Afgiftekantoor / Bureau de dépôt
Gent X

R D C
T B H

Revue de Droit Commercial Belge

Tijdschrift voor Belgisch Handelsrecht

2005 / 1
JANUARI • JANVIER

Maandelijks tijdschrift / Honderd en tiende jaargang
(Verschijnt niet in juli en augustus)
Revue mensuelle / Cent dixième année
(Ne paraît pas en juillet et août)

LARCIER

RECHTSLEER
DOCTRINE

"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

Olivier Goffard[1]

RÉSUMÉ

Après avoir brièvement passé en revue le champ d'application de la loi du 17 juillet 2002 sur le transfert électronique de fonds, nous analyserons plus profondément le régime de responsabilité instauré par celle-ci.

Plus particulièrement, nous nous attarderons sur la question de la responsabilité du titulaire et de l'émetteur d'un instrument de transfert électronique de fonds lors d'une transaction de paiement par Internet. Ainsi, le titulaire sera exonéré de toute responsabilité lorsque l'instrument de transfert électronique de fonds est utilisé à distance et n'est pas vérifié (identifié) électroniquement. Nous analyserons ces deux conditions et verrons dans quelle mesure quelques-unes des techniques de sécurisation/communication (Soft PKI, SSL, SET, Digipass, 3-D Secure, lecteur de carte connecté à un ordinateur) offertes actuellement afin d'effectuer un paiement sur Internet permettent au titulaire de bénéficier de cette exonération de responsabilité.

SAMENVATTING

Na een korte bespreking van het toepassingsgebied van de Wet van 17 juli 2002 betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen volgt een diepere analyse van het aansprakelijkheidsregime uit deze wet.

Er wordt meer bepaald stilgestaan bij de aansprakelijkheid van de houder en van de uitgever van een instrument voor de elektronische overmaking van geldmiddelen bij een betaling via het internet. Zo is de houder niet aansprakelijk wanneer het instrument voor de elektronische overmaking van geldmiddelen van op afstand wordt gebruikt zonder elektronische verificatie (identificatie). Deze twee voorwaarden worden onderzocht en er wordt nagegaan in welke mate de houder bij sommige beveiligings- en /of communicatietechnieken (Soft PKI, SSL, SET, Digipass, 3-D Secure, kaartlezer die verbonden is aan een computer) die vandaag de dag beschikbaar zijn om betalingen te doen via het internet, gevrijwaard is van aansprakelijkheid.

1. Juriste d'entreprise.

INTRODUCTION[2]

1. La notion de "mouvement électronique de fonds" est déjà apparue dans la doctrine des années '80[3]. Il aura donc fallu attendre plus d'une vingtaine d'années pour qu'une législation spécifique régisse en Belgique les relations entre l'émetteur et le titulaire d'un instrument de transfert électronique de fonds. C'est maintenant chose faite car la loi relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds du 17 juillet 2002[4] (ci-après dénommée "la Loi") instaure certaines règles de bonne conduite dans les relations entre l'émetteur et le titulaire d'un instrument de transfert électronique de fonds. Ces règles doivent être respectées en cas d'utilisation par le titulaire d'un système de paiement électronique *sensu lato*. Cela vise entre autre aussi bien les paiements réalisés par le biais d'une carte de paiement que par l'intermédiaire d'Internet ou de son téléphone.

Cette Loi a introduit un régime de partage des responsabilités financières entre l'émetteur et le titulaire de l'instrument de transfert électronique de fonds en cas d'usage abusif de celui-ci. Ce régime vise à régler la part de risques financiers à supporter par chacun de ces acteurs dans le cadre de l'utilisation fautive ou abusive de l'instrument lorsque celui-ci a été volé ou perdu. Pour autant que le titulaire respecte certaines règles préétablies, ce sera à l'émetteur de supporter ces risques. Une exception à ce régime est néanmoins prévue lorsque l'instrument n'est pas identifié électroniquement et lorsqu'il est utilisé à distance. Cette exception, visée par l'article 8, § 4, de la Loi, est susceptible d'avoir une importance considérable sur les moyens de paiement par Internet (et au moyen de son téléphone portable) en fonction de l'interprétation qui en est faite.

2. La présente contribution s'attachera tout d'abord à fixer brièvement le champ d'application de la Loi (§ 1) ainsi que les responsabilités imposées à l'émetteur et au titulaire de l'instrument de transfert électronique de fonds (§ 2). Nous nous pencherons ensuite sur le partage des risques introduit par la Loi (§ 3) pour clore cet article par une analyse plus poussée de l'exception à ce régime lorsque l'instrument est utilisé sans présentation physique et sans identification électronique (§ 4), et plus particulièrement ses conséquences sur le commerce électronique (§ 5).

§ 1. CHAMP D'APPLICATION DE LA LOI

I. Ratione personae

3. La loi sur le transfert électronique de fonds constitue une transposition en droit belge de la recommandation européenne 97/489/CE du 30 juillet 1997 relative aux opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire[5]. Cette recommandation a été prise en conformité avec la tendance législative européenne en faveur de la protection des consommateurs. Il fallait en effet s'efforcer de gagner la confiance des utilisateurs dans les systèmes de transfert électronique de fonds leur étant proposés.

Le champ d'application *ratione personae* de la Loi est bien circonscrit. Elle ne vise qu'à régler les relations entre l'émetteur et le titulaire d'un instrument de transfert électronique de fonds à l'exception de toute autre relation.

L'émetteur est défini comme *"toute personne qui, dans le cadre de son activité commerciale, met un instrument de transfert électronique de fonds à la disposition d'une autre personne (le titulaire) conformément à un contrat conclu avec celle-ci"*[6]. Cette notion recouvre les établissements de crédits qui mettent une carte de paiement de débit ou de crédit, un système de banque par Internet (*e-banking*)... à disposition de leurs clients, mais aussi les grands magasins, les entreprises pétrolières ou encore les organismes de crédit qui mettent des cartes de paiement (parfois de débit différé[7]) à disposition de leurs clients[8].

Il faut ensuite entendre par titulaire *"toute personne physique qui, en vertu d'un contrat qu'elle a conclu avec un émetteur, détient un instrument de transfert électronique de fonds"*[9]. Sont donc visés les clients personnes physiques des

2. Cet article n'engage que l'opinion personnelle de son auteur. L'auteur remercie J. Vandeloise, S. Pochic et C. Radu pour leurs supports techniques ainsi que F. De Clippele et J. Stuyck pour leurs supports juridiques.
3. D. SYX, "Vers de nouvelles formes de signature? Le problème de la signature dans les rapports juridiques électroniques", *Dr. Inf.* 1986/3, p. 133; D. SYX, "Aspects juridiques du mouvement électronique de fonds", Kredietbank, 1982.
4. Loi relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds du 17 juillet 2002, *M.B.* 17 août 2002, p. 35337.
5. *J.O.C.E.* L 208/52, 2 août 1997.
6. Art. 2, 3°, loi du 17 juillet 2002, *o.c.*
7. La carte VISA est un exemple de carte de paiement à débit différé. Les achats effectués au moyen de cette carte ne doivent en effet être remboursés par le titulaire que le mois suivant.
8. Nous rappelons que la loi du 22 mars 1993 (*M.B.* 19 avril 1993) fixe certaines conditions d'établissement nécessaires en vue de constituer un établissement de crédit ou un établissement de monnaie électronique de sorte qu'il n'est pas permis à toute société de mettre à disposition de sa clientèle un instrument de transfert électronique de fonds.
9. Art. 2, 4°, loi du 17 juillet 2002, *o.c.*

banques et des organismes cités *supra* agissant à des fins professionnelles ou non[10].

I. Ratione materiae

4. La notion d'instrument de transfert électronique de fonds permet de délimiter le champ d'application *ratione materiae* de la Loi. La Loi ne s'appliquera en effet que si un tel instrument est utilisé dans une relation de paiement. Cette notion est définie[11] comme tout moyen permettant d'effectuer par voie entièrement ou partiellement électronique, une ou plusieurs des opérations suivantes:

a) des transferts de fonds à un bénéficiaire;
b) des retraits et dépôts d'argent liquide, par exemple effectués par le biais d'un ATM[12];
c) l'accès à distance à un compte, entre autres afin d'en consulter le solde;
d) le chargement et le déchargement d'un instrument rechargeable, typiquement la carte Proton[13].

Le critère déterminant l'application de cette Loi n'est donc pas le caractère électronique de l'instrument utilisé, mais bien la nature électronique du transfert réalisé au moyen de cet instrument[14].

Le concept d'instrument de transfert électronique de fonds recouvre une réalité assez large. Suivant en cela l'approche de la CNUDCI[15], les travaux parlementaires précisent qu'il suffit en effet qu'une seule des étapes du transfert soit de nature électronique pour tomber sous le champ d'application de la Loi[16]. Lors de l'adoption de la recommandation européenne, le paiement par carte était essentiellement visé même s'il était déjà fait mention des applications de banque à domicile ou par téléphone. Mais à l'heure actuelle, l'évolution technologique est telle que cette définition englobe en réalité la quasi-totalité des paiements bancaires, qu'ils soient réalisés dans le monde physique (paiement au moyen de sa carte de débit ou de crédit, opération de paiement de type virement ou ordre permanent réalisée au moyen d'un *self bank*), sur Internet (*e-commerce*, *e-banking*) ou encore les paiements à l'aide de son téléphone (*m-payments* ou *phone banking*)...

Afin de limiter l'étendue de cette notion, la Loi précise toutefois que certaines opérations, bien que pouvant être qualifiées d'opérations effectuées à l'aide d'un instrument de transfert électronique de fonds selon la définition donnée, ne sont pas visées[17]. C'est ainsi que le législateur a exclu les transferts de fonds réalisés par chèque, par lettre de change ou bien encore les transferts réalisés par virement, ordre de paiement ou domiciliation lorsque ces transferts ont été initialement effectués manuscritement[18]. À la lecture de ces exceptions, il faut comprendre que pour tomber sous le champ d'application de cette Loi, il est nécessaire que l'opération ait été initiée de manière électronique[19].

La Loi comprend après la délimitation de son champ d'application un ensemble de dispositions destinées à régler les relations entre l'émetteur et le titulaire de l'instrument de transfert électronique de fonds. Ces dispositions, que nous n'aborderons pas dans le cadre de cet article, concernent entre autres l'information du titulaire de l'instrument, les obligations respectives de l'émetteur et du titulaire, la recherche et la constatation des actes interdits par la Loi, les sanctions et l'action en cessation découlant de la violation de la Loi.

10. C'est une des différences essentielles avec la notion de consommateur de la loi sur les pratiques du commerce. Selon cette dernière, le consommateur est *"toute personne physique ou morale qui acquiert ou utilise à des fins excluant tout caractère professionnel des produits ou services mis sur le marché"*. Art. 1, 7°, de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.* 29 août 1991.
11. Art. 2, 2°, loi du 17 juillet 2002, *o.c.*
12. Automated Teller Machine.
13. Nous laisserons sciemment de côté dans le cadre du présent article les aspects de la Loi ayant trait aux instruments rechargeables du type porte-monnaie électronique Proton.
14. 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.
15. Commission des Nations-Unies pour le Droit du Commerce International dans son *Legal Guide on Eletronic Funds Transfer.*
16. *Doc. parl.* Chambre, sess. 2000-01, 1389/001, p. 8.
17. Art. 3 loi du 17 juillet 2002, *o.c.* Pour une étude plus approfondie du champ d'application de cette Loi, nous nous permettons de renvoyer le lecteur à T. LAMBERT, "La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds", *R.D.C.* 2003, liv. 7, p. 573.
18. Art. 3, § 1, loi du 17 juillet 2002, *o.c.*
19. La définition donnée en 1982 par D. SYX du mouvement électronique de fonds impliquait déjà que le mouvement soit initié par des moyens électroniques et pas par un instrument papier, mais la Loi précise en outre aujourd'hui que l'automatisation d'une seule des étapes du transfert suffit (D. SYX, *o.c.*, p. 13).

§ 2. RÉGIME DE RESPONSABILITÉS ÉRIGÉ PAR LA LOI

I. Responsabilité de l'émetteur[20]

a) Casuistique de responsabilités

5. La Loi énumère une série d'hypothèses dans lesquelles la responsabilité de l'émetteur sera engagée. Il est toutefois précisé que pour mettre cette responsabilité en cause, le titulaire devra au préalable respecter les obligations qui lui sont imposées. Il aurait en effet été incohérent de rendre l'émetteur responsable en cas de non-respect de ses obligations si ce non-respect trouvait sa source dans la négligence du titulaire. Il adviendra alors au juge de vérifier si le respect par le titulaire de ses obligations était suffisant pour briser le lien causal entre la faute de l'émetteur et le dommage qu'a subi le titulaire. Il s'agit d'une appréciation factuelle en fait qui devra s'effectuer au cas par cas.

Trois cas de responsabilités sont ainsi distingués:

Ainsi, l'émetteur sera-t-il dans un premier temps responsable de l'inexécution ou de l'exécution incorrecte des opérations effectuées à l'aide d'un instrument de transfert électronique de fonds qu'il a émis, à partir de dispositifs, terminaux ou au moyen d'équipements qu'il a agréés, que ces moyens soient placés sous son contrôle ou non. -

Il est étonnant que le législateur ait fait reposer cette agréation sur l'émetteur, c'est-à-dire dans la majorité des cas, sur les banques. Dans le domaine des cartes bancaires les terminaux permettant la lecture des cartes bancaires afin d'effectuer des transactions "point de vente" sont en pratique certifiés, non pas au nom des banques, mais bien au nom des gestionnaires des schémas de paiement adéquat. Ainsi ce sera par exemple à Visa d'agréer un terminal voulant entrer sur le marché belge tout en supportant la fonctionnalité Visa. Notons toutefois que par souci de facilité, toujours dans le monde des cartes bancaires, tous les terminaux de paiement mis sur le marché doivent être agréés par une ASBL fondée en 1998 par la plupart des institutions de crédit présentes en Belgique. Cette ASBL, l'EPCI (*Electronic Payment Certification Institute*[21]) octroie une certification aux terminaux répondant à une série de spécifications bien définies. Ainsi, il ne sera par exemple pas permis à un vendeur de terminaux de paiement de distribuer des terminaux munis de la fonctionnalité de paiement Bancontact/Mister Cash sur le territoire belge sans que ces terminaux aient au préalable été certifiés par l'EPCI.

La responsabilité de l'émetteur pourra dans un deuxième temps être engagée lorsque des opérations ont été effectuées sans autorisation du titulaire de même que pour toute erreur ou irrégularité commise dans la gestion du compte en banque du titulaire qui lui sont imputables. En cas de contestation à cet égard, l'émetteur sera présumé responsable de ces erreurs ou irrégularités. Il aura cependant la possibilité de renverser cette présomption et de prouver par toutes voies de droit qu'aucune faute ne peut lui être imputée[22].

Enfin, l'émetteur sera aussi responsable en cas de contrefaçon de l'instrument de transfert électronique de fonds par un tiers ainsi que pour l'usage de cet instrument contrefait. Il revient en effet à l'émetteur de s'assurer que la technologie mise à la disposition du titulaire est la plus sûre possible. La question se pose de savoir si cette obligation doit être considérée comme une obligation de moyens ou de résultat. Nous pensons que l'obligation mise à charge de l'émetteur ne peut être considérée comme une obligation de résultat. Cette dernière l'obligerait en effet à obtenir le résultat escompté (soit fournir un instrument qui ne peut être contrefait), à moins qu'il ne prouve l'existence d'une force majeure l'ayant empêché d'atteindre ce résultat[23]. De surcroît, la loi sur le transfert électronique de fonds présente un caractère impératif, il est par conséquent impossible pour l'émetteur de se décharger de ses obligations par des accords passés avec les titulaires ayant comme objet de permettre à l'émetteur de s'exonérer de toute responsabilité lorsque l'instrument mis à disposition du titulaire présente un stade avancé de développement technologique[24]. En conséquence de quoi, nous pensons que la qualification d'obligation de moyens doit être retenue. L'émetteur s'engage donc à mettre en œuvre tous les moyens nécessaires pour fournir un instrument de transfert électronique de fonds le moins susceptible d'être contrefait. Une faute ne pourra lui être reprochée que si l'on parvient à prouver que, en prenant en compte l'état actuel de la technique, il ne s'est pas donné les moyens pour respecter ses engagements. À titre d'exemple, nous estimons que les émetteurs de cartes de crédit ont mis tous les moyens en œuvre afin de sécuriser leurs cartes de crédit lorsqu'ils ont introduit la carte de crédit répondant aux normes EMV[25], c'est-à-dire la carte de crédit munie d'une puce électronique.

20. Art. 7 loi du 17 juillet 2002, *o.c.*
21. www.epci.be.
22. Pour une étude plus poussée quant à ces dispositions, nous renvoyons à T. LAMBERT, *o.c.*, ainsi qu'à R. STEENNOT, "Elektronisch betalingsverkeer. Een toepassing van de klassieke principes", in *Financieel Recht Instituut reeks*, nr. 2, Intersentia, 2002.
23. Cass. 18 octobre 2001, disponible sur www.juridat.be.
24. Art. 12, 2°, loi du 17 juillet 2002, *o.c.*
25. Pour Eurocard, MasterCard et Visa.

b) Étendue de la responsabilité

6. Lorsque sa responsabilité sera engagée, l'émetteur devra en outre s'acquitter dans les plus brefs délais du remboursement des sommes déterminées par la Loi.

In casu, lorsqu'une opération n'a pas été effectuée ou l'a été mais de manière incorrecte, l'émetteur sera redevable envers le titulaire du montant de cette opération éventuellement augmenté d'intérêts de retard.

Si une opération non autorisée par le titulaire a été effectuée, l'émetteur devra lui rembourser la somme nécessaire pour le rétablir dans la situation financière dans laquelle il se trouvait avant l'opération augmentée, le cas échéant, des intérêts de retard.

Enfin, si l'instrument de transfert électronique de fonds d'un titulaire a été contrefait et que cette utilisation a nuit au titulaire, l'émetteur devra lui rembourser la somme nécessaire pour le rétablir dans la situation dans laquelle il se trouvait avant l'usage de l'instrument contrefait. Il reviendra de plus au titulaire de démontrer l'ampleur du dommage indemnisable et de, si nécessaire, réclamer réparation de celui-ci. À titre d'exemple, les frais encourus afin de déterminer le dommage réellement subi seront considérés comme conséquences financières à charge de l'émetteur.

Aucun délai fixe n'a néanmoins été fixé afin que l'émetteur effectue ce remboursement. Il faut cependant que le remboursement ait lieu de la manière la plus diligente et rapide possible afin de ne pas faire supporter au titulaire les conséquences liées à la violation par l'émetteur de ses obligations.

II. Responsabilité du titulaire[26]

a) Obligations du titulaire

7. Les responsabilités mises à charge du titulaire doivent être analysées comme le corollaire des obligations qui lui sont imposées.

La Loi impose tout d'abord deux obligations générales à charge du titulaire dans le cadre de l'utilisation de son instrument de transfert électronique de fonds: il doit tout d'abord utiliser l'instrument en bon père de famille et de manière conforme aux conditions en régissant l'utilisation, mais il doit aussi prendre les mesures de sécurité nécessaires à l'utilisation correcte et non abusive de cet instrument (comme par exemple ne pas noter son code secret, le code PIN[27], de manière identifiable dans son portefeuille).

La Loi instaure ensuite une obligation de notification à charge du titulaire. Il devra notifier à l'émetteur de l'instrument ou à toute entité que celui-ci désigne (ex.: Card Stop), dès qu'il en a connaissance, la perte ou le vol de l'instrument de transfert électronique de fonds ou des moyens en permettant son utilisation (les travaux parlementaires citent à titre d'exemple la signature digitale du titulaire[28] à laquelle nous ajoutons le code PIN, le numéro de carte de crédit apparent sur la carte...). Il devra de même notifier dans les mêmes délais, l'imputation sur son relevé ou ses extraits de compte de toute erreur, irrégularité ou opération effectuée sans son accord (ce n'est bien entendu qu'à ce moment qu'il pourra constater que des opérations ont été effectuées sans son autorisation, faisant ainsi reposer la responsabilité du remboursement de ces opérations sur l'émetteur).

b) Irréfutabilité des transactions réalisées au moyen d'un instrument de transfert électronique de fonds

8. La Loi énonce le principe de l'irréfutabilité des opérations effectuées à l'aide d'un instrument de transfert électronique de fonds[29]. Ce principe est communément appelé le principe de non-répudiation des opérations effectuées à l'aide d'un instrument de transfert électronique de fonds. En vertu de ce principe, il est dorénavant interdit au titulaire de révoquer une instruction donnée de manière régulière au moyen de son instrument. L'application de ce principe apporte une sécurité juridique aux commerçants acceptant l'utilisation de tels instruments par leurs clients. Ils auront en effet la certitude que la transaction, une fois qu'elle a été autorisée par le client, et pour autant que sa banque l'autorise financièrement, ne pourra plus ultérieurement être mise en cause par le client.

Ce principe ne s'applique cependant pas aux opérations dont le montant n'est pas connu au moment où l'instruction est donnée. Cette exception permet d'éviter toute tentative de fraude de la part d'un commerçant malintentionné. Est entre autres visée la location d'une voiture ou d'une chambre d'hôtel au moyen d'une carte de crédit car le montant à payer ne sera définitivement connu qu'à la fin de la location[30]. Il en est de même lorsque la carte de crédit est donnée à titre de garantie et que le montant de cette garantie n'est pas déterminé à ce moment[31].

26. Art. 8 loi du 17 juillet 2002, *o.c.*
27. PIN pour Personal Identification Number.
28. *Doc. parl.* Chambre, sess. 2000-01, 1389/001, p. 29.
29. Art. 8, § 1, loi du 17 juillet 2002, *o.c.*
30. T. LAMBERT, *o.c.*, p. 581.
31. R. STEENNOT, *o.c.*, p. 239.

§ 3. PARTAGE DES RISQUES EN CAS D'USAGE ABUSIF D'UN INSTRUMENT VOLÉ OU PERDU[32]

I. Avant la notification

9. La Loi prévoit un régime de partage des risques entre le titulaire de l'instrument et son émetteur lorsque l'instrument a été volé ou perdu et qu'il a été utilisé à des fins frauduleuses. Ce régime prévoit que jusqu'à ce qu'il notifie la perte ou le vol, le titulaire sera responsable des conséquences financières liées à l'usage abusif de l'instrument.

La Loi a cependant fixé un plafond maximum à cette responsabilité financière. Le titulaire ne pourra en effet jamais voir sa responsabilité engagée pour un montant supérieur à € 150 sauf s'il a commis une négligence grave ou s'il a agit frauduleusement. Dans ces deux hypothèses le plafond de € 150 ne sera pas applicable et le titulaire sera responsable de l'entièreté des conséquences financières.

10. Attardons-nous un instant sur ces concepts de négligence grave et de fraude.

Quelques exemples de ce qu'il faut entendre par négligence grave sont indiqués dans la Loi: noter son code PIN de manière aisément identifiable[33] sur ou à proximité de son instrument de transfert électronique de fonds, ne pas avoir respecté son obligation de notification du vol ou de la perte de son instrument dans les meilleurs délais... Cette liste ne peut en aucun cas être considérée comme limitative mais bien comme une sorte de ligne directrice dans la détermination par le juge de la négligence grave du titulaire. Nous précisons,de même à l'instar d'autres auteurs[34] que 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. Il faut en effet que le juge décide, de par les circonstances de la cause, qu'il s'agit bien, *in concreto*, d'une négligence grave. À titre d'exemple, un juge a considéré qu'il y avait négligence grave lorsque les circonstances suivantes étaient cumulativement présentes: le code avait été composé sur un terminal de paiement sans aucune précaution de sécurité, le titulaire avait omis de récupérer sa carte auprès de la caissière qui avait utilisé celle-ci afin de la passer dans le terminal de paiement et enfin, le titulaire avait attendu plusieurs jours avant de notifier la perte de sa carte à Card Stop[35].

La Loi apporte cependant un tempérament à l'appréciation par le juge de cette négligence. Le seul fait que l'instrument ait été utilisé avec le code PIN du titulaire n'est en soi pas suffisant pour attester d'une négligence de la part du titulaire. Cet élément devra en effet être accompagné d'un ensemble de présomptions supplémentaires pouvant fonder la conviction du juge quant à la négligence grave du titulaire. Il s'agit d'un revirement total par rapport à la pratique antérieure à cette Loi où il était de jurisprudence constante que si une carte de paiement était utilisée avec son code secret, cela présumait la négligence grave du titulaire qui avait du soit l'inscrire de manière identifiable à proximité de sa carte, soit le communiquer à un tiers[36]. Cette jurisprudence devenait cependant désuète au vu des efforts déployés par les fraudeurs pour prendre connaissance d'un code secret, que ce soit au moyen de procédés techniques bricolés sur les ATM's ou par le biais de stratagèmes de diversion dont la plupart des clients, même s'ils ne sont pas négligents, peuvent facilement être victimes.

La notion de fraude est quant à elle précisée dans les travaux préparatoires. Il faut entre autres entendre par fraude le fait pour le titulaire de donner son instrument avec le numéro d'identification personnel à un tiers et ensuite adresser une notification à l'émetteur ou bien encore, le fait pour le titulaire d'utiliser lui-même l'instrument après avoir sciemment notifié à l'émetteur sa perte ou son vol[37].

II. Après la notification

11. Après la notification du vol ou de la perte de l'instrument de transfert électronique de fonds, le titulaire ne sera plus responsable des conséquences liées à l'usage abusif de l'instrument sauf si l'émetteur apporte la preuve que le titulaire a agi de manière frauduleuse.

Cette disposition est conforme à la tendance doctrinale et jurisprudentielle existante selon laquelle après la notification, la banque supporte l'entière responsabilité des retraits effectués au moyen de l'instrument même si ceux-ci ont été effectués de par la négligence grave du titulaire[38]. La banque supporte ainsi une obligation de résultat de s'assurer que l'instrument ne pourra plus être utilisé après la notification. Cette jurisprudence a été confirmée par une décision selon

32. Nous ne parlons pas sciemment du partage de responsabilité car il est tout à fait possible que ce régime s'applique sans la moindre faute du titulaire ou de l'émetteur. *Cf.* 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", *Ubiqu.*, n° 16, septembre 2003, p. 24.

33. Une polémique existe à cet égard sur le fait de savoir si inscrire son code PIN sous la forme d'un numéro de téléphone dans son agenda constitue une version identifiable du code.

34. R. STEENNOT, *o.c.*, p. 306.

35. Civ. Bruxelles (11e ch.), 7 décembre 1998, *J.T.* 1999, p. 373.

36. L. ROLIN JACQUEMYNS, *o.c.*, p. 9.

37. *Doc. parl.* Chambre, sess. 2000-01, 1389/001, p. 32.

38. E. MEYSMANS et X. THUNIS, "La réglementation des cartes de crédit en droit belge et en droit européen", *DAOR* 1992, p. 81 ou bien encore Comm. Liège 1984, *Dr. inform.* 1984/2, p. 298.

laquelle une société émettrice d'un instrument de transfert électronique de fonds s'est vue déclarée responsable des débits frauduleux opérés au moyen de cet instrument postérieurement à la notification, indépendamment du fait de savoir si le titulaire avait commis une faute génératrice de l'usage abusif[39].

§ 4. De l'exonération de responsabilité du titulaire prévue par l'article 8, § 4: absence de présentation physique et d'identification électronique

I. Objectif sécuritaire

12. Le régime de partage de risques tel que décrit *supra* ne s'appliquera pas, et le titulaire sera alors exonéré de toute responsabilité, si l'instrument de transfert électronique de fonds a été utilisé sans présentation physique et sans identification électronique. Un tel instrument ne pourra donc être utilisé à distance que s'il a fait l'objet d'une identification électronique. La Loi précise toutefois que la seule utilisation d'un code confidentiel (code PIN ou code secret alphanumérique) ou de tout élément d'identification similaire n'est pas suffisante afin d'engager la responsabilité du titulaire.

Le motif avancé pour justifier cette exception est avant tout sécuritaire. Étant donné qu'un tel paiement n'offrait *prima facie* pas un niveau de sécurité suffisant, il a paru logique au législateur d'en faire supporter les risques à l'émetteur[40]. L'objectif sous-jacent de cette disposition est clairement d'obliger les émetteurs à fournir des instruments de transfert électronique de fonds et des systèmes permettant leur utilisation ayant un niveau acceptable de sécurité. Nous allons dans la suite du texte nous attacher à analyser cette disposition plus en profondeur.

II. Conditions d'application

13. Le titulaire bénéficiera donc d'une exonération de responsabilité si deux conditions cumulatives (et pas alternatives comme la recommandation le préconisait[41]) sont remplies. Il faut que l'instrument ait été utilisé sans présentation physique et qu'il n'ait pas été identifié de manière électronique. L'exemple type d'une telle opération est le *phone banking* dans la mesure où l'insertion d'un numéro de compte ou d'un numéro de carte apparent ainsi que d'un code secret est requis sans qu'il n'y ait pour autant de présentation physique ou d'identification électronique[42].

a) Absence de présentation physique

14. Le concept d'absence de présentation physique suscite le moins de commentaire. Il est directement fait référence à l'utilisation à distance de l'instrument de transfert électronique de fonds. Il s'agit donc typiquement d'une transaction effectuée au moyen de son ordinateur, de son GSM, de son téléphone et même, de manière extensive, sur un ATM[43].

Afin de ne pas rentrer sous cette exonération, il faut donc que le titulaire ait la possibilité de présenter son instrument de transfert électronique de fonds au commerçant.

b) Identification électronique

15. La première question à se poser est de savoir quand considérer qu'un instrument de transfert électronique de fonds peut être identifié. À titre préliminaire nous noterons que le vocable d'identification ne reflète vraisemblablement pas la réalité recherchée par le législateur. Il ne suffit en effet pas que l'instrument soit identifié, mais il faut que cet instrument soit vérifié. Il faut en effet contrôler différents aspects de l'instrument dont sa validité, son caractère authentique...

La Loi précise ensuite, comme nous l'avons préalablement annoncé, que la seule utilisation d'un code confidentiel ou de tout autre élément d'identification similaire n'est pas suffisante pour être considérée comme identification électronique et donc pour engager la responsabilité du titulaire. Ainsi, afin que le titulaire ne puisse pas bénéficier de cette exemption, il sera nécessaire que les solutions de paiement qui lui sont offertes présentent, à côté de l'utilisation d'un code confidentiel permettant d'identifier l'utilisateur, une vérification électronique de l'instrument[44]. Un niveau de sécurité complémentaire à l'utilisation d'un code secret utilisé pour identifier l'utilisateur qui permet de vérifier, d'identifier électroniquement l'instrument est donc requis. À titre d'exemple, les travaux préparatoires disposent que l'identification élec-

39. Gand 7 décembre 1995, *R.D.C.* 1996, p. 1059. Entre autres commenté par A. WILLEMS, "Droit bancaire", Chronique de jurisprudence 1995-2001, in *Droit de l'Informatique et des technologies de l'information*, Larcier, 2003, p. 132.
40. *Doc. parl.* Chambre, sess. 2000-01, 1389/001, p. 32.
41. L'interprétation stricte de la solution alternative de la recommandation aurait entraîné des conséquences néfastes et inacceptables pour l'utilisation de la carte de débit et d'un lecteur de carte comme moyen de paiement sur Internet. En effet, cette hypothèse serait rentrée sous l'exception de la recommandation alors que le niveau de sécurité requis lors de l'insertion de sa carte dans un terminal de paiement dans le monde physique et lors de l'insertion de sa carte de débit dans un lecteur de carte connecté à son ordinateur est identique.
42. M. VAN HUFFEL, "Moyens de paiement et protection du consommateur en droit communautaire et en droit belge", *D.C.C.R.* 2000, p. 35.
43. A. DE BOECK et F. DE CLIPPELE, "Betaalkaarten. Juridische analyse van de rechtsverhoudingen en aansprakelijkheid", *NjW* 2002, nr. 14, p. 484.
44. T. LAMBERT propose comme définition d'identification électronique "tout processus de lecture, de vérification et de validation électronique des données relatives à l'instrument de paiement électronique de fonds", T. LAMBERT, *o.c.*, p. 585.

tronique peut entre autre s'entendre comme une insertion de l'instrument dans un terminal de paiement possédant la capacité technique de vérifier qu'il est bien authentique[45].
De la combinaison de ces deux clauses, nous pouvons conclure qu'à partir du moment où le système de paiement électronique à distance ne requiert comme identification du titulaire que l'insertion d'un code secret ou de tout code personnel d'identification, il est nécessaire, afin que le titulaire ne puisse pas bénéficier de l'exonération de responsabilité que nous examinons, que l'instrument de transfert électronique de fonds soit vérifié. Ainsi, dans le monde physique, lors d'un retrait d'argent via un ATM au moyen de sa carte de débit Bancontact/Mister Cash, le titulaire s'identifie par l'insertion de son code secret alors que l'instrument sera quant à lui, à l'heure actuelle, vérifié par le biais de la technologie présente sur la puce électronique dont est munie chaque carte de paiement Bancontact/Mister Cash, et ce afin d'assurer un niveau de sécurité suffisant. La carte sera donc bien identifiée de manière électronique.

§ 5. APPLICATION AU COMMERCE ÉLECTRONIQUE

I. Introduction

16. Les consommateurs utilisent de plus en plus fréquemment le réseau Internet afin d'effectuer des transactions à distance de manière *"on-line"*. Leur souhait serait de pouvoir étendre leur expérience de paiement actuelle dans le monde physique avec les cartes de débit et de crédit aux paiements à distance, en utilisant cette fois-ci toute une série d'instruments (PC, GSM, PDA[46]...) comme moyen d'accès de la même manière qu'ils utilisent leurs cartes de paiement dans l'environnement physique[47].

Trois problèmes sont à résoudre afin de pouvoir offrir au consommateur des infrastructures de paiement sur Internet aussi sécurisées que le paiement dans le monde physique. Il faut dans un premier temps s'assurer de la confidentialité des informations transmises. Il sera recouru à cette fin au mécanisme de la cryptographie (*cf. infra*). Dans un deuxième temps, il est nécessaire d'assurer aux interlocuteurs que le message transféré n'a pas été transformé lors de son passage sur Internet (il s'agit de l'intégrité). Enfin, dans un troisième temps, il faut assurer que les clés électroniques utilisées lors de la cryptographie appartiennent bien à leur titulaire déclaré. Nous parlerons dans ce cas d'authentification qui sera le résultat de la vérification d'un certificat électronique émis par une autorité de certification. Comme nous le verrons, la plupart des systèmes de paiement analysés garantissent la confidentialité et l'intégrité. Mais seuls certains d'entre eux incluent des mécanismes de signature électronique et de certificat électronique.

17. Ce concept de vérification électronique, s'il est interprété de manière trop extensive, peut avoir un effet néfaste sur le e-commerce où les relations se passent, par définition, sans présentation physique. Afin que le titulaire ne puisse bénéficier de cette exonération de responsabilité, il est donc nécessaire que les moyens de paiement électronique offerts au titulaire présentent, à côté de l'identification de celui-ci au moyen d'un mot de passe ou d'un code d'identification personnel, une vérification électronique de l'instrument de transfert électronique de fonds.

Analysons les différents cas de figures disponibles pour l'internaute afin d'effectuer un paiement en ligne dans le but de vérifier si l'instrument de transfert électronique de fonds est bien vérifié électroniquement.

II. Infrastructure de type "soft PKI"[48]

a) Introduction

18. Une infrastructure de type PKI permet aux utilisateurs d'un réseau public non sécurisé (typiquement Internet) d'échanger des données de manière sécurisée et confidentielle en faisant usage d'une paire de clés privée et publique ainsi que d'un certificat obtenu auprès d'une autorité de certification en qui ils ont confiance. Cette infrastructure permet, lorsque deux interlocuteurs ne se connaissent pas préalablement, de faire appel à un tiers constituant un élément de confiance commun afin de sécuriser la transaction. Le passage par cet intermédiaire apporte un niveau de sécurité permettant aux interlocuteurs d'avoir confiance l'un dans l'autre. Le tiers de confiance devient ainsi garant d'une relation de confiance entre les deux interlocuteurs.

In concreto, le système PKI est un système d'encryption basé sur des clés électroniques utilisant des certificats électroniques émis par des autorités de certification qui permet de vérifier et d'authentifier la validité d'une ou de la totalité des parties impliquées dans une transaction électronique.

Pour rappel, la technologie basée sur la signature digitale de type RSA[49] et PKI est actuellement la seule qui, moyennant

45. *Doc. parl.* Chambre, sess. 2000-01, 1389/001, p. 36.
46. Personal Digital Assistant.
47. C. RADU, "Implementing Electronic Card Payment Systems", in *Computer Security Series*, Artech House, 2003, p. 291.
48. PKI signifie "Public Key Infrastructure".
49. *Cf. infra.*

le respect de certaines conditions, est susceptible de pouvoir être qualifiée de signature électronique avancée qualifiée – et donc être assimilable à la signature manuscrite – au sens des législations sur la signature électronique du 20 octobre 2000[50] et du 9 juillet 2001[51,52]. Cette assimilation lui permettra de bénéficier du principe de non-répudiation associé à la signature manuscrite. En application de ce principe, il est impossible pour une personne de répudier (c'est-à-dire de prétendre ne pas avoir signé) un document sur lequel est apposée sa signature digitale réalisée dans un environnement électronique de type PKI et RSA.

b) Cryptographie symétrique

19. Afin de comprendre le fonctionnement de l'infrastructure PKI, nous devons au préalable rappeler quelques notions de cryptographie. L'idée principale derrière la cryptographie est qu'un groupe de personnes puisse utiliser une connaissance secrète afin de garder des messages écrits confidentiels à l'égard de toute autre personne qui n'est pas partie prenante à cette communication. Il s'agit d'un des moyens permettant de transférer des données de manière sûre dans un canal de communication pouvant être victime d'attaques[53].

Cette technologie permet de faire subir des transformations de chiffrement à un texte initial en clair à l'aide d'une formule mathématique appelée algorithme, de manière à le rendre illisible par celui qui ne possède pas la clé de lecture adéquate (il s'agit du cryptage) et à le restituer en clair après un déchiffrement (il s'agit du décryptage). Le destinataire connaissant la clé de lecture appliquera celle-ci sur le message chiffré afin de le déchiffrer[54].

Il existe deux sortes de cryptographie. La cryptographie symétrique basée sur un algorithme pour lequel la même clé (appelée clé secrète) est utilisée pour le cryptage et le décryptage. L'auteur d'un message encrypte celui-ci à l'aide d'une clé secrète puis communique cette clé de manière sécurisée au destinataire de manière à ce que celui-ci puisse déchiffrer le message qu'il aura reçu.

Afin de garantir le bon fonctionnement de ce mécanisme, il faut bien entendu que cette clé reste tout à fait secrète. Seules les personnes connaissant cette clé doivent en effet être en état de déchiffrer le message[55]. Si la cryptographie symétrique apporte la confidentialité des informations partagées, elle présente néanmoins de nombreux désavantages: une paire de clé distincte doit être utilisée pour chaque paire d'utilisateurs[56]; une des parties à la transaction peut non seulement lire les messages envoyés par l'autre partie mais aussi se faire passer pour celle-ci (avec les problèmes d'irréfutabilité que cela peut entraîner) étant donné qu'elle connaît la clé que l'autre partie utilise afin de crypter des messages; l'échange de clés doit se faire par un canal sûr, l'idéal étant même une rencontre physique entre les parties à la communication…

c) Cryptographie asymétrique

20. La cryptographie asymétrique est basée sur un algorithme auquel sont associées deux clés distinctes, une privée connue de son seul utilisateur, et une publique connue de tous au moyen d'une publication dans un annuaire ou sur un site web[57]. Les deux clés sont liées de manière indissociable l'une à l'autre de sorte que tout message chiffré avec la clé publique ne pourra être déchiffré qu'avec la clé secrète correspondante et *vice versa*[58]. Une formule mathématique unit de plus ces deux clés de manière à les rendre complémentaires[59]. La cryptographie asymétrique présente deux caractéristiques très utiles dans le cadre de la sécurisation du transfert de données électroniques: les fonctionnalités de chiffrement et de signature.

La fonctionnalité de chiffrement permet non seulement d'authentifier son interlocuteur, d'assurer l'intégrité ainsi que l'irréfutabilité du message transmis mais aussi de préserver la confidentialité des informations transmises.

En effet, si le destinataire d'un message crypté à l'aide de la clé privée de son auteur arrive à le déchiffrer à l'aide de la clé publique qu'il pense associée à la clé privée de l'auteur, il pourra alors avoir la certitude que la personne lui ayant envoyé le message est bien l'auteur du message car seule la clé privée de ce dernier était en mesure de le chiffrer. L'authentification de l'auteur est donc assurée de même que le principe d'irréfutabilité car il est impossible pour l'auteur d'un message de prétendre ne pas avoir envoyé ce message

50. Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extra-judiciaire, *M.B.* 22 décembre 2000, p. 42698.
51. 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.
52. Pour plus de détail quant à cette affirmation, nous nous permettons de renvoyer le lecteur à E. ROGER FRANCE et E. DE GROOTE, "La valeur probante des signatures électroniques", *R.D.C.* 2002, liv. 3, p. 185.
53. La cryptographie est ancienne. Le premier exemple de cryptographie remonte à 1.900 ACN en Égypte où un scribe a utilisé des hiéroglyphes non-standards lors d'une communication (B. SCHNEIDER, *Secret & lies. Digital security in a Networked World*, Wiley computer publishing, 2000, p. 86).
54. J. HUBIN et Y. POULLET, "La sécurité informatique, entre technique et droit", *Cahier du CRID*, n° 14, E. Story-Scientia, 1998, p. 70.
55. L'exemple-type de cryptographie symétrique est le DES pour Data Encryption Standard. La longueur générale de la clé de chiffrement utilisée est à notre époque de 128 bits.
56. Ainsi, pour un réseau de 100 utilisateurs, 4.950 clés seront nécessaires. B. SCHNEIDER, *o.c.*, p. 89.
57. Les clés publiques utilisées dans ce mécanisme sont certifiées de manière électronique par une autorité de confiance.
58. L'exemple-type de cryptographie asymétrique est le RSA, du nom de ses fondateurs Rivest, Shamir et Adleman. La longueur générale de la clé de chiffrement utilisée est de 1024 bits.
59. E. ROGER FRANCE et E. DE GROOTE, *o.c.*, p. 196.

à partir du moment où le destinataire a réussi à le lire en utilisant la clé publique qui était liée à sa propre clé privée.

La confidentialité du message pourra également être assurée à l'aide de ce mécanisme. L'auteur d'un message utilisera une clé publique afin de crypter le message qu'il désire envoyer. La clé privée permettant de lire le message crypté à l'aide de la clé publique de l'auteur étant unique, l'auteur sera certain que seul le destinataire qui est en possession de la bonne clé privée pourra déchiffrer le message. Il en assure donc la totale confidentialité. Il est bien entendu possible, et même recommandé, de coupler les aspects d'authentification, d'irréfutabilité et de confidentialité en cryptant le message au moyen de deux paires distinctes de clés.

Dans le cadre de la fonctionnalité de signature, la signature prendra la forme technique d'un algorithme de hachage jouant sur un message en clair, cet algorithme étant lui-même crypté par la clé privée de l'auteur. Il faut donc un premier lieu appliquer sur le message en clair un algorithme de hachage (ex.: l'algorithme appelé "SHA-1[60]") permettant de condenser le message de manière à le transformer en une suite de chiffres que l'on appellera d'un point de vue technique le "hash". L'auteur cryptera alors ce "hash" à l'aide de sa clé privée. Il obtiendra alors une seconde suite de chiffres que l'on peut considérer comme étant sa "signature". Il enverra alors à son destinataire le message initial en clair accompagné de cette "signature". Le destinataire va alors décrypter le hash reçu en utilisant la clé publique de l'auteur. Il utilisera alors le même algorithme de hachage ("SHA-1") afin de générer un nouveau "hash" sur le message reçu en clair. Si le résultat obtenu par ce biais est identique au résultat obtenu lorsqu'il ferra jouer sa clé publique sur la "signature" reçue, il pourra alors avoir la certitude que le message provient bien de son émetteur car la clé publique utilisée pour décrypter la signature digitale correspond bien à la clé privée de l'auteur: il authentifiera son interlocuteur (le cas échéant par un jeu de certificats électroniques) grâce à sa signature et confirmera ainsi son identité.

d) Infrastructure PKI

21. L'infrastructure PKI est basée sur le mécanisme de cryptographie asymétrique tel que décrit *supra*. À l'heure actuelle, le mecanisme de cryptographie asymétrique le plus répandu est sans nul doute le RSA[61]. À ce mécanisme cryptographique sera associé une paire de certificats électroniques. L'auteur d'un message signera celui-ci au moyen de sa clé privée selon la procédure décrite ci-dessus et l'enverra au destinataire.

Un problème se pose immédiatement. Comment le destinataire va-t-il prendre connaissance de la clé publique de l'auteur et surtout, comment va-t-il avoir l'assurance que cette clé publique est bien celle de son auteur? La solution initiale a été de publier toutes les clés publiques dans des bases de données immenses. Cette solution fut vite abandonnée car elle entraînait avec elle un autre inconvénient, la sécurisation de cette base de donnée. Il a été décidé de faire appel à un tiers en qui aussi bien l'auteur que le destinataire du message ont confiance. Ce tiers joindra de manière indissociable le nom de l'auteur et sa clé publique dans un certificat qu'il signera à son tour à l'aide de sa clé privée. Il ne suffira plus au destinataire que de vérifier que le certificat est toujours valable[62] afin de pouvoir avoir la certitude que la clé publique appartient bien à l'auteur du message. L'auteur du message enverra donc au destinataire le message accompagné d'un certificat comprenant la clé publique de lecture, le nom de l'auteur, sa fonction, son e-mail, les coordonnées de l'autorité de certification, les renseignements relatifs à la clé publique ainsi que d'autres données.

En Belgique, la loi régit cette matière et fixe un statut spécial pour ces tiers de confiance appelés "prestataire de service de certification"[63]. Le destinataire, qui est en possession de la clé publique de l'autorité de certification, va alors appliquer cette clé sur le certificat afin de vérifier le lien entre l'identité de l'auteur et la clé publique de lecture. Il aura, de par la confiance qu'il a dans l'autorité de certification, obtenu confirmation de l'identité de l'auteur, émetteur du message, il aura authentifié ce dernier. Il pourra ensuite décrypter le message grâce à la clé publique dont il vient de prendre connaissance.

e) Application de l'exemption de responsabilité de l'article 8, § 4 au soft PKI

22. Dans les solutions d'*e-banking* offertes par certains établissements de crédit, les clés et les certificats dont nous venons de faire mention doivent au préalable être enregistrés sur le disque dur de l'ordinateur ou sur une disquette avec les désavantages sécuritaires que cela comporte[64]. C'est ce que l'on nommera le *"soft PKI"* pour *software PKI* car le mécanisme de sécurité est seulement enregistré sur un logiciel et n'est pas incorporé dans un environnement plus sécurisé tel qu'une puce électronique.

Vérifions à présent si les deux niveaux de sécurité requis afin d'empêcher que le titulaire ne puisse bénéficier de l'exemp-

60. Pour Secure Hash Algorithm.
61. *Cf.* note 58.
62. Il devra pour ce faire vérifier que ce certificat n'a pas été publié sur une liste de certificats révoqués (appelée *Certificate Revocation List*).
63. Selon l'art. 2, 10°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *o.c.*, le prestataire de service de certification est *"toute personne physique ou morale qui délivre ou gère des certificats ou fournit d'autres services liés aux signatures électroniques"*.
64. Il est en effet beaucoup plus facile pour un *hacker* de prendre connaissance des clés et des certificats à partir du moment où ils sont enregistrés sur un ordinateur qui est connecté à l'Internet que lorsqu'ils ont été enregistrés dans une carte à puce. De même, lorsque les logiciels et/ou les clés sont enregistrées sur une disquette, comment s'assurer que cette disquette n'a pas été copiée et que la disquette utilisée est bien la disquette originale.

tion de responsabilité prévue par l'article 8, § 4 sont bien présents dans les systèmes de paiement basés sur le *soft PKI*.

Le premier niveau de sécurité, soit l'identification du titulaire, est présent non seulement grâce à l'insertion par le titulaire d'un code secret permettant d'initialiser le mécanisme cryptographique mais aussi grâce à l'infrastructure PKI et ses certificats qui permet de confirmer cette identité, d'authentifier le titulaire.

L'instrument, c'est-à-dire l'infrastructure composée du logiciel, des clés et des certificats électroniques, sera bien vérifiée électroniquement étant donné qu'une autorité tierce (le prestataire de service de certification) apportera l'assurance que les clés et les certificats sont bien originaux et valides de sorte que le second niveau de sécurité sera lui aussi présent.

En conséquence, cette solution, même si pouvant être mise en cause d'un point de vue sécuritaire, répond juridiquement aux attentes de la Loi de sorte qu'un commerçant offrant cette infrastructure de paiement à ses clients pourra bénéficier d'une certaine sécurité juridique étant donné que le titulaire ne pourra pas bénéficier de l'exemption de responsabilité tel qu'établi par la Loi.

III. Mécanisme de paiement SSL[65] et SET[66]

a) Introduction

23. Certains sites de vente par Internet offrent aussi à leurs clients la possibilité d'autoriser un paiement en insérant et confirmant leur numéro de carte de crédit (le PAN) et la date de validité de cette carte. Le protocole utilisé afin de sécuriser la communication des données s'appelle le SSL. 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[67].

SSL est un protocole constitué d'un ensemble de règles régissant l'authentification du serveur d'un marchand, une communication des données de paiement encryptée entre le serveur du marchand et l'ordinateur du client et enfin, mais de manière optionnelle une authentification du client[68].

b) Fonctionnement du SSL

24. Cette infrastructure se compose d'une sorte de canal de communication sécurisé entre le serveur du marchand et l'ordinateur du client. À l'heure actuelle, SSL est intégré d'origine dans la majorité des navigateurs Internet disponibles sur les ordinateurs des clients ainsi que sur les serveurs web des marchands. Les données qui transitent par ce canal seront cryptées au moyen de la cryptographie asymétrique, telle que décrite ci-dessus, de telle manière que la confidentialité en sera assurée.

Une transaction en SSL se déroule de la manière suivante: lors de la phase de transaction, le serveur présentera sur requête du client son certificat électronique contenant sa clé publique encryptée par la clé privée de l'autorité de certification. Le client vérifiera alors la validité du certificat grâce à la clé publique de l'autorité de certification contenue dans le navigateur[69]. Si le certificat est valide, le client enverra les données de paiement de manière cryptée au serveur. Il cryptera ces données à l'aide de la clé publique du serveur marchand qu'il vient d'obtenir. Le serveur pourra alors déchiffrer le message à l'aide de sa clé privée qu'il est le seul à connaître.

c) Critiques du SSL

25. Cette infrastructure SSL présente cependant un défaut majeur. Il suffit en effet pour pouvoir utiliser ce protocole, que le client insère le numéro apparent de sa carte de crédit ainsi que sa date de validité afin d'autoriser le paiement de sorte qu'il n'y a aucune vérification de l'identité du client. Il n'existe en effet pas d'authentification du client au moyen d'un certificat[70]. Ce problème sécuritaire n'est pas neuf puisqu'il avait déjà été effectué par certains auteurs avant l'entrée en vigueur de la Loi[71].

Notons aussi que par cet intermédiaire le commerçant rassemble un nombre important de numéros de carte de crédit et de dates de validité. Si son site venait à être victime d'un piratage, ces données pourraient être utilisées à des fins malhonnêtes par le pirate.

d) Application de l'exemption de responsabilité de l'article 8, § 4 à SSL

26. L'identification du titulaire au moyen d'un code secret ou d'un autre code alphanumérique, n'est pas présente dans les mécanismes de paiement en ligne basés sur SSL. En effet, aucun code secret n'est requis, il suffit juste d'insérer deux

65. Secure Sockets Layer développé par Netscape et MasterCard, récemment remplacé par le protocole TLS (Transport Layer Security).
66. Secure Electronic Transaction développé par Visa et MasterCard.
67. M. GUSTIN, *o.c.*, p. 332.
68. J. BUYLE, "Le paiement sur internet", *J.T.* 2001, n° 6000, p. 130.
69. Cette phase est réalisée lorsqu'une fenêtre à l'écran demande à l'internaute de donner son numéro de carte et sa date de validité.
70. Cette fonctionnalité pourrait cependant être implémentée à la demande de l'utilisateur mais cela n'arrive jamais dans la quasi-totalité des cas pour des raisons pratiques. Il est en effet quasi-impensable d'obliger un utilisateur à effectuer toute une série de démarches afin d'obtenir un certificat vu la complexité desdites démarches.
71. T. VERBIEST et E. WÉRY, *Le droit de l'internet et de la société de l'information*, Larcier, 2001, p. 312.

informations apparentes sur la carte de crédit ne remplissant de ce fait pas les conditions requises par la Loi. L'authentification du titulaire est absente de ce mécanisme de paiement.

L'analyse faite pour le *soft PKI* quant à la vérification électronique de l'instrument s'applique de manière identique à SSL. Les clés d'encryption utilisées dans SSL seront en effet authentifiées et validées par une autorité tierce qui les aura encodées dans un certificat.

En raison de cette absence d'authentification du titulaire, le titulaire pourra selon nous bénéficier de l'exonération de responsabilité prévue par l'article 8, § 4 de la Loi lorsqu'il effectue un paiement en ligne basé sur le protocole SSL.

e) L'alternative SET

27. Afin de palier à cette absence d'authentification du titulaire, diverses sociétés ont mis sur pied un standard appelé SET qui permet d'authentifier le client grâce à un mécanisme de signature électronique avancée[72] qualifiée[73].

Ce standard permettra à la différence du protocole SSL de confirmer l'identité des deux parties à la transaction. La technologie SET est en effet basée sur la technologie de la cryptographie asymétrique utilisée dans un environnement PKI qui permet, comme nous l'avons vu, d'authentifier le commerçant et le client grâce à un système de certificats, d'assurer l'irréfutabilité de la transaction passée par le client et enfin de permettre le cryptage des données de paiement[74]. Ce protocole repose sur la délivrance par une autorité de certification de certificats permettant d'une part d'identifier les parties en présence, mais aussi de les authentifier. Un lien sera créé de par ce certificat entre une carte de crédit et son titulaire.

f) Fonctionnement du SET

28. Le fonctionnement du SET est le suivant: le client accède au site du marchand et remplit le formulaire de commande en spécifiant entre autres la carte de paiement utilisée. Il confirme la commande et fournit les instructions de paiement qu'il enverra (sans que le marchand puisse en prendre connaissance, c'est-à-dire de manière cryptée) accompagnée de la commande au marchand. Celui-ci, s'il accepte la commande, les transférera directement à sa banque afin de les décrypter. La banque vérifiera l'identité de l'acheteur ainsi que la validité du certificat. Si cette vérification est positive, la banque le fera savoir à son client et autorisera ainsi que la transaction se déroule[75]. Le paiement se déroulera ensuite sur base de l'infrastructure PKI[76].

g) Application de l'exemption de responsabilité de l'article 8, § 4 à SET

29. Étant basé sur l'infrastructure PKI, tout comme le *soft PKI*, le SET assure lui aussi la vérification électronique de l'instrument de paiement de par l'intervention du prestataire de service de certification émettant les certificats.

Par contre, l'identification du titulaire par l'insertion d'un code secret ou de tout autre code secret n'est pas plus présente avec le SET qu'avec le SSL de sorte que l'exonération de responsabilité introduite par la Loi trouvera bien à s'appliquer. Le titulaire ne pourra en aucun cas, en cas de paiement en ligne utilisant les protocoles de sécurisation SSL ou SET, être tenu pour responsable des conséquences financières liées à l'utilisation abusive de son instrument de paiement.

IV. 3-D Secure[77,78]

a) Introduction

30. Une autre solution afin d'effectuer des paiements en ligne consiste dans l'utilisation de l'infrastructure de sécurisation mise sur pied par Visa, le *"3 Domain Secure"*. Il s'agit d'une solution de paiement permettant à une banque émettrice d'une carte de paiement d'authentifier son client afin de réduire la fraude sur Internet. Ce mécanisme présente la particularité de diviser une transaction de paiement en trois domaines indépendants. Le premier domaine se situe dans les relations entre le client et sa banque (dite émettrice), le deuxième est constitué des relations entre le marchand et sa banque (dite acquéreuse) alors que le troisième comprend le réseau mis en place par les schémas de paiement Visa et MasterCard permettant de connecter via l'Internet les différentes banques émettrices et acquéreuses. Le 3-D Secure se limite à standardiser le 3ème domaine de sorte que les banques acquéreuses et émettrices peuvent librement définir leur propre domaine.

---

72. Pour rappel, une signature électronique avancée est définie par la loi comme étant *"une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes: a) être liée uniquement au signataire, b) permettre l'identification du signataire, c) être créée par des moyens que son signataire puisse garder sous son contrôle exclusif, d) être liée aux données auxquelles elle se rapporte de sorte que toute modification ultérieure des données soit détectée"*, art. 2, 2°, de la loi du 9 juillet 2001, *o.c.*
73. Une signature électronique avancée sera dite qualifiée lorsqu'elle repose sur des certificats qualifiés répondants aux critères techniques fixés dans la loi.
74. Dont le numéro de carte de crédit et sa date de validité.
75. T. VERBIEST et E. WÉRY, *o.c.*, p. 321; C. RADU, *o.c.*, p. 322.
76. Notons toutefois que Visa et MasterCard ont pris la décision de ne plus supporter le protocole SET.
77. Un autre nom de cette technologie est "Verified by Visa".
78. Ce développement est en partie inspiré de "Visa: 3-D Secure. Introduction. V.1.0.2." disponible sur http://international.visa.com/fb/paytech/secure/pdfs/3DS_70001-01_Introduction_v1.0.2.pdf.

b) Fonctionnement du 3-D Secure

31. Le client désirant effectuer des achats en ligne chez un marchand participant de manière contractuelle au système 3-D Secure doit, de manière générale, au préalable s'inscrire auprès de sa banque (émettrice) de manière à ce que celle-ci, lors d'une transaction puisse l'authentifier[79]. Lors de cette phase d'inscription, le client devra communiquer diverses données lui permettant de s'identifier. La banque vérifiera alors les réponses du client et confirmera l'inscription si ces données sont correctes. Les informations seront enregistrées dans une base de données de la banque appelée *l'Access Control Server* (ci-après "ACS").

Une fois cette phase d'inscription terminée, le client pourra réaliser des transactions en ligne utilisant la technologie 3-D Secure. Il cliquera pour ce faire sur l'icône adéquate lui permettant de choisir le schéma de paiement qu'il désire utiliser, soit Visa ou MasterCard.

Afin de s'identifier, il fournira à la demande du serveur marchand une série d'informations dont son PAN et un numéro d'identification personnel qui lui aura été fourni lors de son inscription. Le logiciel installé sur le serveur du marchand enverra alors de manière cryptée ces informations vers une base de données du schéma de paiement choisi[80]. Cette base de données vérifiera dans un premier temps si la banque émettrice est inscrite afin de pouvoir faire bénéficier ses clients de la technologie 3-D Secure. Elle vérifiera ensuite si le client est bien enregistré et si sa carte est toujours valable. La base de données du schéma de paiement enverra enfin les données relatives à la transaction (dont l'URL[81] de l'ordinateur du porteur de carte) à l'ACS. Celui-ci se connectera alors avec l'ordinateur du client, via l'URL qu'il aura reçu, afin de faire démarrer la troisième phase, la phase d'authentification.

Le client devra ensuite s'authentifier et autoriser la transaction en insérant un code secret qui sera généré par un mécanisme ayant été choisi de manière discrétionnaire par chaque banque (ex.: au moyen d'un Digipass – voir ci-après –, au moyen d'un *"unconnected card reader"*[82] ou grâce aux moyens d'authentification offerts par chaque banque dans le cadre de leurs solutions d'*e-banking*). Au terme de cette phase d'authentification, et pour autant que la réponse soit positive, l'ACS enverra de manière cryptée au serveur marchand un message contenant les données d'authentification du client et précisant que celle-ci fût un succès. Le marchand présentera alors à sa banque (acquéreuse) les données relatives à la transaction, accompagnées des résultats de l'authentification du client. La banque acquéreuse se chargera alors de l'autorisation financière de la transaction.

Le mécanisme de paiement *sensu stricto*, suivant les phases d'identification et d'authentification, se réalisera entre le marchand et le client de manière sécurisée sur base du protocole SSL.

c) Authentification d'un client au moyen d'un Digipass

32. Le Digipass est un module de sécurité fourni par les banques émettrices à leurs clients. Il s'agit d'un mécanisme d'authentification et de signature se présentant sous la 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 (un montant ou un numéro de compte, etc.) et d'un code personnel.

Chaque Digipass est unique car il contient un identifiant unique, une paire de clés cryptographiques spécifiques[83] ainsi qu'un code secret. Lors de la remise du Digipass à son client, la banque crée un lien entre le Digipass et le numéro de carte du client.

Ces Digipass offrent deux grands types de fonction: la fonction d'authentification et la fonction de signature électronique. Chacune de ces fonctions peut être initiée par la pression de la touche adéquate sur le Digipass ainsi que par l'insertion d'un code secret. Dans les deux cas, le résultat obtenu est une combinaison de chiffres dynamique affichée sur l'écran du Digipass et destinée à être insérée sur le clavier de l'ordinateur à des fins d'authentification ou de signature.

De manière pratique, c'est l'ACS qui sera susceptible de générer le code secret à insérer dans le Digipass[84]. Il communiquera ce numéro au client via son ordinateur. Le client initialisera son Digipass au moyen de son code secret obtenu lors de la phase d'inscription puis introduira le numéro qui vient de lui être fourni. Le résultat obtenu sera une suite de chiffres qui devra à son tour être insérée par le client sur son

79. D'un point de vue irréfutabilité de la transaction, il est important de noter que le commerçant qui adhère à 3-D Secure bénéficie d'une garantie conventionnelle d'être payé en toutes circonstances, y compris dans les cas où le titulaire contesterait la transaction ou serait reconnu non responsable de la transaction.

80. Par exemple, la Visa directory si Visa a été choisi comme schéma de paiement.

81. URL signifie *Uniform Resource Locator*, il s'agit de l'adresse permettant de localiser un site, un document ou tout autre élément sur l'Internet.

82. Il s'agit d'un lecteur de carte à puce relié de manière non physique (c'est-à-dire sans fil) à l'ordinateur du client, par exemple au moyen de la technologie Bluetooth.

83. À côté de la technologie du Digipass, il est aussi possible d'utiliser comme moyen d'authentification, une carte à puce et un lecteur de carte. Dans ce cas, les clés électroniques se trouveront dans la puce de la carte et pas dans le lecteur qui, à la différence du Digipass, ne sera pas "lié" à son utilisateur.

84. Il est aussi possible que, lors de l'initialisation originale du Digipass, son détenteur doive lui-même insérer un code qui sera destiné à être utilisé plus tard comme code secret.

ordinateur. Cette suite de chiffre sera transmise à l'ACS afin que celui-ci vérifie si le résultat obtenu est valide.

Si c'est le cas, le serveur bancaire confirmera l'identité du client. Le numéro obtenu après avoir fait calculé le Digipass couplé au numéro de client inséré préalablement donneront effectivement l'assurance à la banque qu'il s'agit bien du client étant donné que le Digipass, lorsqu'il a été octroyé au client, a été personnalisé de manière à créer un lien avec son titulaire, et donc par conséquent aussi avec les numéros obtenus après avoir fait fonctionner celui-ci. Le client, afin d'autoriser une transaction 3-D Secure au moyen de son Digipass, dispose donc de deux éléments: le Digipass qui doit lui-même être activé par un code secret, et le code généré par cet appareil.

d) Application de l'exemption de responsabilité de l'article 8, § 4 au 3-D Secure

33. Après avoir utilisé le protocole SSL nous avions constaté que le client pouvait bénéficier de l'exonération de responsabilité prévue par la Loi car un des deux niveaux de sécurité requis, à savoir l'identification du titulaire, n'était pas présent.

Le mécanisme d'authentification 3-D Secure, qui emploie le protocole SSL comme protocole de sécurisation, a remédié à cette faiblesse en mettant sur pied une procédure de confirmation de l'identité du titulaire fort développée permettant de réduire de manière importante les risques de fraude sur Internet. L'exonération de responsabilité du titulaire ne jouera pas lorsqu'un paiement *on-line* est basé à la fois sur le protocole SSL et le mécanisme d'authentification 3-D Secure, apportant de la sorte une sécurité juridique plus grande aux commerçants.

V. Utilisation de la carte de paiement Bancontact/Mister Cash et d'un lecteur permettant la lecture de cette carte connecté à un ordinateur

34. Une autre possibilité pour le client d'effectuer des transferts de fonds sur l'Internet consiste en l'insertion de sa carte de débit dans un terminal personnel relié à son ordinateur. De tels terminaux, se présentant sous la forme d'un boîtier muni d'un clavier et d'un écran et offrant la possibilité d'y insérer une carte à puce, sont entre autres commercialisés par les sociétés Banksys et Zetes.

Après avoir sélectionné le produit à acheter et le mode de paiement, par exemple Bancontact/Mister Cash, le client verra apparaître sur son écran une série d'informations relatives à sa commande. Lors de la phase de paiement, il sera au préalable demandé au client d'insérer sa carte de débit dans son terminal. Le montant de la transaction apparaîtra sur l'écran de son terminal. Il devra alors, afin d'autoriser la transaction, insérer son code PIN sur le clavier du terminal.

À l'instar du retrait d'argent à un ATM par le biais de sa carte Bancontact/Mister Cash dans le monde physique ou de la réalisation d'un paiement chez un marchand via un terminal point de vente[85], l'identification du titulaire et la vérification de l'instrument seront basés sur l'insertion de la carte de paiement dans un terminal. Le titulaire sera identifié par l'insertion de son code secret alors que la puce électronique de la carte sera ici aussi sollicitée dans le processus de vérification électronique de l'instrument de transfert électronique de fonds.

Ce processus est en tout point similaire au paiement dans le monde physique et répond bien au critère de l'identification électronique car en plus de l'insertion d'un code PIN, premier niveau de sécurité requis, l'autorisation de la transaction nécessite aussi que la puce effectue un calcul de cryptographie symétrique afin de vérifier la validité de la carte. L'identification électronique en cas d'utilisation d'un terminal personnel a de plus déjà été confirmée à différentes reprises par divers auteurs[86] ainsi que par les travaux parlementaires[87].

85. M. GUSTIN, "Les paiements électroniques", *Act. dr.* 2002/3, p. 334.
86. A. SALAÜN, "Transposition de la directive contrats à distance en droit belge: commentaire de l'article 20 de la loi du 25 mai 1999", *J.T.* 2000, p. 44; M. GUSTIN, *o.c.*, p. 351.
87. *Doc. parl.* Chambre, Sess. 2000-01, 1389/001, p. 36.

CONCLUSIONS

35. De l'examen des différents modes de paiement sur Internet présentés, nous pouvons constater que, à l'exception des technologies SET et SSL, les différentes technologies utilisées répondent au critère de "l'identification électronique" tel qu'exigé par la Loi afin que l'exonération de responsabilité en faveur du titulaire de l'instrument de transfert électronique de fonds prévue par l'article 8, § 4 de la Loi ne puisse pas s'appliquer. Les deux niveaux de sécurité – l'identification du titulaire et la vérification électronique de l'instrument – sont en effet présents de sorte que les commerçants qui optent pour une sécurisation basée, par exemple, sur le 3-D Secure ou sur un mécanisme d'authentification reposant sur l'insertion d'une carte à puce dans un lecteur personnel, pourront bénéficier de la même sécurité (juridique et physique) que celle présente dans le monde physique. L'expérience de paiement des titulaires de l'instrument de transfert électronique de fonds sera de surcroît reconstituée puisqu'ils auront l'occasion de s'identifier et que leur instrument de paiement sera vérifié électroniquement tout comme c'est le cas lors d'une transaction "point de vente" normale.

Cependant, bien que les solutions actuellement développées apportent, selon nous, une sécurité juridique suffisante, il ne faut néanmoins pas perdre de vue que ces technologies dépendent en grande partie de leurs mises en œuvre. Afin d'apporter une sécurité quasi-optimale, l'évolution des technologies devra tendre vers des solutions de paiement qui utilisent des moyens d'authentification individualisés et non copiables, couplés à des infrastructures de paiement les plus sophistiqués faisant usage des mécanismes de sécurisation les plus avancés. Cette sécurisation dépendra néanmoins de la faculté d'adaptation des professionnels du secteur qui devront sans cesse tenter de prévenir les tentatives de fraude visant les solutions de paiement qu'ils mettent à disposition des institutions de crédit, des commerçants et des utilisateurs. Cette matière en constante évolution ne trouvera cependant tout son sens que moyennant des adaptations législatives faisant appel à une capacité de réaction rapide du législateur. Il est en effet utopique de penser que les différentes législations qui s'appliquent à l'heure actuelle au domaine du paiement électronique pourront continuer à régir toutes les facettes évolutives de cette matière, sans subir la moindre modification ou adaptation. Prenons par exemple les paiements réalisés au moyen de son téléphone portable. Ce type de paiement, qui obtient un succès sans cesse grandissant au niveau mondial, devrait entre autres être régi par la loi sur le transfert électronique de fonds. Or, en l'état actuel de cette législation, il est pour ainsi dire impossible de répondre à toutes les exigences imposées par la Loi qui a été prise à un moment où le *mobile-payment* n'était encore qu'en gestation.