

## Juridische randvoorwaarden voor goed betalingsverkeer

R.V. De Mulder en P. Kleve

Centrum voor Informatica en Recht  
Erasmus Universiteit Rotterdam

### 1. Juridische aspecten

Er is een tweetal aspecten aan elektronisch geldverkeer, die met name van belang zijn vanuit juridisch oogpunt. Ten eerste is dat natuurlijk het vraagstuk van de *authenticiteit*, en in het verlengde daarvan dat van *aansprakelijkheid en bewijs*. Het gebruik van betaalautomaten, gelduitgifte-automaten en (bank)pasjes brengt met zich mee dat niet altijd met zekerheid is vast te stellen dat zij door een daartoe bevoegd persoon zijn gebruikt. Een aspect van een andere orde is dat van de *privacy*, de vraag in hoeverre het gebruik maken van elektronische betaalmiddelen - en de registratie van betalingen - een inbreuk kunnen vormen op de persoonlijke levenssfeer van de gebruiker. In verband met de aard van dit symposium zullen we bij dit laatste slechts kort stilstaan.

#### 1.1 Privacy

Een kenmerkend verschil met de situatie dat geld wordt opgenomen bij de bank waarmee vervolgens aankopen contant worden betaald is dat bij elektronisch betalingsverkeer de anonimiteit van het koopgedrag verdwijnt. Elektronisch geldverkeer, en dan met name indien de afrekeningen centraal geregistreerd worden, kan voor de organisatie die dit betalingsverkeer beheert - bank of grootwinkelbedrijf bij voorbeeld - inzicht opleveren in de bestedingspatronen en voorkeuren van gebruikers. De informatie die zij hieruit opdoet, kan zij gebruiken voor bij voorbeeld het al dan niet toekennen van een krediet, of voor marketingdoeleinden. Een centrale registratie als hier bedoeld valt onder de werking van de Wet Persoonsregistraties. Dat betekent dat gegevens uit deze registraties niet zonder meer aan derden mogen worden verstrekt. Voorts is het de vraag of deze gegevens wel door de organisatie zelf mogen worden gebruikt, aangezien zij zijn verkregen voor een ander doel dan waarvoor zij vervolgens gebruikt worden. Op voorhand lijkt het een te ver gaande 'oplossing' om dan maar in de doelomschrijving van een registratie die wordt gevoerd met het oog op de verwerking van 'elektronische betalingen' op te nemen dat zij tevens is bedoeld voor het verkrijgen van marketinginformatie. Niettemin is het denkbaar dat geregistreerden uit zichzelf bereid zijn om een gedeelte van hun privacy prijs te geven. Zo zouden zij *toestemming* kunnen geven tot het vastleggen en het gebruiken van gegevens met betrekking tot hun aankopen. Vooral consu-

menten uit de lagere inkomensgroepen zouden daartoe wel eens eerder bereid kunnen zijn, indien zij daarvoor 'beloond' worden met aanbiedingen van de kruidenier.

Dat elektronische vastlegging van persoonsgegevens een ontwikkeling te zien geeft naar een steeds grotere controle over individuen hebben we bij voorbeeld gezien met het fiscaal nummer. Bij de invoering daarvan werd gesteld dat het fiscaal nummer uitsluitend bedoeld was voor intern gebruik door de fiscus. Echter, onder aanvoering van het argument van effectievere fraudebestrijding, werd niet lang na de invoering het fiscaal nummer omgedoopt in sociaal/fiscaal nummer, het SoFi-nummer, opdat ook uitkerende instanties van hetzelfde nummer gebruik konden maken. Nu we aan de vooravond staan van de reorganisatie van de bevolkingsboekhouding met de invoering van de Gemeentelijke Basis-Administratie, is het waarschijnlijk dat we straks kunnen spreken van het SoFi/GBA-nummer, dus hetzelfde nummer ook in de gemeentelijke registers. Voegen we dit bij het gegeven van de beperkte legitimatieplicht, dan zijn we niet ver meer verwijderd van het SoFi/GBA-legitimatiebewijs. E.e.a. zal staatssecretaris Simons dan weer de mogelijkheid geven om medische persoonsgegevens en vermeende risicofactoren eveneens op bij voorbeeld dezelfde chipcard vast te leggen, om zodoende als basis te dienen voor de berekening van het eigen risico in de gezondheidszorg. Om te beginnen.

### *1.2 Authenticiteit*

In het huidig elektronisch betalingsverkeer staat het gebruik van de magneetstripkaart met PIN-code centraal. Het belangrijkste probleem hierbij is dat, hoewel de PIN-code persoonsgebonden is, niet met zekerheid is vast te stellen of de pas ook daadwerkelijk door de daartoe bevoegde persoon is gebruikt. De code kan aan een ander zijn medegedeeld, hij kan zijn opgeschreven (zeker indien men over een aantal pasjes met verschillende PIN-codes beschikt wordt het lastig om ze allemaal te onthouden en uit elkaar te houden), of hij kan door derden zijn uitgelezen. In het geval van een betwiste afschrijving komt de vraag aan de orde welke waarde men kan toekennen aan het gebruik van de PIN-code. De gehanteerde woordkeuzes als 'elektronische handtekening', 'elektronische cheque' en 'elektronische portemonnee' doen te gemakkelijk suggereren dat aan een pas met PIN-code dezelfde juridische gevolgen zijn verbonden als aan een handtekening.

Aan de handtekening kan men in het algemeen drie functies toekennen. Omdat zij met de hand geschreven is, vervult zij de functie van *identificatie* van de ondertekenaar. Omdat zij niet zomaar gezet wordt, doch doorgaans na lezing van het document, wordt de handtekening opgevat als een bevestiging dat *van de inhoud van het document is kennis genomen*. Tenslotte geeft de handtekening weer de *instemming* van de ondertekenaar met de inhoud van het document. De handtekening authentificeert derhalve de fysieke aanwezigheid van de

ondertekenaar, alsmede de wil van de ondertekenaar om van de inhoud kennis te nemen en erdoor gebonden te worden (Vandenbergh, 'De betekenis van de handtekening bij het elektronisch betalingsverkeer en teleshopping').

Vergelijken we dit met de functie van de PIN-code, dan zien we dat de PIN-code niet meer is dan een *toegangscode* om van de gelduitgifte-automaat of van de betaalautomaat gebruik te kunnen maken. De PIN-code vervult noch de functie van identificatie van de gebruiker - gegeven de mogelijkheid dat de code bij een derde bekend is geworden - noch de functie van bewijs voor wilsovereenstemming. De PIN-code wordt immers ingetoetst voordat de transactie plaats heeft, en kan derhalve niet dienen als bekrachtiging daarvan. In dit licht gezien ware het dan ook juister te spreken van een 'elektronische toegangscode' dan van een 'elektronische handtekening'.

### *1.3 Aansprakelijkheid en bewijs*

De relatie tussen bank en consument wordt in Nederland hoofdzakelijk bepaald door de Voorwaarden gebruik Geld- en Betaalautomaten. Deze voorwaarden verklaren tevens van toepassing de Algemene Voorwaarden. Op grond van deze Algemene Voorwaarden worden geschillen omtrent betwiste afschrijvingen van de bankrekening geregeerd door de bekende 'boekenclausule' van de banken (artikel 11): de administratie van de bank geldt als volledig bewijs, behoudens tegenbewijs door de rekeninghouder.

In het geval van verlies of diefstal van de pas, dient de rekeninghouder dit zo spoedig mogelijk te melden bij de bank. Tot het moment van melding draagt de rekeninghouder een eigen risico van f 350,-. Echter, zowel op de bank als op de rekeninghouder rust een zorgplicht. Als we kijken naar die van de rekeninghouder - deze dient zorgvuldig om te gaan met pas en bijbehorende PIN-code - dan zien we dat in de geschillen die voor de Geschillencommissie Bankbedrijf zijn gebracht, bijna zonder uitzondering is aangenomen dat de rekeninghouder niet voldoende zorgvuldig is geweest, zodat de beperking van het eigen risico tot f 350,- veelal niet meer dan papieren bescherming biedt. Men kan zich afvragen of de rekeninghouder die de Algemene Voorwaarden voor het gebruik van pas en PIN-code heeft gelezen, en zich daarmee accoord heeft verklaard vanuit de gedachte dat het hem of haar kennelijk nooit meer dan f 350,- zou kosten, zich hier wel voldoende rekenschap van heeft gegeven.

Eén opmerkelijk feit kan hier nog vermeld worden. Geschillen met betrekking tot betwiste opnames zijn te onderscheiden in die gevallen waarbij de rekeninghouder niet meer beschikte over zijn of haar pas, en geschillen waarbij de rekeninghouder nog wel in het bezit was van de pas.

Welnu, deze laatste type gevallen zijn door de Geschillencommissie Bankbedrijf zonder uitzondering beslecht in het nadeel van de rekeninghouder. De

redenering hierachter is dat de rekeninghouder wel op enige wijze onzorgvuldig moet zijn geweest met de pas en de geheimhouding van de PIN-code, anders zou de opname niet hebben kunnen plaats vinden. Hoewel ook de eerste type gevallen doorgaans in het nadeel van de rekeninghouder worden beslecht, lijkt de diepere wijsheid toch vooral hierin gelegen dat mocht u ooit geconfronteerd worden met een naar uw mening onterechte afschrijving, en u kijkt verschrikt in uw portemonnee of u uw pas nog wel heeft, haal dan niet opgelucht adem als u ziet dat deze niet verloren of gestolen is, maar gooi hem onmiddellijk weg.

## **2. Juridische of technische oplossingen**

Hierboven zijn een drietal gebieden geschetst rond waar de problematiek met betrekking tot vormen van elektronisch geldverkeer en betalingsverkeer zich afspelen. Participanten in dat verkeer - banken, retailers en gebruikers - verwachten veelal een oplossing voor deze problemen van de zijde van het recht. Het valt echter te betwijfelen of hier zo veel heil van het recht te verwachten is:

- er is momenteel een Wet Persoonsregistraties. Er ligt een concept EG-richtlijn over de bescherming van persoonsgegevens, ook met betrekking tot direct marketing. Niettemin zullen deze wettelijke maatregelen slechts van geringe invloed zijn, indien individuen zelfstandig hun privacy opgeven, teneinde daarvoor een - gezien hun omstandigheden - onmisbaar voordeel mee te behalen. Het valt sowieso te betwijfelen of we van de overheid adequate maatregelen ter bescherming van de privacy van burgers mogen verwachten, gezien de geschetste ontwikkeling in het gebruik van persoonsgegevens door de overheid zelf.
- de authenticiteit van PIN-codes is door juridische regels niet op te lossen. Het voor de wet gelijk stellen van een 'elektronische toegangscode', de PIN-code dus, aan een handtekening - iets dat omwege hetgeen hierboven is vermeld reeds verre van aan te bevelen is - zal op zichzelf geen oplossing van het werkelijke probleem bieden. Namelijk dat van misbruik en dat van verminderde betrouwbaarheid.
- er zijn reeds wettelijke regels met betrekking tot aansprakelijkheid en bewijs. Een andere verdeling daarvan - wellicht in sommige gevallen billijker; in andere niet - leidt evenmin tot een oplossing. Het recht maakt een eind aan het geschil, niet aan het daaraan ten grondslag liggende probleem

Het heeft er alle schijn van dat deze door de techniek gecreëerde problematiek, ook door de techniek zal moeten worden opgelost. Het vraagstuk van de identificatie zou kunnen worden verminderd door het gebruik van meer

persoonsgebonden kenmerken zoals vingerafdrukken, netvliesstructuur of hersenimpulsen. Maar los van de ontwikkelingen op het gebied van de biometrische gegevens zou alleen al de vervanging van de huidige magneetstripkaart door de chipcard of smartcard, de omvang van deze problematiek aanzienlijk kunnen doen afnemen:

- door de mogelijkheid gevarieerder algoritmen, door de gebruiker zelf te bepalen, in de chipcard vast te leggen, zal het steeds aannemelijker te maken zijn dat de kaart ook daadwerkelijk door de rekeninghouder is gebruikt. Bovendien lijkt het in dat geval billijker om het bewijsrisico bij de rekeninghouder te leggen, gegeven diens mogelijkheid om onbevoegd gebruik zo goed als onmogelijk te maken.
- omdat gegevens op de chipcard zelf kunnen worden vastgelegd, vervalt tenminste de noodzaak tot het bijhouden van gedetailleerde centrale registraties. (Het zal duidelijk zijn dat de chipcard niet direct de oplossing aandraagt voor de overige hierboven genoemde privacy-aspecten.)

Onze suggestie om de oplossingen van de hier gesignaleerde problemen te zoeken in de techniek, betekent niet dat we met een blind vertrouwen in alleen de techniek kunnen volstaan. Vanzelfsprekend blijven er eisen te stellen aan de organisatie rond het elektronisch betalingsverkeer en (zorgvuldigheids)eisen aan de gebruiker. De banken hebben de afgelopen jaren op grote schaal geïnvesteerd in automaten gebaseerd op de magneetstripkaart. Indien echter de chipcard inderdaad betrouwbaarder zou zijn en voor minder juridische problemen zou zorgen, verdient het aanbeveling de magneetstripkaart te vervangen door de chipcard. Gezien de investeringen door de banken zal dit nog wel een aantal jaren op zich laten wachten. Het is interessant om te volgen of dit nalaten van de banken om door middel van de invoering van een chipcard bij te dragen tot een meer betrouwbaar elektronisch geldverkeer, de Geschillencommissies ertoe zal brengen de bewijspositie van consumenten te versterken.

### **3. Zelfregulering en conflictbeslechting**

Bij gebreke van de mogelijkheid tot adequate wettelijke regelingen, zien we een tendens tot zelfregulering om te trachten de hier besproken problemen rond het elektronisch betalingsverkeer beheersbaar te maken:

- - De Wet Persoonsregistraties biedt de mogelijkheid tot het opstellen van gedragscodes. Een voor een bepaalde branche representatieve organisatie kan, na genoegzaam overleg met organisaties van belanghebbenden, nadere regels opstellen in het belang van de bescherming van de persoonlijke levenssfeer van geregistreerden. Zo zijn er in dit verband gedragscodes

opgesteld door het bankbedrijf en door het direct marketingbedrijf (waaronder ook het gebruik van direct marketing technieken voor het eigen bedrijf wordt gerekend).

- - Deelname aan het elektronisch betalingsverkeer en het gebruik van cards wordt beheerst door privaatrechtelijke overeenkomsten tussen banken en consumenten en de door de banken opgestelde voorwaarden.
- - Geschillen die voortvloeien uit de deelname aan het elektronisch geldverkeer worden beslecht door de Geschillencommissie Bankbedrijf voor wat betreft transacties met de banken, en door de Geschillencommissie Bankzaken waar het de Postbank betreft. Ook hier met als uitgangspunt de algemene bankvoorwaarden en de 'boekenclausule'.

We besluiten deze bijdrage met het signaleren van een ontwikkeling waardoor die tendens tot zelfregulering zich in de toekomst waarschijnlijk nog verder zal voortzetten. Door het onderscheiden van de verschillende functies in het betalingsverkeer zullen in het marktsegment van de bancaire dienstverlening nieuwe aanbieders zich aandienen. Zo kan met de verwachte beëindiging van de monopoliepositie van Beant de verwerking van betalingstransacties ook verzorgd worden door nieuwe facilitaire aanbieders, of bij voorbeeld door de grootwinkelbedrijven zelf. Een ontwikkeling waardoor een onderlinge concurrentieverhouding zal ontstaan, waarbij ook de gehanteerde voorwaarden voor deelname aan het betalingsverkeer betrokken kunnen worden. Voorts zien we dat bij voorbeeld creditcard organisaties inmiddels een belangrijk aandeel hebben in het betalingsverkeer, tot aan de verstrekking van kredietfaciliteiten toe. Tenslotte wijzen we nog op het toenemende belang van EDI als middel voor het tot stand brengen van handelstransacties. Het is zeker niet ondenkbaar dat EDI-netwerkbeheerders ook een rol zullen gaan spelen in de afhandeling van betalingen. Indien er een conflict ontstaat met betrekking tot een (vermeende) onjuiste afschrijving, zal de consument het meest gebaat zijn bij die organisatie die de voor hem of haar aantrekkelijkste voorwaarden hanteert. Voor zover het geen geschil met de facilitaire dienstverlener zelf betreft, zien wij in de toekomst voor deze laatste nog een rol weggelegd in het oplossen van geschillen tussen leveranciers en afnemers indien de transactie via diens netwerk tot stand is gekomen.