DOC 50 **1389/002**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

5 februari 2002

WETSONTWERP

betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen

AMENDEMENTEN

Nr. 1 VAN DE HEER **VAN APEREN**

Art. 3

In § 1, het 4° vervangen als volgt:

«4° op de overmakingen van geldmiddelen verwezenlijkt door middel van een met de hand geschreven tot stand gebrachte overschrijving;

5° doorlopende betaalopdrachten of domiciliëringen.».

VERANTWOORDING

Het is evident dat domiciliëringen en permanente opdrachten niet meer via met de hand geschreven papieren overschrijvingen gebeuren. Meer zelfs: de uitvoering van permanente opdrachten en domiciliëringen gebeurt automatisch tussen de schuldeiser(s) en de bank. Er is geen enkele tussenkomst van

Voorgaande document :

Doc 50 **1389/ (2000/2001)** :
001 : Wetsontwerp.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

5 février 2002

PROJET DE LOI

relatif aux opérations effectuées au moyen d'instruments de transfert électronique de fonds

AMENDEMENTS

N° 1 DE M. **VAN APEREN**

Art. 3

Au § 1er, remplacer le 4° par les dispositions suivantes :

« 4° aux transferts de fonds réalisés au moyen d'un virement manuscrit ;

5° aux ordres de paiement permanents ni aux domiciliations. ».

JUSTIFICATION

Il est évident que les domiciliations et les ordres permanents ne sont plus effectués par des virements manuscrits. Bien plus : l'exécution d'ordres permanents et de domiciliations se fait automatiquement entre le(s) créancier(s) et la banque. Le titulaire du compte n'intervient absolument pas dans tout ce processus

Document précédent :

Doc 50 **1389/ (2000/2001)** :
001 : Projet de loi.

de houder in dit proces van betaling zolang deze toelating niet herroepen is door de titularis van de rekening. Dit wordt duidelijk gemaakt door de doorlopende betaalopdrachten of domiciliëringen onder te brengen in een apart punt.

Nr. 2 VAN DE HEER **VAN APEREN**

Art. 8

In § 1, tussen het derde en vierde lid het volgende lid invoegen:

«Hij zal zijn PIN- en andere codes nergens in een gemakkelijk herkenbare vorm noteren, en met name niet op het elektronisch betaalinstrument, noch op iets dat de houder bij het elektronisch betaalinstrument bewaart of met dat betaalinstrument bij zich draagt.».

VERANTWOORDING

Dit amendement neemt de tekst over van de Europese aanbeveling. Er is geen reden hiervoor een andere regeling uit te werken. Integendeel.

Het wetsontwerp bepaalt in artikel 6, 7°, al heel duidelijk dat, in geval van betwisting, de uitgever van het instrument voor de elektronische overmaking van geldmiddelen, het bewijs moet voorleggen dat de transactie juist werd geregistreerd en geboekt, en niet door een technische storing of een andere faling werd beïnvloed. Hierbij kan concreet worden gedacht aan het voorleggen van de betrokken journaalband. Wat kan de uitgever nog meer doen ? Op enkele zeldzame uitzonderingen na, zal de uitgever immers in de onmogelijkheid zijn te bewijzen dat de code op het instrument of een ander document stond.

Een eenvoudig voorbeeldje kan dit verduidelijken. Persoon A geeft zijn kaart aan persoon B samen met de code en deze persoon B misbruikt die onmiddellijk, uiteraard vóór de kennisgeving van «het verlies of diefstal» voor bijvoorbeeld 2.500 euro. Persoon A, die een uur na «het verlies» de uitgever in kennis heeft gesteld, betaalt maximum 150 euro. Voor het verschil zal de bank moeten opdraaien want deze kan het doorgeven van de code niet bewijzen net zomin als de «onverwijlde» kennisgeving. Vice versa geeft persoon B zijn kaart aan persoon A met hetzelfde effect. A en B zijn elk 2.350 euro rijker ten koste van de banken en dit verhaal kan tot in den treure toe worden herhaald. Zulke hypotheses dienen absoluut onmogelijk te worden gemaakt wil men het elektronisch betaalsysteem geloofwaardig houden.

In dit kader weze benadrukt dat in artikel 7 enkele duidelijke gevallen worden beschreven waarvoor de aansprakelijkheid van de uitgever wordt vastgesteld (bv. In het geval van namaak van het instrument). De schade ten gevolge van gevallen van georganiseerde fraude worden door de uitgevers zonder meer vergoed.

de paiement tant qu'il n'a pas révoqué son autorisation. Afin de clarifier les choses, nous prévoyons un point distinct pour les ordres de paiement permanents et les domiciliations.

N° 2 DE M. **VAN APEREN**

Art. 8

Au § 1er, entre les alinéas 3 et 4, insérer l'alinéa suivant :

« Le titulaire évitera de noter son numéro d'identification personnel ou autre code sous une forme aisément reconnaissable, et notamment sur l'instrument de paiement électronique ou sur un objet qu'il conserve ou porte avec cet instrument. ».

JUSTIFICATION

Le présent amendement reprend le texte de la recommandation européenne. Il n'y a aucune raison de prévoir un autre régime en la matière. Bien au contraire.

L'article 6, 7°, du projet de loi dispose déjà clairement qu'en cas de contestation, l'émetteur de l'instrument de transfert électronique de fonds doit apporter la preuve que l'opération a été correctement enregistrée et comptabilisée et n'a pas été affectée par un incident technique ou une autre défaillance. Concrètement, on peut songer à la production de la bande journal concernée. De quelle autre possibilité l'émetteur dispose-t-il d'ailleurs ? À quelques rares exceptions près, l'émetteur sera en effet dans l'impossibilité de prouver que le code figurait sur l'instrument ou un autre document.

Un exemple simple l'illustrera parfaitement. Une personne A donne sa carte ainsi que son code à une personne B, qui en fait immédiatement un usage abusif, évidemment avant la notification de « la perte ou du vol », pour un montant de, par exemple, 2 500 euros. La personne A, qui a notifié « la perte » à l'émetteur dans l'heure, paie maximum 150 euros. La banque devra prendre la différence à sa charge, car elle ne peut prouver que le code a été communiqué ni que la notification a été faite « immédiatement ». Inversement, la personne B donne sa carte à la personne A et le même scénario se répète. Les personnes A et B ont, chacune, gagné 2 350 euros au détriment des banques et ce scénario peut se répéter à l'infini. Il faut absolument exclure de telles hypothèses si l'on veut que le système de paiement électronique conserve sa crédibilité.

Dans ce contexte, il y a lieu de souligner que l'article 7 prévoit quelques cas concrets dans lesquels la responsabilité de l'émetteur est engagée (par exemple, en cas de contrefaçon de l'instrument). Les dommages subis par suite d'une fraude organisée sont réparés par les émetteurs.

Men kan ook niet naast de vaststelling heen dat het gebruik van de in België uitgegeven instrumenten en de bijhorende pincodes, berust op een zeer betrouwbaar en technologisch zeer beveiligd systeem. Het kraken van een pincode gegenereerd op basis van sleutels en algoritmen is onmogelijk. Het voorgaande betekent concreet dat een derde deze de code niet kan achterhalen zonder actieve (vb. oplichting of fraude) of passieve (vb. meekijken zonder medeweten van de titularis) medewerking van de titularis van het instrument. Het volstaat in dit laatste geval het intikken van de code af te schermen met de vrije hand. Bovendien kan de code steeds worden gewijzigd door de titularis.

Nr. 3 VAN DE HEER **VAN APEREN**

Art. 8

In § 2, de eerste drie leden vervangen als volgt:

«§ 2. Tot aan het tijdstip van de kennisgeving zoals vermeld in § 1 is de houder aansprakelijk voor de gevolgen verbonden aan het verlies of de diefstal van het instrument voor de elektronische overmaking van geldmiddelen tot een bedrag van 150 euro, tenzij in geval van grove nalatigheid van de houder, in strijd met de relevante bepalingen van de vorige paragraaf of in geval de houder frauduleus heeft gehandeld, in welk geval genoemd maximumbedrag niet van toepassing is.».

VERANTWOORDING

Dit amendement moet worden samengelezen met het vorige. De omkering van de bewijslast, zoals voorgesteld in het wetsontwerp, zou een zeer onevenwichtige situatie doen ontstaan: het wetsontwerp bepaalt dat de bewijslast volledig op de rug wordt geschoven van degenen die de betalingssystemen aanbieden. Zoiets zou niet alleen fraude in de hand werken maar kon ook een gevaarlijk precedent scheppen.

In de gehele e-wereld zijn de veiligheidsprincipes immers gegrond op «*non-repudiation*», d.i. de niet-ontkenning van verrichtingen die met een elektronische handtekening zijn ondertekend. Ook de Belgische wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten berust hierop.

Wanneer men gebruikers de kans geeft om verrichtingen of handtekeningen die aldus werden ingebracht, achteraf te ontkennen, dan wordt dit vitaal concept volledig ondergraven. Dan worden alle mogelijkheden van e-banking, e-commerce, maar ook van e-government op losse schroeven gezet.

Ten slotte kan men evenmin naast de vaststelling heen dat de Ombudsman voor de cliënten van de banksector en de beursvennootschappen nog nooit een fundamentele fout heeft gerapporteerd in het veiligheidssysteem van Banksys.

Force est de constater que l'utilisation des instruments émis en Belgique et des codes pin y afférents se fonde sur un système très fiable et très bien sécurisé sur le plan technologique. Il est impossible de déchiffrer un code Pin généré au moyen de clés et d'algorithmes. Concrètement, cela signifie qu'un tiers ne peut déchiffrer le code sans la complicité active (par exemple, escroquerie ou fraude) ou passive (on regarde le titulaire, à son insu, former le code) du titulaire de l'instrument. Il suffit, dans ce dernier cas, de composer le code à l'abri des regards indiscrets. De plus, le code peut toujours être modifié par le titulaire.

N° 3 DE M. **VAN APEREN**

Art. 8

Au § 2, remplacer les trois premiers alinéas par la disposition suivante :

« § 2. Jusqu'au moment de la notification prévue au § 1er, le titulaire est responsable des conséquences liées à la perte ou au vol de l'instrument de transfert électronique de fonds à concurrence d'un montant de 150 euros, sauf en cas de négligence grave du titulaire à l'égard des dispositions du paragraphe précédent ou s'il a agi frauduleusement, auquel cas le plafond précité n'est pas d'application. ».

JUSTIFICATION

Le présent amendement forme un tout avec l'amendement précédent. Le renversement de la charge de la preuve, ainsi que le prévoit le projet de loi, créerait une situation très déséquilibrée : en vertu du projet de loi, la charge de la preuve incombe entièrement à celui qui propose les systèmes de paiement. Une telle mesure favoriserait non seulement la fraude, mais pourrait également créer un dangereux précédent.

Dans l'ensemble du monde électronique, les principes de sécurité se fondent sur la *non-repudiation*, c'est-à-dire la non-contestation d'opérations signées à l'aide d'une signature électronique. C'est également sur ce principe qu'est basée la loi belge du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

Donner aux utilisateurs la possibilité de répudier *a posteriori* la signature qu'ils ont donnée ou des opérations qu'ils ont effectuées de cette manière revient à anéantir totalement ce principe essentiel. C'est remettre en cause toute possibilité d'*e-banking*, *d'e-commerce,* mais aussi d'*e-government*.

Il faut par ailleurs constater que le médiateur au service des clients du secteur bancaire et des sociétés de Bourse n'a encore jamais fait état d'une déficience majeure dans le système de sécurité de *Banksys*.

Het aantal klachten (70) verrekend tegenover het aantal effectieve transacties (600.000.000 in 2000) geeft een betrouwbaarheidsfactor van 99,999999.

Tenslotte wordt verwezen naar een gelijkaardig debat in Nederland waar recent door de minister van financiën resoluut werd gesteld dat «*een omkering van de bewijslast geen oplossing biedt gelet op het zeer laag aantal betwiste transacties per jaar, waarbij het in de meeste gevallen blijkt te gaan om situaties waarbij de klant de pincode niet geheim heeft gehouden. Zoals verder opgemerkt hanteren banken deugdelijke systemen, waardoor het uitgangspunt gerechtvaardigd is dat banken door hun administratieve vastlegging kunnen aantonen dat de pas en de pincode door een bepaalde pashouder zijn gebruikt. Verder zou het omkeren van de bewijslast grote bewijsproblemen met zich meebrengen voor banken, aangezien zij dan voor elke betwiste transactie ook nog zouden moeten bewijzen dat de pashouder deze transactie zelf heeft verricht. Tenslotte valt niet uit te sluiten dat een omkering van de bewijslast leidt tot een belangrijke toename van ten onrechte betwiste transacties…*».

Arnold VAN APEREN (VLD)

Le nombre de plaintes (70) rapporté au nombre de transactions effectives (600 000 000 en 2000) donne un indice de fiabilité de 99,999999.

Il est enfin souligné qu'au cours d'un débat similaire qui a eu lieu récemment aux Pays-Bas, le ministre des Finances a indiqué clairement que «compte tenu du très faible nombre de transactions contestées annuellement, le renversement de la charge de la preuve n'est pas une solution. Ces contestations concernent du reste, le plus souvent, des clients qui n'ont pas gardé secret leur code pin. Comme nous l'observerons plus loin, les systèmes utilisés par les banques sont fiables, de sorte qu'il est justifié que ces dernières partent du principe que la trace administrative qu'elles conservent des transactions leur permet de démontrer que telle carte et tel code pin ont été utilisés par tel titulaire de carte. Le renversement de la charge de la preuve poserait en outre de sérieux problèmes de preuve aux banques, dès lors qu'elles devraient aussi être en mesure de démontrer, pour chaque transaction contestée, que le titulaire de la carte concernée a bien effectué lui-même la transaction. Il n'est pas exclu, enfin, que le renversement de la charge de la preuve entraîne une augmentation importante des transactions contestées abusivement …».

Centrale drukkerij – Imprimerie centrale
Deze publicatie wordt uitsluitend gedrukt op volledig gerecycleerd papier
Cette publication est imprimée exclusivement sur du papier entièrement recyclé