1er et 2, le prestataire du bénéficiaire a bien transmis l'ordre de paiement dans les délais convenus et s'il a bien traité l'opération conformément à l'article 48, c'est le prestataire du payeur qui sera responsable.

147. Dans ces deux hypothèses, dès lors que le prestataire du payeur sera considéré comme responsable de l'exécution fautive de l'opération, il devra « restituer sans tarder au payeur le montant de l'opération de paiement non ou mal exécutée » et rétablir son compte dans la situation qui aurait prévalu si l'acte fautif n'avait pas eu lieu[219]. Il est toutefois évident que cette sanction ne sera pas toujours la plus opportune pour le payeur.

216 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 86.

217 *Ibidem*, p. 64.

218 *Ibidem*, p. 65.

219 Article 50, § 2, al. 1 et article 51, § 3, al.2 de la LSP.

2. *La responsabilité du prestataire du bénéficiaire*

148. Lorsque l'ordre de paiement aura été initié par le payeur, et si son prestataire peut lui démontrer, et le cas échéant démontrer au prestataire du bénéficiaire que ce dernier a bien reçu le montant de l'opération, alors le prestataire du bénéficiaire sera responsable de la bonne exécution de l'opération de paiement à l'égard du bénéficiaire[220].

149. Lorsque l'ordre de paiement est initié par ou via le bénéficiaire, la responsabilité du prestataire du bénéficiaire est double.

Comme prévu à l'article 45, § 3, il est responsable de la bonne transmission de l'ordre de paiement au prestataire du payeur dans les délais convenus.

De plus, il est tenu au terme de l'article 48 de s'assurer que «le montant de l'opération de paiement soit à la disposition du bénéficiaire immédiatement après que ce montant ait été crédité sur le compte du prestataire de services de paiement du bénéficiaire» et que la date valeur du crédit ne soit pas postérieure à celle du jour ouvrable au cours duquel le montant de l'opération de paiement est crédité sur son compte.

150. Dans ces trois cas, à défaut de s'être conformé à ses obligations, le prestataire du bénéficiaire devra immédiatement mettre le montant de l'opération de paiement à la disposition du bénéficiaire[221].

3. *Les limites à la responsabilité des prestataires*

Les prestataires pourront échapper à leur responsabilité dans plusieurs cas.

151. Tout d'abord, la responsabilité des prestataires est conditionnée par le bon respect, par l'utilisateur, de l'article 34 de la loi. L'utilisateur doit donc signaler qu'il a constaté une opération de paiement non autorisée, ou non correctement exécutée, sans délai et au plus tard dans les 13 mois suivant la date de débit ou de crédit.

À défaut d'une telle notification, il n'y aura pas de mise en cause de la responsabilité des prestataires.

152. Deuxièmement, la loi prévoit qu'un paiement exécuté conformément à l'identifiant unique communiqué par l'utilisateur est réputé dûment exécuté. Si l'utilisateur a fourni un identifiant inexact, son prestataire ne sera donc pas responsable de l'inexécution ou de la mauvaise exécution de l'opération. Cet article ne porte toutefois pas préjudice au «contrôle» de la

0 Article 50, § 1er, al. 2 de la LSP.

1 Article 50, § 2, al. 2; article 51, § 1er, al. 2; article 51, § 2, al. 2 de la LSP.

cohérence d'un identifiant unique qui doit être effectué sur base du devoir général de diligence du prestataire de services professionnel, conformément au droit commun[222].

153. Troisièmement, et pour le prestataire du payeur uniquement, il sera dégagé de toute responsabilité s'il démontre au payeur, et le cas échéant au prestataire de services du bénéficiaire, que ce dernier a bien reçu l'intégralité du montant de l'opération de paiement dans le délai prévu[223].

154. Enfin, lorsque l'exécution incorrecte aura eu lieu suite à un cas de force majeure ou en raison d'une obligation légale[224], par exemple le respect de certaines dispositions de la loi anti-blanchiment, le prestataire ne pourra en être tenu pour responsable[225].

4. *Conséquences*

155. Si l'utilisateur de services de paiement affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de prouver que cette opération a bien été authentifiée, dûment enregistrée et comptabilisée et qu'elle n'a pas été affectée par une déficience technique ou autre[226]. C'est à lui qu'incombe la charge de la preuve.

Une remarque doit être faite quant à l'un de ces éléments de preuve que doit rapporter le prestataire. L'authentification est définie comme «la procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité

222 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 85. Au sujet de la technique de déroutement, voy. G. HENNARD, *op. cit.*, n° 15, p. 13 et références citées.

223 Article 50, § 1er, al. 2 de la LSP.

224 Article 54 de la LSP.

225 L'avant-projet prévoyait initialement un alinéa 2 précisant la notion de force majeure et prévoyant que dès que des opérations ont été introduites de manière électronique, à partir de dispositifs, terminaux ou au moyen d'équipements agréés par le prestataire de services de paiement, le prestataire de services de paiement est responsable de la non-exécution ou de l'exécution incorrecte, à condition que le dysfonctionnement n'ait pas été provoqué sciemment par l'utilisateur. Cet alinéa a été supprimé suite à l'avis du Conseil d'État, mais les travaux préparatoires notent que: «Les auteurs de ce projet tiennent toutefois à souligner que, lors de l'évaluation de la force majeure et de la responsabilité du prestataire de services de paiement, il faut tenir compte du fait que le prestataire de services de paiement, en tant que professionnel, est en premier lieu responsable du matériel ou des logiciels que lui-même ou ses préposés ou mandataires mettent à disposition ou acceptent dans le cadre de la fourniture de services de paiement et non l'utilisateur de services de paiement qui, en tant que profane, n'a aucune idée sur la fiabilité du matériel ou des logiciels précités»: Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 89.

226 Article 35, § 1er de la LSP.

personnalisés »[227]. Cette définition est donc limitée aux seuls instruments de paiement. Pourtant, à la lecture de la loi et des travaux préparatoires, rien ne permet d'affirmer que les éléments de preuve de la bonne exécution d'une opération ne se rapporteraient qu'aux d'opérations initiées par un instrument de paiement.

Il faut donc comprendre le terme « authentification » dans une acception plus large et s'en référer à la définition qui avait été proposée dans une version antérieure de la directive, et qui supposait que l'authentification est « la procédure permettant au prestataire de services de paiement de vérifier que l'utilisateur émettant l'ordre de paiement est habilité à le faire »[228].

156. À moins que les prestataires ne soient dans l'un des cas leur permettant de réfuter leur responsabilité, et sauf si les parties ont dérogé contractuellement aux règles énoncées (étant entendu que cela ne sera pas possible si l'utilisateur est un consommateur), les prestataires ne pourront se dégager de leur responsabilité même s'ils parviennent à établir qu'ils n'ont commis aucune faute dans l'exécution du paiement en démontrant, par exemple, que la faute aurait été commise par un intermédiaire. On est donc face à un véritable régime de responsabilité objective.

Le prestataire de services dispose néanmoins d'une action récursoire contre le prestataire ou l'intermédiaire auquel la responsabilité incombe *in fine*, mais il devra assumer toutes les conséquences vis-à-vis de son contractant[229].

B. En cas d'opérations non autorisées

1. *Régime applicable à toutes les opérations de paiement non autorisées*

157. Si l'opération exécutée par le prestataire n'a pas été dument autorisée, l'article 36 de la LSP prévoit que le prestataire doit, après une vérification marginale lui permettant d'exclure toute fraude dans le chef du payeur, lui rembourser immédiatement le montant de l'opération non autorisée, augmenté des intérêts et des autres conséquences financières éventuelles qu'il aurait supportées.

Le payeur ne pourra toutefois obtenir la rectification de l'opération contestée que si sa réclamation a été faite en temps utile, soit à bref délai et en tout état de cause dans les 13 mois du débit non autorisé. Passé ce double délai, son droit au remboursement s'éteint, et l'opération est réputée ratifiée sans que le prestataire n'ait plus à apporter la preuve de la validité de l'opération.

[227] Article 2, 11° de la LSP.
[228] G. Hennard, *op. cit.*, p. 7.
[229] G. Hennard, *op. cit.*, p. 14.

158. Toutefois, il est évident que ce remboursement sera tributaire d'une seconde vérification, celle-ci plus approfondie, et qui portera sur l'absence d'autorisation dans le chef de l'utilisateur. Cette vérification peut, on l'imagine, prendre un certain temps. Par conséquent, l'immédiateté du remboursement, après vérification de l'absence de toute fraude, est acquise à l'utilisateur, mais de manière provisoire seulement. Pour obtenir un remboursement définitif, il faut que le prestataire n'ait pas pu démontrer que l'opération contestée avait bien été authentifiée, dûment enregistrée et comptabilisée, et qu'elle n'a pas été affectée par une déficience technique ou autre.

La charge de la preuve incombe ici aussi au prestataire qui détient tous les moyens propres à établir ses prétentions, à la différence du payeur. À cet égard, toutes clauses contractuelles alourdissant la charge de la preuve du payeur ou allégeant celle du prestataire son réputées interdites et nulles[230], à moins que le prestataire et l'utilisateur, non consommateur, n'aient prévu d'écarter ces règles[231].

La remarque faite ci-dessus au sujet de la signification du terme « authentification » peut être reprise ici.

2. *Régime applicable aux opérations soi-disant autorisées par le biais un instrument de paiement*

a. Preuve de l'autorisation

159. Si l'autorisation de l'opération que le payeur conteste a été donnée au moyen d'un instrument de paiement, la preuve qui doit être rapportée par le prestataire quant à cette autorisation prend une autre forme.

En effet, l'authentification exigée par l'article 35, § 1er doit être ici comprise par référence à la définition que la loi en donne, soit la procédure permettant au prestataire de vérifier l'utilisation d'un instrument de paiement, en ce compris ses dispositifs de sécurité personnalisés[232].

Les dispositifs de sécurité personnalisés sont une notion qui est utilisée dans le texte de la SPD sans pourtant y être définie. Au cours de son élaboration toutefois, il a été affirmé qu'un numéro de carte de crédit et sa date d'échéance ne pouvaient être considérés comme des dispositifs de sécurité personnalisés puisqu'ils sont visibles pour tout le monde. Le législateur belge a proposé de définir ce terme comme étant « l'ensemble des procédures permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument

[230] Article 61, 3° de la LSP.
[231] Article 55 de la LSP.
[232] Article 2, 11° de la LSP.

de paiement donné et d'authentifier l'utilisateur»[233]. Les travaux préparatoires entendent par là que l'instrument doit être identifié et contrôlé quant à sa validité et à son authenticité (date d'échéance et absence de contrefaçon), et que l'utilisateur de l'instrument doit être authentifié[234].

160. L'article 35, § 2 précise que la simple utilisation de l'instrument ne suffit pas *nécessairement*[235] à prouver que l'opération a été autorisée par le titulaire, ni qu'il aurait agi frauduleusement ou n'aurait pas satisfait, intentionnellement ou à la suite d'une négligence grave, aux obligations de sécurité qui lui incombent[236].

On peut donc en déduire que ni la simple communication à un commerçant du numéro d'une carte de crédit et de sa date d'échéance[237], ni l'utilisation d'une carte bancaire et de son code secret ne permettent au prestataire d'affirmer que l'opération a bien été autorisée par le titulaire.

Le prestataire devra donc apporter plus que la preuve de l'utilisation de la carte et de son code pour établir que l'opération a été authentifiée, dûment enregistrée, comptabilisée et non affectée par une déficience technique, comme le requiert la loi.

Cette règle se justifie par le fait qu'une carte assortie d'un code PIN n'offre pas un degré de sécurité absolue. La capacité d'un tiers d'intercepter un code PIN veut que les titulaires de carte qui sont victimes d'agissements rendus possibles en raison du degré de sécurité insuffisant de l'instrument et des risques liés à ces cartes, dont les émetteurs sont conscients, soient protégés.

161. Par ailleurs, l'utilisation de l'instrument de paiement et de son code secret par un tiers ne permettra pas non plus de conclure que le titulaire a commis une fraude, ou n'a pas satisfait, à la suite d'une négligence grave ou intentionnelle, à son obligation de sécurité.

Au contraire, la charge de la preuve de la fraude et de la négligence grave de l'utilisateur incombe ici aussi au prestataire.

La loi précise que sont notamment considérées comme négligences graves, 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

233 Article 2, 24° de la LSP.

234 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 16.

235 On peut être perplexe quant à l'utilisation de l'adverbe nécessairement qui suggère que dans certains cas l'utilisation de l'instrument suffit bien à prouver l'existence d'une autorisation.

236 En vertu de l'article 31 du projet de LSP.

237 Voir les travaux du PSDTG – groupe de travail des experts de la Commission et le projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 69.

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 fournisseur de services de paiement la perte ou le vol, dès qu'il en a eu connaissance»[238].

Concrètement, le juge devra tenir compte de l'ensemble des circonstances de fait pour pouvoir conclure à la négligence de l'utilisateur[239]. L'utilisation du code devra être accompagnée d'autres présomptions pour amener le juge à conclure à l'existence d'une négligence grave[240]. En principe, la seule violation par le titulaire de son obligation générale d'utiliser son instrument d'une manière sécurisée ne constitue pas en soi une négligence grave[241], bien que l'adverbe «nécessairement» utilisé par le législateur puisse prêter à interprétation.

b. Conséquences et responsabilités

162. Lorsque l'autorisation a été donnée au moyen d'un instrument de paiement, le droit au remboursement qui est d'application pour toutes les autres opérations sera quelque peu nuancé.

Ce remboursement sera fonction du moment où l'utilisateur aura notifié la perte, le vol, le détournement, ou l'utilisation non autorisée de son instrument. L'obligation qui est prévue à l'article 31, § 1er, 2° vient en quelque sorte se superposer et préciser celle prévue à l'article 34.

Il est généralement dit que le moment de la notification est le moment clé pour déterminer le partage des responsabilités entre parties. Selon nous, la question n'est pas *«qui est responsable et quand?»* mais *«qui supporte les risques et quand?»*.

Si le payeur a tout intérêt à ce que la notification se fasse le plus rapidement et le plus efficacement possible, ce n'est pas parce que cette notification sonnera

238 Article 37, § 3, al. 2.

239 Voir J.P. Bruxelles, 7 juillet 2006, *D.B.F.*, 2007/II, p. 134 qui conclut à la négligence grave en raison d'un défaut de surveillance dans un hôpital, et Comm. Bruxelles, 27 novembre 2006, *D.B.F.*, 2007/II, p. 137 qui se base sur plusieurs éléments de fait pour en déduire que le code PIN était inscrit à proximité de la carte. *Contra*: Bruxelles, 13 septembre 2005, *D.C.C.R.*, 2006, n° 73, p. 86 qui écarte la négligence grave alors que la carte de crédit est laissée dans la boite à gants d'un véhicule fermé à clé, et Bruxelles, 4 octobre 2005, *D.C.C.R.*, 2006, n° 73, p. 92, ainsi que Bruxelles, 27 mai 2002, *R.D.C.*, 2004, p. 158 qui confirment tout deux que le titulaire d'une carte n'est pas tenu de vérifier systématiquement si sa carte se trouve bien dans son portefeuille même si le portefeuille a été très brièvement égaré.

240 Tel était également le système mis en place par la LTEF, en contradiction avec la jurisprudence antérieure à 2002 qui estimait que si une carte de paiement était utilisée avec son code secret, cela présumait la négligence grave du titulaire qui avait soit communiqué son code à un tiers, soit l'avait vraisemblablement inscrit à proximité de sa carte.

241 Voir Civ. Bxl, 7 décembre 1998, *J.T.*, 1999, p. 373 qui tient compte de plusieurs circonstances pour en conclure à une négligence grave de la part du titulaire de la carte.

l'exonération de sa responsabilité, mais parce que dès ce moment, il ne sera plus tenu de participer aux risques, par la prise en charge d'une « franchise ».

163. Avant la notification, et s'il a agi frauduleusement ou s'il n'a pas respecté ses obligations de sécurité soit intentionnellement, soit en raison d'une négligence grave, il supportera toutes les pertes occasionnées par des opérations de paiement non autorisées[242].

Par fraude, il faut entendre le non-respect intentionnel des obligations de sécurité du titulaire de l'instrument, ou le fait qu'il ait donné son instrument avec son numéro d'identification personnel à un tiers pour ensuite adresser une notification à l'émetteur, ou encore le fait d'utiliser l'instrument après avoir sciemment notifié sa perte ou son vol[243].

Quant à la négligence grave, on a vu qu'elle pouvait être déduite de comportements visés expressément par la loi, ou de tout autre circonstance de fait, sans pour autant que le simple non-respect de son obligation d'utiliser son instrument d'une manière sécurisée, ou le simple fait de l'utilisation de sa carte avec son code ne puisse être considéré comme constitutif de cette négligence[244]. Toutefois, s'il a ignoré son obligation de notifier sans délai la perte, le vol, le détournement ou l'utilisation non autorisée de son instrument, il pourra être considéré comme ayant commis une négligence grave.

164. Avant la notification, et en dehors de ces cas de négligence grave ou de fraude, le payeur devra supporter, à concurrence d'un plafond de 150 euros, les pertes dues aux opérations de paiement non autorisées faites au moyen de l'instrument perdu ou volé ou détourné s'il n'est pas parvenu à préserver la sécurité de ses dispositifs.

Toutefois, il ne devra supporter aucune perte, et le prestataire sera donc seul à assumer les risques dans deux cas.

Premièrement, si l'instrument de paiement a été copié par un tiers ou a été indûment utilisé pour autant que le payeur était bien, au moment de l'opération contestée, en possession de l'instrument de paiement. Il est ici fait référence à la contrefaçon de l'instrument. Par analogie, celle-ci peut être étendue aux cas où l'instrument physique n'est pas contrefait mais où certaines données sont copiées ou le système piraté (« *hacking* »).

242 Voir sur ce point E. Jacobs, « De verdeling van de aansprakelijkheid in geval van frauduleus gebruik van een betaalinstrument », *D.B.F.*, 2009/I, pp. 22 et s.

243 O. Goffart, *op. cit.*, p. 10

244 Voy. Fr. Domont-Naert et A.-L. Evrard, « La négligence grave à l'épreuve des faits », *D.C.C.R.*, 2002, p. 103 qui relèvent que la plupart des institutions bancaires dans leurs conditions générales « considèrent que le simple fait pour le titulaire de méconnaître un des conseils généraux de prudence énoncés dans les conditions générales s'avère être automatiquement constitutif d'une négligence grave ».

Le deuxième cas dégageant entièrement le payeur de toute franchise vise les situations dans lesquelles l'instrument de paiement a été utilisé sans présentation physique et sans identification électronique.

Autrement dit, il faudra que le titulaire de l'instrument et le commerçant ne soient pas en présence l'un de l'autre. Tel sera le cas pour les contrats conclus à distance et où le paiement aura été fait au moyen d'un ordinateur, d'un GSM, ou d'un téléphone. Par ailleurs, il faudra que la transaction ait eu lieu sans identification électronique[245]. Cette identification électronique requiert plus que la seule utilisation d'un code confidentiel. Le texte de l'avant-projet de loi rajoutait d'ailleurs que « 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 ». Ni les travaux préparatoires ni l'avis du Conseil d'État ne nous éclairent sur les raisons de la disparition de cette formule. Ils précisent toutefois que l'identification électronique pourra avoir lieu par l'introduction de l'instrument dans un terminal de paiement qui possède la possibilité technique de vérifier si l'instrument est authentique[246][247]. Il faudra donc, pour que le titulaire de l'instrument soit entièrement déchargé de toutes les conséquences de l'utilisation de son instrument, que la solution de paiement utilisée par le tiers de mauvaise foi ait présenté, à côté de l'utilisation d'un code confidentiel, une vérification électronique. Pour certains commentateurs, cette identification vise « un moyen permettant d'identifier avec certitude le titulaire de l'instrument »[248], pour d'autres « ce qui est demandé est donc une identification électronique de l'instrument et non celle du titulaire »[249].

Si l'autorisation que le titulaire de l'instrument nie avoir donnée, a été donnée au moyen d'un instrument de paiement de faibles montants, et dès lors que cet instrument est utilisé de manière anonyme ou si le prestataire n'est pas en mesure, pour des raisons inhérentes à l'instrument, d'apporter la preuve que l'opération n'a pas été autorisée, les parties peuvent avoir dérogé au droit de remboursement prévu à l'article 36, ou aux règles qui modulent ce droit et le limitent à 150 €.

165. Après la notification par l'utilisateur de la perte, du vol ou du détournement de l'instrument, le prestataire de services a l'obligation d'empêcher toute opération faite avec cet instrument. Il supportera donc l'entière responsabilité

245 Pour une explication détaillée au sujet de l'identification électronique, voy. notamment O. Goffard, *op. cit.*, pp. 5 et s.

246 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 71.

247 Fr. de Clippele et O. Goffard, « Qui va payer ? », *op. cit.*, p. 373.

248 *Ibidem.*

249 Th. Lambert, *op. cit.*, p. 588.

de tout retrait et opération frauduleuse après la notification, même si l'utilisateur a auparavant commis une négligence grave.

Les travaux préparatoires précisent toutefois qu'en cas de comportement frauduleux[250] le prestataire ne supportera aucune responsabilité[251]. Cette indication est difficilement conciliable avec l'obligation à charge du prestataire d'empêcher toute opération après la notification qui joue, précisent ses mêmes travaux préparatoires, « même en cas de négligence grave ou d'utilisation frauduleuse »[252]. Il semblerait ainsi que la loi mette une obligation générale de blocage de la carte à charge du prestataire, qui vaut même en cas de fraude, mais que dans cette dernière hypothèse aucune sanction ne soit attachée au non respect de l'obligation. On suppose que cette exonération de la responsabilité du prestataire est basée sur la présomption qu'en cas de fraude commise par l'utilisateur d'un instrument, tout retrait et toute opération postérieure à la notification serait le fait de l'utilisateur. Si cette logique a un sens, il n'en reste pas moins que baser l'exonération de la responsabilité liée à une obligation de résultat sur une présomption selon laquelle une fraude commise par l'utilisateur aurait un effet de contagion sur toute autre opération postérieure à la notification semble excessif.

Toutefois, la responsabilité totale du prestataire après la notification n'aura pas lieu d'être dès lors que l'instrument ne permet pas le blocage ou la prévention d'une utilisation ultérieure. Dans ce cas donc, l'utilisateur sera entièrement tenu des risques et des pertes liés à son instrument de paiement.

166. Que ce soit avant ou après la notification, le prestataire sera responsable à l'égard du l'utilisateur de toutes les conséquences résultant de l'usage d'un instrument de paiement par un tiers non autorisé dès lors qu'il n'aurait pas respecté son obligation de décrire à l'utilisateur les risques et mesures de prudence qu'il doit prendre pour préserver la sécurité de son instrument de paiement et s'il ne s'est pas suffisamment assuré que les dispositifs de sécurité personnalisés ne sont pas accessibles à des tiers, ou s'il n'a pas mis à disposition de l'utilisateur les moyens appropriés pour procéder comme il se doit à la notification[253].

167. Si l'utilisateur n'est pas un consommateur, les parties auront pu prévoir que ces règles limitant la responsabilité de l'utilisateur, soit entièrement, soit au montant de 150 € seulement, ne s'appliquent pas.

250 Ou d'intention frauduleuse précisent les travaux préparatoires à la page 72.

251 Voir aussi Th. LAMBERT, *op. cit.*, n° 36.

252 Projet de loi relatif aux services de paiement, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2008-2009, n° 2179/01, p. 63.

253 Article 62 de la LSP.

Chapitre III
Les litiges

Les litiges qui peuvent naître des paiements électroniques sont innombrables. Notre attention ne s'arrêtera donc qu'à certains d'entre eux.

Section 1
Litiges entre les utilisateurs et les prestataires de services de paiement dus au non-respect de la LSP

168. Les relations entre les utilisateurs de services et les prestataires sont largement encadrées par la LSP.

Dans son dernier titre, la loi érige en sanctions certains comportements et détermine les recours ouverts aux utilisateurs.

169. Avant de les analyser, soulignons toutefois que l'autorité publique dispose de pouvoirs afin de voir respectées les dispositions légales.

Ainsi, les agents commissionnés par le Ministre du SPF Economie peuvent, par une procédure d'avertissement, notifier à tout contrevenant à la loi une mise en demeure de mettre fin à l'infraction.

Sans réaction, le contrevenant peut être sujet à des poursuites judiciaires de nature pénale, à moins qu'il n'ait accepté un règlement transactionnel. Il peut également être cité en cessation devant le Président du tribunal de commerce. Des sanctions administratives, décidées par l'autorité de contrôle dont il dépend, peuvent aussi lui être imposées.

§ 1. Les sanctions

A. Les sanctions civiles

170. Trois sanctions civiles sont prévues par la loi au bénéfice de l'utilisateur.

Tout d'abord, l'utilisateur pourra se prévaloir de la nullité de toute clause par laquelle il aurait été amené à renoncer, même partiellement, au bénéfice de ses droits, et par laquelle le prestataire s'exonère, même partiellement, de ses obligations légales. Seront également nulles, toutes clauses par lesquelles les parties transfèrent contractuellement la charge de la preuve des obligations du prestataire vers l'utilisateur de services.

Deuxièmement, si le prestataire n'a pas communiqué à l'utilisateur les mesures de sécurité de l'instrument de paiement, s'il n'a pas garanti le caractère secret des dispositifs de sécurité personnalisés ou communiqué les conditions de la notification de la perte, du vol ou de l'utilisation abusive d'un instrument de

paiement, il restera responsable à l'égard de l'utilisateur des conséquences résultant d'une utilisation de l'instrument par un tiers non autorisé.

Troisièmement, l'utilisateur a le droit de résilier par lettre recommandée, sans délai ni frais ni pénalités, le contrat-cadre dès lors que le prestataire n'aurait pas respecté certaines de ses obligations, considérées comme les plus essentielles de la loi. Ce droit de résiliation est à rapprocher de celui prévu à l'article 83*octies* de la LPCC.

B. Les sanctions pénales

171. Quasi toutes les dispositions de la loi sont sanctionnées pénalement.

L'utilisateur, de même que l'autorité publique, pourra donc dans la plupart des cas saisir le parquet pour voir des poursuites pénales initiées à l'encontre du prestataire de services qui n'aurait pas respecté ses obligations légales.

§ 2. Les recours

172. La LSP fait référence à l'action en cessation, qui sera établie à l'article 4 de la loi 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 relative aux services de paiement. Celle-ci prévoit que le Président du tribunal de commerce est habilité à constater l'existence et à ordonner la cessation d'un acte, même pénalement réprimé qui constitue une infraction aux dispositions de la LSP.

173. Par ailleurs, les prestataires doivent instituer, afin de régler les éventuels litiges relatifs aux droits et obligations prévus par la LSP, des recours extrajudiciaires.

Section 2
Litiges nés du dysfonctionnement des infrastructures de paiement électronique

174. Pour pouvoir accepter des paiements par carte[254], le commerçant doit être lié à un acquéreur[255] ainsi qu'à un processeur en charge du traitement opérationnel des transactions de paiement électronique[256].

254 Pour une description détaillée du déroulement d'une transaction par paiement électronique, voir P. Belens, « Aspects généraux du paiement électronique par carte bancaire », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004.

255 Voir n° 59.

256 Pour la carte Bancontact / Mister Cash, l'émetteur et la banque du client, l'acquéreur est BANKSYS, et le processeur est BANKSYS. Pour la carte VISA ou MASTER CARD, les acquéreurs sont Bank Card Company, CITY BANK ou EUROPA BANK. Les émetteurs sont généralement la banque du client et BANKSYS est le processeur. Notez par ailleurs que Bank Card Company et Banksys forment aujourdhui ATOS Worldline.

Ce processeur assume plusieurs obligations. D'une part, il fournit aux commerçants les terminaux de paiement POS qui sont reliés à son réseau et qui permettent aux clients d'effectuer des paiements par cartes bancaires.

Le processeur gère également le réseau qui assure la circulation et le traitement par voie électronique des données financières.

Enfin, le processeur doit mettre à disposition des commerçants (et des institutions bancaires) une connexion à ce réseau[257].

175. La question qui peut se poser est de savoir quelle est la nature de cette obligation de connexion. Cette question a été soulevée lors du passage à l'euro, et l'est régulièrement lors des périodes de fête lorsque le volume d'achats de la population est important et que le réseau est largement sollicité.

Le processeur sera-t-il responsable s'il ne peut offrir à ses contractants une connexion maintenue à son réseau, empêchant ainsi les clients de payer par carte et privant les commerçants de certains bénéfices ?

Selon la cour d'appel de Bruxelles, au vu du contrat liant Banksys à ses clients[258], le transfert d'ordres de paiement doit être exécuté immédiatement après l'introduction du code secret par le client, car il faut que l'ordre de transfert ait la même effectivité qu'un transfert manuel. Cette obligation résulte de la position monopolistique de Banksys et des obligations assumées par celle-ci[259].

Selon la jurisprudence donc, une entreprise qui fournit la transmission de paiements électroniques s'engage à un résultat précis et doit éviter toute discontinuité dans le service offert. À défaut, elle sera tenue pour responsable[260].

Section 3
Litiges nés de la relation entre client et commerçant

176. Lorsque l'on envisage les litiges qui peuvent naître suite à un paiement électronique, on ne peut faire l'économie de la relation entre le payeur et le

257 J.-P. Buyle et O. Creplet, « La responsabilité des gestionnaires des systèmes de paiement électronique, appréciée dans le contexte global de ceux-ci », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, pp. 27 et s.

258 Les termes de ce contrat sont bien entendu modifiables, et les faits de cette affaire datent de 2000.

259 Bruxelles, 12 février 2002, *D.C.C.R.*, 2002, n° 55, p. 73.

260 Voir toutefois la position de R. Steennot, « De aard van de verbintenis om een elektronisch betalingssysteem ter beschikking te stellen », *D.B.F.*, 2002/III, p. 178.

bénéficiaire ou plus exactement, puisque l'on sort du champ de la LSP, entre le client et le commerçant[261].

Nous envisagerons deux situations assez classiques.

177. La première met en scène un client et un commerçant ayant conclu un contrat. En exécution de ce contrat, le client est tenu à un paiement et s'exécute. Le commerçant remplira alors ses propres obligations contractuelles.

Nous avons vu que, en vertu de l'article 38 de la LSP, le payeur peut exiger de son prestataire le remboursement d'un paiement autorisé et déjà exécuté si le montant, manifestement élevé, n'était pas indiqué au moment de l'autorisation[262].

Dans cette situation le prestataire du payeur, qui a recrédité le compte de son client, inscrira le montant remboursé au débit du compte du commerçant.

Le commerçant n'aura alors pour seule possibilité que d'engager la responsabilité contractuelle de son client pour non-exécution de son obligation de paiement. Le prestataire ne peut en effet être tenu pour responsable de l'exécution du contrat entre parties qui est sous-jacent à ses propres obligations légales et contractuelles.

178. La seconde situation à envisager concerne l'application de la LPCC. Pour les contrats à distance, comme ceux conclus par internet, la loi a reconnu au consommateur un droit de renonciation de sept jours[263].

Selon le législateur belge, et à raison, un consommateur hésitera à deux fois avant d'exercer son droit de renonciation s'il a dû effectuer un versement avant de recevoir le bien commandé à distance.

Par conséquent, et pour permettre au consommateur de jouir pleinement de ce droit de renonciation, la LPCC prévoit que « (...) aucun acompte ou paiement quelconque ne peut être exigé du consommateur avant la fin du délai de renonciation de sept jours ouvrables visé au § 1er »[264]. Toutefois, la loi prévoit que « En cas d'exercice du droit de renonciation prévu aux §§ 1er et 2, le vendeur est tenu au remboursement des sommes versées par le consommateur, sans frais. Ce remboursement doit être effectué au plus tard dans les trente jours suivant la renonciation ». Il n'y a donc pas d'interdiction générale du paiement

261 A. Vandoolaeghe, « het aanvarden van kredietkaarten : een gevaarlijke onderneming voor de handelaar ? » *D.A.O.R.*, 2009/90, p. 170.

262 Voir n° 144.

263 Article 80, § 1er de la LPCC.

264 Article 80, § 3 de la LPCC.

anticipé, mais, parmi les modalités de paiement proposées par un vendeur, doit figurer la possibilité pour le consommateur de payer à l'expiration du délai de renonciation. Le vendeur ne peut donc pas exiger un paiement avant la fin du délai de renonciation, mais peut le proposer pour autant qu'un autre mode de paiement différé soit également offert au consommateur[265].

En application de ces principes, le tribunal commerce de Bruxelles[266] a considéré que lorsque les coordonnées d'une carte de crédit sont enregistrées par un commerçant uniquement à titre de garantie, le commerçant commet une faute s'il débite la carte de crédit « à titre de confirmation de la commande » et de manière définitive sans possibilité de remboursement.

Interrogée sur la question de savoir si cette interdiction était conforme aux articles 23, et 28 à 30 du Traité CE, la Cour de Justice des Communautés européennes a jugé que la protection des consommateurs pouvait constituer un objectif légitime d'intérêt général de nature à justifier cette mesure d'effet équivalent à une restriction quantitative. Par contre, l'article 29 du Traité s'oppose à ce qu'il soit interdit au commerçant de demander, avant l'expiration du délai de rétractation, le numéro de la carte de crédit et la date d'expiration s'il s'engage à ne pas utiliser ces données avant l'expiration du délai de renonciation[267].

Dans cette situation, le consommateur aura un recours à l'encontre du commerçant, ainsi qu'à l'encontre de son prestataire de paiement, puisqu'il n'aura pas donné de consentement à l'opération.

Section 4
Les fraudes

179. Les fraudes aux paiements électroniques sont de plus en plus nombreuses. Les prestataires et opérateurs créent régulièrement de nouveaux systèmes antifraudes, mais il est évident que nul ne pourra éradiquer totalement ce fléau.

La fraude opérée lors d'un paiement électronique aura des effets sur la situation du commerçant. Nous verrons toutefois quelles sont les conséquences pénales de tels actes.

265 H. Jacquemin et E. Montero, « L'interdiction d'exiger un paiement anticipé dans les contrats à distance », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, pp. 143 et s.

266 Cité par E. Montero, « Chronique de jurisprudence 2002-2008 », *R.D.T. I.*, 35/2009, p. 17.

267 CJCE, 16 décembre 2008, aff. C-205/07, citée par E. Montero, *ibidem*.

§ 1. Les conséquences de l'utilisation frauduleuse d'un instrument de paiement pour le commerçant

180. Le scénario, malheureusement classique, est celui dans lequel un tiers utilise l'instrument de paiement d'autrui, ou ses dispositifs de sécurité, pour se voir livrer un bien ou un service. Le commerçant aura alors a délivré son produit ou service à un consommateur qui n'était pas habilité à le payer.

Dans ce cas, le titulaire réel de l'instrument de paiement aura introduit les recours nécessaires auprès de son prestataire et, hormis fraude ou négligence grave, n'aura pas à subir les conséquences de l'utilisation par ce tiers de mauvaise foi de son instrument de paiement.

Si le paiement a été fait sur internet, on sait que la responsabilité du titulaire d'une carte de crédit n'est pas engagée s'il n'y a pas eu identification électronique[268]. Dans ce cas, les sommes débitées seront recréditées au véritable titulaire de la carte par l'émetteur de l'instrument.

La question à résoudre sera alors de savoir si le commerçant doit supporter les risques de fraude lorsque la transaction a été autorisée par le prestataire de services, ou si les vérifications effectuées par le prestataire lui donnent l'assurance que le paiement est bien valide et qu'en cas de fraude il revient au prestataire d'assumer l'inexactitude des informations vérifiées.

181. Lorsque la transaction se déroule *off-line,* l'émetteur de la carte ne dispose pas de la possibilité de vérifier et d'authentifier la transaction. Aussi, lorsque le commerçant a recours à ce mode de communication, il en supporte le risque en connaissance de cause[269].

Lorsque la transaction se déroule *on-line,* la jurisprudence tranchera en général dans le sens de la responsabilité du commerçant[270].

Dans un arrêt récent, la Cour d'appel de Bruxelles a estimé qu'en ce qui concerne les transactions sur internet, « tout commerçant en connait ou doit en connaitre les risques, dès lors qu'il utilise un système de paiement par carte de crédit. Si le commerçant ne veut pas courir un tel risque, il lui suffit de ne pas accepter une commande à distance effectuée au moyen des cartes Visa et Eurocard-MasterCard. Il doit être conscient du risque lié à ce type d'instrument »[271]. En l'espèce, le commerçant avait accepté des commandes effectuées par plusieurs cartes de crédit et pour chacune d'elles, il avait demandé

[268] Voir n° 169.

[269] Fr. DE CLIPPELE et O. GOFFARD, « Qui va payer ? », *op. cit.*, p. 375.

[270] R. STEENNOOT, « De handelaar als dupe van het frauduleus gebruik van een kredietkaart op afstand », *D.B.F.* 2009/III, p. 175.

[271] Bruxelles, 19 juin 2008, *D.A.O.R.* 2009/90, p. 167

l'autorisation de BCC en envoyant les données de la carte afin de vérifier si celle-ci, identifiée par son numéro et sa date d'expiration, n'avait pas été volée ou perdue ou si la transaction ne dépassait pas la limite du crédit. Pour chaque transaction, le commerçant avait reçu un code d'autorisation. Les véritables titulaires des cartes se sont toutefois opposés aux transactions. BCC les a remboursés et a débité le commerçant conformément à ses conditions générales d'utilisation.

Selon la cour, « il est normal que ce soit le commerçant qui, lorsqu'il décide d'accepter un paiement par carte sans la présence physique du titulaire de la carte et, partant, en se privant de la possibilité de faire les vérifications requises et d'obtenir la signature de l'intéressé sur la facturette, supporte le risque d'une malveillance de la part de son client, donneur d'ordre, contre lequel il lui appartient, le cas échéant, de se retourner. En délivrant un code d'autorisation, BCC ne validait pas la transaction. Il ne s'agit pas d'une reconnaissance absolue de la validité de la transaction ni d'une garantie certaine de paiement »[272].

Il est exact que lorsqu'un commerçant demande une autorisation à un organisme bancaire en envoyant les données d'une carte, l'autorisation éventuellement accordée signifie uniquement que l'organisme bancaire n'a aucun motif de s'opposer à la transaction sur la base des données fournies. Cette autorisation confirme donc seulement que la carte, identifiée par son numéro et sa date d'expiration, n'a pas été volée ou perdue et que la transaction ne dépasse pas les plafonds autorisés. Il ne faut toutefois pas y voir la reconnaissance absolue de la validité de la transaction alors que l'organisme bancaire est dans l'impossibilité de vérifier si la carte a été effectivement utilisée par son titulaire légitime. C'est donc bien le commerçant qui, lorsqu'il décide d'accepter un paiement par carte sans la présence physique du titulaire, et partant en se privant de la possibilité de vérifier, *de visu* ou électroniquement l'identité de son client[273], doit assumer les risques.

182. Toutefois, même en présence physique du client, le commerçant ne sera pas exempt de toute responsabilité. S'il accepte un paiement par carte de crédit alors que la signature reprise sur la souche est grossièrement imitée, il commet une faute lourde et supporte seul les conséquences de la transaction réalisée. Dans ce cas d'ailleurs, le fait pour la société émettrice de la carte de crédit de transmettre à la banque du titulaire de la carte une souche non signée peut constituer une faute, comme le fait pour le banquier de payer, par débit du compte de son client, le montant repris sur cette souche[274].

[272] Mêmes motifs repris dans Bruxelles, 10 mars 2009, *D.B.F.*, 2009/III, p. 173

[273] E. MONTERO, « Chronique de jurisprudence 2002-2008 », *R.D.T. I.*, 35/2009, pp. 19 et 20.

[274] J.-P. BUYLE et O. POELMANS, *op.cit*, p. 94 et les références citées.

§ 2. Les conséquences pénales de la fraude

183. Comme souvent dans les sphères de l'informatique, les pirates rivalisent d'ingéniosité, et leurs comportements sont dénommés selon des termes anglais. Nous décrirons dans un premier temps les comportements infractionnels les plus répandus pour ensuite les analyser selon l'angle pénal.

A. Les différents types d'infractions

184. La pratique qui consiste à copier frauduleusement les bandes magnétiques de cartes de paiement et à prendre frauduleusement connaissance du code secret qui y est attaché afin de pouvoir confectionner un double de la carte et débiter ainsi compte de son titulaire se nomme le *skimming*[275] .

Lorsqu'on parle de *phishing*[276], on vise le fait d'obtenir, par des moyens fallacieux, des données personnelles et confidentielles qui sont communiquées volontairement par leur titulaire. En général, le *phishing* consiste à envoyer un email comme provenant d'une société bien connue pour détourner les données relatives aux cartes de crédit, les coordonnées bancaires ou mot de passe. L'email reçu par la victime contient généralement un lien renvoyant vers un site pirate, copie conforme du site réel de la société connue par le destinataire de l'email. Le destinataire est alors convaincu de se trouver face au site de sa banque, et n'hésite pas à y introduire ses données qui, ainsi interceptées, permettront aux fraudeurs de débiter ses comptes.

Le *hacking* est l'accès non autorisé à un système informatique. Les hackers peuvent ainsi pénétrer dans le système informatique d'une banque et en copier les données pertinentes à des fins délictuelles. Ils peuvent également accéder, selon des moyens divers, à l'ordinateur d'un particulier et avoir accès à ses données personnelles. Cela leur permettra de s'approprier des données bancaires et de les utiliser en vue, par exemple, de réaliser des transferts de fonds vers des comptes dont ils sont titulaires, et qui seraient hébergés dans des pays où le secret bancaire est bien préservé.

B. Les sanctions pénales

185. Selon les cas et selon la réalité de chaque dossier répressif, les fraudes bancaires pourront être sujettes à des préventions de faux en écriture, d'association de malfaiteurs, d'abus de confiance, ou autres.

5 E. Roger France, « Transactions électroniques et criminalité informatique: quelle répression? », in *Aspects juridiques du paiement électronique*, Waterloo, Kluwer, 2004, p. 238.

6 Contraction entre les mots « fishing » et « phreaking » (pirater un réseau informatique).

Toutefois, depuis la modification du Code pénal par la loi relative à la criminalité informatique[277], le législateur a érigé plusieurs nouvelles infractions qui viennent sanctionner particulièrement les fraudes informatiques[278].

186. Le faux informatique est défini par l'article 210*bis* du Code pénal comme le fait d'introduire dans un système informatique, de modifier ou d'effacer des données stockées, traitées ou transmises par un système informatique, ou de modifier par tout moyen technologique l'utilisation possible des données et par là de modifier la portée juridique de telles données. L'usage de faux informatique est réprimé par l'article 210*bis*, § 2.

Lorsque le faux informatique aura été commis dans le but d'obtenir un avantage patrimonial frauduleux, il constituera, en plus, un cas de fraude informatique[279].

La falsification et la contrefaçon de cartes de crédit, et donc le *skimming*, seront considérées comme un faux informatique[280][281]. Tel est également le cas du *phishing*.

187. Si l'escroquerie a pour objectif de tromper la confiance d'une personne physique ou morale pour obtenir la remise ou la délivrance d'un bien, cette définition était de loin trop restrictive pour viser certains comportements commis à l'égard de systèmes informatiques. Ainsi, la loi sur la criminalité informatique a décidé d'étendre les situations visées aux agissements entre un « escroc » et un système informatique en créant une nouvelle infraction. Lorsqu'une personne se fait remettre des données informatiques, comme des données bancaires, non pas par une personne physique, mais par une machine, on parlera de fraude informatique[282]. Cette infraction est visée par l'article 504*quater* du Code pénal[283]. Cet article sanctionne celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique. Il vise donc la simple manipulation de

277 Loi du 28 novembre 2002 relative à la criminalité informatique, M.B., 3 février 2001.

278 F. de Villenfagne et S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique », A. & M., 2001, p. 60-81.

279 S. Evrard, « La loi du 28 novembre 200à relative à la criminalité informatique », J.T., 2001, p. 242.

280 Selon la jurisprudence inédite citée par E. Roger France, *op. cit.*, p 242.

281 Loi du 28 novembre 2002 relative à la criminalité informatique, Exposé des motifs, *Doc. Parl.* Ch. repr., sess. ord. 1999-2000, n° 0213/004, p. 5.

282 E. Roger France, op. cit, p. 240.

283 Pour une étude approfondie de la matière: O. Leroux, « Le faux informatique », *J.T.*, 2004, p. 509.

données informatiques dès lors que l'avantage économique obtenu ou poursuivi est illégale et que l'intention frauduleuse est démontrée[284].

Sont ainsi visés l'utilisation d'une carte de crédit volée pour retirer de l'argent à un guichet, le *skimming*, mais également le dépassement illicite du crédit par le biais de sa propre carte de crédit. Les travaux préparatoires visent aussi l'hypothèse de l'introduction d'instructions de programmation permettant d'obtenir à la suite de certaines transactions d'autres résultats en vue d'un avantage financier illicite, par exemple la modification du solde d'un compte[285].

88. Le *hacking* est visé par un article qui le sanctionne en tant que tel selon que celui qui accède au système informatique possède ou non l'autorisation d'y pénétrer. Il est qualifié comme un comportement qui porte atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises.

L'article 550*bis* du Code pénal sanctionne le hacker qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, c'est-à-dire le fait pour une personne extérieure à l'entreprise de contourner le dispositif de sécurité d'un réseau fermé et d'accéder ainsi au système. Si le hacker n'est pas extérieur à l'organisation, il est sanctionné également si, avec une intention frauduleuse ou dans le but de nuire, il outrepasse son pouvoir d'accès au système informatique.

Le *hacking*, l'espionnage informatique, le vol de données mais également le *phishing* sont incriminés par cette disposition.

Nous renvoyons au texte de ces articles pour les sanctions qui y sont prévues.

Conclusion

9. La matière relative au paiement électronique est éminemment dynamique. D'abord, par la profusion des initiatives législatives, essentiellement d'origine européenne, qui encadrent aujourd'hui la matière des paiements et visent quasi tous ses aspects, que ce soit au niveau de ses modalités ou de ses applications transfrontalières. Il est évident que les trois nouvelles lois prises en vue de la transposition de la SPD vont ouvrir le champ à des adaptations importantes dans le secteur, même si aucun bouleversement à proprement parler n'est à prévoir. Par contre, il serait intéressant de faire le point sur l'avancée du processus législatif, européen d'abord puis national, relatif à la monnaie électronique. Si le marché s'ouvre effectivement, comme l'appelle de ses vœux la Commission, on pourrait voir apparaitre nombre de nouveaux prestataires européens, et par là même de nouvelles initiatives technologiques.

Ensuite, ce dynamisme est fonction des innovations technologiques. En quelques années seulement, internet est devenu incontournable et a acquis le statut de première source d'information. Aujourd'hui les échanges commerciaux sur internet sont courants, et comme *l'accessoire suit le principal*, les moyens de paiement s'adaptent aux besoins de commerçants et des consommateurs. On ne doute donc pas que tous les moyens utiles d'identification électronique et d'authentification des parties apparaitront, pour leur plus grande sécurité et leur plus grande confiance dans ce mode de paiement. Aucun doute non plus quant au développement du M-paiement dans les prochaines années, et à l'éclosion de nouveaux modes de paiement électronique.

La LSP est le fruit d'un consensus murement travaillé au niveau européen. Si les prestataires de services devraient pouvoir s'adapter aux les nouvelles règles qu'elle contient sans trop de difficultés, reste à voir comment la jurisprudence tranchera les questions sémantiques qu'elle laisse ouvertes, en matière d'authentification ou d'identification électronique par exemple, mais aussi en matière de négligence. Même s'il existe une obligation de sécurité à l'égard des titulaires d'instruments de paiement, dans cette matière, les fraudeurs seront toujours les plus subtils.

B. Docquir, « La loi du 15 mai 2006 : Nouvelles définitions des infractions en matière de criminalité informatique », *R.D.T.I.*, 2006, p. 289.

Loi du 28 novembre 2002 relative à la criminalité informatique, Exposé des motifs, *Doc. Parl.* Ch. repr., sess. ord. 1999-2000, n^{os} 0213/001, 0214/001 et 0213/04.