

Identiteitsdiefstal: lessen uit het buitenland

*J.E.J. Prins en N.S. van der Meulen**

Deze zomer verscheen in de media het bericht dat de Informatie Beheer Groep, maar vooral ook de Nederlandse Spoorwegen miljoenen euro's schade lijden door fraude met de OV-studentenkaart (Persbericht NS, 20 juli 2006). Uit cijfers van de IB-groep bleek dat in 2005 niet minder dan 29.000 duplicaten van deze kaart zijn aangevraagd nadat eerder aangifte was gedaan van diefstal of verlies van het origineel. In een deel van de gevallen blijkt het origineel echter helemaal niet verdwenen: het komt tevoorschijn zodra de student stopt met de studie en zijn kaart moet inleveren. Met de 'extra' – oude – kaart reist de student vrolijk gratis de rest van het jaar verder. Identiteitsdiefstal? Nee. In dit geval niet. Het is immers dezelfde student die zich met behulp van de frauduleuze truc onterecht een voordeel toe-eigent. Maar op basis van het voorbeeld vallen zeker wel situaties te bedenken waarin sprake is van identiteitsdiefstal: een bevriende student reist met de extra kaart of een student is onwetend van het feit dat een medestudent langs slinkse weg een duplicaat van zijn of haar kaart heeft weten te bemachtigen. Het voorbeeld laat ook zien hoe eenvoudig het in feite is om te frauderen met een middel dat een bepaalde persoon (in dit geval een student) het recht geeft om van bepaalde voorzieningen (hier: gratis openbaar vervoer) gebruik te maken. En daarin is het voorbeeld van de OV-studentenkaart zeker niet uniek. De afgelopen jaren verschenen in de media regelmatig berichten over fraude met soft-nummers, zorgpassen en betaalkaarten. We geven een tweetal andere voorbeelden uit de pers van de afgelopen maanden. In mei van dit jaar meldde de Koninklijke Marechaussee dat er in ons land per jaar voor zeker drie miljard euro aan fraude wordt gepleegd met

* Prof. mr. Corien Prins is als hoogleraar verbonden aan de faculteit der rechtsgeleerdheid, TILT – Tilburg Institute for Law, Technology, and Society. Zij is tevens verbonden aan Intervict – International Victimology Institute Tilburg (beide bij de universiteit Tilburg). Nicole van der Meulen MSc is als promovendus verbonden aan Intervict – International Victimology Institute Tilburg.

identiteitspapieren als paspoorten en rijbewijzen.¹ Twee maanden later liet het kabinet weten dat er jaarlijks in driehonderd gevallen kan worden aangetoond dat mensen fraude plegen met vervalste buitenlandse akten om zich daarmee te laten inschrijven in het Nederlandse bevolkingsregister en bij diverse instanties een aanvraag in te kunnen dienen voor sociale voorzieningen. Minister Bot van Buitenlandse Zaken gaf echter ook aan geen idee te hebben hoe hoog het daadwerkelijke aantal fraudegevallen met buitenlandse documenten is.²

Of het nu om de bovengenoemde, wat meer 'ouderwetse' voorbeelden gaat, of om geheel nieuwe varianten: identiteitsfraude lijkt hand over hand toe te nemen. Bij de nieuwe varianten rukt met name het zogenaamde 'phishing' op: fraudeurs verkrijgen persoonlijke gegevens door zich door middel van een, als zeer betrouwbaar voorkomende e-mail, voor te doen alsof ze een financiële instelling of andere organisatie zijn en verzoeken de klant zijn of haar persoonlijke informatie te verifiëren. Vervolgens gebruiken zij de informatie voor de ID-fraude. De Nederlandse Vereniging van Banken (NVB) constateerde in haar jaarverslag over 2005 dat veel financiële fraudegevallen bij bancaire instellingen zijn terug te voeren op phishing en andere vormen van identiteitsdiefstal (Jaarverslag NVB, 2005).

Om kort te zijn: identiteitsdiefstal is een groeiend probleem.

Toch is het zeker geen probleem dat zich pas recentelijk heeft geopenbaard of waarvoor nu pas vanuit het veld of wetenschap aandacht wordt gevraagd. Zo werd bij de introductie van de plannen voor het Burger Service Nummer al direct op het risico van identiteitsfraude gewezen (Prins, 2003). Beleidsmakers en politiek lijken zich echter pas zeer recent voor het fenomeen te zijn gaan interesseren (Prins, 2006a). De eerste publiekscampagne is aangekondigd, maar veel meer maatregelen staan vooralsnog niet op stapel.³ Meevaller voor ons land is dan nu gelukkig wel dat bij het nadenken over het 'hoe, waarom en wat te doen' veel van het buitenland is te leren. In landen als het Verenigd Koninkrijk, maar met name de Verenigde Staten, prijkt identiteitsdiefstal al enkele jaren op de agenda van menig beleidsmaker, bedrijf en organisatie. Welke lessen vallen er

1 www.security-online.nl.

2 Antwoord Minister van Buitenlandse Zaken op kamervragen LPF-fractieleden Van As en Varela, 11 juli 2006.

3 Het Maatschappelijk Overleg Betalingsverkeer liet in 2005 weten met een voorlichtingscampagne te komen. Zie: www.dnb.nl/dnb/pagina.jsp?pid=tcm:12-40007-64.

voor Nederland te trekken? Het is deze vraag die wij in de bijdrage centraal stellen. We beginnen echter met een korte uiteenzetting van de verschillende vormen van identiteitsdiefstal.

Identiteitsdiefstal: een veelkoppig concept

Wie op zoek gaat naar een uniforme en breed geaccepteerde definitie van identiteitsdiefstal, zal niet snel resultaat boeken. Lezing van het scala aan rapporten dat inmiddels in de Verenigde Staten en het Verenigd Koninkrijk over het onderwerp is verschenen, laat een diversiteit aan omschrijvingen zien. Ook op wetgevingsniveau is variatie troef. Het ontbreken van een standaarddefinitie heeft alles te maken met de discussie over de reikwijdte van het delict. Zo bestaan er verschillende opvattingen tussen de publieke sector enerzijds en de private sector anderzijds over welke delicten al dan niet tot identiteitsdiefstal behoren. Illustratief is bijvoorbeeld de vraag of creditcardfraude en het plunderen van rekeningen als identiteitsdiefstal moet worden aangemerkt. Met name vertegenwoordigers uit de bancaire wereld menen van niet (Cheney, 2005, p. 2) en hierin kan ook een verklaring worden gevonden voor het feit dat in de Verenigde Staten de definitie zoals gehanteerd in de *Federal Identity Theft and Assumption Deterrence Act* uit 1998 als te ruim wordt ervaren. Volgens deze definitie is van identiteitsdiefstal sprake wanneer iemand: 'knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law' (18 U.S.C. 1028, Pub. Law 105-318, 112 Stat. 3007). Een ander discussiepunt betreft de vraag op welk moment in de keten van handelingen er sprake is van identiteitsdiefstal: is dit reeds het geval op het moment dat een naam wordt vervalst of een rekeningnummer wordt afgetrokkeld, of is pas sprake van het delict als ook daadwerkelijk met behulp van deze naam of rekeningnummer een persoon wordt benadeeld? Wie de diverse rapporten nauwkeurig leest, stelt bovendien vast dat er tussen landen ook verschillen in opvattingen over de reikwijdte van het delict bestaan. Een mooi overzicht hiervan is te vinden in het rapport van Roberto Binder en Martin Gill uit 2005 (Binder en Gill, 2005, p. 8-9). De auteurs menen daarbij dat het van belang is een onderscheid te

maken tussen identiteitsdiefstal (wederrechtelijk overnemen en misbruiken van andermans identiteit) enerzijds en identiteitsfraude (aannemen van fictieve identiteit: men kan immers een fictieve identiteit niet stelen) anderzijds (Binder en Gill, 2005, p. 8). Alhoewel momenteel vanuit diverse zijden wordt gewerkt aan een betere conceptualisering van het probleem en daarmee stappen worden gezet op weg naar een meer uniforme definitie van het delict (voor een overzicht, zie: Van der Meulen, 2006), blijft het vooralsnog aanmodderen: termen in zowel rapporten als wetgeving lopen door elkaar heen: ‘Unfortunately, when you review the legislation, many times the term identity theft appears to be used interchangeably with the term identity fraud’ (Binder, Gill, 2005, p. 8 voetnoot 11).

Het gevolg van het ontbreken van een uniforme definitie is dat het onder meer niet eenvoudig is een goed beeld te krijgen van de omvang en ernst van het probleem: ‘The lack of a standard definition makes it difficult to collect comprehensive, accurate data for quantifying the costs and incidents of identity theft’ (US Department of Treasury, 2005, p. 9). Ook voor ons land geldt dat we in feite niet weten hoe groot de omvang van het probleem is. Sommige commentatoren menen dat het allemaal wel meevalt. Anderen claimen dat we wel degelijk met een belangrijk maatschappelijk probleem te maken hebben, maar dat we onvoldoende zicht hebben op de omvang van het probleem omdat we de instrumenten ontberen om het boven tafel te krijgen en in kaart te brengen. Wij menen dat we – los van een oordeel over de daadwerkelijke omvang van het probleem – in ieder geval aandacht moeten hebben voor de zwakke schakels in onze identificatie-infrastructuur om ons aldus zoveel mogelijk te wapenen tegen het fenomeen.

Een ander probleem is dat bij wetgevingsinitiatieven de verschillende vormen waarin de nieuwe vorm van criminaliteit zich uit als het ware op één hoop worden gegooid, terwijl – gegeven de kenmerken van de specifieke handelingen – een afzonderlijke aanpak wenselijk zou zijn. Al is het maar omdat er vanuit strafrechtelijk perspectief verschillende voorwaarden gelden voor een kwalificatie inzake fraude enerzijds en diefstal anderzijds. Bovendien valt te betwijfelen of sprake is van diefstal van identiteitsgegevens, nu deze gegevens waarschijnlijk niet zijn te kwalificeren als een goed dat kan worden weggenomen (Koops, Leenes, 2006) en niet aan iemand toebehoren in de zin van diens eigendom zijn (Prins, 2006b).

Als we ten slotte nog even terugkeren naar het hiervoor gesigna-

leerde probleem dat het moeilijk is een goed beeld te krijgen van de omvang van identiteitsfraude, stellen we vast dat sommige onderzoekers in de Verenigde Staten voorzichtig menen te kunnen concluderen dat niet langer sprake is van een groeiend probleem. Mogelijk kan zelfs worden geconcludeerd dat het aantal gevallen afneemt (Lenard en Rubin, 2006, p. 44). Een zorgvuldige analyse van de cijfers uit de diverse rapporten laat echter zien dat Lenard en Rubin mogelijk wat te snel juichen. Weliswaar neemt het percentage fraude met creditcards af, het percentage van het scala aan vormen dat onder de brede noemer 'other' worden geschaard neemt nog steeds toe (toename van 6% tussen 2003 en 2005: Identity Theft Data Clearinghouse 2006). Onduidelijk blijft vooralsnog welke vormen van identiteitsfraude precies verantwoordelijk zijn voor de stijging in deze categorie. Meer duidelijkheid op dit punt zou ook van belang zijn om inzicht te verkrijgen in nieuwe en opkomende vormen van fraude, dat wil zeggen vormen die momenteel nog niet als afzonderlijke categorie worden genoemd, maar waarvan het wel duidelijk is dat ze in aantal voorkomende gevallen duidelijk aan een opmars bezig zijn. Wij willen er daarom voor pleiten dat Nederland in een zo vroeg mogelijk stadium aandacht besteedt aan het belang van een zo gedetailleerd mogelijk inzicht en overzicht van de onderscheiden vormen van identiteitsdiefstal en op basis daarvan via meldingen van gedupeerde individuen, bedrijven en organisaties een nationaal klachtenbestand opbouwt.

Hoe reageren landen zoal?

De afgelopen jaren heeft een aantal landen via diverse beleids- en wettelijke maatregelen de aanval ingezet op identiteitsdiefstal. Gegeven de beperkte omvang van deze publicatie, beperken we de onderstaande bespreking tot de belangrijkste van die maatregelen (zie een omvattend overzicht: Van der Meulen, 2006). Om later in deze bijdrage onze suggesties voor een aanpak van de problematiek in Nederland scherp neer te kunnen zetten, bespreken we de buitenlandse maatregelen langs drie lijnen: transparantie, preventie en handhaving.

Transparantie

Het opbouwen van een nationaal klachtenbestand is een maatregel die al vele jaren geleden in de VS is geïnitieerd. Via het zogenoemde Identity Theft Data Clearinghouse wordt al sinds november 1999 informatie verzameld waarmee slachtoffers van identiteitsdiefstal de helpende hand wordt geboden in het zoveel mogelijk beperken van hun schade en (emotionele) ellende. Ook worden met deze voorziening waardevolle inzichten verkregen in de omvang van identiteitsfraude en de verschillende gedaantes waarin deze fraude zich uit. Het Clearinghouse is een direct gevolg van de expliciete wettelijke erkenning – een jaar eerder via de hiervoor al genoemde *Federal Identity Theft and Assumption Deterrence Act* – van identiteitsfraude als een strafrechtelijk delict.

Momenteel worden in de Europese Unie ook stappen gezet om beter overzicht en inzicht te verkrijgen in het fenomeen identiteitsdiefstal. Tot voor kort leek de algemene conclusie dat het (met uitzondering van het Verenigd Koninkrijk) in Europa nogal meevalt met de kwetsbaarheid voor en intensiteit van identiteitsfraude. Als verklaring werd veelal gewezen op de verschillen tussen de Verenigde Staten en de Europese Unie in gebruik en functie van identiteitsdocumenten en identificerende nummers. Maar inmiddels voeren ook in Europa bezorgde observaties de boventoon, zoals recentelijk nog in een rapport van Europol (Europol, 2006), en komt de Europese Commissie met de in haar ogen noodzakelijke maatregelen. Daarbij is transparantie een belangrijk thema. Zo ontvouwde de Commissie in 2004 via het *Action Plan for 2004-2007 to prevent fraud on non-cash means of payment* (COM (2004) 679 final. Brussels, 20.10.2004), de volgende plannen:

- ‘The Commission will promote the creation of a database of original and counterfeit identity documents accessible to both the public authorities and the private sector’.
- ‘The Commission will assess the merits of establishing an EU single contact point for citizens and businesses on identity theft, which could include a register of bodies engaged in the prevention of identity theft’.
- ‘The Commission will continue to discuss the implementation of a single phone number in the EU for notification of lost or stolen cards’.

Preventie

De omvang van identiteitsdiefstal staat in een directe relatie met de kwetsbare kanten van een identificatiemiddel of -infrastructuur. Een eerste stap in de preventie is daarom kwetsbare plekken zoveel mogelijk aanpakken en ervoor zorgen dat nieuwe identificatietoepassingen minder zwakke kanten vertonen. In de Verenigde Staten realiseren beleidsmakers zich inmiddels dat vooral het social security number (SSN) een zeer zwakke schakel in de identificatieketen is en uitgangspunt voor overheidsorganen en andere instanties is tegenwoordig dan ook een zo restrictief mogelijk gebruik van het nummer. De vanuit een fraudebestrijdingsbelang zo noodzakelijke algehele herziening van het SSN-stelsel lijkt voorlopig echter vanwege onder meer de kosten politiek niet haalbaar. Bovendien is het kwaad in feite allang geschied: het nummer waart allang rond in alle hoeken en gaten van de nationale identiteitsinfrastructuur, eenvoudig toegankelijk voor wie er maar kwaad mee wil.

Twee andere zaken die eveneens hand in hand lijken te gaan zijn preventie en bewustzijn. Wanneer consumenten en burgers zich realiseren dat er kwetsbare kanten zitten aan het gebruik van bepaalde identificatie-instrumenten, dat ze minder slordig moeten zijn met het afgeven van allerhande persoonlijke gegevens zoals hun social security number en alert moeten zijn op onregelmatigheden rondom financiële transacties of andere handelingen met organisaties en bedrijven, valt er een hoop te winnen. Vanuit deze gedachte wordt de laatste tijd in zowel de Verenigde Staten als de Verenigd Koninkrijk flink ingezet op bewustwordingscampagnes. In de Verenigde Staten dateert het meest recente initiatief van voorjaar 2006, toen onder de vlag van het programma getiteld *Avoid Theft: Deter, Detect, Defend* (consumer.gov/idtheft/) een grote hoeveelheid voorlichtingsmateriaal beschikbaar kwam. De actie kwam tegelijkertijd met de oprichting op federaal niveau van de Identity Theft Task Force, nadat President Bush daarvoor via nieuwe wetgeving de basis had gelegd (Executive Order 13402 – Strengthening Federal Efforts To Protect Against Identity Theft, 2006). Voor wat betreft het Verenigd Koninkrijk wijzen we op de Identity Fraud Steering Committee (IFSC) en de Identity Fraud Forum (IFF), beide in 2003 opgericht, die publieksvoorlichting tot een van de belangrijke taken rekenen. Daarnaast is inmiddels een speciale website opgezet met als doel het publiek beter bekend te maken met het fenomeen identiteitsfraude: www.identity-theft.org.uk.

Ten slotte is het nog de moeite waard te wijzen op een maatregel die de staat Californië met het oog op preventie heeft genomen: private ondernemingen zijn daar wettelijk verplicht hun klanten direct op de hoogte te stellen van een inbreuk op de beveiliging van het computersysteem (afgekondigd in de California Security Breach Information Act uit 2003). Doel is klanten bewust te maken van eventuele risico's die ze lopen mochten hun betreffende gegevens in handen van criminelen zijn gekomen en hen in staat te stellen eventuele maatregelen te nemen. Inmiddels is er ook op het niveau van de federale wetgever aandacht voor een dergelijke regeling. Op federaal niveau zijn overigens al wel via de Fair and Accurate Credit Transactions Act (Facta – Public Law 108-159) van 2003 maatregelen genomen die op organisaties een zwaardere verantwoordelijkheid leggen om consumenten (houders van creditcards) van allerhande informatie te voorzien die hen in staat stelt fraude te ontdekken of te voorkomen. Interessant voor de situatie in ons land, maar overigens ook het Verenigd Koninkrijk – waar het politieke vertrouwen in biometrische toepassingen opvallend hoog lijkt te zijn – is daarbij dat tijdens de behandeling in het Congres van deze Act een studie werd toegezegd naar de wijze waarop biometrie kan bijdragen aan het voorkomen van identiteitsfraude bij creditcards. Het Department of Treasury stelde in 2005 naar aanleiding van de uitkomsten van deze studie vast: 'Biometrics are not likely in the near term to be very useful to confirm the true identity of an individual at the initial point of opening an account or submitting an application to a financial institution if the person has no prior relationship with the institutions' (US Department of Treasury 2005, p. 70). Biometrie is, aldus het departement, momenteel een sub-optimale oplossing vanwege een gebrek aan accuraatheid en betrouwbaarheid van de technologie, kosten, consumentenbelangen en de afwezigheid van voldoende interoperabiliteit tussen de verschillende systemen.

Handhaving

Zoals hiervoor al gesignaleerd, kozen de Verenigde Staten er in 1998 voor om identiteitsfraude via een afzonderlijke regeling op federaal niveau strafbaar te stellen. Men wilde daarmee het duidelijke signaal afgeven dat deze vorm van criminaliteit niet een specifieke variant van al bestaande delicten zoals fraude en diefstal is. En om opsporingsambtenaren en handhavingsautoriteiten te stimuleren

serieuzer werk te maken van de aanpak van identiteitsfraude, werden zes jaar later via de Identity Theft Penalty Enhancement Act de straffen opgetrokken. Volgens Betsy Broder, assistant director van de afdeling Planning en Information van de Federal Trade Commission, moeten deze maatregelen dan ook niet zozeer worden gezien als een poging criminelen te ontmoedigen (McGuire, 2004). De boodschap was veeleer: handhaving heeft prioriteit. In dit verband valt ook te wijzen op een aantal recente maatregelen die mei 2006 zijn genomen door het Office of Community Oriented Policing Services (COPS, www.cops.usdoj.gov). Via een zevental aanbevelingen moeten de bij opsporing en handhaving betrokken autoriteiten meer slagkracht hebben in de aanpak van identiteitsfraude en de ondersteuning van slachtoffers. De aanbevelingen betreffen noodzakelijke samenwerking tussen autoriteiten, rapportage van alle voorvallen van identiteitsfraude, ondersteuning van slachtoffers, vergroting van het publieke bewustzijn via een campagne gericht op preventie en reactie en het opzetten van een database waarin alle wettelijke, beleids- en andere maatregelen zijn opgenomen, zodat bedrijven een allesomvattend beeld hebben van alle geldende maatregelen alsmede de verplichtingen waaraan men heeft te voldoen. Ook het Verenigd Koninkrijk kent sinds 2003 een expliciete wettelijke regeling voor identiteitsdiefstal. Maar van een afzonderlijke strafbaarstelling, zoals in de Verenigde Staten, is het voorsnog niet gekomen. De huidige regeling is in maart 2006 opgenomen in de toen afgekondigde Identity Cards Act (www.opsi.gov.uk/ACTS/acts2006/20060015.htm), een nogal omstreden wet die voorziet in een scala aan maatregelen om vijf beleidsdoelen te realiseren (behalve de aanpak van identiteitsfraude zijn dit onder meer de strijd tegen terrorisme en aanpak van georganiseerde misdaad). In tegenstelling tot de Verenigde Staten gelooft de Britse regering wel in biometrie: een van de instrumenten in de aanpak van terrorisme, criminaliteit en derhalve ook identiteitsdiefstal is de introductie van een nationale identiteitskaart. Deze zal worden voorzien van welgeteld drie biometrische kenmerken: vingerafdruk, gelaatsscan en irisscan. Behalve via de expliciete strafbaarstelling, tracht de Britse regering identiteitsdiefstal aan te pakken via aanvullende wettelijke maatregelen, zoals bijvoorbeeld door het ophogen van de strafmaat voor het op frauduleuze wijze verkrijgen van een rijbewijs. Overigens leert een blik op de situatie in de overige landen van de Europese Unie dat het Verenigd Koninkrijk een redelijk unieke stap

heeft gezet met de specifieke aanpak van identiteitsfraude: slechts enkele landen, zoniet geen enkel ander land buiten het Verenigd Koninkrijk, kent momenteel specifieke wetgeving (de inventarisaties spreken elkaar op dit punt tegen, zie Van der Meulen, 2006). Vooralsnog opteren de overige landen ervoor het fenomeen aan te pakken via bestaande (strafrechtelijke) bepalingen, zoals fraude en onrechtmatig gebruik van persoonsgegevens. Vooralsnog, omdat er inmiddels op EU-niveau wel stemmen opgaan nader te onderzoeken of een expliciete strafbaarstelling niet toch gewenst zou zijn (EU Fraud Prevention Expert Group, 2006). Mogelijk zullen dit najaar tijdens de EU High Level Conference *Maintaining the integrity of identities and payments; two challenges to fraud prevention* verdere plannen en stappen worden ontvouwd.

Meer kennis en inzicht heeft topprioriteit

Welke lessen kunnen we voor ons land trekken uit de voornoemde initiatieven? Eén ding zal duidelijk zijn: identiteitsdiefstal valt niet effectief aan te pakken met uitsluitend een simpele pennenstreek in wetgeving of een snel op te zetten publiekscampagne. Willen we criminelen aanpakken, slachtoffers helpen – of liever: op voorhand voorkomen dat mensen slachtoffer worden van deze vorm van criminaliteit – dan zullen beleidsmakers en wetgevingsjuristen verder moet denken dan het delict en de slachtoffers. Immers, het fenomeen identiteitsdiefstal is een product van onze huidige maatschappij. Een maatschappij waarin we ons voor het verlenen dan wel verkrijgen van bepaalde voorzieningen, diensten, toegang, enzovoort afhankelijk hebben gemaakt van identificatiemiddelen. Daarbij sturen beleidsmakers – om redenen van efficiëntie, kostenbesparing en effectiviteit – aan op een steeds verdere integratie en centralisatie van identificatie-instrumenten en -systemen. Maar met iedere stap in de richting van integratie wordt onze samenleving tegelijkertijd ook steeds afhankelijker van het adequaat functioneren van die ene centrale identificatie-infrastructuur. Met als gevolg: deze ontwikkeling maakt ons juist kwetsbaarder voor identiteitsfraude. ‘Want zodra instrumenten zoals het BSN en biometrie belangrijke maatschappelijke en juridische instrumenten voor identificatie blijken, is het per definitie een gewild object voor fraudeurs. Daarbij versterkt de vermeende hogere kwaliteit van deze

nieuwe instrumenten ook nog eens het vertrouwen in de geclaimde valse identiteit' (Prins, 2006a). Deze opvatting is overigens al veel langer in de Verenigde Staten te horen en werd recentelijk in het Verenigd Koninkrijk nog eens in een studie door de Londen School of Economics and Political Science onder de aandacht gebracht naar aanleiding van de introductie van de Britse nationale identiteitskaart (LSE, 2005). En zoals Solove het twee jaar geleden tijdens een congres in de Verenigde Staten formuleerde, de misvatting uit zich onder meer in de term identiteitsdiefstal: ten onrechte zien we het fenomeen als "theft" rather than as the product of inadequate security' (Solove, 2004, p. 4).

De aanpak van identiteitsdiefstal zal een samenstel van verschillende maatregelen moeten zijn. Maatregelen die niet alleen zien op de criminalisering en handhaving van het delict als zodanig, maar ook op de preventie ervan en het verwerven van de noodzakelijke kennis daarvoor. Daarbij staat voorop dat bij het denken over de mogelijk te nemen maatregelen, ook andere relevante belangen voor ogen gehouden moeten worden. Bovendien kunnen de negatieve gevolgen van identiteitsfraude variëren afhankelijk van het type fraude (pinpasfraude, paspoortfraude, phishing, enzovoort) en zullen daarmee de mogelijk te nemen maatregelen – en eventuele andere belangen die dan moeten wijken (zoals privacy als het om bepaalde vormen van handhaving aankomt) – ook verschillen. Juist ook om een goede discussie te voeren over de legitimiteit van de mogelijke maatregelen, is meer inzicht en kennis vereist van de omvang van de problematiek in ons land. Juist hierom ook is meer aandacht voor het fenomeen van groot belang. Het argument dat vooralsnog uit niets blijkt dat we in ons land met een belangrijk maatschappelijk probleem te maken hebben en alle aandacht voor identiteitsfraude daarmee voorlopig nogal overdreven is, geeft wat ons betreft blijk van een veel te passieve en afwachtende houding. Als het aan ons ligt zetten we daarom in Nederland, vergelijkbaar met het Identity Theft Data Clearinghouse in de Verenigde Staten, zo snel mogelijk een nationale databank op waarmee kennis wordt verzameld over de verschillende vormen van het fenomeen, de kenmerken en de aantallen. Alleen wanneer we beschikken over deze kennis valt een goede discussie te voeren over de omvang van de problematiek en de te nemen maatregelen. Deze databank kan daarnaast een rol spelen bij het ondersteunen van slachtoffers en het voorkomen van identiteitsfraude doordat het als een soort

van signaleringsinstrument kan fungeren. Alhoewel in ons land het Computer Emergency Response Team (Govcert.nl) wel aan de registratie van het brede scala aan 'ICT-incidenten' doet en vanuit een werkgroep van het Nationaal Platform Criminaliteitsbestrijding (waarin publieke en private sector samenwerken) stappen worden gezet om te komen tot het inrichten van een meldpunt voor signalen van identiteitsfraude, valt er nog enorm veel werk te verzetten alvorens ook ons land over een zodanig gedetailleerde en vooral ook centraal aangestuurde databank beschikt dat identiteitsdiefstal op een effectieve en gecoördineerde wijze in kaart wordt gebracht. Verder vallen lessen te trekken uit de publiekscampagnes die in andere landen zijn ingezet. Weliswaar kent ons land de algemene waarschuwingdienst van het hiervoor genoemde Govcert, www.waarschuwingdienst.nl en was identiteitsdiefstal het thema van de maand juli 2006 bij deze dienst, van een specifiek rondom dit probleem opgezette brede publieksvoorlichting is nog geen sprake. Juist omdat identiteitsdiefstal geheel eigen dimensies kent en wel eens een veel breder maatschappelijk probleem kan blijken te zijn dan de overige 'incidenten' waar de waarschuwingdienst zich momenteel op richt, mag met een aparte voorlichting en campagne wat ons betreft niet langer worden gewacht.

Bij diverse van de genoemde maatregelen kan ons land natuurlijk wachten tot op Europees niveau de nodige acties worden afgekondigd. Internationale afstemming en samenwerking is voor dit type delict van groot belang, zo kan men stellen. Dat klopt. Maar het is absoluut onwenselijk als Nederland met het ontwikkelen van een visie en het nemen van eigen maatregelen zou wachten tot op Europees niveau de neuzen één kant op staan en de nodige (compromis) maatregelen genomen zijn. Daarbij komt ook nog eens dat ons land zijn eigen identificatie-infrastructuur kent met specifiek Nederlandse kenmerken. De te nemen maatregelen zullen daarom ook op de context van ons land zijn afgestemd. Dat betekent niet dat we niet tevens aandacht moeten hebben voor de grensoverschrijdende implicaties van de problematiek en waar nodig de zaken internationaal moeten afstemmen dan wel aanpakken. Een voorbeeld daarvan kan zijn het entameren van dan wel actief betrokken zijn bij een discussie over de vraag of de EU moet blijven kiezen voor de huidige – sterk nationaal bepaalde – strafrechtelijke kwalificatie van identiteitsdiefstal (waarbij het delict onder een bestaande strafbepaling wordt gebracht, wat per lidstaat kan verschillen), dan wel

dat men in navolging van de VS moet kiezen voor een afzonderlijke strafrechtelijke regeling. Voordeel van dit laatste standpunt is niet alleen dat er in de toekomst een uniform Europees strafrechtelijk kader is. Ook wordt hiermee dan een duidelijk signaal aan zowel criminelen als slachtoffers afgegeven dat het de Europese Unie ernst is met de aanpak van het fenomeen.

Wij willen deze bijdrage afsluiten met het cruciale belang van preventie. Invulling geven aan dit belang is in onze ogen veel meer dan consumenten waarschuwen voor het gevaar van identiteitsdiefstal dan wel hen te wijzen op hun eigen verantwoordelijkheid in het voorkomen daarvan. Preventie is zeker ook het ontwikkelen van een zorgvuldige en toekomstgerichte, niet door de waan van de dag of politieke motieven ingegeven, visie op een veilige informatiesamenleving. Het is de overheid die hiervoor in eerste instantie de verantwoordelijkheid draagt. Niet alleen omdat het deze overheid zelf is die het functioneren van burgers in onze samenleving in toenemende mate – en dwingend – afhankelijk maakt van het gebruik van nieuwe identificatie-instrumenten. De overheid draagt de verantwoordelijkheid om ons zoveel als mogelijk is te beschermen voor de vele negatieve consequenties van identiteitsdiefstal, zeker ook omdat zij dat vanuit haar beschermende rol ten opzichte van de burgers verplicht is.

Literatuur

Binder, R., M. Gill

Identity theft and fraud; learning from the USA

Perpetuity research & consultancy international Ltd., 2005, p. 7-8. Beschikbaar via: (www.perpetuitygroup.com/prci/pdfs/identitytheftandfraudreport.pdf)

European Commission

A new EU action plan 2004-2007 to prevent fraud on non-cash means of payment
Brussels, COM (2004) 679 final., 20.10.2004

Europol 2006

EU organised crime threat assessment of 2006
Den Haag, 2006 (www.europol.europa.eu/index.asp?page=publications)

Executive Order 13402

Strengthening federal efforts to protect against identity theft
Washington DC, 2006

Cheney, J.S.

Do definitions still matter?

Discussion Paper Payment Cards Center, Federal Reserve Bank of Philadelphia, August 2005, p. 2. (www.phil.frb.org/pcc/discussion/identity-theft-definitions.pdf)

Fraud Prevention Expert Group (FPEG)

Draft minutes of the 10th meeting of the fraud prevention expert group

Brussels, MFSD, 22.05.2006

Gill, M.

The fight against identity fraud; a brief study of the EU, the UK, France, Germany, and the Netherlands

Perpetuity Research & Consultancy International Ltd, 2006 (www.perpetuitygroup.com)

Identity Theft Data Clearinghouse

Identity theft victim complaint data; figures and trends, January 1 – December 31, 2005

Federal Trade Commission, Washington DC, 2006

Koops, B.J., R. Leenes

ID theft, ID fraud and/or ID-related crime; definitions matter
Datenschutz und Datensicherheit (2006, nog te verschijnen)

Lenard, T.M., P.H. Rubin

Much ado about notification
Regulation, 29e jrg., nr. 1, 2006, p. 44-50

LSE, London School of Economics and Political Science

The identity project; an assessment of the UK identity cards bill & its implications

Londen, Interim Report, 2005 (www.lse.ac.uk)

McGuire, D.

Bush signs identity theft bill

Washington Post Online, 15 juli 2004. (www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul15.html)

Meulen, N. van der

The challenge of countering identity theft; recent developments in the United States, the United Kingdom, and the European Union

Rapport ten behoeve van het Nationaal Infrastructuur Cyber Crime programma (NICC), september 2006

Nederlandse Vereniging van Banken

Jaarverslag 2005, p. 26 (www.nvb.nl)

Prins, J.E.J.

Het BurgerServiceNummer en de strijd tegen de Identiteitsfraude
Computerrecht, nr. 1, 2003, p. 2-3

Prins, J.E.J.

Variaties op een thema; van paspoort- naar identiteitsfraude

Nederlands juristenblad, nr. 1,
2006a

Prins, J.E.J.

Property and privacy; European perspectives and the commodification of our identity

In: Guibault, L., P.B. Hugenholtz, (red.), *The future of the public domain*, The Hague, Kluwer Law International, 2006b, p. 223-258

Solove, D.J.

The legal construction of identity theft

Paper gepresenteerd tijdens het symposium Digital Cops in a Virtual Environment Yale Law School, 26-28 maart 2004 (islandia.law.yale.edu)

US Department of Treasury

The use of technology to combat identity theft; report on the study conducted pursuant to section 157 of the fair and accurate credit transactions act of 2003

Washington D.C., 2005, p. 9