Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy

Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy

J.E.J. Prins*

Identificatie, anonimiteit en privacy: het zijn in de virtuele wereld van het internet welhaast beladen begrippen geworden. Voor de komst van de ongekende mogelijkheden van informatie- en communicatietechnologie, was de identiteit van een persoon en het proces van identificeren een redelijk beheersbaar proces. Identificeren was veelal beperkt tot het tonen van een fysiek identiteitsdocument. Bovendien waren afwegingen tussen anonimiteit enerzijds en kenbaarheid anderzijds voorheen nauwelijks aanleiding voor problemen en (maatschappelijk) debat. Dat is inmiddels duidelijk veranderd. Diverse actoren in het maatschappelijk speelveld worden in onze huidige maatschappij geconfronteerd met de vraag onder welke omstandigheden en voorwaarden burgers en consumenten in hun doen en laten getraceerd en gevolgd mogen dan wel moeten worden. Waar liggen de grenzen van anonimiteit en kenbaarheid en welke rol spelen technologische ontwikkelingen en erkende privacybeginselen in de discussie over deze grenzen?

In deze bijdrage staan enkele actuele ontwikkelingen rondom het grensvlak tussen anonimiteit en identiteit centraal. Daarbij zal allereerst gekeken worden naar het terrein van opsporing, handhaving en terrorismebestrijding. Vervolgens wordt een beeld gegeven van de aandacht binnen de private sector voor kwesties rondom identiteit en anonimiteit. Ook hier blijken grote belangen gemoeid met het steeds beter en nauwkeuriger in beeld brengen van het doen en laten van individuele consumenten en andere gebruikers van internet. Indirect komt daarmee een scala aan nieuwe gegevens voor opsporingsautoriteiten vrij. Aan de hand van recente rechtspraak zal vervolgens worden bezien waar momenteel bij opsporing en handhaving door priva-

* De auteur is hoogleraar recht en informatisering, Tilburg Institute for Law, Technology, and Society (TILT), Universiteit van Tilburg.

te partijen de grenzen lijken te liggen tussen kenbaarheid en anonimiteit. Ten slotte zal in deze bijdrage worden afgesloten met enkele discussiepunten voor een nader debat over de nieuwe dilemma's rondom identificatie, anonimiteit en privacy.

De tandemtechnologie en opsporing

Een grote rol bij de huidige tendens naar het identificeren van personen en hun gedrag speelt natuurlijk de sterk toegenomen politieke aandacht voor opsporing, handhaving en terrorismebestrijding en de nieuwe opsporingsbevoegdheden die als uitvloeisel hiervan worden geïntroduceerd. Zo wijzen de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties er in hun nota over terrorismebestrijding, die zij in september 2004 naar de Tweede Kamer stuurden, op dat informatie de belangrijkste grondstof is voor terrorismebestrijding.[1] En waar informatie de grondstof is, is techniek het gereedschap om de grondstof aan de oppervlakte te krijgen. Het is daarom niet verwonderlijk dat technologische ontwikkelingen in de groei van het arsenaal aan opsporingsbevoegheden een geheel eigen rol spelen. Een blik op de ontwikkelingen van de afgelopen jaren laat namelijk zien dat met iedere nieuwe technologie die het identificeren en opsporen van personen optimaliseert, ook het arsenaal aan wettelijke bevoegdheden wordt uitgebreid. Illustratief is het recente voorstel van de minister van Binnenlandse Zaken en Koninkrijksrelaties, Remkes, om nieuwe vormen van geautomatiseerde data-analyse (datamining) toe te laten. In zijn brief van medio juli 2004 aan de Tweede Kamer stelt de minister: 'De inzet moet voor alles gericht zijn op het zo vroeg mogelijk identificeren van de voorbereiding van mogelijke terroristische acties en de daders daarvan. Nieuwe vormen van geautomatiseerde data-analyse worden daarvoor ingezet, zoals het zoeken aan de hand van profielen en het opsporen van bepaalde patronen met behulp van datamining. Daartoe moeten grote bestanden met persoonsgegevens van niet-verdachte personen doorzocht worden (....)'.[2] Bij al deze ontwikkelingen is het van belang te onderkennen dat we slechts aan de vooravond staan van een wereld waarin een breed scala

1 Ik verwijs hiervoor naar nieuwe technieken als datamining (het zoeken naar relaties en patronen in databases), datawarehousing (het verzamelen, vastleggen en analyseren van gegevens), oscint (openbronnenonderzoek), enzovoort.

2 *Kamerstukken II*, 2004/05, 5306302/504.

aan technieken voorhanden is om personen 'in beeld' te brengen. Met andere woorden, vergeleken bij hetgeen ons te wachten staat, zijn de huidige mogelijkheden slechts peanuts. Illustratief zijn bijvoorbeeld de ontwikkelingen op het terrein van 'domotica'. Hierbij worden diverse technologische applicaties in (apparaten in) de woning ingebouwd, teneinde de huiselijke omgeving te laten reageren op de wensen van de bewoner.[3] De verwachting is dat daarbij voornamelijk gebruikgemaakt gaat worden van draadloze verbindingen, waardoor onze woning steeds onlosmakelijker wordt verbonden met computernetwerken en een diversiteit aan activiteiten binnen de woning van buitenaf te volgen zal zijn (Koops e.a., 2004). Ook de momenteel nog relatief onbekende techniek van Radio Frequency IDentification (RFID) zal het in de afzienbare toekomst mogelijk maken om op afstand gedetailleerde informatie te vergaren over het dagelijkse doen en laten van burgers en consumenten. RFID, waarvan de eerste toepassingen al in gebruik zijn, is een technologie waarbij met behulp van minuscule chips personen en of objecten uniek geïdentificeerd en gevolgd kunnen worden.[4] Ten slotte zijn de verwachtingen hoog gespannen over de mogelijkheden van technologische ontwikkelingen, waaronder die op het terrein van nanotechnologie, die het lichaam kunnen verkennen en binnendringen (Prins, 2004b).

Met het nieuwe scala aan technologische mogelijkheden treden ook de welhaast ongekende mogelijkheden en voordelen van unieke identificatie, koppeling, stroomlijning en pro-actief beleid naar voren. En onder het huidige kabinet krijgen politie, justitie en inlichtingendiensten ook steeds meer armslag om dergelijke mogelijkheden daadwerkelijk te gebruiken ten behoeve van opsporing en handhaving. Het voornoemde plan van minister Remkes is zeker niet het enige. Zoals bekend zijn de afgelopen periode diverse initiatieven gepresenteerd dan wel wetswijzigingen doorgevoerd die een verruiming beogen van de bestaande regels voor het verzamelen, verkrijgen, gebruiken, uitwisselen en koppelen van informatie en persoonsgegevens. Zo biedt de in september 2004 in werking getreden Wet vorderen gegevens telecommunicatie diverse nieuwe mogelijkheden voor het opvragen van gegevens met betrekking tot de telecommunicatie.[5] Op 1 januari 2005 zal de Wet op de uitgebreide identificatieplicht in werking treden.[6]

3 *Kamerstukken II*, 2003/04, 27925, nr. 123.

4 Zie bijvoorbeeld <www.newscenter.philips.com/Assets/Downloadablefile/HomeLab_Fact_Sheet-3143-1213.doc>.

5 Zie voor nadere informatie het tijdschrift op: <www.rfidjournal.com>.

6 *Stb.* 2004, 105. Tevens is het Besluit vorderen gegevens telecommunicatie op die datum in werking getreden (*Stb.* 2004, 394).

Verder zullen de opsporingsbevoegdheden nog worden uitgebreid met onder meer de hierna nog nader te vermelden regelingen uit het wetsvoorstel 'bevoegdheden vorderen gegevens'.[7]
Ook op Europees niveau is de tendens naar ruimere bevoegdheden duidelijk waarneembaar. Najaar 2004 spraken de verantwoordelijke ministers van de diverse EU-lidstaten af dat het grensoverschrijdend uitwisselen van politie- en justitiegegevens verder geïntensiveerd zal worden. Eerder maakten diverse lidstaten zich al sterk voor een uitbreiding van de bewaarplicht voor verkeersgegevens. Waar de Raad van Europa zich in het (elders in dit nummer door Kaspersen besproken) Cybercrime-verdrag uiteindelijk niet wilde branden aan de discussie over het bewaren van deze gegevens, lijken de EU-landen inmiddels welhaast moeiteloos over de negatieve consequenties voor de privacy heen te stappen. Ook Nederland heeft zich een voorstander getoond van het voorstel om te komen tot een wettelijke plicht voor telefoonbedrijven en internetaanbieders om verkeers- en locatiegegevens van hun klanten te bewaren (welke telefoonnummers bellen met elkaar, hoe lang en vanuit welke locatie (hetgeen met mobiele telefonie soms tot op honderd meter nauwkeurig is vast te stellen), welk internetadres (IP-adres) surft naar welke website, enzovoort). Ons land kent momenteel alleen voor telecommunicatieaanbieders een wettelijke regeling voor het bewaren van verkeersgegevens (Koops, 2003). Indien het ontwerp-kaderbesluit zoals dat in april 2004 door Engeland, Frankrijk, Ierland en Zweden is gepresenteerd,[9] wordt aangenomen, geldt in de toekomst echter een bewaarplicht voor een veel groter arsenaal aan gegevens: alle informatie over het bel-, e-mail- en surfgedrag van burgers in de Europese Unie. En waar voorheen bij vaste telefonie kennis als 'wie belt met wie' geen inzicht verschafte in de inhoud van de communicatie, is dit met de komst van internet drastisch veranderd. Immers, wie een webadres (online locatie) intypt met in dat adres zelf een verwijzing naar pornografie of illegale software, verschaft daarmee niet alleen informatie over de communicatie maar tevens over de inhoud van die communicatie. Met andere woorden, het traditioneel heldere onderscheid tussen inhoud (brief) en adressering (adres op enveloppe) vervaagt.

7 *Stb.* 2004, 300.
8 *Kamerstukken II*, 2003/04, 29 441.
9 Beschikbaar via <www.europapoort.nl/9294000/modules/vgbwr4k8ocw2f=/vgq8mzge32zu.pdf> Voor het Nederlandse standpunt, zie <www.europapoort.nl/9294000/modules/vgbwr4k8ocw2f=/vgs0c11ojpk6.doc>.

Het beeld dat bij al deze initiatieven opkomt, is dat van een verregaande invloed van technologie op het creëren van opsporingsbevoegdheden. Bovendien beperken diverse van de nieuw verleende bevoegdheden zich niet tot het opsporen van gegevens over verdachte personen. Wanneer justitie daartoe aanleiding ziet, biedt het wetsvoorstel 'bevoegdheden vorderen gegevens' de bevoegdheid om ook gegevens over niet-verdachte burgers op te vragen. Ten slotte lijkt de wens van de overheid tot het versterken van haar informatiepositie duidelijke consequenties te hebben voor zogenoemde 'zachte informatie' die in voorfasen wordt verzameld. Juist met behulp van de nieuwe mogelijkheden van de techniek is een groeiende hoeveelheid zachte informatie boven tafel te krijgen, waarbij deze ook in een toenemend aantal gevallen direct wordt ingezet uit vrees voor de potentieel enorme gevolgen die een terreuraanslag kan hebben. Voor het Openbaar Ministerie vormt de kwetsbare status van zachte informatie inmiddels aanleiding om zelfstandig tot het verzamelen van informatie over te gaan (*NRC Handelsblad*, 8 oktober 2004). Als zodanig behoeft deze ontwikkeling niet direct te worden afgewezen, maar wederom leidt ze wel tot extra risico's. Immers, wat de bevoegdheden van de ene dienst (lees: Algemene Inlichtingen en Veiligheidsdienst) zijn, moeten natuurlijk ook de bevoegdheden van de andere organisatie (Openbaar Ministerie) worden. De eigen informatiehonger moet immers gestild worden. Met andere woorden, de spiraal van uitdijende bevoegdheden in optima forma.

Met deze introductie van aanzienlijk ruimere opsporingsbevoegdheden en het steeds verder optimaliseren van 'de informatiepositie' van de overheid treedt de belangrijke vraag naar voren welke *checks and balances* in de nieuwe relatie tussen burger en overheid worden ingebouwd. Bovendien, wanneer meer aandacht voor bepaalde maatschappelijke dreigingen (momenteel: terrorisme) ten koste gaat van de intensiteit van het opsporen van andere vormen van criminaliteit – zoals ook door het Openbaar Ministerie zelf ten aanzien van een verminderde aandacht voor drugszaken wordt erkend – is het van groot belang dat de overheid verantwoording aflegt ten aanzien van noodzaak, effectiviteit en implicaties van de voorgestelde bevoegdheden. Of zoals het jongstleden juli in de VS gepresenteerde eindrapport van de National Commission on Terrorist Attacks Upon the United States, ook wel bekend als de 9/11 Commission, het expliciet formuleert: 'The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually

materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.'[10]

Van individueel persoonsgegeven naar identiteit

Niet alleen de belangen van opsporing en handhaving lijken te profiteren van de toenemende mogelijkheden van de technologie. Ook voor een verdere optimalisering van de (commerciële) dienstverlening liggen er belangrijke kansen en indirect komen daarmee ook weer nieuwe gegevens voor opsporingsinitiatieven vrij. Omdat de nieuwe gegevensverzamelingstechnieken steeds verfijnder en complexer worden, is het mogelijk om zeer accurate marketingstrategieën op basis van gebruikersprofilering te ontwikkelen. Het is derhalve niet verwonderlijk dat steeds meer aanbieders van internetdiensten inzetten op het selecteren, filteren en classificeren van persoonsgegevens teneinde een individuele informatierelatie met een consument vorm te geven. Zo mag de ontwikkeling van zogeheten gepersonaliseerde diensten zich over een toenemende populariteit verheugen (Van der Hof, Lips e.a., 2004). Een voorbeeld van een dergelijke dienst is Movielens. Deze dienst werkt met 'recommender systems': systemen die het gebruikers mogelijk maken om elkaar iets aan te bevelen. Bij Movielens kunnen gebruikers films waarderen en vervolgens op hun specifieke voorkeuren andere films aangeboden krijgen.[11] Maar niet alleen de private sector ziet belangrijke kansen liggen in het aanbieden van gepersonaliseerde diensten. Dat geldt, zo laten ontwikkelingen in de Verenigde Staten zien, zeker ook voor de overheid. In de VS heeft de staat Virgina sedert 1998 een 'one-stop' overheidsportaal op het internet (www.virginia.gov) waar burgers en bedrijven gepersonaliseerde publieke diensten kunnen krijgen. Zo kunnen burgers een gepersonaliseerde 'My Virginia' webpagina instellen, waarop informatie en diensten worden getoond conform het interesse- en behoeftepatroon van de burger.

10 Het rapport is onder meer beschikbaar via: <www.epic.org/privacy/terrorism/911report.pdf>.

11 Zie <movielens.umn.edu/login>. Een ander mooi voorbeeld is de op mobiele communicatie en location-based systemen gebaseerde dienst *Buddy alert* van het Duitse Mobiloco voor jongeren bij het gepersonaliseerd vinden van nieuwe vrienden: <www.mobiloco.de>.

Personalisatie betekent in veel gevallen ook identificatie, waardoor de risico's ten aanzien van de privacy van de gebruiker toenemen. Deze risico's kunnen zich voordoen wanneer de gevraagde persoonsgegevens niet strikt noodzakelijk zijn voor de levering van of toegang tot de dienst, de persoonsgegevens zonder toestemming van de gebruiker (mede) voor andere doeleinden worden gebruikt dan waarvoor deze aanvankelijk waren verzameld en vastgelegd, en de gebruiker geen of onvoldoende toegang (bijvoorbeeld via de website) krijgt tot diens persoonsgegevens. Een gevaar is bovendien dat gebruikersinformatie wordt verzameld zonder dat dit voor de gebruiker kenbaar is. Het is juist deze ontwikkeling – de inzet van zogenoemde spionagesoftware, spyware – die anonimiteit op internet verder op scherp stelt. Bij spyware betreft het programma's die zich – zonder dat de gebruiker van de computer daar weet van heeft – nestelen op een computer, aldaar informatie over deze gebruiker verzamelen en deze vervolgens doorspelen aan een centraal punt dan wel specifiek bedrijf (bijvoorbeeld een online adverteerder). Met de verzamelde gegevens worden gebruikers vervolgens bestookt met reclamevensters, de standaardinstellingen van webpagina's veranderd, bij zoekopdrachten naar een foutieve website verwezen en gebruikers zelfs ongemerkt op hoge kosten gejaagd omdat ze ongewild gebruikmaken van betaalde internetdiensten. Met name aanbieders van spam (ongewenste elektronische reclame) nemen – nu het voor hen met de huidige filtersystemen steeds moeilijker wordt computergebruikers effectief te bereiken en spamming bovendien sinds juni 2004 aan wettelijke regels is gebonden – de laatste tijd hun toevlucht tot dergelijke spionageprogramma's. Illustratief voor de toenemende populariteit van spyware is het bericht dat een Amerikaanse internetdienst in april 2004 ruim elf miljoen van dergelijke programma's aantrof op 420.000 computers, terwijl dit aantal een maand eerder 'slechts' zeven miljoen programma's op 237.000 computers was (*Computable*, 25 juni 2004). Inmiddels heeft de minister van Economische zaken in juli 2004 in reactie op kamervragen aangegeven dat een wetsvoorstel voor de aanpak van deze problematiek en meer breder tot het creëren van verplichtingen voor aanbieders van informatiediensten in het tweede kwartaal van 2005 aan de Kamer zal worden aangeboden.[12]

12 *Kamerstukken II*, 2003/04, nr. 1907.

Alle voornoemde ontwikkelingen hebben met elkaar gemeen dat ze inspringen op de groeiende belangstelling van bedrijven en overheden voor profielen van consumenten in plaats van individuele persoonsgegevens. Onder invloed van de mogelijkheden die de techniek daartoe biedt, verschuift de aandacht naar marketing op basis van 'identiteiten' van personen, omdat de context waarin gegevens worden verkregen (welke persoon, met welke (gedrags)kenmerken heeft welke voorkeur in welke situatie en onder welke (sociale en economische) omstandigheden) steeds inzichtelijker wordt en daarmee een prominente rol gaat spelen. Kortom, personen zullen in verschillende 'identiteiten' kenbaar en transparant worden. Nu zou men kunnen stellen dat hiermee nog niet is gezegd dat privacy ontoelaatbaar onder druk komt te staan. Echter, veelal wordt vergeten dat deze in eerste instantie door de private sector gegenereerde 'identiteiten' in principe ook voor politie en justitie beschikbaar komen. Immers, onder het eerdergenoemde wetsvoorstel 'bevoegdheden vorderen gegevens' krijgt de officier van justitie de bevoegdheid om 'andere dan identificerende' gegevens op te vragen. Het gaat daarbij ook om gegevens over iemands koopgedrag of uitleenvoorkeur (video's, boeken), waarbij het uitleveringsverzoek tevens 'toekomstige' gegevens kan betreffen. Alhoewel van deze bevoegdheid pas gebruikgemaakt mag worden bij verdenking van zwaardere misdrijven, is ze niet beperkt tot gegevens van verdachte personen. Wanneer justitie daartoe aanleiding ziet, betreft het ook gegevens over niet-verdachte burgers. Daarmee komen alle in onze maatschappij nu beschikbare en toekomstige gegevens, ook die gegenereerd door de private sector (dat zijn er inmiddels heel wat!) vrij voor politie en justitie. Weliswaar zijn er beperkingen gesteld (gegevens voor persoonlijk gebruik zijn uitgezonderd; voor gevoelige gegevens is machtiging van de rechter-commissaris nodig), maar zodra er verdenking is van een misdrijf is het credo: vragen staat justitie vrij en private instanties dienen gehoor te geven.

Tot hoever reikt anonimiteit?

Bij al deze aandacht voor identificatie en personalisatie lijkt er nauwelijks nog ruimte voor handelingen op het internet waarbij de betrokken personen zich in volstrekte anonimiteit kunnen hullen. Toch zijn er zeker situaties waarin onduidelijk is met wie men precies van doen heeft en in sommige gevallen leidt dit tot problemen en juridische

vragen over de grenzen van anonimiteit. Illustratief zijn de pogingen van de muziek- en filmindustrie om achter de identiteit te komen van de gebruikers van zogenaamde uitwisseldiensten, zoals het bekende KaZaA. Organisaties van auteursrechthebbenden, zoals in ons land de Stichting Brein, volgen het voorbeeld van zusterorganisaties in de Verenigde Staten, die grote aantallen dagvaardingen aan individuele personen uitvaardigen omdat ze gebruik zouden maken van internetdiensten voor het illegaal uitwisselen van muziek- en filmbestanden (Ekker, Van Daalen, 2003). In de VS zijn inmiddels diverse procedures gevoerd over de vraag of internetaanbieders verplicht zijn de persoonsgegevens van abonnees vrij te geven zodat auteursrechthebbenden kunnen achterhalen wie inbreuk op hun rechten pleegt en hen daarvoor kunnen aanpakken. In een uitspraak van een New York district court van juli 2004 formuleerde de rechtbank op basis van eerdere soortgelijke rechtszaken een toets aan de hand waarvan beoordeeld kan worden of abonneegegevens verstrekt dienen te worden.[13] Alhoewel de privacyverwachting van de anonieme abonnee in dit toetsingskader zeker een rol speelt, lijkt de verstrekking van gegevens en dus het opheffen van anonimiteit toch prioriteit te krijgen.
Tot op heden hebben zich in ons land geen rechters gebogen over de vraag of en onder welke omstandigheden internetaanbieders de namen vrij dienen te geven van hun abonnees wanneer deze worden verdacht van het illegaal uitwisselen van auteursrechtelijk beschermde muziek en films. Wel heeft het Hof Amsterdam zich recentelijk uitgelaten in een andere kwestie over een soortgelijke vraag (Hof Amsterdam, 24 juni 2004, Lycos/Pessers). Het betrof hier de weigering van internetaanbieder Lycos om de persoonsgegevens van een abonnee af te staan omdat deze abonnee naar het oordeel van de eiser (Pessers) onrechtmatig jegens hem had gehandeld. Eerder oordeelde de President van de rechtbank Haarlem dat Lycos inderdaad verplicht was abonneegegevens bekend te maken (Pres. Rb. Haarlem, 11 september 2003). Het Hof kwam tot de conclusie dat er weliswaar geen sprake was van onmiskenbaar onrechtmatig handelen door de abonnee, maar dat de internetaanbieder toch verplicht was de gevraagde gegevens te verstrekken. Het Hof betrok in dit oordeel vier factoren, te weten: 1) de mogelijkheid dat de handelingen van de abonnee onrechtmatig zijn, of 2) de derde partij een reëel belang heeft bij de gegevens, of 3) er geen andere, minder ingrijpende mogelijkheden zijn

13 Sony Music Entertainment Inc. v. Does 1-40, S.D.N.Y., 04 Civ. 473 (DC), 7/26/04.

om de gegevens te achterhalen en 4) of een afweging is gemaakt tussen de belangen van de internetaanbieder en diens abonnee tegenover de belangen van de derde. Het Hof oordeelde dat art. 8 Wet bescherming persoonsgegevens voldoende ruimte biedt om de verstrekking van de persoonsgegevens door de internetaanbieder te rechtvaardigen. Indien 'voldoende aannemelijk' is dat de informatie op de website onrechtmatig is en schadelijk kan zijn, kan een vordering tot het verstrekken van de persoonsgegevens worden toegewezen, aldus het Hof. Opvallend is dat het Hof de plicht tot het verstrekken van persoonsgegevens relateert aan de algemene zorgvuldigheidsplicht in het maatschappelijk verkeer. Daarmee stelt het Hof impliciet dat de nieuwe wettelijke regeling van art. 6:196c BW ter implementatie van de Europese Richtlijn elektronische handel (2000/31/EG) geen limitatieve regeling inzake de aansprakelijkheid van internetdienstverleners kent. Deze richtlijn stelt als criterium 'onmiskenbaar onrechtmatig', terwijl het Hof daar op grond van de algemene zorgvuldigheidsplicht het veel minder zware criterium 'voldoende aannemelijk' aan toevoegt. Met andere woorden, een ieder die anoniem op het internet uitlatingen doet dan wel op andere wijze onrechtmatig jegens een ander handelt en daarmee schade berokkent, zal er serieus rekening mee moeten houden dat zijn of haar anonimiteit door een internetaanbieder wordt opgeheven omdat van de aanbieder in het kader van diens zorgvuldigheidsplicht in het maatschappelijk verkeer wordt verlangd dat deze persoonsgegevens van de anonieme abonnee verstrekt.

Afsluiting: aandacht voor de andere zijde van de medaille

De hiervoor beschreven ontwikkelingen laten overduidelijk zien dat anonimiteit op internet stevig onder druk staat. Identificatie prijkt om diverse redenen hoog op de agenda van zowel publieke als private organisaties en de ontwikkelingen binnen de politiek en rechtspraak laten zien dat veel van deze organisaties ook daadwerkelijk de ruimte krijgen om de identiteit van personen in beeld te brengen. De nieuwe mogelijkheden van ICT spelen daarbij een prominente rol. Bij deze vlucht naar voren mag echter niet worden vergeten dat identificatie ook kwetsbare kanten kent.
Zo is allereerst het proces van identificeren kwetsbaarder geworden. De berichten uit de VS, waar identiteitsfraude inmiddels de snelst

groeiende vorm van criminaliteit is, noodzaken alhier op z'n minst tot waakzaamheid. Kenmerkend voor deze nieuwe vorm van criminaliteit is dat iemand, door gebruik te maken van de identiteit van een ander, dan wel van een niet-bestaand of overleden persoon, bewust de schijn oproept van een identiteit die hem of haar niet toebehoort. Met andere woorden, er is dus geen sprake van een persoonsverwisseling middels een vervalst identiteitsbewijs, maar de fraudeur gaat met een fictieve of 'geleende' identiteit aan de slag. En juist de nieuwe technologie blijkt ook bij deze nieuwe vorm van fraude een 'faciliterende' rol te spelen (Prins, 2003). Vlak voor het zomerreces 2004 ontving de Tweede Kamer de kabinetsreactie op het rapport *Identiteitsfraude en (reis)documenten* van de Koninklijke Marechaussee.[14] Uit de reactie van het kabinet blijkt dat het huidige beleid rondom identiteitsfraude nog te zeer gericht lijkt op de aanpak van vervalste identiteitsbewijzen in plaats van identiteitsfraude zonder vervalste documenten. Zowel in ons land als daarbuiten duiken in toenemende mate bewijzen op dat identiteitsfraude een snel groeiend probleem is en nieuwe maatregelen nodig lijken om de fraudegevoeligheid van 'identiteiten' in de toekomst te verminderen en de controle op fraude te verbeteren, aldus het kabinet. Alhoewel het beeld van identiteitsfraude voor ons land vooralsnog anders is dan in de VS, en het bovendien nog onvoldoende duidelijk is of onze identificatieprocessen in eenzelfde mate als in de VS kwetsbaar voor fraude zijn, is het in ieder geval noodzakelijk dat het proces van identificatie en de identificerende informatie die daarmee beschikbaar komt en vervolgens wordt gebruikt, met een kritische blik tegemoet wordt getreden.

Ten tweede knaagt de toenemende drang tot identificeren aan enkele centrale beginselen in onze rechtsstaat. Terecht trekt het kabinet zich de huidige dreiging van het internationaal terrorisme aan en initieert maatregelen, waaronder maatregelen om de informatiepositie van de opsporingsinstanties te verstevigen. Maar deze vlucht naar voren mag de overheid niet blind maken voor de kwetsbare posities die daarmee dreigen open te vallen: het veronachtzamen van essentiële beginselen van de rechtstaat en het verwaarlozen van de aandacht voor andere vormen van criminaliteit. Is een doeltreffende strafrechtspleging voor een rechtsstaat immers niet zeker zo belangrijk als een die behoorlijk functioneert? Kortom, het is aan de regering om vooraf – en niet achteraf wanneer een weg terug nauwelijks meer een realistisch

14 *Kamerstukken II*, 2003/04, 29200 VI, nr. 166.

scenario is – te komen met een kosten-batenanalyse van de voorgestelde maatregelen.

En daarmee wordt ook de vraag relevant of het huidige wettelijke regime voor privacybescherming nog wel voldoende is geëquipeerd om burgers de noodzakelijke bescherming te bieden in een maatschappij waarin identificatie en 'identiteiten' centraal lijken te komen te staan. Immers, het voorgaande betoog heeft onder meer laten zien dat het toenemende mate niet alleen gaat om de vraag *of* persoonsgegevens (mogen) worden verwerkt, maar ook om de vraag *hoe en in welke combinatie* ze worden verwerkt. De huidige Wet bescherming persoonsgegevens (Wbp) beperkt de rechten van betrokkenen echter tot enkelvoudige verwerkingen (losse persoonsgegevens). Maar de 'identiteit' van burgers, consumenten, (potentiële) terroristen, criminelen en personen in andere 'hoedanigheden' wordt samengesteld uit verschillende puzzelstukjes, zoals gedragspatronen en sociale omstandigheden (Prins, 2004c). En juist wanneer deze personen inzicht willen krijgen in de achterliggende processen en de wijze waarop de totale puzzel tot stand is gekomen, kent de wet nauwelijks instrumenten voor transparantie, toetsing en controle. Kortom, in een maatschappij waarin identificeren en 'identiteiten' een steeds prominentere rol spelen maar de randvoorwaarden voor privacybescherming niet zijn toegesneden op deze verschuiving in aandacht, is een discussie gewenst over de vraag welke randvoorwaarden we moeten stellen voor controle op, transparantie van en verantwoording over de creatie en het gebruik van 'identiteiten'.

Hiermee treedt ten slotte een laatste punt naar voren. De privacydiscussie lijkt de laatste jaren voornamelijk te zijn gevoerd vanuit een focus op persoonsgegevensbescherming en een krampachtige poging greep te krijgen op technologie. Daarmee is echter die geheel andere dimensie van privacy, de persoonlijke levenssfeer, verregaand verwaarloosd. In feite is gegevensbescherming – de Wbp – ook totaal niet belangrijk. Het is niet meer dan een wettelijk systeem voor het maken van afspraken over de omgang met persoonsgegevens, de juistheid en beveiliging daarvan. Privacy is echter veel meer dan dat. Het is vrijheid, zelfbeschikkingsrecht en de mogelijkheid om ons persoonlijk leven in te richten. Zolang deze dimensie niet daadwerkelijk handen en voeten krijgt in de discussie over de inrichting van onze huidige maatschappij en wordt gezien als een serieus te nemen belang, lijken belangen waar privacy echt voor staat het onderspit te delven.

Als men zo met dit recht omspringt, kan het net zo goed uit de grondwet worden verwijderd.

Natuurlijk is het juist deze dimensie van privacy die zo moeilijk in simpele termen, laat staan regels, is te vatten. Voor privacy is immers geen calculatie te maken. Daarbij komt dat privacy een zeer contextafhankelijk iets is en juist daardoor zo nauw samenhangt met maatschappelijke ontwikkelingen en beleidsprioriteiten. Voor de dag van vandaag lijken dat vooral veiligheid, terrorismebestrijding, handhaving, efficiëntie en commerciële belangen te zijn. En het kan ook zijn dat deze ontwikkelingen en prioriteiten inderdaad verlangen dat privacy momenteel een stapje terug doet. Maar als we die keuze ook werkelijk wensen te maken, zijn we het aan onze rechtsstaat verplicht dit op een goed beredeneerde en onderbouwde wijze te doen. Een keuze waarbij duidelijk is wat precies de implicaties zijn van de ruimte die aan die andere belangen wordt gegeven. Want juist de implicaties reiken vaak veel verder dan men op het eerste oog zou menen. Zo stelt de technologie ons in staat geheel nieuwe verbanden te leggen. En zo bieden recente aanpassingen in wetgeving de mogelijkheid dat gegevens die in eerste instantie door de private sector voor commerciële doeleinden worden blootgelegd, ook automatisch beschikbaar komen voor opsporingsdoeleinden. Kortom, de discussie moet zich niet beperken tot de noodzakelijke bevoegdheid of technische mogelijkheid in zijn isolement, maar moet zeker ook de optelsom van al die bevoegdheden en mogelijkheden helder maken. Gekoppelde rechten, bevoegdheden en plichten stellen ons voor uitdagende en complexe vervolgvragen die we niet kunnen en mogen negeren. En welke plaats privacy in onze huidige maatschappij ook moge krijgen, recht doen aan de plaats van privacy in onze Grondwet betekent in ieder geval dat dit recht als kritisch klankbord moet
kunnen fungeren. Privacy is immers in essentie de cruciale metafoor om politici, burgers, organisaties, bedrijven en andere betrokkenen de plaats van vrijheid, transparantie, zelfbeschikking en individuele controle voor ogen te laten houden.

Literatuur

Ekker, A., O. van Daalen
De provider als speurhond van de muziekindustrie
JAVI, 2003/4, p. 129-134

Hof, S. van der, M. Lips e.a.
Personalisatie van publieke en private dienstverlening
JAVI, nr. 4, 2004, p. 128-134

Koops, B.J., J.E.J. Prins
De toenemende strafbaarstelling van technische hulpmiddelen: over intenties, bestemmingen en instrumentele wetgeving
In: M.S. Groenhuijsen, J.B.H.M. Simmelink (red.), *Glijdende schalen; liber amicorum J. de Hullu*, Nijmegen, Wolf Legal Publishers, 2003, p. 341-386

Koops, B.J.
Verkeersgegevens en strafrecht; een agenda voor discussie
In: L.F. Asscher, A.H. Ekker (red.), *Verkeersgegevens; een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever, 2003, p. 59-92

Koops, B.J., H. van Schooten e.a.
Recht naar binnen kijken; een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken
Den Haag, Sdu, 2004

Net, C. van der
De civielrechtelijke aansprakelijkheid van internetproviders na de Richtlijn elektronische handel
JAVI, nr. 1, 2002, p. 10-15

Prins, J.E.J.
Het BurgerServiceNummer en de strijd tegen de identiteitsfraude
Computerrecht, nr. 1, 2003, p. 2-3

Prins, J.E.J.
De stilzwijgend uitdijende opspoorvergaarbak
Nederlands Juristenblad, afl. 16, 2004, p. 823

Prins, J.E.J.
Algemene voorwaarden in een technisch jasje
Nederlands Juristenblad, afl. 79, 2004b, p. 1291

Prins, J.E.J.
The propertization of personal data and identities
Electronic journal of comparative law, 8e jrg., nr. 3, 2004c
<www.ejcl.org/>