Technology Assessment

Databases

Over ICT-beloftes, informatiehonger en digitale autonomie

Geert Munnichs, Mirjam Schuijff & Michiel Besters (redactie)

Rathenau Instituut

Het **Rathenau Instituut** laat de invloed van wetenschap en technologie op ons dagelijks leven zien en brengt de dynamiek ervan in kaart; door onafhankelijk onderzoek en debat.

Databases

Over ICT-beloftes, informatiehonger en digitale autonomie

Rathenau Instituut
Anna van Saksenlaan 51

Postadres:
Postbus 95366
2509 CJ Den Haag

Telefoon: 070-342 15 42
Telefax: 070-363 34 88
E-mail: info@rathenau.nl
Website: www.rathenau.nl

Uitgever: Rathenau Instituut
Ontwerp en opmaak: Smidswater
Foto's: Hollandse Hoogte, iStockphoto
Drukwerk: Drukkerij Groen, Hoofddorp

Dit boek is gedrukt op FSC gecertificeerd papier

Eerste druk: november 2010

ISBN/EAN 978-90-77364-33-8

Deze publicatie kan als volgt worden aangehaald:
Munnichs, G., M. Schuijff & M. Besters (red.):
Databases – Over ICT-beloftes, informatiehonger en digitale autonomie.
Den Haag, Rathenau Instituut 2010

Databases
Over ICT-beloftes, informatiehonger en digitale autonomie

Redactie
Geert Munnichs
Mirjam Schuijff
Michiel Besters

Voorwoord

Onze samenleving digitaliseert in hoog tempo. Computers en internet zijn niet meer weg te denken uit ons leven. De voordelen zijn dan ook legio: verbetering van de communicatie, verhoging van de efficiëntie, meer gemak voor de burger. Databases spelen hierbij een belangrijke rol. Ze maken het mogelijk om grote hoeveelheden gegevens op te slaan, uit te wisselen en te bewerken. Ze vormen de digitale ruggengraat van de informatiemaatschappij.

Maar het gebruik van databases is niet onproblematisch, zoals deze studie laat zien. De studie vergelijkt zes digitale informatiesystemen. Daaruit komt naar voren dat de belangen van degene over wie gegevens worden verzameld vaak een ondergeschikte rol spelen. Dat blijkt niet alleen uit de veelal tekortschietende aandacht voor de beveiliging van gegevens – waarvan vooral de burger of consument de dupe wordt – maar ook uit hun veelal zwakke rechtspositie. Zo is het voor betrokkenen vaak lastig om fouten in databestanden hersteld te krijgen. Het gebruik van databases kan bovendien leiden tot verdergaande afhankelijkheden van de overheidsbureaucratie of het bedrijfsleven. De burger, cliënt of consument dreigt daarmee steeds meer grip te verliezen op wie wat met zijn gegevens doet. Databases zijn dan ook geen risicovrije systemen.

De studie waarschuwt ook voor te hoge verwachtingen van de mogelijkheden van ICT. Databases zijn geen panacee voor ieder probleem. Meer data leiden niet per definitie tot meer efficiëntie of een betere dienstverlening. Een gerichte inzet van databases en een verantwoorde omgang met de risico's die aan het gebruik ervan kleven, vragen om een doordachte keuze van het ontwerp van databases.

De digitalisering van de samenleving is een voortgaand proces, dat de komende decennia verder zijn beslag zal krijgen. De afhankelijkheid van de samenleving van het functioneren van digitale informatiesystemen zal dan ook alleen maar verder toenemen. Met de aanbevelingen die we in deze studie formuleren, hoopt het Rathenau Instituut een bijdrage te leveren aan het debat over de toekomst van de informatiemaatschappij.

Jan Staman, directeur Rathenau Instituut

Inhoudsopgave

Samenvatting

Deze studie laat zien dat het toenemend gebruik van databases in onze gedigitaliseerde samenleving niet zonder risico's is en dat we lessen moeten trekken uit de ervaringen die daarmee tot nu toe zijn opgedaan.

Databases worden in onze samenleving ingezet voor een groeiend aantal doeleinden. Ze lijken ongekende mogelijkheden te bieden om gegevens op te slaan, uit te wisselen, te bewerken en te analyseren. Zo gebruiken bedrijven klantengegevens voor een betere afstemming van hun productaanbod op de behoeften van de klant, worden onze reisbewegingen in het openbaar vervoer bijgehouden voor een efficiëntere inzet van treinstellen en conducteurs en wisselen zorgverleners elektronische dossiers uit voor een betere medische zorg.

Maar dit gebruik van databases is niet zonder risico's. Hierbij spelen vragen als: voor welke doeleinden worden ze gebruikt, hoe staat het met de beveiliging van gegevens, hoe betrouwbaar zijn die gegevens, welke mogelijkheden hebben burgers om fouten in registraties te herstellen en dragen databases daadwerkelijk bij aan de doelstelling waarvoor ze in het leven zijn geroepen?

Deze studie gaat aan de hand van zes casestudies op deze vragen in. Daarvoor is gekozen voor de volgende actuele onderwerpen:
- de OV-chipkaart en de kilometerheffing
- het elektronisch patiëntendossier
- het elektronisch kinddossier
- klantenprofielen op internet
- het Schengen Informatie Systeem
- de gemeentelijke basisadministratie.

In de casestudies staat de architectuur – of: het ontwerp – van databases centraal. Daarbij gaat het niet alleen om het technisch ontwerp van databases – zoals het al dan niet versleutelen van gegevens, of een centrale of decentrale opslag van gegevens – maar ook om de bredere context waarbinnen databases functioneren. Het gaat bijvoorbeeld ook om de controle die burgers kunnen uitoefenen op de gegevens die over hen worden verzameld; of om de mate waarin het gebruik van databases afhankelijkheden van burgers versterkt of juist hun (digitale) autonomie. De casestudies laten zien dat afhankelijk van de architectuur van een database daarmee andere doeleinden kunnen worden bewerkstelligd, maar aan het gebruik ook andere risico's kleven.

De casestudies maken bovendien duidelijk dat bij het ontwerp van databases vaak onvoldoende bij de risico's wordt stilgestaan. De beveiliging van persoonsgegevens bijvoorbeeld blijft vaak een heet hangijzer. Zo is voor de OV-chipkaart gebruikgemaakt van de Mifare Classic-chip, die vrij eenvoudig te kraken bleek.

Dat had kunnen worden voorkomen als voor een ander type kaart was gekozen. Maar ook de beveiligingsmaatregelen rond het landelijk elektronisch patiëntendossier, die er op papier goed uit mogen zien, lijken kwetsbaar. Die beveiliging had beter gekund, door meer gebruik te maken van technische beveiligingsmaatregelen, die bepaalde vormen van inzage in gegevens eenvoudigweg onmogelijk maken.

Daarnaast vormen fouten in registraties en daarop gebaseerde risicoprofielen een probleem. Zo kan het elektronisch kinddossier ertoe leiden dat kinderen door een samenloop van omstandigheden ten onrechte als 'risicokind' worden aangemerkt, terwijl er eigenlijk niets aan de hand is. Ook kunnen klanten over wie bedrijven op internet gegevens verzamelen door een toevallige *match* van gegevens worden uitgesloten van een bepaalde dienstverlening, zoals een verzekering, of daarvoor een hogere premie moeten betalen. Een aandachtspunt daarbij vormt de veelal zwakke rechtspositie van degene over wie gegevens worden verzameld. Het wettelijke inzage- en correctierecht blijft vaak een papieren recht, dat zich moeilijk laat effectueren. Fouten in de gegevensverzameling en -verwerking laten zich dan moeilijk herstellen. En daarvan is vooral de burger, cliënt of consument de dupe.

Het ontwerp van een database is bovendien vaak toegesneden op de behoeften en belangen van de opdrachtgever of exploitant (de overheid, de vervoersmaatschappijen, het bedrijf dat klantengegevens op internet verzamelt), met voorbijgaan aan die van de burger of consument. Als gevolg daarvan worden afhankelijkheidsrelaties eerder versterkt dan afgezwakt. Zoals onder meer de casestudie over de gemeentelijke basisadministratie laat zien, biedt ICT ook de mogelijkheid om juist de positie van de burger te versterken, bijvoorbeeld door hem meer regie te geven over zijn gegevens. Maar daar wordt vaak niet voor gekozen.

Ten slotte kunnen vraagtekens worden geplaatst bij de doelmatigheid van het gebruik van databases. Uit de casestudie over het Schengen Informatie Systeem volgt dat databases niet altijd doen wat ze zouden moeten doen. Te hoge ambities kunnen in hun tegendeel omslaan. Zo dreigt het Schengen Informatie Systeem door een veelheid aan doelstellingen technisch en organisatorisch vast te lopen.

Alles bij elkaar genomen schetsen de casestudies een vrij onthutsend beeld van wat er in de praktijk mis kan gaan bij het gebruik van databases. En deze risico's hangen samen met de keuzes die worden gemaakt over de architectuur van de betreffende database. Op grond hiervan kunnen de volgende lessen worden getrokken voor een doordacht ontwerp van databases:

Maak gebruik van technische maatregelen om gegevens te beschermen.

Versterk de positie van de burger. Faciliteer het inzage- en correctierecht van burgers en geef hen zo veel mogelijk de regie over de eigen gegevens.

Houd het simpel. Kies een welomschreven doel en beperk de gegevensverzameling tot de voor dat doel noodzakelijke gegevens.

Deze drie aanbevelingen hangen nauw met elkaar samen. Zo maakt een sterkere, technische beveiliging van gegevens andersoortig gebruik van die gegevens, bijvoorbeeld voor opsporingsdoeleinden, moeilijker of onmogelijk. Middel en doel moeten dan ook in onderlinge samenhang worden bezien. Dat maakt besluitvorming over de inzet van databases tot een complexe aangelegenheid.

Met de voortschrijdende digitalisering van de samenleving groeit het belang van een doordachte architectuur van databases. Daarvoor is zicht nodig op de risico's die aan het gebruik van databases kleven en op mogelijke alternatieve ontwerpkeuzes. Dat vereist kennis van de mogelijkheden en beperkingen van ICT. Om de besluitvorming over het ontwerp van databases te toetsen, zou een onafhankelijke ICT-autoriteit in het leven moeten worden geroepen. Deze zou tevens moeten toezien op een adequaat functioneren van databases. Dit leidt tot een vierde aanbeveling:

Roep een ICT-autoriteit in het leven die het ontwerp van databases toetst en toeziet op het functioneren ervan.

In de voorliggende studie treft u de zes casestudies aan. Deze worden voorafgegaan door een overkoepelend essay dat een overzicht geeft van de opbrengst van de casestudies en daaruit lessen trekt.

1 Databases in beeld

1 Databases in beeld

Geert Munnichs, Michiel Besters & Mirjam Schuijff

1.1 Inleiding: digitale architectuur

We leven meer en meer in een informatiemaatschappij. De samenleving digitaliseert in een hoog tempo. Niet eerder maakten we zoveel gebruik van de mogelijkheden die ICT ons biedt, en niet eerder lieten we in ons dagelijks leven zoveel digitale sporen achter: als we met een pinpas betalen, met de OV-chipkaart reizen, mobiel bellen, op internet surfen of een bezoek brengen aan de huisarts. Zoals Van 't Hof, Van Est en Daemen (2010) laten zien, raakt de ons vertrouwde, fysieke wereld meer en meer verweven met de virtuele wereld van bits en bytes. In deze studie gaan we in op de rol die databases hierbij spelen. Onder databases verstaan we digitale gegevensbestanden en informatiesystemen die het mogelijk maken om grote hoeveelheden data op te slaan, met andere bestanden uit te wisselen, te bewerken en te analyseren. Ze vormen de digitale ruggengraat van de informatiemaatschappij.

De digitalisering van de samenleving biedt ongekende mogelijkheden om communicatie te versnellen, de efficiëntie van bedrijfsprocessen te verhogen, overheidsorganisaties beter te laten samenwerken en het gemak van burger en consument te dienen. Daar wordt ook meer en meer gebruik van gemaakt. Zo gebruiken supermarktketens klantenkaarten om hun productaanbod beter af te stemmen op de behoeften van de klant; wordt het elektronisch kinddossier ingevoerd om de communicatie tussen jeugdhulpverleners te verbeteren; en kent de overheid een stelsel van basisregistraties zodat burgers niet bij ieder loket hun gegevens hoeven in te vullen. Het gebruik van databases is de laatste jaren dan ook explosief gegroeid. Een onderzoek in opdracht van het College bescherming persoonsgegevens laat zien dat de gemiddelde Nederlander in ten minste 250 tot 500 publieke of private databestanden staat geregistreerd (Schermer & Wagemans 2009).

Het staat buiten kijf dat het gebruik van databases grote voordelen met zich meebrengt voor overheid, bedrijven en burgers. De mate waarin allerlei digitale diensten deel zijn gaan uitmaken van ons dagelijks leven, maakt dat een weg terug ook eigenlijk niet meer tot de mogelijkheden behoort. Wel kunnen kanttekeningen worden geplaatst bij het gebruik van digitale gegevensbestanden en informatiesystemen. De centrale stelling van de studie luidt dat databases geen risicovrije systemen zijn, met onbeperkte mogelijkheden. Het zijn geen neutrale instrumenten die te pas en te onpas kunnen worden aangewend om de efficiëntie van processen of het gemak van de burger te verhogen. Ze kennen een eigen logica en een eigen dynamiek, die eisen stellen aan een doordacht gebruik ervan.

Deze studie gaat in op de voorwaarden voor een verantwoord gebruik van databases en formuleert daarover aanbevelingen. De digitalisering van de samenleving is een voortgaand proces, dat de komende decennia verder zijn beslag zal krijgen. Er zijn inmiddels voldoende ervaringen opgedaan met het gebruik van databases om daaruit lessen te trekken voor onze omgang met digitale informatiesystemen. Aan de hand van zes actuele voorbeelden gaan we in op deze ervaringen. De behandelde cases zijn:

- de OV-chipkaart en de kilometerheffing
- het elektronisch patiëntendossier
- het elektronisch kinddossier
- klantenprofielen op internet
- het Schengen Informatie Systeem
- de gemeentelijke basisadministratie.

In de casestudies staat de architectuur – of: het ontwerp – van databases centraal. In zijn bijdrage aan deze studie over het elektronisch patiëntendossier (EPD) omschrijft Jacobs deze architectuur als "(…) de structurele organisatie van hardware, applicaties, processen en gegevensstromen, tezamen met de daarmee samenhangende organisatorische consequenties, binnen bedrijven, overheden, of binnen de samenleving in brede zin". Deze omschrijving maakt duidelijk dat het niet alleen gaat om het technisch ontwerp van databases – het al dan niet automatisch verwijderen van gegevens na een bepaalde termijn, versleuteling van gegevens, centrale of decentrale opslag van data – maar tevens om het functioneren van de informatiesystemen binnen een bredere context. Het gaat bijvoorbeeld ook om hoe artsen omgaan met de voor het EPD vereiste controle van het burgerservicenummer van patiënten, of om de wijze waarop het inzage- en correctierecht van patiënten vorm krijgt.

Met deze studie willen we laten zien dat afhankelijk van de architectuur van een database daarmee andere doeleinden kunnen worden bewerkstelligd, maar aan het gebruik ook andere risico's kleven. De studie is niet in de eerste plaats bedoeld om de doelstellingen van bijvoorbeeld de kilometerheffing of het Schengen Informatie Systeem tegen het licht te houden. We stellen ons niet de vraag of deze ICT-informatiesystemen de beste manier zijn om de filedruk te verminderen of grensoverschrijdende criminaliteit te bestrijden. Het gaat ons vooral om een beter begrip van de dynamiek tussen ontwerp, kansen en risico's van databases. De inzichten die hieruit voortvloeien, kunnen uiteraard wel aanleiding zijn om die doelstellingen te heroverwegen. Zo roept de casestudie over het elektronisch kinddossier de vraag op of het wel zo verstandig is van ieder kind een risicoprofiel te willen maken.

In dit essay brengen we de opbrengst van de casestudies in kaart en formuleren we aanbevelingen voor politiek en beleid. De casestudies worden besproken aan de hand van thema's. Per thema lichten we enkele casestudies eruit.

Achtereenvolgens behandelen we de doeleinden waarvoor databases worden ingezet (§2), de beveiliging van gegevens (§3), de betrouwbaarheid van gegevens (§4), de rechtspositie van de burger (§5), de mate waarin databases de autonomie van de burger versterken dan wel verzwakken (§6) en de doelmatigheid van het gebruik van databases (§7). We sluiten af met conclusies en aanbevelingen (§8).

1.2 Efficiëntieverhoging, profilering en verder gebruik

Zoals hierboven reeds kort is aangestipt, worden databases gebruikt voor verbetering van de communicatie, verhoging van de efficiëntie of meer gemak voor de burger. Dit zien we terug in de beschreven cases. De digitalisering van gegevensbestanden en informatiesystemen moet leiden tot verbetering, versnelling of opschaling van organisatorische of bedrijfsmatige processen. Zo moet de modernisering van de gemeentelijke basisadministratie (GBA) overheidsorganisaties efficiënter maken, beter laten samenwerken en de dienstverlening aan de burger verbeteren. En de invoering van de OV-chipkaart moet leiden tot meer inzicht in de reisbewegingen, zodat de beschikbare vervoerscapaciteit gerichter en efficiënter kan worden ingezet.

Gedigitaliseerde gegevensbestanden bieden daarnaast de mogelijkheid gegevens op allerlei manieren te bewerken. Door diverse gegevensbestanden aan elkaar te koppelen en deze gegevensverzameling vervolgens met behulp van computerprogramma's te doorzoeken aan de hand van bepaalde sleuteltermen of statistische verbanden, kunnen nieuwe inzichten ontstaan in bijvoorbeeld het gedrag van individuen of groepen personen. Dit geautomatiseerd doorzoeken van grote gegevensbestanden wordt datamining genoemd (Hildebrandt & Gutwirth 2008). Zo maken bedrijven gebruik van online- en offlineklantengegevens om patronen te ontdekken in consumentengedrag – klantenprofielen – op grond waarvan 'potentiële' behoeftes van klanten kunnen worden voorspeld. Dat stelt hen bijvoorbeeld in staat om meer op de persoon gerichte aanbiedingen te doen.

Datamining en profilering scheppen ook nieuwe toepassingsmogelijkheden. De gegevens die in het elektronisch kinddossier worden verzameld, stellen de jeugdgezondheidszorg in staat om aan de hand van risicoprofielen kinderen in te delen in risicocategorieën. Hun score op risicofactoren moet duidelijk maken in welke mate kinderen kans lopen psychosociale problemen te ontwikkelen. Dit moet de jeugdgezondheidszorg in staat stellen om (potentiële) probleemkinderen in een vroeg stadium in beeld te krijgen, zodat preventief kan worden ingegrepen.

Eenmaal aangelegde databases lenen zich ook gemakkelijk voor andersoortig gebruik. Doordat digitale data zich veel gemakkelijker en op grotere schaal laten verzamelen, uitwisselen en bewerken dan papieren gegevens, kost het relatief weinig moeite om een database die voor een bepaald doel is aangelegd in een later stadium ook voor een ander doel te gebruiken. Zo was het elektronisch patiëntendossier (EPD) oorspronkelijk vooral bedoeld voor uitwisseling van medische gegevens tussen zorgverleners. Maar tijdens de ontwikkeling van het EPD heeft de Tweede Kamer bedongen dat het medisch dossier ook zelfstandig door patiënten, via internet, moet kunnen worden ingezien.

Een tweede voorbeeld van andersoortig gebruik zien we bij de OV-chipkaart. Deze kaart is ingevoerd om de bewegingen van reizigers nauwkeurig in kaart te brengen, zodat een meer gerichte inzet van personeel en materieel mogelijk wordt. Bij de OV-chipkaart is ervoor gekozen alle reisbewegingen op te slaan in een centrale database. De database bevat ook de persoonsgegevens van reizigers die met een niet-anonieme kaart reizen. Deze centrale database kan door politie en justitie worden ingezien voor opsporingsdoeleinden. Hoewel mogelijk handig vanuit opsporingsperspectief, is dat gebruik nooit de bedoeling geweest van de OV-chipkaart. In zijn casestudie over de OV-chipkaart verbindt Teepe hieraan de vraag of een dergelijk gebruik, waarmee politie en justitie de handel en wandel van gewone burgers kunnen volgen, wenselijk is (zie ook Vedder et al., 2007).

Deze voorbeelden laten zien dat gedigitaliseerde gegevensbestanden nieuwe toepassingsmogelijkheden kunnen creëren, waar vaak veel voor te zeggen valt, maar waaraan ook haken en ogen kunnen zitten. In paragraaf 7 komen we uitgebreider terug op de doelstellingen waarmee databases in het leven worden geroepen en de vraag of databases doen wat ze moeten doen.

1.3 Procedurele en technische beveiligingsmaatregelen

In het politieke en maatschappelijke debat over databases krijgt het thema beveiliging veel aandacht. Zoals uit de casestudies volgt, is dat niet meer dan terecht. De beveiliging van persoonsgegevens is en blijft een heet hangijzer. Dat is eens te meer het geval als het gaat om extra gevoelige, medische gegevens, zoals bij het elektronisch patiëntendossier of het elektronisch kinddossier, of als de data een vergaande inkijk kunnen geven in iemands persoonlijk leven, zoals het geval is bij de OV-chipkaart of de klantengegevens die bedrijven verzamelen op internet.

Ondanks de aandacht die voor het thema bestaat, blijkt uit diverse cases dat de beveiliging van persoonsgegevens vaak niet goed op orde is. Teepe laat in zijn casestudie over de OV-chipkaart zien dat de invoering ervan gepaard is gegaan met diverse incidenten rond de beveiliging van de kaart. Zo bleek de Mifare Classic-chip, die gebruikt wordt voor de anonieme en de persoonsgebonden kaart, vrij eenvoudig te kraken is. Dat had voorkomen kunnen worden als Trans Link Systems voor een ander type kaart had gekozen.

Het landelijk elektronisch patiëntendossier lijkt op het eerste gezicht wat beveiliging betreft een positieve uitzondering te vormen. Bij de ontwikkeling van het

EPD is relatief veel aandacht besteed aan beveiligingsmaatregelen. Zo moeten zorgverleners aan strenge veiligheidseisen ('goed beheerd zorgsysteem') voldoen voordat ze mogen aansluiten op het landelijk EPD. In vergelijking met veel, reeds langer bestaande, regionale elektronische patiëntendossiers lijkt het landelijk EPD dan ook een stap vooruit.

Maar ook bij de beveiliging van het landelijk EPD zijn de nodige kanttekeningen te plaatsen. Volgens Jacobs berusten de getroffen beveiligingsmaatregelen in te hoge mate op procedurele maatregelen, die een strikte naleving door betrokkenen behoeven om het gewenste beveiligingsniveau te halen. Zo vraagt de UZI-pas waarmee zorgverleners toegang krijgen tot het EPD om een grote zorgvuldigheid van de kant van zorgverleners (geen passen delen, na gebruik direct uitloggen), terwijl de zorgsector juist bekend staat om zijn gebrekkige risicobewustzijn. In combinatie met het grote aantal UZI-passen, dat in de honderdduizenden loopt, maakt dat het systeem kwetsbaar.

Dat roept de vraag op of een andere architectuur van het EPD, die sterker op technische beveiligingsmaatregelen berust, niet de voorkeur verdient. Jacobs wijst hiervoor op de mogelijkheid van een decentrale opslag van medische gegevens, waarbij de patiënt zelf de toegang tot zijn of haar dossier beheert. Dan ligt in de architectuur van het systeem verankerd dat zorgverleners alleen toegang kunnen krijgen tot medische gegevens als patiënten daar *vooraf* toestemming voor hebben gegeven. Volgens Jacobs is het onduidelijk waarom het Ministerie van Volksgezondheid, Welzijn en Sport niet voor de decentrale variant heeft gekozen. Wellicht wreekt zich hier het feit dat bij het ontwerp van het landelijk EPD de positie van de patiënt niet van meet af aan centraal stond, maar pas in een later stadium aandacht heeft gekregen.

Ook Teepe gaat in op de mogelijkheden die technische maatregelen bieden voor een stringentere beveiliging van persoonsgegevens. Hij doet dat aan de hand van de 'dikke variant' van de kilometerheffing. In deze variant wordt de afgelegde route van een auto zo opgeslagen dat alleen de automobilist zelf daar inzage in heeft. De exploitant krijgt alleen inzage in versleutelde gegevens op grond waarvan hij een factuur kan opmaken, maar hij kan de ritgeschiedenis van individuele auto's niet nagaan. Teepe presenteert deze variant – waarvan momenteel overigens onduidelijk is of die ooit zal worden ingevoerd – als een voorbeeld van hoe het ook kan, in contrast met het gedetailleerde inzicht dat de OV-chipkaart biedt in de reizigersbewegingen in het openbaar vervoer.

Voor de dikke variant van de kilometerheffing wordt gebruikgemaakt van *zero-knowledge*-cryptografie. Deze technologie was in het verleden niet toepasbaar op RFID-chips als de OV-chipkaart. Maar volgens Teepe is daar recentelijk verandering in gekomen. Dat roept de vraag op of de openbaarvervoersbedrijven niet zouden moeten overstappen op een zero-knowledge-versie van de OV-chipkaart, of in ieder geval de reiziger de keuze zouden moeten geven daarvan gebruik te maken.

Ten slotte kan over de beveiliging van databases worden opgemerkt dat deze nooit 'af' is. De bescherming van een groot ICT-informatiesysteem als het elektronisch patiëntendossier tegen hackers en identiteitsdiefstal, maar ook tegen onzorgvuldig gebruik van toegangspassen of wachtwoorden vraagt volgens Jacobs om continue aandacht en monitoring. Tijdens een expertmeeting over het EPD in de Eerste Kamer voegde Jacobs daaraan toe dat voor het toezicht op omvangrijke ICT-systemen als het EPD een onafhankelijke ICT-autoriteit in het leven zou moeten worden geroepen. Instanties als het College bescherming persoonsgegevens of de Inspectie voor de Gezondheidszorg zouden daarvoor onvoldoende zijn toegerust (Eerste Kamer 2009-2010a; zie ook Eerste Kamer 2009-2010b).

1.4 Betrouwbaarheid van data

Naast een adequate beveiliging vormt de betrouwbaarheid van data een belangrijke voorwaarde voor een goed functioneren van databases. Als opgeslagen, uitgewisselde of bewerkte gegevens fouten bevatten, kan dat vervelende consequenties hebben voor betrokkenen. Deze fouten kunnen bijvoorbeeld een gevolg zijn van een incorrecte invoer van gegevens, identiteitsdiefstal of problemen met de interpretatie van gegevens.

Een van de doelen van het elektronisch patiëntendossier is het aantal medicatiefouten terugdringen. Een betere communicatie tussen zorgverleners moet leiden tot betrouwbaardere medische dossiers. Jacobs waarschuwt in zijn casestudie over het EPD echter voor te veel optimisme. Niet alle medicatiefouten zijn volgens hem een gevolg van een gebrekkige communicatie tussen zorgverleners en bovendien kan het EPD ertoe leiden dat sommige fouten – zoals per ongeluk het 'naastliggende' medicijn aanklikken – vaker zullen voorkomen.

Daaraan kan worden toegevoegd dat de uitwisseling van medische dossiers via het EPD een gestandaardiseerde 'eenheid van taal' vereist, die aanleiding kan geven tot interpretatieproblemen. In het patiëntendossier worden namelijk niet alleen 'objectieve' gegevens vermeld, zoals medicatie- of laboratoriumgegevens, maar ook 'subjectieve', zoals klachten van de patiënt of de diagnose van de arts. Deze subjectieve gegevens kunnen vaak alleen binnen hun context goed worden begrepen. Het is de vraag of de landelijke standaarden voor registratie van medische gegevens – die nog in ontwikkeling zijn – voldoende ruimte bieden om deze context te vermelden (Munnichs 2009). Het risico bestaat dat door een gebrek aan context interpretatieproblemen ontstaan en deze tot verkeerde behandelingen leiden.

Ook bij het gebruik van profielen om grote bestanden met gegevens te doorzoeken, doen zich problemen voor met de betrouwbaarheid van gegevens. In haar casestudie over het elektronisch kinddossier (EKD) laat Van der Hof zien dat de grote hoeveelheden gegevens die over kinderen worden verzameld en de risicoprofielen die op grond daarvan worden opgesteld, het zicht kunnen vertroebelen op wat relevante gegevens zijn.

Het EKD verzamelt van alle kinderen in de leeftijd tot 19 jaar informatie over de fysieke, cognitieve en psychosociale ontwikkeling, alsook over gezinsfactoren als gescheiden ouders, werkloosheid of psychiatrische problemen van ouders. Afhankelijk van hun score op risicofactoren worden kinderen ingedeeld in risicoprofielen. In het voorbeeld waarnaar Van der Hof verwijst, worden kinderen ingedeeld in de categorieën 'geel' (laag risico), 'oranje' (medium risico) of 'rood' (hoog risico). De aandacht verschuift daarmee van het individuele kind naar het type kind. Volgens Van der Hof is het gevaar van deze typering dat er een virtuele identiteit van het kind wordt gecreëerd die niet overeen hoeft te komen met de werkelijkheid. Door een samenloop van omstandigheden kan een kind ten onrechte 'rood' scoren en als (potentieel) probleemkind worden aangemerkt, of juist 'geel' scoren terwijl er wel degelijk wat aan de hand is. Met in beide gevallen ongewenste gevolgen voor het kind.

Voor het gebruik door het bedrijfsleven van klantenprofielen op internet geldt in wellicht nog sterkere mate dat profielen leidend zijn voor hoe, in dit geval, klanten worden behandeld. Hildebrandt en Van Dijk schetsen hoe op basis van eerder koopgedrag, door consumenten vrijwillig afgestane persoonsgegevens en onbewust 'gelekte' gegevens – bijvoorbeeld surf- en klikgedrag op internet – bedrijven grote hoeveelheden klantengegevens verzamelen. Uit deze zee aan gegevens worden vervolgens met behulp van geavanceerde computerprogramma's statistische patronen in consumentengedrag blootgelegd. Marketeers claimen met de aldus vergaarde 'kennis' toekomstig koopgedrag beter te kunnen voorspellen dan met informatie die klanten, bijvoorbeeld in focusgroepen, zelf verstrekken. Deze kennis over consumentengedrag moet bedrijven onder meer in staat stellen om klanten meer op de persoon gerichte aanbiedingen te doen (*targeted advertising*).

Net als bij het EKD wordt met klantenprofilering een virtuele identiteit gecreëerd, die niet overeen hoeft te komen met de 'echte' identiteit van de consument. Hildebrandt en Van Dijk wijzen erop dat bedrijven daarmee gemakkelijk de plank kunnen misslaan. Maar omdat het om grote aantallen klanten gaat, blijft het voor bedrijven een lucratieve manier om klanten te benaderen. Vanuit consumentenperspectief is deze profilering echter niet onproblematisch. De consument heeft immers geen zicht op de gegevens die over hem worden verzameld, het klantenprofiel waarin hij 'past' en welke consequenties zijn profiel heeft voor de manier waarop hij door het betreffende bedrijf wordt behandeld.

Nu hoeft dat nog niet zo'n probleem te zijn met onjuist 'gerichte' advertenties. Maar dat wordt anders als bedrijven op basis van een onjuist klantenprofiel klanten uitsluiten van dienstverlening – bijvoorbeeld van een verzekering – of daar een hogere premie voor vragen.

1.5 Rechtspositie van de burger

De vorige paragrafen maken duidelijk dat betrokkenen (burgers, patiënten, consumenten) er nadeel van kunnen ondervinden als er wat misgaat met de beveiliging of de betrouwbaarheid van gegevens. Dat is bijvoorbeeld het geval als er fouten sluipen in een medisch dossier, anderen ongevraagd inzicht krijgen in gevoelige informatie over psychiatrische aandoeningen of betrokkenen benadeeld worden door een onjuist risico- of klantenprofiel.

De vraag is dan ook relevant welke mogelijkheden personen hebben om inzage te krijgen in de gegevens die over hen worden verzameld en om fouten te laten corrigeren. Volgens de Wet bescherming persoonsgegevens (WBP) hebben individuen recht op inzage in en correctie van persoonsgegevens die op hen van betrekking zijn. De casestudies laten zien dat de effectuering van deze rechten meer dan eens te wensen overlaat. Bij het elektronisch patiëntendossier en (de dikke variant van) de kilometerheffing lijkt dat goed geregeld. Maar bij het elektronisch kinddossier is het de vraag of kinderen (of hun ouders) voldoende mogelijkheden hebben om fouten in hun gegevens of profiel gecorrigeerd te krijgen.

Bij het Schengen Informatie Systeem (SIS) lijkt de rechtspositie van betrokkenen zelfs ronduit zwak. Het SIS is ingevoerd om de buitengrenzen van het Schengengebied te bewaken. Dat gebeurt door registratie van 'ongewenste vreemdelingen' (die het Schengengebied niet binnen mogen komen) en personen die door politie en justitie worden gezocht (die het gebied niet mogen verlaten). Besters laat zien dat de rechten van geregistreerde personen er bekaaid afkomen. Ten eerste is er sprake van rechtsongelijkheid tussen de Schengenlanden, omdat ieder land zelf (nadere) invulling kan geven aan de criteria voor registratie. Daardoor ontstaan grote verschillen tussen de deelnemende landen. Zo valt het niet nakomen van alimentatieverplichtingen in Spanje onder het strafrecht, en kan dat een reden zijn voor registratie in het SIS. Dit in tegenstelling tot veel andere landen, waarin het niet nakomen van deze verplichting een civielrechtelijke aangelegenheid is. Ten tweede berust een gedeelte van de registraties in het SIS op een onrechtmatige grondslag. Zo registreren de Duitse autoriteiten afgewezen asielzoekers als ongewenste vreemdeling, wat strijdig is met de criteria in het Schengenverdrag. Daarnaast worden personen niet altijd op de hoogte gesteld van hun registratie, waardoor ze daartegen ook geen verweer kunnen aantekenen. En als ze daar wel van op de hoogte zijn, ontbreken bovendien vaak effectieve procedures om een registratie aan te vechten. De gebrekkige rechtspositie vormt eens te meer

een probleem omdat registratie in het SIS ingrijpende gevolgen kan hebben voor de betrokkene. In sommige gevallen kan iemand voor een periode van tientallen jaren de toegang tot het Schengengebied worden ontzegd.

Hildebrandt en Van Dijk laten zien dat ook de rechtspositie van consumenten over wie op internet gegevens worden verzameld, gebreken vertoont. Dat hangt samen met de veelal voor de consument onzichtbare wijze waarop bedrijven die gegevens verzamelen. Met behulp van op zijn of haar computer geïnstalleerde *cookies* kan het toetsenbord-, muis- en surfgedrag van de internetgebruiker worden vastgelegd. Daarmee kan allerlei gedetailleerde informatie over de gebruiker worden verzameld zonder dat deze dat in de gaten heeft. Het kan daarbij ook om gevoelige informatie gaan. Zo kan aan de hand van het toetsenbordgedrag het risico worden ingeschat dat iemand de ziekte van Parkinson krijgt – informatie die interessant kan zijn voor ziektekosten- of levensverzekeringsmaatschappijen. Doordat de consument geen weet heeft van deze gegevensverzameling of van de klantenprofilering die op grond daarvan plaatsvindt, kan hij niet controleren of die gegevens wel kloppen. Hij is ook niet in staat om voor hem nadelige beslissingen die op grond van die informatie worden genomen, aan te vechten.

Deze voor de consument nadelige situatie wordt nog eens extra gecompliceerd doordat onduidelijk is of het toetsenbord- en muisgedrag volgens de Wet bescherming persoonsgegevens als persoonsgegeven kan worden aangemerkt. Daarmee is het tevens onduidelijk of het wettelijke inzage- en correctierecht van toepassing is op het verzamelen door bedrijven van op internet 'gelekte' gegevens. Dat roept de vraag op of die wettelijke bepalingen nog voldoende bij de tijd zijn.

1.6 Digitale autonomie

De casestudies maken duidelijk dat er bij het gebruik van databases meer aan de hand is dan inzage door (onbekende) anderen in soms zeer persoonlijke gegevens. Het gaat er tevens om dat anderen op basis van die gegevens zich een bepaald beeld vormen van iemand en op grond daarvan beslissingen nemen die ingrijpen in diens leven. Zo kan een gezin te maken krijgen met Bureau Jeugdzorg omdat het als probleemgezin te boek staat, kan een klant een levensverzekering worden geweigerd omdat analyse van zijn toetsenbordgedrag uitwijst dat hij een verhoogde kans heeft op de ziekte van Parkinson, of kan een asielzoeker worden uitgewezen omdat hij als ongewenste vreemdeling staat geregistreerd.

Maar de positie van de burger is ook in bredere zin in het geding. Het gebruik van databases kan ook implicaties hebben voor de verhouding tussen patiënt en arts, consument en bedrijf of burger en overheid. Zo wijzen Hildebrandt en Van Dijk erop dat de vaak onzichtbare wijze waarop bedrijven op internet klantengegevens verzamelen tot een informatieachterstand van de consument

leidt. En bedrijven kunnen daarmee hun voordeel doen. Die informatieachterstand van de consument verstoort de verhoudingen van 'de vrije en gelijke markt', volgens welke de consument en de producent in een gelijke ruilverhouding tot elkaar staan. Om tegenwicht te bieden aan die inbreuk op de positie van de consument, pleiten Hildebrandt en Van Dijk voor meer transparantie van de kant van bedrijven. Ze zouden consumenten meer inzicht moeten geven in de wijze waarop ze gegevens over hen verzamelen en gebruikmaken van klantenprofielen.

De casestudie over de gemeentelijke basisadministratie (GBA) gaat uitgebreid in op de invloed van overheidsregistraties op de relatie tussen burger en overheid. Volgens Boschker, Castenmiller en Zuurmond wordt bij de modernisering van de GBA te eenzijdig de nadruk gelegd op een efficiënte inrichting van de overheid, waarbij het denken in termen van controle en beheersing vooropstaat. Dit gaat hand in hand met een schier onstilbare informatiehonger van de kant van de overheid (zie ook BB Digitaal Bestuur 2010). De auteurs schetsen hoe het vastleggen van persoonsgegevens in databases meer en meer een ingesleten en vanzelfsprekende administratieve routine wordt. Zoals ook al aangestipt in de inleiding, gaat deze tendens gepaard met een explosieve groei van het aantal databestanden van de overheid. Overheidsinstanties krijgen volgens Boschker, Castenmiller en Zuurmond daarmee een steeds completer beeld van de burger. Bovendien hebben digitale gegevensbestanden volgens hen een dwingender karakter dan hun papieren voorgangers. Computersystemen laten (nog) minder ruimte voor persoonlijke interactie en afwijkende gevallen. Het nog steeds toenemende gebruik van databases leidt volgens hen dan ook vooral tot nieuwe afhankelijkheden van de burger.

Dit laatste kan worden geïllustreerd met een voorbeeld dat de Nationale ombudsman aanhaalt in zijn rapport *De burgers in de ketens*. Het betreft een zakenman die jarenlang als drugscrimineel stond geregistreerd in informatiesystemen van de overheid. Als gevolg daarvan kreeg hij herhaaldelijk te maken met aanhoudingen en huiszoekingen, met funeste gevolgen voor zijn privé- en zakenleven. De foutieve registraties waren het gevolg van identiteitsdiefstal door een oude bekende van hem. Hoewel de zakenman elke keer kon aantonen dat hij niet degene was die de politie zocht, was hij niet in staat zijn naam te zuiveren en de onterechte registraties te laten verwijderen (Nationale ombudsman 2009).

Volgens Boschker, Castenmiller en Zuurmond hoeft digitalisering echter niet per se tot verdergaande afhankelijkheden te leiden. Overheidsregistraties worden van oudsher niet alleen gekenmerkt door een nadruk op controle en beheersing, maar vervullen ook een emancipatoire functie. Zo leggen registraties het stemrecht van burgers of hun aanspraken op sociale voorzieningen vast en bevorderen zo hun autonomie. Door de eenzijdige nadruk die efficiëntieverhoging in de modernisering van het GBA krijgt, dreigt deze emancipatoire

dimensie echter uit het oog te worden verloren. Maar uitgerekend ICT biedt volgens hen ook mogelijkheden om de positie van burgers te versterken en ze meer regie te geven over de eigen persoonsgegevens. Bijvoorbeeld door het inzage- en correctierecht beter te faciliteren. Nu is dat vaak – letterlijk – een papieren recht. Zo moeten burgers over het algemeen een *schriftelijk* verzoek indienen om foutieve gegevens in bestanden te laten corrigeren (zie ook Leenes 2010). Databases zouden ook zo kunnen worden ingericht dat burgers via internet hun gegevens kunnen inzien en desgewenst kunnen wijzigen. Zo biedt de site www.mijnoverheid.nl burgers inzicht in een aantal gegevens die de overheid over hen vastlegt. Maar deze website lijkt vooralsnog de uitzondering die de regel bevestigt.

Voor de meeste casestudies geldt dat de architectuur van databases vaak vooral is toegesneden op de behoeften van de opdrachtgever of exploitant, met weinig oog voor de belangen van degenen van wie persoonsgegevens worden verzameld. Dat geldt zowel voor de gemeentelijke basisadministratie als voor de gebrekkige rechtspositie van geregistreerde personen in het Schengen Informatie Systeem of consumenten van wie klantengegevens op internet worden verzameld. Ook de OV-chipkaart vormt daarvan een voorbeeld. Teepe laat zien dat de inrichting van de database met reizigersgegevens vooral is afgestemd op het belang van een optimale bedrijfsvoering. De al eerder genoemde problemen met de beveiliging van de OV-chipkaart, maar ook de lange bewaartermijn van gegevens van zeven jaar, de prijsdruk op niet-anoniem reizen en de slechte rechtspositie van reizigers bij geschillen met vervoersbedrijven lijken erop te wijzen dat bij het ontwerp van de OV-chipkaart het belang van de reiziger van ondergeschikte betekenis is geweest.

We kunnen hieruit concluderen dat voor de inrichting van databases de vraag relevant is in welke mate het gebruik ervan de afhankelijkheden versterkt van patiënten, reizigers of consumenten dan wel hun autonomie.

1.7 Doen databases wat ze moeten doen?

Ten slotte is de vraag van belang of databases datgene doen waarvoor ze bedoeld zijn. Draagt het elektronisch patiëntendossier daadwerkelijk bij aan een goed beveiligde uitwisseling van medische gegevens, waardoor onnodige medische fouten worden voorkomen? Leidt het elektronisch kinddossier tot minder kindermishandeling? En draagt het Schengen Informatie Systeem bij aan een adequate bewaking van de buitengrenzen van het Schengengebied?

Niet alle casestudies gaan in op de vraag naar de doelmatigheid van databases. Waar dat wel gebeurt, worden vooral twijfels geuit. Zoals reeds vermeld, waarschuwt Jacobs voor te hoge verwachtingen over het elektronisch patiëntendossier en moet er rekening mee worden gehouden dat het EPD tot nieuwe medische fouten kan leiden. Daarnaast lijkt de medische sector de beveiliging van gegevens niet goed op orde te hebben. Jacobs komt op grond daarvan tot de tamelijk verontrustende conclusie dat op dit moment niet goed valt in te schatten of de voordelen van het landelijk EPD opwegen tegen de nadelen.

Ook Van der Hof plaatst vraagtekens bij de invulling die het elektronisch kinddossier krijgt. Ze vraagt zich af of de vele gegevens die in het EKD worden verzameld wel tot betere zorg leiden. Het streven om steeds meer data te verzamelen, dossiers van verschillende instanties aan elkaar te koppelen en met behulp van risicoprofielen (potentiële) probleemkinderen op te sporen, dreigt volgens haar zijn doel voorbij te schieten. Het kan namelijk leiden tot onwerkbaar grote aantallen risicokinderen, die het zicht ontnemen op welke kinderen en gezinnen daadwerkelijk hulp nodig hebben. Bovendien kunnen ze ertoe leiden dat zorgverleners hun aandacht moeten verdelen over zoveel *mogelijke* probleemkinderen dat ze weinig tijd overhouden voor de werkelijke probleemgevallen. Volgens schattingen heeft alleen al de regio Rotterdam te kampen met circa 30.000 mogelijke probleemkinderen (NRC Handelsblad 2007; zie ook www.iederkindwint.nl). Dat lijkt inderdaad een voor de jeugdzorg onwerkbaar groot aantal. Van der Hof vraagt zich dan ook af of het niet de voorkeur verdient om gerichter gegevens te verzamelen over probleemgevallen die reeds bij de jeugdzorg bekend zijn.

De casestudie over het Schengen Informatie Systeem schetst een mogelijk nog dramatischer beeld. Dit informatiesysteem dreigt in zichzelf vast te lopen doordat het een veelheid aan doelstellingen moet realiseren. Besters laat zien hoe de ontwikkeling van de diverse varianten van het SIS vrij continu geplaagd wordt door technische en organisatorische problemen, steeds opnieuw verlengde deadlines en oplopende kostenplaatjes. De problemen hangen samen met de steeds nieuwe eisen die aan het systeem worden gesteld. Gaandeweg is niet alleen het aantal deelnemende landen fors uitgebreid – van oorspronkelijk 7 lidstaten naar de huidige 27 – maar is ook het aantal functies toegenomen dat het systeem moet kunnen dienen. Zo moet de tweede generatie SIS (SIS II) onder meer een bredere toegang voor autoriteiten mogelijk maken en moet het vingerafdrukken kunnen bevatten voor biometrische identificatie. Daar komt bij dat ook de uitvoeringspraktijk ingewikkeld is. Behalve dat de uitvoeringscriteria niet zijn geharmoniseerd, waardoor elk van de 27 landen andere registratiemaatstaven hanteert, kent elk land andere uitvoerende organisaties. Daarnaast spelen problemen met een gebrekkig democratisch toezicht op het functioneren van het systeem en – zoals we reeds zagen – een tekortschietende rechtsbescherming van in het SIS geregistreerde personen. Besters vraagt zich dan ook af of een database met de grootte en complexiteit van het Schengen Informatie Systeem wel naar behoren *kan* functioneren.

1.8 Conclusies en aanbevelingen

De casestudies schetsen al met al een onthutsend beeld van wat er in de praktijk mis kan gaan bij het gebruik van databases. Zie het gemak waarmee de OV-chipkaart kon worden gekraakt, de nadelen die consumenten kunnen

ondervinden van een onjuist klantenprofiel of de zwakke rechtsbescherming van personen die in het Schengen Informatie Systeem staan geregistreerd. De belangrijkste conclusie die uit de casestudies kan worden getrokken, luidt dan ook dat databases inderdaad geen risicovrije systemen zijn. In deze afsluitende paragraaf formuleren we aandachtspunten voor een adequate omgang met deze risico's en aanbevelingen voor een verantwoord ontwerp van databases.

De risico's die zijn verbonden aan het gebruik van databases hangen samen met de context waarbinnen ze functioneren. Zie het voorbeeld van het elektronisch patiëntendossier. Op papier mogen de getroffen beveiligingsmaatregelen er goed doordacht uitzien, met UZI-passen, inlogcodes en de vereisten van een goed beheerd zorgsysteem. Maar het functioneren van het landelijk EPD staat of valt uiteindelijk met de zorgvuldigheid waarmee artsen en andere zorgverleners in de praktijk de beveiligingsvoorschriften naleven. De kans dat er met de beveiliging van gegevens iets fout gaat, kan worden verkleind door sterker in te zetten op het gebruik van technische beveiligingsmaatregelen. Deze maatregelen maken bepaalde vormen van inzage in of verwerking van gegevens eenvoudigweg onmogelijk. Het gebruik van zero-knowledge-cryptografie in de 'dikke variant' van de kilometerheffing is daarvan een goed voorbeeld. Een eerste aandachtspunt voor het ontwerp van databases zijn dan ook de technische mogelijkheden om gegevens te beschermen. Zo zou ook bij de OV-chipkaart kunnen worden overgestapt op een zero-knowledge-variant, die reizigers de mogelijkheid van kortingsrechten biedt zonder dat ze daarvoor hun anonimiteit hoeven prijs te geven.

Een tweede aandachtspunt betreft de positie van de patiënt, burger of consument over wie gegevens worden verzameld. De casestudies laten zien dat bij het ontwerp van databases de belangen van de burger of consument vaak een ondergeschikte rol spelen. Dat blijkt niet alleen uit de vaak tekortschietende aandacht voor de beveiliging van gegevens, maar ook uit de veelal zwakke rechtspositie van de burger. Zo blijft diens recht op inzage in de gegevens die over hem worden verzameld en op correctie van fouten, veelal een papieren recht, dat zich moeilijk laat effectueren. En als er wat misgaat, is vooral de burger, cliënt of consument daarvan de dupe. De burger dreigt daarmee het kind van de rekening te worden. En dat probleem wordt groter naarmate burgers in hun dagelijks leven afhankelijker worden van het functioneren van databases.

Hierbij is tevens de meer fundamentele vraag van belang of het gebruik van databases de afhankelijkheid van de burger, patiënt of consument versterkt, of juist diens (digitale) autonomie. Alleen al het stellen van deze vraag vergt een kanteling van perspectief. Vaak wordt het ontwerp van een database als bijna vanzelfsprekend toegesneden op de behoeften en belangen van de opdrachtgever of exploitant – de overheid, de vervoersmaatschappijen of het bedrijf

dat klantengegevens op internet verzamelt – met voorbijgaan aan die van de burger of consument. Maar databases kunnen ook zo worden ingericht dat ze de belangen en de autonomie van de burger dienen. Bij het ontwerp van databases dient dan ook de vraag aan de orde te komen in welke mate de burger de regie kan voeren over zijn eigen gegevens, waardoor hij grip houdt op wie wat met zijn gegevens doet. De Duitse *Gesundheitskarte* en het voorbeeld van de kilometerheffing laten zien dat regie over de eigen gegevens een reëel alternatief vormt. Digitale autonomie van de burger zou ook kunnen betekenen, om terug te komen op de OV-chipkaart, dat *de reiziger* de keuze krijgt om al dan niet gebruik te maken van een zero-knowledge-variant.

Een derde aandachtspunt heeft betrekking op de doelmatigheid van databases. Vaak leven er bij beleidsmakers en politici en in de top van het bedrijfsleven hoge verwachtingen van de mogelijkheden die databases bieden om de efficientie van processen te verhogen, de communicatie te verbeteren of problemen aan te pakken. Zo waarschuwt de Algemene Rekenkamer in haar rapport *Lessen uit ICT-projecten bij de overheid* voor te hoge beleidsambities op het gebied van ICT (Algemene Rekenkamer 2007; zie ook Automatisering Gids 2010). De moeizame, zo niet stokkende ontwikkeling van het Schengen Informatie Systeem vormt daarvan een duidelijk voorbeeld. Doordat het systeem aan te veel uiteenlopende beleidsdoelstellingen moet voldoen, dreigt het systeem technisch en organisatorisch vast te lopen. Daaruit kan worden geconcludeerd dat aan een database geen willekeurige doeleinden kunnen worden gesteld.

Die conclusie geldt ook voor het elektronisch kinddossier. Het streven om van ieder kind tot 19 jaar een risicoprofiel te maken, wordt gevoed door de wens om alle kinderen die problemen dreigen te ontwikkelen in het vizier te krijgen, zodat tijdig kan worden ingegrepen. Dit streven lijkt vooral te leiden tot onwerkbaar grote aantallen – *mogelijke* – risicokinderen. Met als keerzijde dat aandacht wordt besteed aan kinderen die bij nader inzien geen 'probleemkinderen' blijken te zijn, ten koste van kinderen die dat wel zijn – en van wie bovendien vaak reeds bekend is dat ze zorg nodig hebben. Het EKD dreigt daarmee zijn doel voorbij te schieten. Dit roept de vraag op of het niet de voorkeur verdient om veel gerichter gegevens te verzamelen over reeds bekende probleemgevallen.

De voorbeelden van het SIS en het EKD laten zien dat te hoge ambities in hun tegendeel kunnen omslaan. Dat kan worden voorkomen door het doel dat een database moet dienen preciezer te formuleren en alleen die gegevens te verzamelen die nodig zijn voor dat – welomschreven – doel. Een doelmatig gebruik van databases vereist dat men de verleiding weerstaat om maar zoveel mogelijk gegevens te verzamelen. In plaats daarvan verdient het uitgangspunt 'selecteer voor je verzamelt' navolging (Commissie-Brouwer 2009).

Op grond van het bovenstaande komen we tot de volgende aanbevelingen voor het ontwerp van databases:

Maak gebruik van technische maatregelen om gegevens te beschermen.

Versterk de positie van de burger. Faciliteer het inzage- en correctierecht van burgers en geef hen zo veel mogelijk de regie over de eigen gegevens.

Houd het simpel. Kies een welomschreven doel en beperk de gegevensverzameling tot de voor dat doel noodzakelijke gegevens.

Deze drie aanbevelingen hangen nauw met elkaar samen. Zo maakt een sterkere, technische beveiliging van gegevens andersoortig gebruik van die gegevens, bijvoorbeeld voor opsporingsdoeleinden, moeilijker of onmogelijk. En een meer gerichte inzet van ICT om probleemkinderen op te sporen betekent dat de doelstelling om van *ieder* kind een risicoprofiel op te stellen, zal moeten worden losgelaten.

Architectuurkeuzes kunnen dan ook dwingen tot heroverweging van de aanvankelijke doelstelling. Middel en doel moeten in onderlinge samenhang worden bezien. In die zin heeft iedere keuze een prijs. Dat maakt besluitvorming over de inzet van databases tot een complexe aangelegenheid.

Met de voortschrijdende digitalisering van de samenleving groeit het belang van een doordachte architectuur van databases. De casestudies laten zien dat bij het ontwerp van databases meer dan eens sprake is van een tekortschietende aandacht voor de risico's die gepaard gaan met het gebruik ervan. Om deze risico's naar behoren te kunnen inschatten en zicht te hebben op mogelijke alternatieve ontwerpkeuzes is kennis vereist van de mogelijkheden en beperkingen van ICT. Eerder in dit essay is al gewezen op de noodzaak van een continue monitoring van databases, omdat de beveiliging ervan nooit af is. Daarvoor zou een onafhankelijke ICT-autoriteit in het leven moeten worden geroepen. We willen ons aansluiten bij dat pleidooi. Maar zo'n ICT-autoriteit zou niet alleen het functioneren van databases moeten bewaken, maar tevens moeten toezien op een adequaat ontwerp ervan. Binnen het besluitvormingsproces over het ontwerp van databases dient een toetsingsmoment te worden gecreëerd waarop onafhankelijke deskundigen nagaan of voldoende rekening is gehouden met beveiligingsvereisten, de positie van de burger en de noodzaak van gegevensverzameling. We sluiten dit essay dan ook af met een vierde aanbeveling:

Roep een ICT-autoriteit in het leven die het ontwerp van databases toetst en toeziet op het functioneren ervan.

De OV-chipkaart en de kilometerheffing: een elektronisch enkelbandje voor reizigers?

2

2 De OV-chipkaart en de kilometerheffing: een elektronisch enkelbandje voor reizigers?

Wouter Teepe

2.1 Inleiding: efficiëntieverbetering van het personenvervoer

Met de invoering van de OV-chipkaart in het openbaar vervoer en de kilometerheffing voor de auto kunnen, afhankelijk van de gekozen technologie, centrale databases worden gecreëerd waarin van iedereen alle reisbewegingen jarenlang worden opgeslagen. Alsof reizigers onder toezicht staan en een elektronisch enkelbandje dragen. Databases met zoveel detail over het gaan en staan van Nederlandse burgers bestonden nog niet eerder.

Een belangrijk doel van de OV-chipkaart en de kilometerheffing is efficiëntieverbetering. Door een nauwkeurig inzicht in de (piek)belasting van het openbaar vervoer kan de planning van de inzet van materieel en personeel precisiewerk worden. De kostbare capaciteit wordt dan efficiënter ingezet en dat is goed voor het reizigersgemak en de kostprijs. Door automobilisten gericht te laten betalen voor het rijden tijdens de spits, worden zij aangespoord tot gedragsverandering. Bijvoorbeeld om meer buiten de spits te reizen. De filedruk wordt daardoor lager en het milieu wordt er beter van, zo gaat de redenering.

Voor het nadenken over efficiëntieverbeteringen kan het leerzaam zijn een kijkje te nemen bij de moderne grondstofverwerkende industrie, waar men probeert elk beetje verspilling te voorkomen. Dat is goed voor het bedrijfsresultaat en vaak ook goed voor het milieu. Voor het meten van efficiëntieverbeteringen wordt gebruikgemaakt van nauwkeurige metingen en sturingsinstrumenten. Nauwkeurige metingen verschaffen inzicht in de feitelijke efficiëntie van een industrieel proces, bijvoorbeeld door te laten zien of er ergens in het proces een overschot of een tekort aan materialen is. Metingen zorgen voor transparantie: waar zitten knelpunten? En wat zijn de kosten van de verschillende delen van het proces? Nauwkeurige sturingsinstrumenten kunnen de efficiëntie verhogen, bijvoorbeeld door een lopende band langzamer of sneller te laten lopen. Wanneer meetinstrumenten en sturingsinstrumenten nauwkeurig zijn en goed op elkaar zijn afgestemd, kan een efficiëntieoptimum worden bereikt.

Net zoals in een fabriek goederen op een lopende band kunnen worden gevolgd en bijgestuurd, kan dat gebeuren met mensen in het personenvervoer. Er valt in het personenvervoer nog veel te optimaliseren. Nauwkeurige metingen ontbreken en sturingsinstrumenten zijn grof. De wens om eens goed bij te houden hoe er van de vervoerscapaciteit in Nederland gebruik wordt gemaakt, is zo gek nog niet. Metingen in het personenvervoer maken het mogelijk de kosten nauwkeuriger – en dus rechtvaardiger – door te berekenen aan de gebruikers. Ook kunnen de subsidies voor het openbaar vervoer eerlijker worden verdeeld. De metingen leveren ook een nauwkeurig sturingsinstrument: bepaalde vervoersgedragingen kunnen worden aangemoedigd, en andere ontmoedigd, door een gedifferentieerde prijsstelling. Bij de kilometerheffing wordt dit doel openlijk benoemd: de kilometerheffing moet volgens de exploitant (de rijksoverheid) de filedruk verlagen en het gebruik van milieuonvriendelijke voertuigen terugdringen. Bij de OV-chipkaart is dit doel ook terug te vinden: de samenwerkende vervoersbedrijven, verenigd in Trans Link Systems (TLS), willen de reizigersgegevens gebruiken om reizigers gericht te verleiden buiten de spits te reizen.

2.2 Procedurele en technische privacywaarborgen

De invoering van de OV-chipkaart en die van de kilometerheffing worden beschouwd als een moderne, elektronische manier van betalen voor mobiliteit. Een dergelijk systeem kan bijzonder effectief en gebruiksvriendelijk zijn, maar kan ook gezien worden als een bedreiging voor de privacy. Hoe dit uitvalt, is afhankelijk van de systeemarchitectuur.

De OV-chipkaart en de kilometerheffing kunnen leiden tot grote, centrale databases waarin alle reisbewegingen worden opgeslagen. Daaruit kan een gedetailleerd beeld worden afgeleid van iemands leven: waar hij woont, waar en wanneer hij werkt, wanneer hij op vakantie is, wanneer hij uitgaat en waar en in wat voor soort wijken zijn vrienden en familie wonen. Dit beeld is vele malen gedetailleerder dan wat er bijvoorbeeld af te leiden valt uit de gegevens die de luchtvaartmaatschappijen over reizigers naar de VS moeten verzamelen. Daarbij wordt niet continu van iedereen opgeslagen waar hij of zij zich bevindt.

Voor de omgang met privacyvraagstukken die dit soort ICT-toepassingen oproepen, kunnen twee soorten maatregelen worden onderscheiden: procedurele maatregelen en technische maatregelen. Procedurele maatregelen richten zich op afspraken: wie mag er bij de database, en wie is er verantwoordelijk voor de beveiliging van de database. Procedurele maatregelen stellen weinig voor als er geen serieuze sancties staan op oneigenlijk gebruik van data of op het veronachtzamen van de beveiligingsvoorzorgen. In de praktijk ontbreekt het daar vaak aan. Technische maatregelen zijn constructies in computerprogramma's die ongewenste gedragingen fysiek onmogelijk maken. Bijvoorbeeld door gebruik te maken van cryptografie. Cryptografie is een verzamelnaam voor wiskundige technieken om gegevens zo te bewerken dat ze niet meer voor algemeen gebruik geschikt zijn, maar alleen voor vooraf bepaalde, specifieke toepassingen.

Technische maatregelen bieden in de praktijk hardere garanties voor privacybescherming dan procedurele maatregelen. Dat wordt hieronder verduidelijkt

aan de hand van de verschillende architecturen waarvan gebruik wordt gemaakt bij de OV-chipkaart en de kilometerheffing. De architectuur van de huidige OV-chipkaart kent weinig technische maatregelen ter bescherming van de privacy. De variant van de kilometerheffing die hier wordt behandeld, berust daarentegen in hoge mate op technische maatregelen.

2.3 De OV-chipkaart: privacy op de tocht

De OV-chipkaart is een vervoersbewijs in de vorm van een bankpas. Bij begin en eind van een reis moet er respectievelijk 'ingecheckt' en 'uitgecheckt' worden bij een kaartlezer. Door toepassing van zogeheten RFID-chips kan dit snel en draadloos gebeuren, door de pas binnen tien centimeter van een kaartlezer te brengen. Deze kaartlezers zijn kleine computers die gekoppeld zijn aan een centrale database. De kaart, de kaartlezers en de database zorgen er samen voor dat er gedetailleerde reisgegevens worden opgeslagen, en dat de gemaakte reizen worden betaald.

Betaling met de OV-chipkaart kan op basis van saldo op de kaart, eventueel in combinatie met kortingsrechten die op de kaart zijn vastgelegd (zoals het NS-voordeelurenabonnement), maar ook op basis van 'reisproducten' die op de kaart zijn geladen (zoals een dagkaart voor de metro in Amsterdam). In plaats van een kaartje te kopen moet een reiziger een combinatie van reisproducten, kortingsrechten en saldo op zijn kaart laden. Saldo kan desgewenst automatisch worden opgeladen, als een incassomachtiging wordt afgegeven. De strippenkaart als betaalmiddel wordt in de komende jaren regiogewijs afgeschaft. De OV-chipkaart zal uiteindelijk als enig vervoersbewijs overblijven.

Er zijn drie varianten van de OV-chipkaart: de persoonsgebonden kaart, de anonieme kaart en de wegwerpkaart. Met de persoonsgebonden kaart kunnen alle hierboven beschreven handelingen worden uitgevoerd: je kunt er alle mogelijke reisproducten en kortingsrechten op laden. Op de anonieme kaart kunnen geen kortingsrechten worden gezet, maar wel niet-persoonsgebonden reisproducten en saldo. De wegwerpkaart bevat bij aanschaf een reisproduct van beperkte waarde. Na gebruik van het reisproduct is de wegwerpkaart niet meer te gebruiken. De wegwerpkaart kan niet gebruikt worden voor duurdere reizen, zoals grote afstanden per trein.

Voor sporadische gebruikers van het openbaar vervoer is de wegwerpkaart de gemakkelijkste optie. Voor wie met enige regelmaat met het openbaar vervoer reist, is de persoonsgebonden kaart de goedkoopste en gemakkelijkste optie. De kortingsrechten die op de persoonsgebonden kaart kunnen worden gezet, verdienen zich meestal snel terug, maar kunnen niet op de anonieme kaart worden gezet. Een voorbeeld is het reizen voor kinderen onder de 12 jaar en senioren vanaf 65 jaar: zij mogen in het streekvervoer met korting reizen. Na afschaffing van de 'roze strippenkaart' kan dit alleen nog met een persoonsgebonden OV-chipkaart. Ook het populaire NS-voordeelurenabonnement kan

alleen op een persoonsgebonden kaart worden geladen. Er is dus een prijsdruk om niet-anoniem te reizen.

2.3.1 Welke gegevens worden opgeslagen?

Om een persoonsgebonden kaart te bemachtigen moet de reiziger onder andere naam, adres, geboortedatum en een pasfoto afgeven. De kaart wordt naar het opgegeven adres gestuurd, en de naam, geboortedatum en pasfoto worden op de kaart afgedrukt. Deze gegevens zijn centraal bij Trans Link Systems opgeslagen. De individuele vervoersbedrijven hebben geen toegang tot deze gegevens. Voor sommige reisproducten en kortingsrechten, zoals de OV-jaarkaart en het voordeelurenabonnement moet daarnaast ook nog een kopie van een geldig legitimatiebewijs worden afgegeven aan het desbetreffende vervoersbedrijf. De anonieme kaart en de wegwerpkaart zijn gewoon te koop bij verkooppunten zoals de sigarenboer en de krantenkiosk.

Iedere keer als een reiziger in- en uitcheckt, wordt er een transactie gemaakt. De transactiegegevens worden zeven jaar bewaard. TLS is van mening dat het hiertoe is verplicht door de Belastingdienst, maar de Belastingdienst ontkent dit (De Winter 2008). De gegevens van de laatste tien transacties worden ook bewaard op de kaart.

Per transactie worden onder meer de volgende gegevens vastgelegd:

- het kaartnummer;
- de datum;
- de tijd (op de minuut nauwkeurig);
- de locatie (inclusief halte of station);
- het type vervoer: bus, tram, metro of trein;
- bij de trein: eerste of tweede klas;
- bij de bus en de tram: het nummer van het voertuig;
- de wijze van betalen: met een reisproduct of op saldo, en of er van een kortingsrecht gebruik is gemaakt.

Een vervoersbedrijf kan per kaartnummer de transacties inzien van alle reizen die over zijn infrastructuur zijn gemaakt. Als gebruik wordt gemaakt van een persoonsgebonden kaart, kan het betreffende vervoersbedrijf de reiziger aan de hand van het kaartnummer identificeren. TLS kan per kaartnummer de transacties van alle vervoerders zien, plus de eventueel daaraan gekoppelde persoonsgegevens.

Maar ook van reizigers die gebruikmaken van een anonieme kaart kunnen reisbewegingen worden getraceerd. De overgrote meerderheid van de oplaadautomaten accepteert namelijk geen papiergeld. Bij die automaten kan het laden van saldo en reisproducten alleen met munten of met een PIN-betaling. Van PIN-betalingen wordt door de bank aan de ontvangende partij het rekeningnummer van de klant doorgegeven. Voor reizigers die regelmatig

gebruikmaken van het openbaar vervoer is betalen met munten bijzonder onpraktisch. Gebruikers van anonieme kaarten zullen normaal gesproken dan ook met PIN betalen en daarmee indirect te identificeren zijn aan de hand van hun bankrekeningnummer. Het koppelen van bankrekeningnummer aan persoonsgegevens is door de Nederlandsche Bank verboden voor commerciële doeleinden. Politie en justitie zijn echter wel bevoegd om deze gegevens te koppelen. Tevens zijn ze bevoegd inzage te vorderen in de centrale database.

Met de database kunnen de vervoersbedrijven zien hoeveel mensen er op ieder moment in een gegeven vervoersmiddel op een bepaalde locatie zaten. Tegelijkertijd kunnen de vervoerders en TLS ook voor iedere reiziger zien wat diens transacties zijn. Dit laatste is natuurlijk niet mogelijk wanneer iemand de duurdere wegwerpkaartjes gebruikt, voor iedere reis een nieuwe anonieme kaart koopt of zwartrijdt.

Naast optimalisering van de bedrijfsprocessen dient elektronisch betalen een tweede doel: de OV-chipkaart kan door de vervoersbedrijven voor dienstverlening worden benut. Aan de hand van de reisgegevens kunnen reizigers gericht bepaalde diensten worden aangeboden, bijvoorbeeld informatie over gewijzigde treintijden of storingen. Hiervoor geldt een 'opt-out'-regeling. Reizigers met een persoonsgebonden kaart krijgen deze diensten aangeboden – en de bedrijven mogen daarvoor relevante reisgegevens opslaan – tenzij ze aangeven dat niet te willen. Dit voorstel is goedgekeurd door het College bescherming persoonsgegevens (CBP 2008). Een actievere profilering van reizigers voor commerciële doeleinden – bijvoorbeeld met aanbiedingen van winkels op het station waar de reiziger zich bevindt – is niet toegestaan, tenzij reizigers daarvoor expliciet toestemming geven. Dit heet een 'opt-in'-regeling. In dat geval mogen de vervoersbedrijven veel meer gegevens opslaan en verwerken.

2.3.2 Hoe zijn de gegevens beveiligd?

TLS heeft gezocht naar een betrouwbare chipkaart die zich in de praktijk al had bewezen. Het bedrijf heeft gekozen voor de Mifare Ultralight-chip voor de wegwerpkaart, en de Mifare Classic-chip voor de anonieme en de persoonsgebonden kaart. Dit ondanks twijfels die er leefden over de beveiliging van deze chips. Deze twijfels werden in 2008 bewaarheid. In januari 2008 demonstreerde Radboud-student Roel Verdult dat de Mifare Ultralight-chip is na te bootsen op een apparaat van enkele tientjes. En in maart 2008 ontdekte een team van de Radboud Universiteit Nijmegen dat de Mifare Classic-chip vrij eenvoudig gekraakt kan worden. Een standaard kaartlezer van tien euro en een standaard pc volstonden daarvoor.

TLS heeft lange tijd volgehouden dat er niets mis was met de beveiliging van de OV-chipkaart, zonder overigens inzage te geven in de wijze van beveiligen. Pas na demonstraties in de media van diverse zwakheden heeft TLS zijn openbare standpunt (gedeeltelijk) aangepast. Desondanks suggereert TLS in de gebruikersinformatie nog steeds dat er weinig aan de hand is. Zo staat in de sectie veelgestelde vragen op www.ov-chipkaart.nl bij de vraag "Kunnen onbevoegden geld van mijn OV-chipkaart boeken?" het antwoord "Nee, (…)". Dat antwoord is feitelijk onjuist.

De problemen met de beveiliging van de OV-chipkaart hadden voorkomen kunnen worden door een ander chiptype te kiezen. Op het moment dat TLS voor de Mifare-chips koos, waren er ook andere chiptypes beschikbaar. Deze alternatieven zijn niet meegenomen in de ontwikkeling van de OV-chipkaart. De Mifare-chips leken te voldoen aan de eisen van TLS en de beveiligingszwakheden van de chips waren op het moment van selecteren nog niet algemeen bekend. Nu alsnog van chiptype veranderen is een kostbare en ingewikkelde operatie. Ondertussen is TLS trouwens wel bezig met een opvolger voor de Mifare Classic, namelijk de SmartMX.

De beveiligingsproblemen met de Mifare-chips betekenen dat grootschalige fraude mogelijk is, bijvoorbeeld door het saldo naar eigen keuze aan te passen. In theorie kan bijna alle fraude door de database herkend worden, en kunnen de gemanipuleerde kaarten geblokkeerd worden. Door een combinatie van technische en organisatorische redenen is de fraudedetectie echter niet sluitend en duurt het herkennen ervan minstens een volle dag. 'Hit-and-run fraude' blijft daardoor mogelijk.

Een ander gevolg van de kraakbaarheid van de Mifare Classic is dat kwaadwillenden een verloren of gestolen OV-chipkaart kunnen uitlezen en manipuleren. Zij kunnen er zo achterkomen waar de betreffende persoon de laatste tien ritten is geweest. Ook kunnen ze het saldo op de pas aanpassen. Hoogleraar computerbeveiliging Bart Jacobs beschouwt de de OV-chipkaart dan ook als "een open portemonnee". Hij deed die uitspraak tijdens een hoorzitting in Tweede Kamer over de OV-chipkaart.

Over de beveiliging van de centrale database is weinig bekend. Het is wellicht een interessant doelwit voor hackers. Ook is onbekend in hoeverre de infrastructuur van de OV-chipkaart is beveiligd tegen fraude door en fouten van de vervoersbedrijven en TLS zelf. Wel is het duidelijk dat fouten voorkomen. Gertjan Kroon, directeur van het Gemeentelijk vervoersbedrijf Amsterdam, vertelde tijdens de hoorzitting in de Tweede Kamer dat sommige oplaadautomaten aangaven dat een saldo was bijgeboekt op een kaart, terwijl dat niet het geval was. De klanten die daarover klaagden kregen het verwijt dat zij de automaat onjuist hadden bediend, en hebben voor zover bekend hun geld niet teruggezien. Dat wijst op een volgend probleem met de OV-chipkaart. Kaarthouders die een conflict hebben met een vervoersbedrijf ontbreekt het aan bewijsmateriaal om hun bewering te onderbouwen. De kaarthouder is afhankelijk van de coulance van de vervoersbedrijven.

2.4 De kilometerheffing: technische privacywaarborgen

In tegenstelling tot bij de OV-chipkaart, is bij de plannen voor invoering van de kilometerheffing nadrukkelijk gekeken naar technische mogelijkheden om de privacy te waarborgen. Er zijn twee varianten ontwikkeld voor invoering van de kilometerheffing: de 'dunne' en de 'dikke' variant. Bij de dunne variant worden de gegevens over de afgelegde reisroute door een private dienstverlener verzameld en doorgestuurd naar de innende instantie, die de gegevens in een centrale database opslaat (Kolman & Van Est 2010). Bij de dikke variant worden de gegevens *in* de auto verzameld en daarna – zonder tussenkomst van een private partij – naar de innende instantie gestuurd.

2.4.1 Een privacyvriendelijk ontwerp

De voorheen verantwoordelijke minister Camiel Eurlings (Verkeer en Waterstaat) heeft in de media (bijvoorbeeld in het RTL nieuws van 30 januari 2008) een voorkeur uitgesproken voor de dikke variant. Deze geeft een betere bescherming van de privacy omdat alléén de reiziger zélf zijn reisbewegingen kan nagaan. Het is echter nog niet duidelijk welke variant zal worden gekozen. Het is zelfs niet duidelijk of de kilometerheffing op afzienbare termijn zal worden ingevoerd. In het hiernavolgende wordt alleen ingegaan op de dikke variant, omdat deze goed illustreert hoe technische maatregelen kunnen worden ingebouwd ter bescherming van de privacy.

De dikke variant van de kilometerheffing maakt de volgende functies mogelijk:
- er wordt betaald voor vervoer met een gedifferentieerde prijsstelling;
- alleen de reiziger heeft toegang tot naar hemzelf herleidbare reisgegevens;
- fraude en fouten door de reiziger kunnen gedetecteerd worden door de exploitant;
- fraude en fouten door de exploitant kunnen gedetecteerd worden door de reiziger;
- bij een meningsverschil over de afrekening heeft zowel de reiziger als de exploitant bewijsmateriaal om claims te onderbouwen.

Het laatste punt laat goed de voordelen zien van een technische maatregel boven een procedurele maatregel. Als de exploitant een fout maakt en bijvoorbeeld een onverklaarbaar hoge 'spookrekening' stuurt aan een reiziger, is de reiziger niet overgeleverd aan de goede wil van de exploitant om de fout te erkennen en te herstellen. Dit in tegenstelling tot bij de OV-chipkaart, zoals we in de vorige paragraaf zagen.

2.4.2 Hoe werkt de kilometerheffing?

In de auto van de reiziger zit een gps-ontvanger die bijhoudt waar de auto rijdt. Door de ritgeschiedenis te combineren met een beprijzingstabel kan de rekening worden opgemaakt door het navigatiesysteem van de automobilist. De rekening wordt samen met een cryptografisch bewerkte versie van de ritgeschiedenis digitaal ingeleverd bij de exploitant. Auto-eigenaren die lange tijd geen rekening indienen, krijgen een herinnering en bij voortdurend in gebreke blijven een boete. Desgewenst kan de automobilist het berekenen van de facturen en het inleveren ervan uitbesteden aan een gespecialiseerd bedrijf, zodat hij of zij er geen omkijken naar heeft.

Om fraude tegen te gaan kan de exploitant controle uitvoeren, door op een willekeurige plek langs de weg na te gaan welke auto's langsrijden, om vervolgens te verifiëren of het stukje weg voorkomt in de ingeleverde ritgeschiedenis van de corresponderende auto's. Komt het wegdeel voor in de ritgeschiedenis, dan is er ook betaald voor dat specifieke weggebruik. Als het wegdeel niet voorkomt in de ritgeschiedenis krijgt de automobilist een bekeuring. De ingeleverde ritgeschiedenissen zijn op zo'n manier cryptografisch bewerkt, dat de handhaver wel kan zien dat het gecontroleerde wegdeel in de ritgeschiedenis zit, maar niet op welke andere wegdelen de auto nog meer heeft gereden.

De dikke variant is een systeem voor kilometerheffing waarbij een technische maatregel ervoor zorgt dat de inbreuk op de privacy van de reiziger minimaal is (De Jonge & Jacobs 2008). Het systeem levert een nauwkeurig sturingsinstrument, omdat reizigers gestuurd kunnen worden met gedifferentieerde prijsstellingen voor tijd, locatie en type voertuig. Tevens vinden er nauwkeurige metingen plaats (wie is waar en wanneer met welk voertuig?), maar die zijn niet centraal toegankelijk: alleen de reiziger zelf kan de metingen inzien.

2.5 Een privacyvriendelijke OV-chipkaart?

Het is de vraag of ook voor de OV-chipkaart een privacyvriendelijke variant mogelijk is. Hierbij zijn twee verschillen tussen de OV-chipkaart en het systeem voor kilometerheffing van belang.

In de eerste plaats maakt de dikke variant van de kilometerheffing gebruik van satellietnavigatie voor iedere individuele reiziger. Dit is niet geschikt voor toepassing in het openbaar vervoer. Er zijn een aantal praktische bezwaren. Zo moet de reiziger een apparaat met een voldoende opgeladen batterij bij zich hebben. Daarnaast moet het apparaat voldoende zicht hebben op oriëntatiepunten zoals de gps-satellieten. Het is de vraag of smartphones hiervoor voldoende betrouwbaar zijn. Ook valt het onderscheid niet te maken tussen een reiziger op de fiets, die niet hoeft te betalen, en een reiziger op dezelfde rijbaan in de bus. Het ontwerp van de OV-chipkaart met een RFID-pas, waarmee de reiziger in- en uitcheckt, is wat dat betreft zo gek nog niet.

Het tweede verschil heeft te maken met het gebruik van cryptografie. Het systeem voor de kilometerheffing maakt gebruik van een complex soort cryptografie, genaamd 'zero-knowledge'. Met zero-knowledge kunnen technische beperkingen worden opgelegd aan het gebruik van informatie,

waardoor de privacygevoelige gegevens kunnen worden afgeschermd voor de exploitant, terwijl de benodigde functionaliteit – zoals gemaakte reizen factureren – wel kan worden geleverd (Brands 2000; Camenisch & Lysyanskaya 2002).

Ook voor de OV-chipkaart is een ontwerp met zero-knowledge mogelijk, waarbij de reiziger nog steeds in- en uitcheckt. Deze variant heeft dezelfde privacyvriendelijke eigenschappen als de dikke variant van de kilometerheffing, terwijl er wel een centrale database wordt gecreëerd. Het belangrijkste verschil met het huidige systeem van de OV-chipkaart is dat met behulp van zero-knowledge de reisgegevens niet tot individuele personen herleidbaar zijn. Op basis van de centrale database kunnen de vervoersbedrijven wel nauwkeurige metingen doen om hun materieel en personeel efficiënter in te zetten, maar het is niet mogelijk om per persoon in te zien wat diens transacties zijn. In dit alternatieve ontwerp worden dezelfde gegevens bijgehouden als bij de huidige OV-chipkaart, met uitzondering van de kaartnummers. De verschillende reizen met dezelfde kaart kunnen daardoor niet met elkaar of met de kaarthouder in verband worden gebracht.

De benodigde rekenkracht voor zero-knowledge is vele malen groter dan de rekenkracht die in de huidige OV-chipkaart zit. Tot medio 2009 waren er geen RFID-chips commercieel beschikbaar die hier krachtig genoeg voor zijn. Ten tijde van het ontwerp van de huidige OV-chipkaart kon dan ook nog geen zero-knowledge worden toegepast. Er bestonden al wel beter beveiligde chips, die manipulatie en fraude beter het hoofd konden bieden, maar nog geen chips die het mogelijk maakten reizigers anoniem te laten reizen.

2.6 Conclusies: een elektronisch enkelbandje voor iedere reiziger?

Bij het reizen per openbaar vervoer wordt met de invoering van de OV-chipkaart het reisgedrag van de reiziger tot in detail bijgehouden. De gegevens in de centrale database worden ten minste zeven jaar bewaard. Dat is vele malen langer dan bijvoorbeeld de bewaartermijn voor telecommunicatiegegevens volgens de Europese richtlijn dataretentie. Met het recentelijk beschikbaar komen van RFID-chips die privacyvriendelijke technieken ondersteunen wordt het praktisch mogelijk om een privacyvriendelijke OV-chipkaart in te voeren. Gezien de kosten die daarmee gemoeid zijn, zal er zware politieke en publieke druk nodig zijn om zo'n OV-chipkaart ingevoerd te krijgen.

Voor de kilometerheffing is een variant voorhanden die weinig tot geen offers op het gebied van privacy vraagt. Voor het terugdringen van files en milieubelasting is het volgens de voormalige minister van Verkeer en Waterstaat niet nodig te weten waar individuele auto's zich bevinden. De technieken om dit te bewerkstellingen zijn beschikbaar.

De privacyvriendelijke, 'dikke' variant van het systeem voor kilometerheffing wordt overigens deels ondergraven door de ANPR-systemen (automatische nummerplaatherkenning) van de politie. Deze camerasystemen registreren momenteel de nummerborden van alle auto's op de uitvalswegen rond Zwolle en Rotterdam. Hoewel de doelmatigheid en rechtmatigheid ervan nog onderwerp van discussie zijn, is het de ambitie van de politie om in de nabije toekomst meer ANPR-systemen te plaatsen. Voor het vervoer per auto voert de overheid dan ook een dubbel beleid: terwijl de politie op steeds grotere schaal auto's registreert, voert het (voormalige) Ministerie van Verkeer en Waterstaat een veel terughoudender beleid.

In tegenstelling tot bij de kilometerheffing heeft de overheid voor het openbaar vervoer nauwelijks kaders gesteld. De centrale database die met de OV-chipkaart is gecreëerd, heeft tot weinig discussie over privacy geleid. Tot voor kort werd van vrijwel niemand structureel bijgehouden waar hij of zij zich bevond. Met de invoering van systemen als de OV-chipkaart en de nummerbordregistraties verandert dit. En omdat het onmogelijk is om grote afstanden te reizen zonder gebruik te maken van de auto of het openbaar vervoer, betekent dit dat de overheid en de vervoersbedrijven kunnen achterhalen wie waar op welk moment is.

Een vergelijking met het elektronisch enkelbandje dringt zich op. Bepaalde groepen veroordeelden mogen deelnemen aan het maatschappelijk leven onder voorwaarde dat zij een elektronisch enkelbandje dragen. Met het elektronisch enkelbandje kan de politie of de reclassering hun handel en wandel volgen. Hun privacy is ingeperkt omdat door de rechter is vastgesteld dat zij een gevaar voor hun omgeving kunnen zijn. Met de grootschalige registratie en opslag van reisgegevens in centrale databases lijkt zich een situatie af te tekenen waarin iedereen, brave burgers incluis, het equivalent van een elektronisch enkelbandje draagt. Het is de vraag of dat wenselijk is.

Dankwoord

Dit hoofdstuk had nooit tot stand kunnen komen zonder de kennis die is opgedaan in een groot aantal gesprekken met direct betrokkenen. Hun aantal is te groot om ieder bij naam te noemen, maar uitdrukkelijke dank voor hun tijd en openheid is op zijn plaats. De auteur is betrokken geweest bij het onderzoek aan de Radboud Universiteit Nijmegen naar de OV-chipkaart, de Mifare Classic en de kilometerheffing.

Het elektronisch patiëntendossier vanuit informatiebeveiligings-perspectief

3

VERTROUWELIJK

3 Het elektronisch patiëntendossier vanuit informatiebeveiligingsperspectief

Bart Jacobs

3.1 Inleiding

Het landelijk elektronisch patiëntendossier (EPD) wordt in Nederland ingevoerd om de onderlinge communicatie tussen hulpverleners in de zorg te verbeteren, met als achterliggend doel daarmee de kwaliteit van de medische zorg te verbeteren. Daartoe wordt een landelijke ICT-infrastructuur opgezet waarbij medische hulpverleners, na toestemming van de patiënt, tot verschillende medische gegevens van die patiënt toegang kunnen krijgen. Dit artikel zal de invoering van het EPD bezien vanuit het oogpunt van het vakgebied informatiebeveiliging. Daarbij zal gekeken worden naar: de architectuur van het EPD, beveiligingseisen, toegangsprocedures, beveiligingsrisico's en de consequenties van de invoering van het EPD voor artsen en patiënten. De nadruk zal niet zozeer liggen op de gebruikte technieken en middelen, maar meer op de wijze waarop ermee wordt omgegaan.

Het landelijk EPD bevindt zich nog in de voorbereidende fase. De eerste operationele onderdelen van het EPD zullen het elektronisch medicatiedossier en waarneemdossier huisartsen zijn. De precieze fasering van het EPD zal in het onderstaande een ondergeschikte rol spelen. De nadruk zal veeleer liggen op de inhoudelijke aspecten. De belangrijkste conclusies zijn dat het EPD nieuwe eisen met betrekking tot zorgvuldigheid, identiteitscontrole, transparantie en verantwoording voor de zorgsector met zich meebrengt, en behalve medische voordelen ook nieuwe kwetsbaarheden introduceert. De materie is te complex voor een simpel 'voor' of 'tegen'. Daar zal dan ook niet op worden aangestuurd.

3.2 Architectuur

Voor een landelijk patiëntendossier zijn drie ICT-architecturen denkbaar, elk met eigen voor- en nadelen. Ik bespreek achtereenvolgens een centrale databank, de mogelijkheid van een decentrale opslag van gegevens en een verwijsinfrastructuur. Het begrip architectuur verwijst hier niet naar het ontwerp van bruggen of gebouwen, maar naar het ontwerp van ICT-informatiesystemen. In brede zin wordt daaronder verstaan de structurele organisatie van hardware, applicaties, processen en gegevensstromen, tezamen met de daarmee samenhangende organisatorische consequenties, binnen bedrijven, overheden, of binnen de samenleving in brede zin.

3.2.1 Centrale databank

De eerste mogelijkheid voor een EPD bestaat uit een centrale databank met daarin opgeslagen alle dossiers van alle patiënten. Deze aanpak lijkt de simpelste en de meest voor de hand liggende. Zo'n centrale databank maakt het systeem echter zeer kwetsbaar voor mogelijk misbruik, uitval of overbelasting. Tevens vormt het mogelijke 'omvallen' van een dergelijke databank – door toedoen van kwaadwillende hackers of beheerders, of simpelweg door beheersfouten – met een concentratie van zeer privacygevoelige gegevens een te groot risico. Deze centrale aanpak is dan ook niet geschikt.

3.2.2 Decentrale opslag bij de patiënt

Hiertegenover staat de tweede mogelijkheid: een volledig decentrale architectuur waarbij patiënten zelf hun eigen dossier bewaren en beheren. Vanuit het perspectief van privacy is dit niet zo'n slecht idee, omdat controle over de toegankelijkheid van persoonlijke gegevens een essentieel onderdeel is van de notie van privacy. Vooral in landen waar geen fijnmazige eerstelijns medische zorg bestaat, is het gebruikelijk dat mensen bijvoorbeeld na het nemen van een röntgenfoto de resultaten zelf mee naar huis krijgen en ook zelf weer meenemen naar een volgend consult. In Duitsland wordt onder het motto *Der Patient muss Herr seiner Daten bleiben* de *Gesundheitskarte* ingevoerd: een chipkaart waarmee burgers een belangrijk deel van hun medische dossier zelf bij zich dragen. Bij deze decentrale aanpak hoeven mensen de eigen medische gegevens niet noodzakelijk ook zelf op te slaan. De gegevens kunnen ook in versleutelde vorm op internet staan, waarbij alleen de patiënt zelf beschikt over de voor toegang noodzakelijke cryptografische sleutels. De patiënt is hierbij ook de enige die kan besluiten om kopieën van die sleutels, bijvoorbeeld voor de zekerheid, aan anderen te geven.

Een principieel aspect van deze aanpak is dat in de architectuur zelf verankerd is dat toegang tot het dossier zonder toestemming van de patiënt niet mogelijk is. Zo'n technische onmogelijkheid geeft sterkere garanties dan wanneer op procedurele gronden toestemming van de patiënt nodig is, want procedures kunnen gemakkelijk veranderd of genegeerd worden.

Voor deze decentrale architectuur is in Nederland niet gekozen. De precieze redenen hiervoor zijn onduidelijk – en mogelijk een aparte studie waard – maar lijken vooral te zijn dat de patiënt onvoldoende in staat wordt geacht zorgvuldig met de eigen gegevens om te gaan, en de medische sector controle over medische gegevens niet uit handen wil geven.

Dit laatste wijst er al op dat de architectuur van ICT-systemen nauw samenhangt met machtsverhoudingen. Patiënten hebben in Nederland weinig te zeggen. De Amerikaanse privacyvoorvechter Mitchell Kapor spreekt daarom terecht van *architecture is politics*. De ICT-architectuur die gekozen wordt, geeft een goed

beeld van de onderliggende machtsverhoudingen. In Nederland is gekozen voor een tussenvorm tussen centrale en decentrale opslag van medische gegevens, die hieronder wordt beschreven.

3.2.3 Landelijke verwijsinfrastructuur

Tussen deze twee uitersten, centraal en decentraal, bestaan verschillende tussenvormen. In Nederland is ervoor gekozen de medische gegevens onder het beheer van de betreffende zorgverleners te laten, en toegankelijk te maken door middel van een landelijke verwijsinfrastructuur, het zogeheten landelijk schakelpunt (LSP). Via het burgerservicenummer (BSN) kan een arts informatie over een patiënt bij een collega uit diens computer opvragen. De betrouwbaarheid van het EPD is daarmee mede afhankelijk van de betrouwbaarheid van het BSN. Een zorgverlener dient zich er dan ook goed van te vergewissen, zeker bij een onbekende patiënt, of de koppeling tussen persoon en BSN juist is. Identiteitscontrole wordt daarmee onderdeel van betrouwbare zorgverlening. Het belang daarvan wordt in de praktijk echter nog nauwelijks ingezien. "Ik ben toch geen politieagent", verzucht menig zorgverlener. Het EPD vereist echter wel zo'n rol.

De LSP-infrastructuur is in feite een netwerk van gekoppelde computers waarbinnen verschillende fragmenten van een patiëntendossier via versleutelde verbindingen verzonden worden. Deze digitale uitwisseling van medische gegevens vindt primair plaats tussen zorgverleners, maar maakt het ook mogelijk dat een patiënt zijn eigen dossier kan inzien. Zorgverleners die aangesloten worden op het landelijk schakelpunt moeten aan de beveiligingseisen voldoen van het 'goedbeheerd zorgsysteem' en via het landelijk schakelpunt patiënten toegangsrechten verlenen. Ook het LSP zelf wordt ontwikkeld op basis van bepaalde beveiligingseisen (Van 't Noordende 2010). Dit vindt plaats onder regie van het Nationaal ICT Instituut in de Zorg (Nictiz), dat opereert onder verantwoordelijkheid van de minister van Volksgezondheid, Welzijn en Sport (VWS). In het hiernavolgende wordt verder ingegaan op deze derde variant, die in het dagelijks woordgebruik wordt aangeduid met de term 'het (landelijk) EPD'.

3.3 Beveiligingseisen voor het EPD

Aan welke beveiligingseisen moet het landelijk EPD voldoen? De belangrijkste voorwaarden voor een goed functioneren van het landelijk EPD zijn vertrouwelijkheid, integriteit en beschikbaarheid van medische gegevens. Hieruit vloeien beveiligingseisen ten aanzien van de landelijke verwijsinfrastructuur voort.

De eerste voorwaarde van vertrouwelijkheid houdt in dat alleen bevoegde partijen de inhoud van een bepaald medisch dossier kunnen lezen. Het debat over de privacy van patiënten die op het spel staat, of zou staan, concentreert zich op dit punt. Vertrouwelijkheid kan verbroken worden door onder meer slordigheid, lekken of hacken. Eenmaal verbroken vertrouwelijkheid kan niet meer worden hersteld: wanneer eenmaal bekend is geraakt dat een bekende of onbekende Nederlander een psychiatrisch verleden heeft, zal die informatie niet meer verdwijnen.

Integriteit van medische gegevens betekent dat medische gegevens alleen door bevoegde partijen kunnen worden veranderd, zodat artsen op de gegevens kunnen vertrouwen. De integriteit kan worden geschonden wanneer de identiteit van een patiënt niet goed is vastgesteld voordat informatie aan een dossier wordt toegevoegd, zodat bijvoorbeeld de verkeerde bloedgroep wordt genoteerd. Integriteit kan ook geschonden worden indien bevoegdheden voor toegang tot of wijziging van gegevens niet adequaat worden vastgesteld. Ook zouden kwaadwillenden de integriteit van medische gegevens moedwillig kunnen schenden, bijvoorbeeld door hackers in te schakelen om een bepaalde persoon of groep kwaad te doen. Schending van integriteit kan grote nadelige gevolgen hebben, maar kan bij tijdige ontdekking in principe hersteld worden.

Ten derde is de beschikbaarheid van medische dossiers belangrijk voor een adequate medische behandeling. Naarmate zorgverleners afhankelijker worden van elektronische dossiers wordt het belangrijker dat de dossiers op het gevraagde moment daadwerkelijk op het scherm verschijnen. Indien de gegevens via het landelijk schakelpunt van elders moeten komen, is het essentieel dat vertrouwd kan worden op de juiste werking van deze infrastructuur en op een effectieve bescherming ervan tegen kwaadwillenden.

In paragraaf 5 kom ik terug op de beveiligingsrisico's die samenhangen met deze voorwaarden voor een goed functionerend EPD. Eerst wordt nader ingegaan op de manier waarop de toegang tot de medische dossiers wordt geregeld.

3.4 Toegangsprocedures

Bij de toegang tot het EPD dient een onderscheid gemaakt te worden tussen de toegang door zorgverleners tot de dossiers van hun patiënten en de toegang door patiënten tot hun eigen dossier.

3.4.1 Toegang door zorgverleners

Om toegang te krijgen tot de medische gegevens van een patiënt via het LSP gebruiken zorgverleners de zogenoemde unieke zorgverlener identificatiepas (UZI-pas). Deze pas wordt gelezen door een paslezer die verbonden is met de computer die de zorgverlener gebruikt. Gebruik van de pas vereist een persoonlijke 6-cijferige PIN-code voor authenticatie. Zorgverleners mogen alleen gegevens opvragen van patiënten met wie zij een behandelrelatie hebben. Bij de toegang tot dossiers wordt niet met technische middelen gecontroleerd of er daadwerkelijk sprake is van een behandelrelatie. Wel bestaat er een aantal procedurele controles en wordt iedere raadpleging geregistreerd, zodat achteraf valt vast te stellen of de raadpleging terecht heeft plaatsgevonden.

De UZI-pas is strikt persoonlijk. In de praktijk ziet men echter dat meerdere mensen voor het gemak van één en dezelfde pas gebruikmaken. Dit heeft niet alleen risico's voor de patiënten, maar ook voor de zorgverleners zelf. De raadpleging van medische gegevens wordt geregistreerd en kan bijvoorbeeld gebruikt worden bij aansprakelijkheidskwesties. Het gebruik van de UZI-pas vereist dan ook een nieuwe discipline en zorgvuldigheid van zorgverleners. Tevens introduceert het een nieuwe vorm van controle en aansprakelijkheid: als iemand met de UZI-pas van een collega ongeoorloofd in een dossier heeft gekeken, heeft die collega mogelijk een probleem.

Er zullen naar schatting meer dan een half miljoen UZI-passen in Nederland worden verspreid. Grofweg is dat 1 op de 25 volwassenen. Nu geeft niet iedere UZI-pas toegang tot medische gegevens – dat hangt af van de rolafhankelijke authorisatie (bijvoorbeeld arts of verpleegkundige). Maar de grote hoeveelheid UZI-passen betekent wel dat iedereen meerdere mensen in de eigen omgeving heeft met toegang tot medische gegevens. Het is uitgesloten dat die half miljoen mensen met toegang zich altijd netjes en zorgvuldig zullen gedragen. Dat is ook nu niet het geval. Maar met het EPD hebben die (mogelijk) kwaadwillenden wel gemakkelijker toegang tot meer gegevens.

Hierboven is reeds vermeld dat zorgverleners de identiteit van de patiënt dienen vast te stellen. Patiënten hebben dan ook een legitimatieplicht. Ook dit brengt nieuwe verantwoordelijkheden en aansprakelijkheden met zich mee voor de zorgaanbieder: indien bijvoorbeeld een onverzekerde zich ongemerkt als mij kan voordoen, kunnen er verkeerde gegevens in mijn dossier terechtkomen. Door landelijke koppelingen zullen zulke fouten zich verspreiden, waardoor de kans groter wordt dat een patiënt er daadwerkelijk mee geconfronteerd zal worden. Het zal nog moeten blijken in welke mate een patiënt een zorgverlener aansprakelijk kan stellen voor schade door vervuiling van zijn dossier als gevolg van onvoldoende identiteitscontrole.

3.4.2 Toegang door patiënten

Volgens de Wet op de Geneeskundige Behandelovereenkomst (WGBO) hebben patiënten recht op toegang tot hun eigen medische dossiers. Voormalig minister Klink (VWS) heeft laten weten dat dit een essentieel onderdeel vormt van het EPD. Patiënten moeten op eenvoudige wijze, via elektronische weg inzage kunnen krijgen in hun medische gegevens. Deze toegang tot het EPD is voorzien via een versterkte versie van DigiD, waarbij burgers zich eerst een keer fysiek (*face-to-face*) moeten authenticeren.

Burgers krijgen niet alleen inzage in hun medische gegevens, maar ook in zogenoemde log-bestanden met informatie over welke hulpverlener wanneer toegang heeft gehad tot hun dossier. Indien deze log-informatie op inzichtelijke wijze wordt gepresenteerd, kan dit een krachtig en belangrijk controlemiddel

vormen. Zorgverleners zullen er dan ook rekening mee moeten houden dat ongepast gluurgedrag eerder opgemerkt zal worden, en tot klachten zal leiden.

Patiënten kunnen in principe ook de toegang tot hun dossier selectief, voor bepaalde zorgverleners afsluiten, bijvoorbeeld indien de eigen buurman een arts is en men er niet op wil vertrouwen dat deze buur zijn nieuwsgierigheid voldoende kan bedwingen.

3.5 Beveiligingsrisico's

Vanuit beveiligingsoogpunt kunnen er problemen ontstaan met het EPD met betrekking tot vertrouwelijkheid, integriteit of beschikbaarheid (zie paragraaf 3). Beschikbaarheidsrisico's zijn in dit stadium moeilijk in te schatten en zullen hier buiten beschouwing gelaten worden – zonder overigens het grote belang ervan te onderschatten. Risico's met betrekking tot vertrouwelijkheid en integriteit zullen samen worden bekeken als vormen van ongeoorloofde toegang.

Het is een probleem van majeure omvang als iemand in de databank van bijvoorbeeld een ziekenhuis of een huisartsenpost weet door te dringen en daar dossiers inziet of verandert. Dit risico is reëel en bestaat ook zonder EPD, zoals bleek uit geslaagde inbraakpogingen in 2005, georganiseerd door publiciste Karin Spaink (Spaink 2005). Door invoering van het landelijk EPD zou dit risico verder worden vergroot, indien het mogelijk blijkt om via het landelijk schakelpunt dergelijke databanken binnen te dringen. Omdat de infrastructuur van het LSP aan hoge beveiligingseisen moet voldoen, lijkt dat gevaar niet zo groot. Een eventuele breuk van de beveiliging van het schakelpunt zelf zou echter een nationale ramp zijn, omdat via het LSP alle medische gegevens worden uitgewisseld.

Risico's bestaan veeleer bij de authenticatie van zorgverleners. Zij moeten de UZI-pas nauwgezet gebruiken, geen passen of PIN-codes delen, na gebruik direct uitloggen, passen niet in paslezers laten zitten, enzovoort. Eind 2008 toonde de actualiteitenrubriek NOVA aan dat werknemers van een ziekenhuis zonder veel aandringen inlognamen en wachtwoorden over de telefoon aan een onbekende doorgaven (NOVA 2008). Diverse onderzoeken bevestigen dat ziekenhuizen hun beveiliging niet op orde hebben. Zorgverleners zijn opgeleid om zorg te verlenen, maar zijn niet adequaat getraind om informatie te beveiligen. Daar zal nog veel moeten verbeteren. Beveiligingsincidenten – ingegeven door nieuwsgierigheid of kwade wil – zullen in de media waarschijnlijk veel aandacht krijgen, met aantasting van de reputatie van de medische sector en het EPD als mogelijk gevolg.

Ook bestaan er beveiligingsrisico's bij individuele patiënten die hun eigen dossier via internet inzien. Het is de eigen verantwoordelijkheid van iedere burger om zorgvuldig met de DigiD-authenticatiemiddelen om te gaan.

Dat zal ongetwijfeld nu en dan fout gaan, net zoals er af en toe mensen ongewild toegang geven tot hun bankrekening bij internetbankieren, als gevolg van onzorgvuldigheid of een computerbesmetting. Omdat het hier gaat om individuele gevallen, zal de schade echter minder groot zijn dan bij een inbraak in een medische databank.

Het EPD geeft patiënten de mogelijkheid de toegang door zorgverleners tot hun dossier te beperken, of zelfs helemaal af te sluiten. Het valt te verwachten dat mensen dat in grotere aantallen gaan doen als serieuze beveiligingsincidenten optreden. Deze *feedback loop* zal naar verwachting de verantwoordelijken voor de beveiliging van het systeem onder gezonde druk zetten.

Nu reeds bestaan op regionaal niveau allerlei initiatieven tot elektronische uitwisseling van patiëntgegevens, bijvoorbeeld via huisartsenposten of samenwerkende ziekenhuizen. Deze initiatieven zijn niet onderworpen aan strenge beveiligingseisen. Het landelijk EPD moet daar een eind aan maken, via een nationaal gereguleerde infrastructuur, die zorgverleners en patiënten uniforme en controleerbare toegang moet bieden. Het opschonen van deze (goedbedoelde) lokale houtje-touwtje- initiatieven – die ook bekritiseerd zijn door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg – is een positieve bijkomstigheid van het EPD. Misschien is het wel het sterkste argument om het landelijk EPD in te voeren.

3.6 Consequenties van invoering van het EPD

Het EPD is primair bedoeld om de communicatie tussen zorgverleners onderling te verbeteren. Er wordt gesproken over jaarlijks meer dan duizend sterfgevallen en bijna twintigduizend toedieningen van verkeerde medicatie die te wijten zouden zijn aan slechte communicatie. Het is te hopen dat met het EPD dit aantal drastisch afneemt. Al te veel optimisme is echter niet terecht. Het EPD zal bepaalde structurele fouten niet uitbannen – zoals verpleegkundigen die niet kunnen rekenen en verkeerde doses toedienen – en zal bovendien leiden tot andersoortige categorieën van medische fouten. Nu al is 'het naastliggende medicijn' de meest gemaakte computerfout, waarbij een arts in het rijtje van mogelijkheden in een menu met de muis abusievelijk het medicijn net boven of onder het bedoelde medicijn aanklikt. Slimme software zal echter wel bepaalde fouten en inconsistenties in dossiers kunnen detecteren.

Mogelijk zal het EPD zijn grootste impact niet hebben op de communicatie tussen zorgverleners onderling, maar tussen zorgverlener en patiënt. De laatste kan immers in het eigen dossier de ontwikkelingen precies volgen, en zal sneller en vaker om nadere uitleg of verantwoording vragen, of zelf een *second opinion* organiseren. Zorgverleners zullen noodgedwongen transparanter moeten gaan werken en zullen hun houding daarop moeten aanpassen. Dus niet meer noteren 'patiënt is een zeurkous', maar bijvoorbeeld de even adequate, maar

respectvollere omschrijving 'patiënt is extreem bezorgd'. In lijn hiermee kan huisartsen de suggestie worden gedaan om twee identieke schermen op het bureau te plaatsen, één voor zichzelf en één voor de patiënt, zodat door rechtstreekse inzage in het eigen dossier en in de mutaties die de arts doorvoert, vertrouwen wordt gewekt.

3.7 Conclusies

De laatste jaren is duidelijk geworden dat incidenten rond beveiliging en privacy grote ICT-projecten kunnen maken of breken. Dat geldt ook voor het EPD. Naast het beoogde doel van verbetering van de medische zorg, brengt het EPD ook nieuwe kwetsbaarheden en risico's met zich mee, vooral bij beveiliging, identiteitsfraude en propageren van foutieve gegevens. Een geslaagde aanval op de infrastructuur van het EPD kan desastreuze gevolgen hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van medische gegevens. Het grootste risico schuilt evenwel in een onzorgvuldige omgang door zorgverleners met de authenticatieverplichtingen, zowel wat het gebruik van de UZI-pas betreft, als de vereiste identiteitscontrole van patiënten. Het is in dit stadium redelijkerwijs niet in te schatten of de voordelen van het landelijk EPD tegen de nadelen zullen opwegen. In ieder geval zal het EPD de zorgsector tot een nieuwe manier van werken dwingen, met grotere transparantie en verantwoording. Vooral de directere toegang van patiënten tot hun eigen dossiers zal daarbij een positieve rol spelen.

Wanneer het EPD eenmaal operationeel is, zal het een eigen dynamiek krijgen, die nu niet voorspelbaar is. Ongetwijfeld zullen betrokkenen mogelijkheden zien waaraan nu niet wordt gedacht. Patiënten zouden bijvoorbeeld toch hun eigen, decentrale dossier kunnen inrichten, door hun medische gegevens voor iedereen af te sluiten en op een eigen USB-stick te zetten. Mogelijk kopiëren anderen hun gegevens liever naar Google Health. Het heeft geen zin om dit soort initiatieven te onderdrukken. Hooguit kunnen ze in goede banen worden geleid, of ontmoedigd door het EPD ook voor patiënten werkelijk nuttig te maken, zodat zij minder geneigd zijn om op andere systemen over te stappen. Te denken valt aan mogelijkheden om zelf gegevens aan het eigen dossier toe te voegen, bijvoorbeeld eigen bloeddrukmetingen, of om binnen de elektronische omgeving van het dossier beveiligd met artsen te communiceren. Het is daarom raadzaam de infrastructuur die nu wordt opgetuigd flexibel in te richten, zodat deze ruimte biedt voor zulke nieuwe mogelijkheden.

De beveiliging van het EPD vereist transparantie en continue aandacht en monitoring, 24 uur per dag. Banken, die ook werken met gevoelige gegevens, houden hun internetoperaties ook continu in de gaten. Die transparantie en monitoring zijn nodig voor het vertrouwen van zowel zorgverleners als patiënten, wat essentieel is voor het succes van het EPD. De praktijk zal moeten uitwijzen of de in Nederland gekozen verwijzingsarchitectuur goed aansluit bij onze

cultuur en de werkwijze van de medische sector. De Duitse decentrale variant, met de eerdergenoemde *Gesundheitskarte*, geeft burgers grotere controle. Het geeft te denken dat daar in Nederland niet voor is gekozen.

Dankwoord

De auteur dankt Simone van der Hof, Sjaak Nouwt, Guido van 't Noordende, en de redacteuren van het Rathenau Instituut voor hun constructieve adviezen.

Het elektronisch kinddossier: kansen en kanttekeningen

4

4 Het elektronisch kinddossier: kansen en kanttekeningen

Simone van der Hof

4.1 Inleiding: de invoering van het EKD

De papieren dossiers in de jeugdgezondheidszorg (JGZ) worden omgezet in digitale bestanden, een operatie die bekend is onder de naam 'elektronisch kinddossier' (EKD) of, sinds kort, 'digitaal dossier jeugdgezondheidszorg'. Deze verplichting volgt uit de Wet publieke gezondheid en betreft de dossiers van alle kinderen in de leeftijd tot 19 jaar die het consultatiebureau of de schoolarts bezoeken. Het EKD heeft tot doel een efficiëntere en effectievere jeugdgezondheidszorg te bewerkstelligen, waarbij opvoedingsproblemen en andere sociale of gezondheidsrisico's vroegtijdig worden gesignaleerd.

De kinddossiers bevatten informatie over de fysieke, cognitieve en psychosociale ontwikkeling van het kind, zijn sociale situatie (familie, vrienden, school) en – op termijn – prenatale data. De gestandaardiseerde lijst aan gegevens – de 'basisdataset' – aan de hand waarvan artsen en verpleegkundigen informatie verzamelen tijdens consulten met ouders en kind, beslaat zo'n dertig pagina's. Deze lijst is gebaseerd op het papieren dossier, aangevuld met een aantal gegevens die volgens artsen ook relevant zijn. Het EKD omvat verder profielen die aangeven in welke mate een jongere risico loopt op psychosociale problemen. Als een kind hoog scoort op risicofactoren zoals gescheiden ouders, armoede, agressief gedrag of depressiviteit, komt het in de categorie 'rood' en behoeft het extra aandacht van JGZ-professionals. In andere gevallen komen kinderen in de categorieën oranje (medium risico) dan wel geel (laag risico).

Het EKD bevat niet alleen medische data, maar wordt juridisch gezien toch gekwalificeerd als medisch dossier. Dat betekent dat ouders of – boven een bepaalde leeftijd – kinderen toestemming moeten geven voordat gegevens aan derden worden verstrekt. De gegevens in het EKD moeten volgens de wet bewaard worden tot vijftien jaar nadat de JGZ-relatie met het kind is beëindigd – dat wil zeggen vanaf diens negentiende jaar – of langer als de omstandigheden dat vereisen – bijvoorbeeld om de continuïteit in de zorg te garanderen. Zowel de ouders (totdat het kind 12 jaar is) als het kind hebben recht op inzage in en correctie van gegevens in het dossier. Inzage kan worden verleend door het verstrekken van een afdruk van het dossier of door mee te kijken tijdens het bezoek. Inzage mag worden geweigerd in het belang van de persoonlijke levenssfeer van het kind, bijvoorbeeld bij abortus bij een 15-jarige, of die van een van de ouders, bijvoorbeeld bij echtscheiding. In het Kidos-systeem dat hierna wordt besproken, kunnen bijvoorbeeld gegevens als het verblijfadres van de moeder on-screen worden afgeschermd voor de meekijkende vader.

Oorspronkelijk was het de bedoeling het EKD vanuit het oogpunt van uniformiteit en efficiëntie nationaal te ontwikkelen. Na een mislukt aanbestedingsproces is besloten om het – onder ministeriële verantwoordelijkheid van de voormalige minister voor Jeugd en Gezin – door gemeenten en JGZ-organisaties te laten invoeren. Het EKD moet wel aan nationaal vastgestelde specificaties voldoen om informatie-uitwisseling tussen JGZ-organisaties te vergemakkelijken. Het is de bedoeling dat het EKD mettertijd wordt gekoppeld aan het elektronisch patiëntendossier, zodat ook huisartsen toegang krijgen. Tegen die tijd zal de toegang tot het systeem verlopen via een speciale smartcard (UZI-pas), maar vooralsnog wordt gebruikgemaakt van een gebruikersnaam in combinatie met een wachtwoord. Afhankelijk van iemands functie (bijvoorbeeld arts of verpleegkundige) kunnen in de toekomst inzagerechten worden toegekend, zoals inzage in (een deel van) het dossier. Het systeem zal dan ook registreren welke raadplegingen van dossiers hebben plaatsgevonden en bijhouden met behulp van welke UZI-pas de dossiers zijn geraadpleegd.

4.2 EKD-basis of EKD-groot?

Het voorgaande is slechts een deel van het verhaal. De meningen over het doel en de toegankelijkheid van het EKD lopen inmiddels uiteen: moet het inderdaad uitsluitend een JGZ-dossier zijn, of zou het EKD de jeugdzorg in bredere zin moeten dienen? Informatie over de sociale omgeving van kinderen en hun psychosociale ontwikkeling kan tevens relevant zijn voor het maatschappelijk werk, scholen of de politie. Door deze informatie breder beschikbaar te maken kan de zorg voor kinderen en jongeren beter worden afgestemd tussen de betrokken organisaties en – zo is de redenatie – wordt de kans groter dat misstanden met kinderen kunnen worden voorkomen. Deze bredere insteek van het EKD wordt gevoed door de wens om de kans op tragische en soms fatale voorbeelden van kindermishandeling uit te bannen. Denk aan het Maasmeisje of de driejarige peuter Savanna, die beiden op gruwelijke wijze om het leven kwamen. Kinderen moeten veilig kunnen opgroeien. Hiertoe moeten verschillende instanties binnen de jeugdzorg beter samenwerken. Het EKD moet dat bevorderen door informatie over kinderen integraal te ontsluiten binnen de gehele jeugdzorg. Beleidsmakers willen het in aanleg medische EKD ('EKD-basis') daarom uitbouwen tot een EKD voor de jeugdzorg ('EKD-groot'). Met het EKD-groot willen zij een completer beeld van kinderen en hun sociale omgeving creëren.

Het EKD-groot past in een trend waarin 'risicojongeren' steeds centraler komen te staan. Een risicojongere is een jongere die kampt met meervoudige sociale en individuele problemen en het risico loopt om vroegtijdig schoolverlater, werkloos of crimineel te worden. Signalering en monitoring van risicojongeren wordt tevens beoogd met de Verwijsindex risicojongeren (VIR). De VIR is een informatiesysteem dat professionals in de jeugdzorg met elkaar in contact brengt op basis van risicomeldingen over jongeren in de leeftijd tot 23 jaar, bijvoorbeeld meldingen over contacten met de politie, drugs- en alcoholverslaving

of kindermishandeling. De VIR moet bijdragen aan een tijdige coördinatie en gezamenlijke interventie binnen de jeugdzorg in geval van probleemgevallen. Evenals het EKD wordt de VIR lokaal geïmplementeerd op basis van nationale standaarden die landelijke gegevensuitwisseling mogelijk maken. Anders dan het EKD worden in de VIR geen gegevens over kinderen uitgewisseld. Maar door beide te koppelen, snijdt het mes aan twee kanten.

Voormalig minister voor Jeugd en Gezin André Rouvoet wil het EKD – vooralsnog – beperken tot het domein van de jeugd*gezondheid*szorg. Op dit moment is de technische en organisatorische diversiteit binnen die sector te groot om een breed opgezet EKD tot stand te kunnen brengen. Daarmee sluit hij een verbreding op termijn echter niet uit.

De lokale behoefte aan een EKD-groot heeft inmiddels een eigen dynamiek gekregen. De vier grote steden (Amsterdam, Den Haag, Rotterdam en Utrecht) vinden dat het EKD in het belang van het kind méér dan alleen een medisch dossier moet zijn. Het moet ook ruimte bieden aan gegevens van onder meer het maatschappelijk werk, de scholen, Bureau Jeugdzorg en de geestelijke gezondheidszorg. Alleen door integratie van alle beschikbare gegevens over kinderen kan er voldoende zicht ontstaan op (potentiële) problemen in gezinnen. Bovendien is het voor de vier grote steden essentieel om de VIR en het EKD-groot te koppelen, om de risicomeldingen en de informatie over het kind en zijn omgeving samen te brengen. De vier grote steden hebben inmiddels aanzienlijk geïnvesteerd in een EKD-groot, waardoor er ook economische belangen in het spel zijn.

De medische geheimhoudingsplicht van de JGZ-medewerkers vormt overigens een belangrijke barrière voor gegevensuitwisseling tussen de diverse instanties en staat daarmee de ontwikkeling van een EKD-groot in de weg. Alleen in uitzonderlijke gevallen – zoals kindermishandeling – kunnen artsen na een zorgvuldige afweging ertoe besluiten medische informatie over patiënten te delen. Op artsen wordt echter in steeds sterkere mate een beroep gedaan om misstanden te melden.

Om te illustreren wat een EKD-groot behelst, schetst de volgende paragraaf de plannen op het gebied van de jeugdzorg in Rotterdam.

4.3 Ieder kind wint

Het Rotterdamse EKD-groot is onderdeel van het brede actieprogramma risicojeugd, Ieder kind wint. Dit programma wil een integrale samenwerking tot stand brengen van alle relevante instanties in de jeugdzorg. Hieronder vallen de stadsregio, de jeugdgezondheidszorg, het onderwijs, de welzijnssector, Bureau Jeugdzorg, de jeugdzorgaanbieders, de Jeugd-GGZ, de Raad voor de Kinderbescherming, de politie, het openbaar ministerie en de kinderrechter.

Het doel van Ieder kind wint is vroegtijdige risicosignalering en probleempreventie bij kinderen.

Sinds 2008 is in Rotterdam onder de naam Kidos het EKD in de jeugdgezondheidszorg operationeel. Hierin worden alle gegevens, inclusief risicoprofielen, over kinderen vanaf de zwangerschap geregistreerd. Het beleid van de gemeente is erop gericht honderd procent deelname re realiseren. Er wordt overwogen een verschijningsplicht in te voeren voorzien van sanctiemogelijkheden, omdat ouders nu niet verplicht zijn gebruik te maken van de jeugdgezondheidszorg.

Kidos wordt beheerd door de GGD, maar via het Centrum voor Jeugd en Gezin zullen betrokken jeugdzorgprofessionals toegang krijgen tot de informatiebank. Het Centrum voor Jeugd en Gezin is een samenwerkingsverband van het consultatiebureau, de GGD en Bureau Jeugdzorg. Het is bovendien de beoogde spin in het web van de gemeentelijke jeugdzorg. Daarnaast wordt Kidos gekoppeld aan de Rotterdamse VIR, genaamd SISA (SIgnaleren en SAmenwerken), om potentiële risicokinderen uit het systeem te filteren. In de toekomst zullen gegevens over kinderen uit het onderwijs (leerlingvolgsysteem, schoolmaatschappelijk werk), de jeugd-GGZ en de jeugdzorg hieraan worden toegevoegd, om een compleet beeld te krijgen. Het is de bedoeling om op basis hiervan te gaan differentiëren in het aantal contactmomenten met ouders en kinderen. Risicokinderen krijgen dan meer contactmomenten dan kinderen met wie volgens het systeem niets aan de hand is.

4.4 Kansen en kanttekeningen

Het EKD vergemakkelijkt informatieprocessen binnen de jeugdgezondheidszorg, en daarbuiten. Via de landelijke infrastructuur kunnen de gedigitaliseerde dossiers eenvoudig worden overgedragen tussen de JGZ-instellingen. Hierdoor wordt de kans kleiner dat kinderen ‘verdwijnen’ bij een verhuizing naar een andere gemeente. Het EKD zou daarnaast tot administratieve lastenverlichting kunnen leiden, wanneer na koppeling aan het elektronisch patiëntendossier bredere verwijzingsmogelijkheden binnen de gezondheidszorg mogelijk worden. De digitalisering van informatieprocessen binnen de jeugdzorg biedt tevens kansen voor een betere onderlinge afstemming van werkprocessen en voor een vroegtijdige signalering van problemen bij jongeren. De invoering van digitale dossiers in de jeugdzorg is bovendien kenmerkend voor een bredere ontwikkeling naar een informatiesamenleving, en lijkt dan ook niet meer dan een logische stap in de modernisering van dit beleidsterrein.

Deze voordelen nemen niet weg dat de digitalisering van de papieren dossiers ook minder positieve gevolgen kan hebben voor het kind. De invoering van het EKD gaat gepaard met een grotere data-intensiteit in de jeugd(gezondheids)zorg. Niet alleen kunnen meer gegevens van het kind worden vastgelegd, ook

kunnen meer instanties gemakkelijker inzage krijgen in de gegevens, of kunnen dossiers van verschillende instanties aan elkaar worden gekoppeld. Bij het EKD-groot is het de bedoeling gegevens breder te delen, om een zo compleet mogelijk beeld van kinderen te krijgen. Meer informatie leidt echter niet per definitie tot betere zorg. De grotere data-intensiteit kan het zicht vertroebelen op wat wel of niet relevante gegevens zijn. Zorgverleners moeten op zoek naar de spreekwoordelijke speld in de hooiberg. De digitalisering van het kinddossier kan daarnaast leiden tot meer interpretatieproblemen en daaruit voortvloeiende fouten, wanneer de gegevens een contextspecifieke inhoud hebben, maar door diverse partijen binnen de jeugdzorg worden gebruikt. Het streven naar een compleet beeld van het kind kan bovendien leiden tot zorgmijding bij ouders. In de media zijn berichten verschenen over hoogopgeleide ouders die vanwege een gebrek aan vertrouwen in het EKD weigeren de psychosociale vragenlijsten van de schoolarts in te vullen.

Digitalisering van data maakt bovendien de weg vrij voor het gebruik van risicoprofielen. Het is niet langer alleen de bedoeling om de ontwikkeling van een kind te volgen door het periodiek vastleggen van gegevens. Het kinddossier wordt daarnaast gebruikt voor geavanceerde analyses van het kind en zijn omgeving. Aan de hand van een reeks risicokenmerken worden inschattingen gemaakt van de kans dat individuele kinderen lichamelijke en (vooral) psychosociale ontwikkelingsproblemen zullen ontwikkelen. Risicoprofilering moet ertoe leiden dat – potentiële – probleemkinderen in een vroeg stadium in kaart worden gebracht.

Op basis van de risicoprofielen worden kinderen in een bepaalde risicocategorie ondergebracht en overeenkomstig gelabeld – denk aan het eerdere voorbeeld met de categorieën geel, oranje en rood. Daarmee verschuift de aandacht van het individuele kind naar het type kind. Het is niet ondenkbaar dat deze risicotypering leidend wordt in de manier waarop zorgverleners het kind tegemoet treden. Het label kan daarmee een stigmatiserende en zelfs discriminerende werking krijgen, en leiden tot een ongerechtvaardigd onderscheid in de wijze waarop kinderen (en ouders) worden behandeld. Ook mogelijke langetermijngevolgen van stigmatisering van kinderen verdienen de aandacht. De lange bewaartermijn van het kinddossier kan ertoe leiden dat jeugdzonden iemands latere leven beïnvloeden, door de wijze waarop hij of zij wordt beoordeeld en bejegend door de overheid (en wellicht anderen). Bovendien is het vaak onduidelijk welke grenzen worden gesteld aan het gebruik van deze gegevens.

Met de digitalisering van het kinddossier verandert de relatie tussen het kind en de zorgprofessional, doordat het kind vaker wordt gerepresenteerd door een dataset of door een daaraan verbonden risicoprofiel. Het gebruik van risicoprofielen kan een eigen werkelijkheid creëren die losstaat van het fysieke individu. Dit wordt ook wel aangeduid met de term ‘geabstraheerde identiteit’.

Zolang deze identiteit overeenstemt met de ‘echte’ werkelijkheid is er niet veel aan de hand. Anders wordt het wanneer de geregistreerde identiteit niet of onvoldoende meegroeit met de realiteit waarin het kind leeft, of incorrecte gegevens bevat. Het kan voor betrokkenen lastig zijn om data of profielen gecorrigeerd te krijgen, wanneer deze in een keten worden gebruikt en daarbinnen een eigen leven gaan leiden. Uit het jaarrapport *De burger in de ketens* van de Nationale ombudsman (2009) blijkt dat burgers tegen grote problemen kunnen aanlopen als ze verkeerd geregistreerd staan in zo’n informatieketen. Bovendien is het veelal niet duidelijk bij welke instantie betrokkenen kunnen aankloppen als er iets misgaat. De ombudsman noemt de jeugdzorg als voorbeeld van een uiterst complexe organisatie, waarbij alleen al de VIR 24 verwijzende instanties kent.

De vertrouwelijkheid van gegevens vormt tevens een probleem. Het EKD-groot is bedoeld om gegevens toegankelijk te maken voor een bredere kring van zorgprofessionals. Eerder werd al gerefereerd aan het medisch beroepsgeheim dat uitwisseling van gegevens binnen de jeugdzorg in de weg kan staan. Hoe daarmee in het Rotterdamse project wordt omgegaan is niet helder. Het is ook niet ondenkbaar dat zorgprofessionals gevoelige informatie uit het dossier houden om de vertrouwensrelatie met het kind of de ouder niet te beschadigen. Zie ook de eerder genoemde neiging van bepaalde groepen ouders om niet mee te willen werken aan een uitgebreide sociaalpsychologische screening.

Het vertrouwen van betrokkenen in het systeem kan ook aangetast worden door de centrale plaats die technologie erin krijgt. Het EKD kan een dirigerende werking krijgen door het gebruik van standaardinstellingen, keuzemenu’s of andere in de software vastgelegde werkwijzen, die de professionele autonomie van de zorgverlener inperken. Een zorgverlener die het kind moet beoordelen op basis van een standaard afvinklijst, kan afwijkende bevindingen niet melden en ziet ze wellicht ook eerder over het hoofd. De centrale rol van ICT-technologie maakt het EKD bovendien kwetsbaar voor beveiligingsrisico’s zoals een onzorgvuldige omgang met wachtwoorden of het onbevoegd binnendringen van het systeem. Deze risico’s wegen zwaarder naarmate de gevoeligheid van de data groter is. En in het geval van het EKD gaat het om gevoelige gegevens.

4.5 Het belang van het kind?

Hoe je het ook wendt of keert, de grote vraag is in welke mate het EKD bijdraagt aan het belang van het kind om zich in een veilige omgeving te ontplooien tot een gezonde, gelukkige en verantwoordelijke burger. Het bevorderen van het welzijn van kinderen vormt – naast bescherming van de samenleving tegen ontsporende jongeren – een belangrijk doel van de hier besproken varianten van de jeugdgezondheidszorg. Maar vaak wordt niet duidelijk op welke wijze de belangen, behoeften en rechten van kinderen en ouders daadwerkelijk een rol spelen. Ze worden zelden concreet gemaakt in de plannen voor het EKD.

Bij de beleidsplannen voor het EKD-groot wordt nauwelijks ingegaan op de juridische randvoorwaarden waarbinnen het moet gaan functioneren. Dit zet de legitimiteit van de ontwikkelingen op zijn minst op de tocht. Zowel de Eerste Kamer als het College bescherming persoonsgegevens heeft nadrukkelijk gewezen op fundamentele bezwaren als het gaat om de vertrouwelijkheid van gegevens en de privacy van kinderen en ouders. Bovendien is het opmerkelijk dat er voor het EKD in het algemeen geen bijzondere waarborgen voor beheer en gebruik zijn vastgelegd in formele wetgeving, zoals bijvoorbeeld wel het geval is bij het elektronisch patiëntendossier. Op dit moment lijkt snelheid belangrijker dan zorgvuldigheid als het gaat om de ontwikkeling van het dossier.

Het EKD is een sterk technologiegedreven oplossing voor een grote diversiteit aan psychosociale en gezondheidsproblemen. Het is dan ook de vraag of dit de meest effectieve benadering is voor de problemen waar de jeugdzorg mee kampt. Daarnaast is niet helder wat langetermijnconsequenties zijn van de gekozen richting – denk aan de lange bewaartermijn van gegevens – en hoe mogelijke negatieve effecten voor kinderen kunnen worden ondervangen.

4.6 Conclusies

Het is relevant om helderder te krijgen waaruit de behoeften in de jeugdzorg bestaan en hoe het EKD daarin kan voorzien. In de discussie over het EKD lopen verschillende doelen door elkaar: een efficiëntere jeugdgezondheidszorg, een verbeterde coördinatie binnen de jeugdzorg, het voorkomen van kindermishandeling en het vroegtijdig opsporen van risicojongeren. Het is onduidelijk of het EKD in alle gevallen het meest geschikte middel is om deze doelen te realiseren.

Ook is meer aandacht vereist voor de keuzen die worden gemaakt in het ontwerp van het EKD. Meer gegevens verzamelen over kinderen en de omgeving waarin ze opgroeien, leidt niet per definitie tot betere zorg. Het is zelfs de vraag of het in kaart brengen van potentiële probleemkinderen op basis van risicoprofielen zijn doel niet dreigt voorbij te schieten. Het kan immers leiden tot onwerkbaar grote aantallen (mogelijke) risicojongeren, waardoor zorgverleners het zicht wordt ontnomen op de werkelijke probleemgevallen of hen te weinig tijd rest voor benodigde ondersteuning. Veel probleemgevallen zijn ook al bekend bij de jeugdzorg. Volgens het principe van selectiviteit (*select before you collect*) zou er ook voor kunnen worden gekozen gericht gegevens te verzamelen over deze probleemgevallen, zodat passende zorg kan worden geboden.

Het is ook de vraag of het wel zo wenselijk is om kinderen en jongeren minutieus en continu in de gaten te houden. Kunnen ouders hun kinderen nog wel vrij en onbevangen laten opgroeien? Kunnen kinderen nog wel door schade en schande wijs worden?

Ten slotte is het voor alle betrokkenen – zorgverleners, kinderen en ouders – relevant dat zij weten welke gegevens verzameld worden, waarvoor die gegevens door wie worden gebruikt, en hoe fouten in registraties en profielen kunnen worden hersteld. Ouders en kinderen zouden zelfstandig toegang tot het dossier kunnen krijgen om inzage te vergemakkelijken. Deze maatregelen kunnen het vertrouwen in het EKD stimuleren.

5 Klantenprofielen: de onzichtbare hand van internet

5 Klantenprofielen: de onzichtbare hand van internet

Mireille Hildebrandt & Niels van Dijk

5.1 Inleiding: e-commerce

Data zijn de nieuwe grondstof van de informatiesamenleving. In februari 2010 wijdde *The Economist* een speciale uitgave aan de 'monsterlijke hoeveelheid data' die inmiddels beschikbaar zijn. Zoals Ayres (2007) in *Super Crunchers* beschrijft, gaat het daarbij niet meer om 10.000 of een paar miljoen gegevens, maar om biljoenen gegevens die tegen geringe kosten kunnen worden opgeslagen en razendsnel kunnen worden doorzocht. Het gaat hierbij niet alleen om door personen verstrekte gegevens, maar vooral ook door webgebruikers gelekte gegevens (surf- en klikgedrag). Om in die datalawine door de bomen nog het bos te zien, zijn computertechnieken ontwikkeld die patronen in de gegevens zichtbaar maken. Deze technieken worden aangeduid met de term datamining. De gevonden patronen worden 'profielen' genoemd.

Dataminingtechnieken worden in verschillende contexten toegepast. Banken maken gebruik van profilering om de kredietwaardigheid van klanten in te schatten of om fraude en witwaspraktijken te ontdekken. In de forensische wetenschap worden profielen gebruikt om misdrijven op te lossen of om risicoprofielen van potentiële daders op te stellen. Werkgevers kunnen profilering gebruiken om hun werknemers te controleren op frauduleus gedrag of om hun vaardigheden en geschiktheid voor bepaalde taken in te schatten.

In deze bijdrage richten we ons op profilering in de commerciële sector, meer specifiek op het gebruik van klantenprofielen op internet. Dit maakt deel uit van de bredere ontwikkeling van e-commerce. Het is hierbij van belang onderscheid te maken tussen individuele profielen die voortkomen uit het samenvoegen van allerlei gegevens over een bepaald persoon, en groepsprofielen die het resultaat zijn van meer algemene patroonherkenning. We zullen vooral ingaan op de wijze waarop deze groepsprofielen worden toegepast in het bedrijfsleven, met welke motieven dat gebeurt en welke gevolgen dit kan hebben. Ten slotte bespreken we kort welke juridische en technische instrumenten nodig zijn om onwenselijke gevolgen te beperken.

5.2 Marketing en klantenbinding

In de marketing wordt in de jaren zeventig al gepoogd dichter bij de klant te komen. In plaats van reclamecampagnes gericht op 'de gemiddelde consument' wordt gepoogd de markt in segmenten op te delen, gebruikmakend van gegevens als woonplaats, familie, sekse, leeftijd, opleiding en inkomen. Een segment staat voor een consumententype met bepaalde eigenschappen en behoeften

en elk type kan met een specifiek aanbod worden benaderd. Deze benadering kent echter beperkingen. De marktsegmenten zijn relatief statisch en stereotypisch, gebaseerd op algemene geodemografische gegevens.

Met de exponentiële groei van het opslag- en verwerkingsvermogen van computers is er inmiddels veel meer informatie over personen voorhanden. In de onlinewereld van internet laten mensen voortdurend digitale sporen achter, die door middel van cookies, web bugs en andere technieken kunnen worden achterhaald. Via mobiele apparatuur zoals telefoons en laptops komen daarnaast allerlei data voorhanden die betrekking hebben op de locatie en communicatie van de gebruiker. Deze overdaad aan gegevens vormt een goudmijn voor de commerciële sector. In combinatie met krachtige profileringstechnieken komt een veel grotere hoeveelheid kennis over individuen beschikbaar dan ooit tevoren (Hildebrandt & Gutwirth 2008).

Waar de datalawine in eerste instantie nog leidt tot een overdaad aan reclame (spam), heeft het bedrijfsleven inmiddels de weg gevonden naar steeds meer toegespitste aanbiedingen: *targeted advertising*. Marketing legt zich meer en meer toe op het herkennen van voorkeuren van (mogelijke) klanten, en is daartoe steeds beter in staat dankzij de geavanceerde dataminingtechnieken die patronen in consumentengedrag zichtbaar maken. De daarmee voortgebrachte 'kennis' van de klant is niet langer gebaseerd op vooronderstellingen van marketingbureaus of op wat klanten in focusgroepen of interviews over hun voorkeuren *vertellen*, maar op wat zij online en vaak ook offline *doen*. De gedachte hierachter is dat het geaggregeerde gedrag van klanten een betere voorspelling oplevert van toekomstig koopgedrag dan de informatie die klanten over zichzelf geven. Wie de beste technieken voor datamining in huis heeft, zal dan ook beter en sneller in kunnen spelen op wensen en voorkeuren, waarvan de klant zich misschien niet eens bewust is. Een positief gevolg voor de klant is dat hij of zij daardoor veel minder wordt lastiggevallen met irrelevante aanbiedingen.

5.3 Wat is het doel van klantenprofilering?

Het primaire doel van klantenprofielen is een betere afstemming van het aanbod van diensten en producten van een bedrijf op de behoefte van (potentiële) klanten. Het moet leiden tot vergroting van de effectiviteit van reclame, meer gerichte aanbiedingen en betere klantenbinding. Dit alles maakt deel uit van wat inmiddels heet *Customer Relationship Management* (CRM), dat zich richt op het verwerven en behouden van zoveel mogelijk lucratieve klanten. Klanten aan wie het bedrijf weinig kan verdienen of die een risico op wanbetaling vormen, worden zo veel mogelijk uitgesloten. Profilering wordt dan ook mede ingezet om de kredietwaardigheid van klanten te vergelijken.

Een andere functie van profilering is prijsdiscriminatie: welke prijs is een consument bereid te betalen voor een product of dienst? Prijsdiscriminatie is een

reguliere en in beginsel legale praktijk, die extra winst op kan leveren voor het bedrijf. Onder omstandigheden van een 'ideale markt' zou het aanpassen van de prijs aan de wensen van individuele consumenten kunnen leiden tot een win-win situatie omdat de prijs precies is afgestemd op de wensen en behoeften van de klant. In de praktijk is prijsdiscriminatie echter vaak gebaseerd op een informatieachterstand: als de klant wist dat hij of zij een bepaalde dienst elders voor minder geld had kunnen krijgen, had de klant de koop niet gesloten. De moeite die het de klant kost om daarachter te komen, werkt in het voordeel van het bedrijf, dat er dan ook belang bij heeft deze situatie in stand te houden. Internet leent zich goed voor dit soort prijsdiscriminatie. Prijsvergelijkingssites heffen de informatieachterstand van consumenten deels op, maar het is niet altijd duidelijk wat de belangen zijn van de eigenaren van deze sites (Stone 2010). Bovendien kunnen deze sites opnieuw een goudmijn aan klantengegevens opleveren die aan andere bedrijven verkocht kunnen worden en onwenselijke gevolgen kunnen hebben voor bijvoorbeeld de privacy van de klant.

5.4 Hoe werkt klantenprofilering?

Profilering wordt ingezet om inzicht te krijgen in mogelijk interessante klanten, de aanbiedingen waarin die klanten waarschijnlijk geïnteresseerd zijn, de prijs die ze bereid zijn te betalen, hun bereidheid om over te stappen naar een ander merk of juist klant te blijven. Een goed voorbeeld hiervan is Google Analytics, een van de grote spelers op de markt van webstatistieken. Omdat deze toepassing door veel bedrijven wordt gebruikt en een goed beeld geeft van de verschillende vormen van klantenprofilering, gaan we hier wat dieper op in.

Google Analytics maakt het mogelijk om in detail bij te houden wat voor type bezoekers vanuit welke site of zoekmachine op een bepaalde site zijn 'beland', hoelang zij daar verblijven, waarop ze klikken, hoe vaak ze terugkeren, en zo meer. De gegevens worden verkregen door software te plaatsen op de site van de eigenaar van de website die Google Analytics gebruikt, alsook op de computer van de bezoekers van die website. Google Analytics produceert statistische verbanden en overzichten die de gebruiker in staat stelt om zijn website zo effectief mogelijk in te richten en om geld te verdienen aan het klikgedrag van bezoekers. Dat laatste gebeurt door advertentieruimte te veilen in de omgeving van specifieke trefwoorden. Bedrijven kunnen hierop bieden als zij menen dat hun producten of diensten interessant zijn voor bezoekers van sites die het betreffende trefwoord gebruiken. Het bedrijf dat het hoogste biedt, kan adverteren en betaalt een bedrag per klik aan de eigenaar van de website. Het bedrijf kan tevens analyseren hoeveel die advertenties uiteindelijk opleveren, zodat het zich kan richten op de meest lucratieve sites.

Om te begrijpen hoe een webstatistiek als Google Analytics werkt, moeten we onderscheid maken tussen verschillende soorten profielen (Custers 2004). Ten eerste zijn er *groeps*profielen, die zijn afgeleid uit gegevens van grotere

aantallen personen, hun gedrag en de context waarin zij bepaald gedrag vertonen. Een voorbeeld hiervan is marktsegmentering. Op basis van kenmerken als de postcode, het onlinesurfgedrag, het onlinekoopgedrag of het gebruik van zoektermen worden statistisch onderbouwde indicaties afgeleid voor toekomstig gedrag, vooral aankoopgedrag of kredietrisico's. Een ander voorbeeld van een groepsprofiel is de correlatie tussen toetsenbordgedrag en de ziekte van Parkinson. Ziektekosten- of levensverzekeringsmaatschappijen kunnen hierin geïnteresseerd zijn.

Een groepsprofiel kan op het geaggregeerde niveau van het betreffende marktsegment kloppen. Maar omdat het meestal om statistische verbanden gaat, is zo'n groepsprofiel niet zomaar toepasbaar op individuele personen. In de epidemiologie is dat een welbekend probleem: het feit dat een groep met bepaalde kenmerken gemiddeld genomen een kans van 1 op 24 heeft om borstkanker te ontwikkelen, geeft geen uitsluitsel over wie van de 24 in een concreet geval borstkanker zal krijgen. Een bedrijf kan bij het toepassen van groepsprofielen op individuen de plank dus gemakkelijk misslaan. Maar omdat het gaat om grote aantallen, is de verwachting dat de toepassing ervan uiteindelijk toch veel oplevert.

Naast groepsprofielen worden er *individuele* profielen gemaakt, die zijn afgeleid uit de gegevens van één persoon. Door het opslaan en analyseren van zoveel mogelijk online- en offlinegedrag – bijvoorbeeld mijn surfgedrag, aankoopgedrag, download- en uploadgedrag, mail- en chatgedrag, mijn vriendennetwerk binnen sociale netwerken online, de blogs die ik schrijf en de zoektermen die ik gebruik – kunnen patronen zichtbaar worden die kennis opleveren over mijn interesses, voorkeuren, de volgorde waarin ik dingen doe en mijn dag- en nachtritme.

De combinatie van een individueel profiel met groepsprofielen kan leiden tot inzicht in het doel van mijn bezigheden, het risico op ziekte, ongevallen of andere vormen van schade, belastingontduiking of andere vormen van regelovertreding, en een rangorde in mijn wensen en mogelijkheden. We kunnen daarbij denken aan uiteenlopende aspecten als welke krant ik lees, hoe mijn inkomen zich waarschijnlijk zal ontwikkelen, hoeveel geld ik uit wil geven aan een auto, welk type ondergoed ik draag, wat voor films ik graag zie of hoeveel ik uit wil geven aan de kermis dan wel een dansvoorstelling. Het mag duidelijk zijn dat zulke gepersonaliseerde profielen 'goud' waard zijn. De door het bedrijfsleven vaak beleden mantra van gratis *content*, bijvoorbeeld een gratis onlinekrant, in ruil voor het mogen opslaan en analyseren van data bevestigt dan ook de volkswijsheid: *there is no such thing as a free lunch*.

5.5 Onwenselijke gevolgen

Wanneer groepsprofielen op individuen worden toegepast, zullen vaak onjuiste verbanden worden gelegd, zoals hierboven is uiteengezet. Een onwenselijk

gevolg hiervan is dat een eventuele in- of uitsluiting vaak onjuist zal zijn, nog los van de vraag hoe rechtvaardig dat is. Afhankelijk van de specifieke context, kan dat kleinere of grotere nadelen met zich meebrengen voor een individuele klant: bepaalde aanbiedingen kunnen haar worden onthouden, ze moet een hogere premie betalen, ze wordt uitgesloten van een verzekering, et cetera. We richten ons hier op drie onwenselijke gevolgen die ook optreden als de gelegde verbanden *wel* juist zijn: onzichtbare schendingen van de privacy, oneerlijke vormen van uitsluiting en gebrek aan *due process* (Zarsky 2002-2003).

5.5.1 Schending van de privacy

In de wereld van ICT wordt privacy vaak uitgelegd in termen van bescherming van persoonsgegevens. Dat is een wat schrale definitie. Bescherming van persoonsgegevens is één manier om privacy te beschermen. Privacy is in onze ogen een ruimer begrip, dat door Agre en Rotenberg als volgt onder woorden is gebracht: het recht op privacy in de informatiesamenleving is "(…) het recht om vrij te zijn van onredelijke beperkingen op de constructie van de eigen identiteit" (Agre & Rotenberg 2001, p. 7). 'Identiteit' wordt hierbij niet begrepen als een verzameling persoonsgegevens, maar als de manier waarop iemand zijn of haar eigen identiteit vormgeeft en ontwikkelt in relatie tot anderen. Dat strekt zich uit tot het beeld dat anderen (waaronder het bedrijfsleven) creëren van die identiteit.

Stel dat mijn toetsenbordgedrag matcht met een vergroot risico op de ziekte van Parkinson, of dat uit mijn vriendenkring op Facebook wordt afgeleid dat ik waarschijnlijk homoseksueel ben (Jernigan & Mistree 2009). Het is onwenselijk dat anderen op voor mij onzichtbare wijze kennis verkrijgen van zulke gevoelige persoonlijke informatie, en daar mogelijk naar handelen.

Maar het gebruik van dit soort informatie kan ook nog een stap verder gaan. Stel dat mijn surf- en klikgedrag wordt geregistreerd zonder dat ik daarbij wordt geïdentificeerd – bijvoorbeeld doordat ik aan de hand van mijn toetsenbord- en muisgedrag als dezelfde persoon word herkend. Mijn naam, adres en IP-adres (dat meestal als persoonsgegeven wordt aangemerkt) zijn voor die 'herkenning' niet nodig, waardoor onduidelijk is of het wettelijke regiem van gegevensbescherming van toepassing is. Het aldus gevormde individuele profiel wordt vervolgens gematcht met diverse groepsprofielen. Daaruit wordt bijvoorbeeld afgeleid dat ik op het punt sta voortaan vegetarisch te gaan eten. Deze informatie wordt verkocht aan een landelijke kruidenier waar ik online mijn boodschappen bestel. Deze kruidenier schat op grond van webstatistieken in dat de kans dat ik van mijn voornemen afzie aanzienlijk toeneemt als ik wat gratis vleesproducten krijg bij mijn volgende bestelling. Aldus wordt getracht om mijn voorkeur voor vegetarische producten te beïnvloeden. Dat zou ook kunnen gebeuren door het plaatsen van gepersonaliseerde *banners* bij websites die ik regelmatig bezoek, waarin wordt verwezen naar wetenschappelijk onderzoek dat de negatieve gezondheidseffecten van een vleesloos dieet belicht. Het kan

goed zijn dat ik naar aanleiding van die aanbiedingen en *advertorials* besluit om toch maar vlees te blijven eten.

Dit soort beïnvloeding komt neer op een grotere aantasting van mijn autonomie – en daarmee samenhangend, van mijn privacy – dan het simpele feit dat bepaalde gegevens bij anderen bekend zijn. In het genoemde voorbeeld wordt immers achter mijn rug kennis over mijn voorkeuren gegenereerd en gebruikt. Op basis van geanonimiseerde groepsprofielen waarvan ik geen weet heb word ik gecategoriseerd en tot bepaald koopgedrag verleid. Of sterker nog: mijn voorkeuren worden beïnvloed door doelgerichte interventies waarvan ik mij niet bewust ben. Dit is een vorm van subliminale beïnvloeding.

5.5.2 Ongerechtvaardigde uitsluiting

Ongerechtvaardigde uitsluiting in het tijdperk van datamining is extra problematisch omdat het een onzichtbaar probleem betreft. Werkgevers kunnen bij sollicitaties softwareprogramma's gebruiken die uitgebreide profielen maken van kandidaten op basis van informatie die zij op internet hebben gelekt. Niet alleen kan dat als een inbreuk op de privacy worden beschouwd, voor zover de kandidaat wordt beoordeeld op basis van informatie die hij of zij zelf ziet als onderdeel van zijn of haar privéleven. Tevens kunnen factoren een rol gaan spelen die normaliter niet mee mogen tellen bij de selectieprocedure. Zo kan de profilering onthullen dat de sollicitant zwanger is of aan een bepaalde ziekte lijdt, hetgeen zaken zijn waarnaar de werkgever in de sollicitatiegesprekken niet mag vragen. Datamining maakt het namelijk mogelijk om gevoelige informatie van medische aard af te leiden uit een veelheid van triviale gegevens (Custers 2004). Het feit dat deze profilering zich achter onze rug afspeelt, maakt het ook lastig, zo niet onmogelijk, om je tegen uitsluiting te verdedigen.

5.5.3 Gebrek aan due process

Due process verwijst naar het beginsel dat de overheid de rechten moet respecteren die toekomen aan een persoon. Zo hebben individuen recht op een eerlijke behandeling en moeten ze de mogelijkheid hebben om beslissingen of handelingen aan te vechten. Transparantie maakt deel uit van due process, evenals de mogelijkheid om onafhankelijk vast te (laten) stellen op grond waarvan beslissingen zijn genomen en in hoeverre een beslissing in strijd is met bijvoorbeeld de privacy, *fair play* of non-discriminatie. In meer algemene zin gaat het om de mogelijkheid om handelingen of beslissingen aan te vechten die een bepalende invloed hebben, ook als het niet om overheidshandelen gaat.

Onzichtbare profilering is problematisch omdat het niet mogelijk is bezwaar te maken tegen iets wat verborgen blijft. Hoewel er transparantierechten zijn geformuleerd in de Europese Richtlijn Gegevensbescherming, is het niet eenvoudig om daar handen en voeten aan te geven. Artikel 12 van de Richtlijn kent personen het recht toe kennis te nemen van 'de logica van de gegevensverwerking'. Op dit moment is het echter niet mogelijk om als consument

inzicht te krijgen in de manier waarop je wordt geprofileerd. Zelfs als een bedrijf bereid zou zijn om daarover informatie te verstrekken, beschikt een consument niet over mogelijkheden om te controleren of die informatie klopt. Daar komt bij dat het recht om te weten hoe men wordt geprofileerd volgens de preambule (overweging 41) van de Richtlijn moet worden afgewogen tegen het bedrijfsgeheim en de intellectuele rechten op databanken, software en mogelijk ook de profielen zelf (Van Dijk 2009 & 2010).

5.6 Conclusies: controle en feedback

Over de positieve aspecten van klantenprofielen zijn we hier noodzakelijkerwijs kort. E-commerce biedt nieuwe en veelbelovende kansen om bij te dragen aan meer welvaart en welzijn. Om die kansen te benutten is echter meer aandacht nodig voor de positie van de consument. Individuele consumenten hebben nauwelijks zicht op wat voor gegevens over hen op internet worden verzameld en wat daar vervolgens mee gebeurt. Het is van belang dat de nationale en de Europese wetgevers effectieve bescherming bieden tegen de onwenselijke gevolgen van klantenprofilering (Hildebrandt & Koops 2010). Dat kan bijvoorbeeld door *controle door* en *feedback voor* de klant in te bouwen in de software en hardware die klantenprofilering mogelijk maken.

Controle betekent dat het technisch mogelijk en gemakkelijk is om gegevens achter te houden of te anonimiseren. Daarvoor is inmiddels een verscheidenheid aan *privacy enhancing technologies* (PETs) ontworpen (Borking & Raab 2001, Dolinar et al. 2009).

Feedback betekent dat iemand zicht kan krijgen op de gevolgen die anderen verbinden aan zijn of haar onlinegedrag. Dat kan bijvoorbeeld door bedrijven te verplichten aan te geven op grond waarvan zij de klant bepaalde aanbiedingen wel of niet doen. Tegelijk moet het voor de klant mogelijk zijn om snel en eenvoudig te controleren of die informatie klopt. Daartoe moeten *transparency enhancing technologies* (TETs) worden ontwikkeld. Als ik bijvoorbeeld kan zien dat ik word geprofileerd als iemand die op het punt staat te stoppen met roken, kan ik de gratis aangeboden sigaretten 'plaatsen' als een poging om mij daarvan af te houden. Als ik kan zien dat ik ben ingedeeld in de categorie wanbetalers vanwege een combinatie van postcode en een incident rond een niet-betaalde rekening van enkele jaren geleden, moet ik bezwaar kunnen maken tegen die indeling.

Inzicht in de processen van klantenprofilering is een voorwaarde voor de individuele consument om de rechten uit te oefenen die hem of haar toekomen. Alleen zo worden consumenten ook in staat gesteld intelligenter om te gaan met de stroom aan gegevens die zij genereren als zij hun commerciële gedrag in toenemende mate verplaatsen naar internet.

De schaduwzijden van het Schengen Informatie Systeem

6

6 De schaduwzijden van het Schengen Informatie Systeem

Michiel Besters

6.1 Inleiding: een Europese database

Met de inwerkingtreding van de interne markt in het Schengengebied in 1995 worden de binnengrenzen opgeheven tussen België, Duitsland, Frankrijk, Luxemburg, Nederland, Portugal en Spanje. De buitengrenzen van het Schengengebied vormen vanaf dat moment het belangrijkste controlepunt voor personen en goederen die de Schengenlidstaten in- of uitreizen. Door de opheffing van de grenscontroles tussen de afzonderlijke lidstaten wordt het noodzakelijk maatregelen te treffen voor de handhaving van de publieke orde en veiligheid binnen het Schengengebied. Deze maatregelen zijn vastgelegd in de Schengen Uitvoeringsovereenkomst uit 1990. Een van deze maatregelen betreft de invoering van een informatiesysteem ter ondersteuning van de samenwerking tussen de politiële en justitiële autoriteiten van de lidstaten: het Schengen Informatie Systeem (SIS).

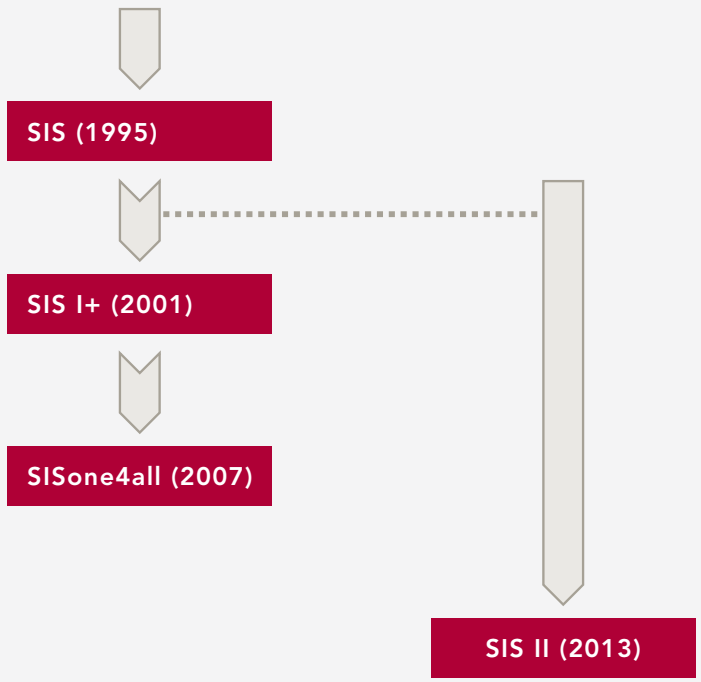
Deze bijdrage beschrijft de ontwikkeling van het Schengen Informatie Systeem door de jaren heen. Ze gaat in op de wijze waarop personen in het SIS worden geregistreerd, de rechtspositie van die personen, het toezicht dat plaatsvindt op het functioneren van het systeem en de technische en organisatorische problemen waar het tegenaan loopt.

In het SIS worden personen en goederen geregistreerd die de toegang tot het Schengengebied moet worden geweigerd of die juist door een Schengen-lidstaat worden gezocht, zoals ongewenste vreemdelingen, vermiste personen, gestolen auto's of identiteitsdocumenten. Een registratie betekent dat er een 'signalering' in het SIS wordt geplaatst. In totaal staan er momenteel meer dan 31 miljoen signaleringen in het SIS, waarvan ruim 25 miljoen identiteits-documenten, bijna vier miljoen voertuigen en één miljoen personen. Meer dan 75% van het aantal personen staat gesignaleerd als ongewenste vreemdeling. Hieronder vallen bijvoorbeeld niet-EU-onderdanen met een visumverplichting waarvan de vrije verblijfstermijn is overschreden.

In de loop der jaren is het aantal Schengenlidstaten sterk gegroeid. Als in 1996 de Scandinavische landen lid worden van het Schengen Verdrag, moet het SIS worden uitgebreid. De technische capaciteit van het SIS is op dat moment ontoereikend om de nieuwe lidstaten te kunnen integreren. Er wordt besloten een tweede generatie SIS (SIS II) te ontwikkelen. Deze moet niet alleen de toegang voor nieuwe lidstaten, maar ook nieuwe technische functies mogelijk maken. Als duidelijk wordt dat SIS II niet voor de millenniumwisseling gereed

zal zijn, wordt besloten tot een tijdelijke capaciteitsuitbreiding van het SIS, om de Scandinavische landen alvast toegang te kunnen geven tot het systeem. Deze tijdelijke oplossing wordt SIS I+ genoemd. Het belang van de ontwikkeling van SIS II wordt nog groter in 1999, als een aantal bepalingen uit het verdrag (het Schengenacquis) in het Verdrag van de Europese Unie wordt geïntegreerd. De buitengrenzen van het Schengengebied komen hierdoor gelijk te staan aan die van de Europese Unie. Dit betekent ook dat alle EU-lidstaten toegang tot het SIS moeten kunnen krijgen.

Aanvankelijk is het de bedoeling om SIS II in 2006 klaar te hebben, op het moment dat de Oost-Europese landen lid van de EU werden. Door vertragingen in de ontwikkeling van SIS II is dit echter niet gelukt. Een tijdelijke technische aanpassing van SIS I+ moet uitkomst brengen: SISone4all, de huidige versie van het systeem. In 2009 is de oplevering van SIS II opnieuw uitgesteld, ten minste tot 2013. Deze gang van zaken is niet ideaal, zoals voormalig minister Ter Horst van Binnenlandse Zaken en Koninkrijksrelaties heeft opgemerkt: "Ik zal niet zeggen dat het [huidige systeem, MB] houtje-touwtje is, maar het is minder geavanceerd dan mogelijk" (ANP 15-01-2009).



Figuur 1: een chronologische weergave van de diverse varianten van het SIS.

Door de aanwas van nieuwe lidstaten zijn de uitvoeringspraktijk en de politieke besluitvorming steeds complexer geworden. Dit maakt de ontwikkeling van de eerste en tweede generatie SIS welhaast tot sisyfusarbeid. De complexe politieke besluitvorming heeft geresulteerd in een grote stroom aan informatie: voorstellen van de Europese Commissie, besluiten van de Raad van de Europese Unie en verslagen en werkdocumenten van verschillende werkgroepen. Deze grote hoeveelheid informatie maakt het moeilijk om de ontwikkelingen rond de eerste en tweede generatie SIS scherp in het vizier te krijgen. Dit heeft in 2003 stevige kritiek opgeleverd van het Europees Parlement. De aanpak met betrekking tot SIS II was volgens het parlement "(…) zeer ondoorzichtig, zelfs voor deskundigen moeilijk te volgen en voor leken helemaal niet te vatten" (Europees Parlement 2003, p. 12).

6.2 Signalering van personen

Het SIS kent vijf soorten signaleringen voor personen: (1) uitlevering, (2) weigering toegang tot het Schengengebied, (3) vermissing, (4) getuigen of veroordeelden en (5) verdachten en staatsgevaarlijke personen. Naast personalia worden, afhankelijk van het soort signalering, gegevens ingevoerd over de reden van registratie, de te nemen maatregelen en of een persoon bijvoorbeeld gewapend of gewelddadig is. Per dag worden ongeveer een miljoen signaleringen ingevoerd, gewijzigd of verwijderd.

Het SIS is een 'hit – no hit'-systeem. Wanneer een persoon op de grens of in het Schengengebied wordt gecontroleerd en in het systeem staat geregistreerd, dan genereert het systeem een 'hit'. Een hit kan leiden tot aanhouding of uitzetting van de betreffende persoon, of inbeslagname van goederen. In 2008 heeft het SIS ruim 120.000 hits gegenereerd, waarvan ongeveer 6500 in Nederland.

De beslissing een signalering van een persoon of object in het SIS op te nemen, ligt bij de politiële en justitiële autoriteiten van de lidstaten. In Nederland kan onder andere de Immigratie en Naturalisatie Dienst (IND) deze beslissing nemen. Het nationale recht van een lidstaat is bepalend voor de beoordeling van de 'Schengenwaardigheid' van een signalering. Zo valt in Spanje het niet nakomen van alimentatieverplichtingen onder het strafrecht, en kan dat – in Spanje – leiden tot een signalering in het SIS. Dit in tegenstelling tot Nederland, waarin dit een civielrechtelijke aangelegenheid is.

Het besluit van een lidstaat iemand tot ongewenst vreemdeling te verklaren, betekent dat alle lidstaten de betreffende persoon de toegang tot het Schengengebied moeten weigeren. Dit kan ingrijpende gevolgen hebben voor de persoon in kwestie. Indien bijvoorbeeld het besluit tot ongewenstverklaring afkomstig is van de minister van Justitie, kan die persoon de toegang worden ontzegd voor een periode van tientallen jaren.

6.3 Architectuur

Het SIS bestaat uit twee delen: een centraal deel (C.SIS) dat in Straatsburg is gevestigd, en een nationaal deel (N.SIS) dat in de lidstaten is ondergebracht. De lidstaten zijn verantwoordelijk voor registraties in het nationale systeem. In totaal zijn er meer dan een half miljoen terminals aanwezig in de Schengenlidstaten met toegang tot het SIS. Om de informatie uit een nationaal systeem voor andere lidstaten beschikbaar te maken, wordt het N.SIS gesynchroniseerd met het centrale systeem. De nationale systemen vormen derhalve de actieve delen van de eerste generatie SIS.

Voor SIS II is gekozen voor een andere verhouding tussen de centrale en nationale systemen. In SIS II worden de gegevens via een nationale interface direct in de centrale database gestopt – eveneens gevestigd in Straatsburg, met een back-upsysteem in Sankt Johann im Pongau (Oostenrijk). De nationale systemen functioneren als een soort doorgeefluik. Lidstaten kunnen er daarnaast voor kiezen een kopie van de gegevens in het nationale deel op te slaan. Het zwaartepunt van SIS II ligt daarmee meer bij het centrale systeem.

Tijdens de ontwikkeling van SIS II is gekozen voor een flexibele architectuur om het systeem toekomstbestendig te maken. De architectuur is zo ontworpen dat de technische mogelijkheden voor nieuwe functies al in het systeem liggen verankerd. Deze latente functies kunnen dan op basis van een gezamenlijk besluit van de lidstaten worden geactiveerd. Voor deze oplossing is gekozen om de bouw van SIS II niet te laten blokkeren door de onderhandelingen tussen de lidstaten over die nieuwe functies. In de architectuur zijn vijf nieuwe functies ingebouwd:

- bredere toegang voor nationale en internationale veiligheids- en opsporingsdiensten zoals Interpol, Europol en Eurojust;
- biometrische identificatie, door toevoeging van vingerafdrukken in een ondersteunende database;
- nieuwe signaleringen: van terreurverdachten, hooligans en ontvoerde kinderen;
- koppeling van signaleringen, bijvoorbeeld van criminelen aan terreurverdachten;
- koppeling aan het Visum Informatie Systeem, waarin personen worden geregistreerd die een visumaanvraag indienen.

Ter ondersteuning van het SIS zijn nationale SIRENE-bureaus (*Supplementary Information REquest at the National Entry*) opgericht. In Nederland is het SIRENE-bureau ondergebracht bij het Korps Landelijke Politiediensten te Zoetermeer. De SIRENE-bureaus vormen de menselijke schakel in het SIS. Zij hebben een controlerende taak met betrekking tot de signaleringen die in het systeem worden gezet. Daarnaast kan een SIRENE-bureau worden gevraagd om aanvullende informatie te verstrekken aan politiële en justitiële autoriteiten van andere lidstaten.

6.4 Rechtspositie van personen

Registratie binnen het SIS kan grote gevolgen hebben voor de betreffende persoon, bijvoorbeeld als hij of zij tot ongewenst vreemdeling wordt verklaard. Aandacht voor de rechtspositie van personen is dan ook van groot belang. Vanuit dit perspectief kunnen kritische kanttekeningen worden geplaatst bij het functioneren van het SIS. Zo vormt de interpretatie van de criteria om een persoon te signaleren door de afzonderlijke lidstaten een heikel punt, want het leidt tot rechtsongelijkheid binnen Europa. Uit een rapport van de Algemene Rekenkamer blijkt zelfs dat er kort na de invoering van SIS in Nederland tussen de 25 regiokorpsen grote verschillen bestonden in de hantering van de criteria voor de signalering van personen (Tweede Kamer 1996-1997a). Daarnaast laat onderzoek van nationale dataprotectieautoriteiten, in opdracht van de Gemeenschappelijke Controle Autoriteit Schengen, zien dat er ook tussen lidstaten grote interpretatieverschillen bestaan (Joint Supervisory Authority of Schengen 2005, 2007, 2009a & 2009b).

Een voorbeeld van dit laatste is de signalering door de Duitse autoriteiten van afgewezen asielzoekers als ongewenste vreemdelingen. De Franse Conseil d'État (Raad van State) heeft in 1999 geoordeeld dat deze signaleringen onwettig zijn. Volgens de Schengen Uitvoeringsovereenkomst mag een persoon alleen als ongewenste vreemdeling worden geregistreerd als het gaat om een 'derdelander' die een reëel gevaar vormt voor de publieke orde en veiligheid van een lidstaat, of zich schuldig heeft gemaakt aan illegale immigratie. Het simpele feit dat een asielaanvraag is afgewezen, valt niet onder dit criterium. Uit rapporten van de Duitse dataprotectieautoriteiten blijkt echter dat de politiële en justitiële autoriteiten in 2004 nog steeds afgewezen asielzoekers als ongewenste vreemdeling in het SIS signaleerden.

Het is overigens maar de vraag of met de komst van SIS II de harmonisatie van criteria voor de signalering van personen zal verbeteren. De Britse mensenrechtenorganisatie JUSTICE heeft hiervan geen hoge verwachtingen (House of Lords 2007). Zij baseert zich hiervoor op het verschil tussen de voorgestelde en de definitieve verordening voor SIS II. In het oorspronkelijke voorstel stond dat de criteria voor signaleringen moesten worden geharmoniseerd. In de uiteindelijk aangenomen verordening is deze noodzaak tot harmonisatie afgezwakt. Daarin staat slechts dat 'het beraad over de harmonisatie moet worden voortgezet'.

De rechtspositie van personen behoeft ook om een tweede reden aandacht. De rechtsbescherming van geregistreerde personen blijkt diverse lacunes te vertonen. Een eerste lacune is dat ongewenste vreemdelingen niet op de hoogte worden gesteld van hun signalering in het SIS. In Nederland wordt hun wel verteld dat zij 'ongewenst' zijn verklaard, maar niet dat zij in het SIS worden gesignaleerd. Daar komen ze pas achter als ze Europa weer in willen reizen. Met dit eerste punt hangt een tweede samen: het uitoefenen van het inzage-, correctie- en verwijderingsrecht door gesignaleerde personen. In de Schengen

Uitvoeringsovereenkomst wordt voor de uitoefening van deze rechten verwezen naar het nationale recht van de lidstaten. Maar volgens jurist Evelien Brouwer ontbreken dikwijls effectieve procedures om een signalering aan te vechten (Brouwer 2008).

Als een persoon vervolgens zijn inzage-, correctie- of verwijderingsrecht wil uitoefenen, treden er regelmatig complicaties op. In de Schengen Uitvoeringsovereenkomst staat bijvoorbeeld dat de uitspraak van een rechter uit een lidstaat bindend is voor alle lidstaten. In de praktijk is dit vaak *wishful thinking*. In diverse zaken oordeelde een Nederlandse rechter dat de signalering van een persoon door Spaanse autoriteiten onrechtmatig was, en dat de signalering uit het systeem moest worden verwijderd. Maar hieraan werd pas gevolg gegeven na bemiddeling door het College bescherming persoonsgegevens en de Spaanse dataprotectieautoriteit.

6.5 Toezicht en controle

Ook op het gebied van toezicht en controle valt er het nodige aan te merken op de manier waarop het SIS functioneert. In Nederland is de IND verantwoordelijk voor de meeste signaleringen van personen. Het gaat dan om vreemdelingen die de toegang tot het Schengengebied moet worden geweigerd. Bij grenscontroles worden ongewenste vreemdelingen aangehouden door de Koninklijke Marechaussee, die vervolgens een voorstel tot signalering indient bij de IND. Uit een onderzoek van de Nationale ombudsman blijkt dat de IND het voorstel tot signalering vrijwel altijd overneemt van de Koninklijke Marechaussee, zonder zelf een inhoudelijke afweging te maken (Nationale ombudsman 2010). Hierdoor kan een lichte misstap – zoals het overschrijden van de vrije verblijfstermijn met enkele dagen – al tot een signalering in het SIS leiden.

Voor alle andere persoonsregistraties is de officier van justitie eindverantwoordelijk. De officier van justitie beslist op basis van een onderliggend dossier of een signalering aan de criteria van het Schengen Verdrag voldoet. Uit onderzoek van het College bescherming persoonsgegevens blijkt echter dat deze onderliggende documentatie niet altijd beschikbaar is, waardoor de rechtmatigheid van de registraties niet kan worden getoetst (College bescherming persoonsgegevens 2008).

Daarnaast is kritiek uitgeoefend op het gegevensbeheer binnen het SIS. In het ontwerp van het Nederlandse nationale systeem voor SIS I was niet voorzien in de mogelijkheid overzichten te maken van ingevoerde, uitstaande en in te trekken signaleringen. Om die reden, zo stelt de Algemene Rekenkamer in een rapport uit 1997, bood het systeem onvoldoende mogelijkheden om bestandsvervuiling tegen te gaan en de effectiviteit van het systeem te evalueren (Tweede Kamer 1996-1997a). Naar aanleiding van het rapport van de Algemene Rekenkamer zijn de voorzieningen om een effectief gegevensbeheer mogelijk te maken in 1999 alsnog geregeld.

Op Europees niveau doen zich vergelijkbare problemen voor. Rapportages worden sinds de invoering van het SIS onregelmatig en via verschillende kanalen gepubliceerd. Volgens kritiek van het Europees Parlement leidt deze aanpak tot geheimzinnigheid over de gegevens, wat democratische controle op het functioneren van het systeem bemoeilijkt (Europees Parlement 2003). Momenteel worden er wel jaarlijks statistieken gepubliceerd door de EU, maar alleen van het centrale systeem. Rapportages blijven daardoor onvolledig en incorrect.

Het Europees Parlement heeft herhaaldelijk gepleit voor de instelling van een agentschap dat het strategisch beheer voert over het SIS en andere grootschalige Europese informatiesystemen zoals het Visum Informatie Systeem. Dit agentschap zou het functioneren van die informatiesystemen transparanter moeten maken en de democratische controle erop vergroten. In 2009 heeft de Europese Commissie een voorstel gepubliceerd voor zo'n agentschap. Het is een ambitieus voorstel, waarin het agentschap niet alleen de verantwoordelijkheid krijgt voor het operationele beheer van databases, maar ook een expertisecentrum moet worden. De *European Data Protection Supervisor* heeft positief gereageerd op het voorstel van de Europese Commissie, maar maant tot voorzichtigheid: een agentschap zou alleen moeten worden opgericht als zijn taken en verantwoordelijkheden duidelijk zijn afgebakend. Volgens het EDPS is dat in het huidige voorstel niet het geval (European Data Protection Supervisor 2010).

6.6 De toekomst van SIS II

Het belang van oplevering van SIS II is in de loop der jaren steeds urgenter geworden. De ontwikkeling van SIS II heeft echter de nodige vertraging opgelopen. Onduidelijkheid over de begrotingsmiddelen, problemen tijdens de aanbestedingsfase en de onderhandelingen over nieuwe functies van het systeem zijn hiervan de oorzaak. Wat dat betreft lijkt de geschiedenis zich te herhalen. De eerste generatie SIS kampte met vergelijkbare problemen. Recente ontwikkelingen tijdens de testfase van SIS II hebben ertoe geleid dat er door de Raad van de Europese Unie en de Europese Commissie van een heuse crisis wordt gesproken.

Tijdens een test van SIS II in 2008 zijn verschillende problemen geconstateerd. Gegevens uit het nationale en het centrale deel bleken niet overeen te komen, signaleringen verdwenen of kwamen dubbel voor, en het centrale systeem bleek niet bestand tegen de invoer van de hoeveelheid gegevens. Het capaciteitsprobleem van het centrale systeem lijkt het grootste probleem. Het centrale deel is ontworpen om 15 miljoen signaleringen te kunnen verwerken. Momenteel staan er al meer dan 31 miljoen signaleringen in SIS II, en dit aantal zal alleen maar groeien door de deelname van nieuwe lidstaten. Met het oog op de uitbreiding van de lidstaten moet het centrale systeem probleemloos kunnen blijven functioneren tot 60 miljoen signaleringen, zo blijkt uit een voortgangsrapportage over SIS II uit 2009 (Council of the European Union 2009).

Om de crisis van SIS II te bezweren zijn er de nodige maatregelen getroffen. Uit voorzorg voor het eventuele mislukken van SIS II is er een alternatief scenario verkend. Daarnaast zijn externe IT- consultants aangetrokken die een diagnose van SIS II hebben opgesteld. Deze diagnose is gematigd positief: met wat reparatiewerkzaamheden en verbeteringen zou het ontwerp van SIS II gered kunnen worden. Ondanks deze positieve diagnose is er toch voor gekozen het noodplan verder uit te werken. Dit geeft de indruk dat de Europese Commissie en de lidstaten er nog niet van overtuigd zijn dat het goed komt met SIS II.

Door de vertragingen neemt het belang van het oplopende kostenplaatje alleen maar toe. De ontwikkeling van het centrale systeem van SIS II wordt betaald uit EU-gelden. Deze kosten bedragen tot 2013 meer dan 140 miljoen euro. De kosten voor de ontwikkeling van de nationale systemen komen voor rekening van de lidstaten. Tot nog toe bedragen deze kosten voor Nederland ongeveer 21 miljoen euro, terwijl aanvankelijk een bedrag van 14 miljoen euro was begroot. De vertraging die is veroorzaakt door de problemen tijdens de testfase van SIS II, kost Nederland namelijk nog eens zeven miljoen euro extra voor ontwikkelingskosten van het nationale systeem. Daarbij komen nog de kosten voor het in de lucht houden van het oude systeem. Deze kosten zijn door het Ministerie van Binnenlandse Zaken geschat op drie miljoen euro (Computable 2009).

Voormalig minister Ter Horst van Binnenlandse Zaken en Koninkrijksrelaties heeft in januari 2009 laten weten dat er hoe dan ook een opvolger komt voor de eerste generatie SIS. Voorlopig hebben de lidstaten ervoor gekozen verder te gaan met het initiële ontwerp van SIS II. De redenering hierachter lijkt te zijn dat er al zoveel geld in SIS II is gestoken, dat het zonde is om de ontwikkeling ervan stop te zetten. De toekomst zal uitwijzen of dit een juiste politieke keuze is geweest. Bezwijkt het miljoenen verslindende SIS II alsnog onder zijn eigen gewicht en moeten er aanzienlijke kosten worden gemaakt voor de realisatie van een noodplan? Of lukt het SIS II om zich met een Von Münchenhausen-act aan de lusjes van zijn laarzen uit het moeras omhoog te trekken?

6.7 Conclusies: SISyfusarbeid

Door de opheffing van de binnengrenzen in het Schengengebied ontstaat er een duidelijke behoefte aan Europese informatiesystemen als het SIS, waarmee politiële en justitiële autoriteiten informatie kunnen uitwisselen. Maar zoals we hebben kunnen zien, verloopt de ontwikkeling van het SIS allesbehalve vlekkeloos. Vanaf het begin kampt het systeem met aanloopproblemen. Sindsdien is het door de uitbreiding van het aantal Schengenlidstaten en de voorgenomen functie-uitbreiding alleen maar verder onder druk komen te staan. Behalve met technische en bestuurlijke problemen heeft het SIS te maken met lacunes in de rechtspositie van geregistreerde personen. Ook laat het toezicht op het functioneren van het systeem te wensen over.

Gezien bovenstaande kanttekeningen dringt de vraag zich op of een database van deze orde van grootte en complexiteit wel naar behoren *kan* functioneren. In ieder geval kan worden geconcludeerd dat een database voor 27 lidstaten zijn beperkingen kent. Indien hiermee geen rekening wordt gehouden, dan is het SIS welhaast gedoemd om een 'wrak vehikel' te worden – om de woorden van Jaap de Hoop Scheffer uit zijn tijd als Tweede Kamerlid te gebruiken (Tweede Kamer 1996-1997b).

Dankwoord

Graag wil ik een aantal mensen bedanken die mij hebben geholpen bij mijn sisyfusarbeid, in willekeurige volgorde: E. van Beek en L. Kröner (College bescherming persoonsgegevens), P. van Dorst (Nationale ombudsman), P. Michael (Raad van de Europese Unie), R. Rinkens (Europese Commissie), D. Hoogenboezem, S. Lasschuit-Lavalaye, C. Michel, W. van der Zwan, W. Ruytenbeek, J. Hoogesteger en P. Tazelaar (Korps Landelijke Politiediensten), W. Schel (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties), H. Dijstelbloem en D. Broeders (WRR), G. Munnichs en M. Schuijff (Rathenau Instituut).

Dynamiek in de gemeentelijke basisadministratie

7

7 Dynamiek in de gemeentelijke basisadministratie

Ellen Boschker, Peter Castenmiller & Arre Zuurmond

7.1 Inleiding

Het is van alle tijden dat overheden gegevens van hun onderdanen registreren. De opmars van informatie- en communicatietechnologie (ICT) gedurende de twintigste eeuw heeft een belangrijke invloed gehad op deze registraties. De omvang en de kwaliteit van registraties zijn daarmee sterk toegenomen. Ook is de functie van registraties veranderd. Sommige registraties hebben de functie van basisregistratie gekregen. Hiermee wordt een register bedoeld dat in de gegevenshuishouding van overheden en verwante organisaties fungeert als authentieke bron van gegevens over objecten of personen. In Nederland hebben we bijvoorbeeld de gemeentelijke basisregistratie persoonsgegevens (GBA), de basisregistratie adressen en gebouwen (BAG), de basisregistratie kadaster en topografie en de basisregistratie bedrijven. Het stelsel van basisregistraties heeft tot doel de onderlinge gegevensuitwisseling tussen overheden, overheidsorganisaties en zorginstellingen, en daarmee de kwaliteit van overheidsdiensten en zorg, te verbeteren.

De discussie rond basisregistraties heeft meestal betrekking op een zo efficiënt mogelijke inrichting ervan, waarbij het gemak van de burger vooropstaat. Ten onrechte raakt daardoor de bredere politieke en maatschappelijke betekenis van basisregistraties op de achtergrond. Dit politieke en maatschappelijke belang van basisregistraties wordt in dit essay uitgewerkt aan de hand van de gemeentelijke basisadministratie persoonsgegevens. Op basis van een historische schets van de ontwikkeling van de GBA willen we in dit essay laten zien dat basisregistraties niet alleen nodig zijn voor het zo goed mogelijk functioneren van de overheid, maar dat zij tevens van betekenis zijn voor de rechtsstaat en de samenleving. We betogen dat in het gebruik van basisregistraties een spanning tussen beheersing en emancipatie schuilt. Basisregistraties kunnen zowel als instrument van de overheid worden ingezet om de samenleving te beheersen, als een emancipatoire functie voor de samenleving vervullen.

Dit argument wordt als volgt uitgewerkt. In de volgende paragraaf wordt de modernisering van de gemeentelijke basisadministratie persoonsgegevens als casus geïntroduceerd. Daarna worden de centrale begrippen van het essay uiteengezet, te weten beheersing en emancipatie. In de vierde paragraaf volgt een schets van de historische ontwikkeling van de gemeentelijke basisadministratie. Deze historische schets maakt zowel het belang van registraties voor rechtsstaat en samenleving inzichtelijk alsook de spanning tussen emancipatie en beheersing. Vervolgens beschrijven we de huidige ontwikkelingen, inclusief de belangrijke rol die informatisering daarin speelt. In de laatste paragrafen vatten we onze bevindingen samen en doen we aanbevelingen voor de modernisering van de GBA.

7.2 De gemeentelijke basisadministratie persoonsgegevens

Zoals in de inleiding gesteld, maakt de gemeentelijke basisadministratie persoonsgegevens deel uit van het stelsel van basisregistraties. Basisregistraties bevatten gegevens over alle burgers, bedrijven en instellingen en zijn van groot belang voor een goed functioneren van de overheid. De GBA is op 1 oktober 1994 in Nederland ingevoerd. Het Agentschap Basisadministratie Personen en Reisdocumenten (BPR) van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties beheert de GBA. De GBA kan worden omschreven als "(…) een geheel van gemeentelijke geautomatiseerde basisadministraties van persoonsgegevens die door middel van een datacommunicatienetwerk met elkaar en met andere overheden in verbinding staan" (Lütter & Van Troost 2008, p. 21).

Deze definitie bevat twee kernelementen van de GBA. Ten eerste legt de gemeente de bevolkingsadministratie in een geautomatiseerd systeem van persoonslijsten vast. De GBA bevat alle algemene persoonsgegevens en wijzigingen daarop, van geboorte tot overlijden. Van elk lid van de Nederlandse bevolking wordt in de GBA een elektronische persoonslijst aangelegd. Het gaat hierbij om de volgende gegevens:

- burgerlijke staat (naam, geslacht, geboortedatum, geboorteplaats, persoonsgegevens van de ouders, huwelijksgegevens, geregistreerd partnerschap, kinderen en overlijden);
- gegevens over kinderen en over het ouderlijk gezag;
- nationaliteit;
- verblijfsrecht (bij vreemdelingen);
- de gemeente waar iemand is ingeschreven en het adres in die gemeente;
- gegevens over het verblijf en het vertrek uit Nederland (als mensen hier tijdelijk verblijven);
- administratienummers van de ingeschreven persoon en van zijn of haar ouders, (eerdere) echtgenoot of geregistreerde partner en kinderen;
- burgerservicenummer (BSN) van de ingeschreven persoon en bovengenoemde relaties;
- gebruik van de achternaam van de (ex-)partner.

Ten tweede vindt er via een elektronisch communicatienetwerk uitwisseling van berichten plaats met andere gemeenten en afnemers, bijvoorbeeld een adreswijziging of een melding van overlijden. De GBA is een 'authentieke' basisregistratie voor alle (semi)overheidsinstanties die voor de uitvoering van hun taak over persoonsgegevens moeten kunnen beschikken. Het gaat hier om honderden afnemers. Voorbeelden zijn de Belastingdienst, de waterschappen, de Sociale Verzekeringsbank en pensioenfondsen. Alle instanties met een publieke taak zijn verplicht de GBA te gebruiken als basis voor persoons-

gegevens. De GBA is bijvoorbeeld maatgevend om iemand al dan niet een voorziening van de (rijks)overheid toe te kennen. Iemand heeft alleen recht op een AOW-uitkering als hij volgens de gegevens van de GBA daarvoor in aanmerking komt. Via de GBA kan dit recht ook worden ingenomen. Als een persoon overlijdt, wordt vanuit de GBA een bericht doorgegeven aan de Sociale Verzekeringsbank en wordt de uitkering van de AOW stopgezet. De GBA is dus de bron van informatie aangaande persoonsgegevens.

Begin 2001 is met de tijdelijke Adviescommissie Modernisering GBA (commissie-Snellen) het startsein gegeven voor de modernisering van de GBA. Dit traject moet in 2010 afgerond zijn. Volgens de commissie moet onder andere de toegankelijkheid van de GBA voor gebruikers verbeteren door de GBA online raadpleegbaar te maken. Afnemers moeten 7 dagen per week en 24 uur per dag toegang hebben tot alle GBA-gegevens van iedere gemeente in Nederland (Lütter & Van Troost 2008).

7.3 Beheersing en emancipatie

De moderne staat berust op de bureaucratie als organisatievorm. Een moderne bureaucratie heeft systemen nodig van gestandaardiseerde registratie om burgers te identificeren, aan te spreken en informatie over hen te vergaren. De overheid heeft deze informatie nodig om te 'beheersen'. Vanuit het perspectief van de burger kunnen registraties daarnaast een emancipatoire functie krijgen. We zullen hieronder beide aspecten toelichten.

Onze kijk op de moderne staat stoelt in belangrijke mate op de bureaucratietheorie van de Duitse socioloog Max Weber (1978/1922). Weber heeft de bureaucratie als rationele organisatievorm bestudeerd. Weber stelt dat de bureaucratie als toppunt van rationele administratieve organisatie onvermijdelijk is. Aan de ene kant moet dit volgens hem positief worden geduid, omdat organisaties alleen op die manier rationeel, zorgvuldig en onpartijdig kunnen functioneren. Aan de andere kant (voor)zag Weber ook dat in vergaande bureaucratisering gevaren schuilen. Zonder politieke waarborgen bestaat het gevaar dat bureaucratie in eigenmacht verandert en wildgroei ontstaat. De bureaucratie vormt zowel een voorwaarde voor democratie, als een bedreiging ervan. Met andere woorden, in Athene schuilt Orwell.

In het dagelijks gebruik heeft het begrip 'beheersing' vaak de laatstgenoemde, negatieve connotatie; bij ons echter niet, of beter gezegd: niet bij voorbaat. Zoals Weber aangeeft is het beheersingsaspect van identificatie en registratie wezenlijk voor het functioneren van de bureaucratie. Zo kan met gegevens uit de GBA de overheid toezien op het nakomen van de belastingplicht. Door middel van het handelsregister kan vastgesteld worden of een organisatie die zich presenteert als onderneming, dat ook daadwerkelijk is. Alleen dan kunnen marktpartijen op betrouwbare wijze onderling zakendoen. En het Kadaster verschaft de garantie dat bepaalde onroerende goederen daadwerkelijk eigendom zijn van degene die ze te koop of te huur aanbiedt. Deze voorbeelden laten zien dat door middel van (basis)registraties de samenleving beheersbaar wordt.

De emancipatoire kant van persoonsregistraties blijft vaak onderbelicht. Dit terwijl registratie en documentatie essentieel zijn om personen mee te laten tellen in een complexe, grootschalige en moderne wereld. Talloze (negatieve) voorbeelden illustreren dit. Denk bijvoorbeeld aan de positie van burgers in ontwikkelingslanden. Nog altijd hebben grote groepen mensen geen toegang tot onderwijs, omdat zij door de staat niet als staatsburger erkend worden. Weliswaar garanderen internationale verdragen en handvesten van de VN dat elke persoon bepaalde rechten heeft, maar zonder een adequate registratie, zonder 'officiële papieren', zijn deze rechten lastig te verzilveren. Het gaat hier bijvoorbeeld om het stemrecht en het recht op onderwijs of zorg. Zonder persoonsregistratie is iemand ook niet vrij om te reizen (want beschikt niet over geldige reisdocumenten zoals een paspoort), kan geen bedrijf opzetten (want kan zich niet registreren in het handelsregister of bij het Kadaster) en kan geen stem uitbrengen (want staat niet geregistreerd). Met andere woorden, hij kan de rechten van een vrij individu niet uitoefenen. Deze emancipatoire dimensie ligt ook ten grondslag aan het dictum 'Ieder kind zal meteen na de geboorte geregistreerd worden en een naam hebben' uit het United Nations International Covenant on Civil and Political Rights van 1966.

Zoals we hierna zullen betogen, schuilt tussen beide aspecten van het gebruik van persoonsregistraties – beheersing en emancipatie – een continue spanning. Deze spanning hangt samen met de vormgeving van de relatie tussen burger en overheid. De positie van de overheid wordt verstevigd wanneer de registratie primair gericht is op beheersing. Wanneer daarentegen veel aandacht uitgaat naar het realiseren van rechten, versterkt de registratie juist de positie van de burger (Caplan & Torpey 2001). In aansluiting bij Weber stellen wij dat beide aspecten in evenwicht dienen te zijn om de samenleving bestuurbaar te houden en tegelijkertijd te voorkomen dat de bureaucratie in eigenmacht verandert.

7.4 De ontwikkeling van de gemeentelijke basisadministratie

Deze paragraaf schetst in grote lijnen de historische ontwikkeling van persoonsregistraties. Hiermee willen we de spanning tussen beheersing en emancipatie die eigen is aan het stelsel van persoonsregistraties inzichtelijk maken.

7.4.1 Het ontstaan van de eerste registers

Tegen de achtergrond van een groeiende handel, de opkomst van steden, de invoering van de geldeconomie en een toenemende bevolking, kortom een complexere samenleving, werd de behoefte aan regelgeving en informatie in de zestiende eeuw groter. Deze behoefte werd ervaren door zowel de machthebbers, met het oog op het efficiënter innen van allerlei belastingen onder hun steeds rijkere onderdanen, als door de onderdanen zelf, die behoefte hadden aan regulering en garanties in het onderlinge zakelijke verkeer. Het gold ook

voor kerkelijke autoriteiten die greep wilden blijven houden op het morele gedrag van hun volgelingen. Doop-, trouw- en begrafenisregisters van de kerk werden ingevoerd om misstanden als bigamie, het leven in concubinaat, huwelijken met minderjarigen en incest tegen te gaan.

Om belasting te kunnen heffen had vanaf de late middeleeuwen elk gewest zijn eigen belastingregister met informatie over belastingheffing op huizenbezit (haardsteden, vuurplaatsen en schoorsteengeld), grondbezit (de verponding) en vermogen en vererving. Daarmee wordt het beheersingsaspect van registratie geïllustreerd. Maar ook toen werden registraties reeds gekenmerkt door emancipatoire aspecten. Stadsrechten, die vanaf de dertiende eeuw worden verleend, garandeerden enige mate van zelfstandigheid van inwoners van een stad ten opzichte van de 'willekeur' van de wereldlijke heren. Om daarop een beroep te kunnen doen, moest een persoon ingeschreven zijn als 'poorter'. In het poorterregister werd bijgehouden welke burgers het poorterrecht, oftewel het burgerrecht dat gold in de middeleeuwse steden, bezaten. Een poorter kon binnen de poorten van een stad met stadsrechten wonen. Vrijwel alleen de personen die zichzelf financieel konden redden en een bijdrage konden leveren aan het welzijn van de stad, kregen – al dan niet tegen betaling – dit poorterrecht (Holthuizen-Seegers & Wens 1993).

7.4.2 De vastlegging en uitvoering van vrijheidsrechten

Tot in de zestiende eeuw lag het accent in registratie op het beheersingsaspect van identificatie en registratie, vooral met het oog op belastingheffing. Het was vooral in de zestiende eeuw dat, zeker in de Nederlanden, stadsrechten en privileges van steden en hun inwoners een politiek thema werden, in het verzet tegen de Habsburgse machthebbers Karel V en zijn zoon Filips II. In de zeventiende en in de loop van de achttiende eeuw kwam in Europa het emancipatoire aspect steeds sterker naar voren. Kenmerkend voor deze tijd was het opkomende streven, vooral in Engeland en Frankrijk, naar bescherming van de burger tegen de macht van de koning. De zogenoemde klassieke vrijheidsrechten als het recht op meningsuiting en het recht op eigendom werden geformuleerd en met toenemende kracht gepropageerd.

Volgens Bovens (1998) werd in deze tijd de liberale laag van de rechtsstaat gevormd, die de burger bescherming biedt tegen de macht van de overheid. Met de vastlegging van eigendomsverhoudingen konden de opkomende burgerij en de grootgrondbezitters hun economische vrijheden en zakelijke belangen veiligstellen tegenover de 'almachtige', grillige en al te veeleisende monarch. De vastlegging van eigendomsrechten emancipeerde de opkomende burgerij en maakte verdere economische ontwikkeling mogelijk (Bovens 1998; Hoof & Ruysseveldt 1996). Natuurlijk was het niet eenvoudig om deze rechten ten opzichte van de koning af te dwingen, zeker niet omdat de onafhankelijke rechtspraak zich nog nauwelijks ontwikkeld had. Een sprekende illustratie daarvan vormde de legitimatie van de Nederlandse opstand als een verdediging van door de Spaanse koning geschonden stadsrechten en privileges. Er was vervolgens wel een 'tachtigjarige' oorlog voor nodig om de vermeende schending van rechten erkend te krijgen. In Engeland uitte deze strijd zich in decennialang touwtrekken tussen de koning en het Lagerhuis, waarbij de laatste er stapje voor stapje in slaagde om voorrechten te ontnemen aan de koning. In Frankrijk duurde het tot achter in de achttiende eeuw voordat de koning, met veel geweld, het veld moest ruimen.

7.4.3 De invoering van de burgerlijke stand en de bevolkingsadministratie

Ook in de negentiende eeuw kunnen we zowel het emancipatoire als het beheersingsaspect van identificatie en registratie ontwaren. In het uitgebreide rijk van Napoleon waren centralisatie van bestuur en een uniforme wetgeving onontbeerlijk om het rijk te kunnen besturen. Daarvoor was inzicht in de bevolkingsomvang en -structuur een vereiste. Op grond daarvan kon de dienstplicht ten behoeve van het leger beter worden afgedwongen en kon een efficiëntere belastingheffing worden ingevoerd. In 1811 voerde Napoleon de burgerlijke stand in het grootste deel van Nederland in. Daarmee werden de kerkelijke huwelijks-, geboorte- en overlijdensregisters overgedragen aan de overheid (Holthuizen-Seegers & Wens 1993).

Met de burgerlijke stand werd ook *le droit citoyen* ingevoerd. Deze ontwikkeling is van groot belang geweest voor de emancipatie van de burger. Burgers kregen hiermee een gelijke status voor de wet en ten opzichte van elkaar. Vrije individuen werden als dusdanig erkend. In Frankrijk en Nederland betekende dit bijvoorbeeld dat de Joodse gemeenschap kon participeren en integreren in de maatschappij (Caplan & Torpey 2001). Door de registratie van personen konden voorts politieke rechten als kiesrechten en het recht van demonstratie uitgeoefend worden. De democratische laag van de rechtsstaat vormde zich (Bovens 1998).

In de negentiende eeuw werd de aftrap voor de huidige gemeentelijke basisadministratie gegeven. In 1815 werd in Nederland een constitutionele monarchie uitgeroepen en ontstond het Koninkrijk der Nederlanden. In 1828 werd de bevolkingsregistratie een rijksaangelegenheid. Ze verving de tienjaarlijkse volkstellingen. Hierbij werd in eerste instantie gewerkt met vastbladige registers, dat wil zeggen dat de akten met de pen geschreven werden in een tevoren ingebonden boek. Later werd overgestapt op losbladige gezinskaarten. De voordelen van een losbladig systeem betroffen de leesbaarheid en de mogelijkheid om met behulp van carbon origineel en duplicaat uniform en in één handeling te maken. In 1938 werd besloten dat elke gemeente een persoonskaartensysteem moest invoeren. De persoonskaart gaf naast de personalia van de betrokkene (geslachtsnaam en voornaam, nationaliteit, woonadres, geboortedatum en -plaats, plaats in het gezinsverband, beroep en verhuizingen) ook vaak de namen en personalia van de ouders en kinderen weer (Centraal bureau voor genealogie 2009). De bevolkingsboekhouding dient

niet verward te worden met de burgerlijke stand. De burgerlijke stand geeft een momentopname en enkel gegevens rondom geboorte, huwelijk, scheiding of overlijden weer. In de bevolkingsboekhouding werden veranderingen in de totale levensloop van burgers opgetekend (Holthuizen-Seegers & Wens 1993).

7.4.4 Emancipatie en beheersing in uitersten

De twintigste eeuw werd gekenmerkt door uitersten als het gaat om de spanning tussen beheersing en emancipatie. Aan de ene kant stonden de gruwelijkheden van het naziregime, aan de andere kant de ontwikkeling van de verzorgingsstaat. De grote dienst die de bevolkingsboekhouding en de identificatieplicht de bezetters tijdens de Tweede Wereldoorlog bewezen bij het opsporen van onderduikers, verzetsmensen en Joden, ligt nog vers in het geheugen. Tijdens de Tweede Wereldoorlog werd duidelijk dat het vastleggen van identiteitsgegevens perverse gevolgen kan hebben.

In de verzorgingsstaat komt daarentegen het emancipatoire aspect sterk tot uitdrukking. Deze kreeg vorm in sociale grondrechten als het recht op bijstand, het recht op onderwijs of pensioenvoorzieningen. Met de groei van het aantal overheidstaken nam ook het aantal persoonsregistraties explosief toe. Zo vroeg de uitbreiding van het onderwijs om bestanden van leerplichtige kinderen, vereiste de gezondheidszorg een overzicht van werknemers met een ziektekostenverzekering en noopte het pensioenstelsel tot een overzicht van pensioengerechtigden. Verder werden er gegevens verzameld ten behoeve van bijstandregelingen, eenmalige uitkeringen en huursubsidies (Holthuizen-Seegers & Wens 1993).

Maar de verzorgingsstaat werd tevens gekenmerkt door – een vergaande mate van – beheersing. In het streven om alle burgers adequaat te bedienen, waren omvangrijke persoonsregistraties nodig. In dat proces dreigt het gevaar van overbureaucratisering, waarbij 'cliënten' verworden tot niet meer dan een dossiernummer. Dit gevaar is door Weber reeds voorzien. Volgens hem wordt in de moderne wereld de individuele vrijheid van een persoon bedreigd door een verstikkende bureaucratie: de mens raakt gevangen in een 'ijzeren kooi'.

7.4.5 De intrede van de computer

Door de ontwikkeling van de verzorgingsstaat ontstond een explosieve groei in het gebruik van persoonsgegevens. Dit werd nog eens in de hand gewerkt door het toenemend gebruik van computers, die het werk van de ambtenaren op de registrerende afdelingen enorm vergemakkelijkten. Eind jaren zeventig beschikte een groot aantal gemeenten over een geautomatiseerd systeem van bevolkingsboekhouding. Nog altijd werden echter binnen de gemeente onafhankelijk van elkaar in verschillende bestanden mutaties aangemaakt. In 1984 kondigde de staatssecretaris van Binnenlandse Zaken een nieuwe opzet aan van de gemeentelijke bevolkingsadministratie, de gemeentelijke basisadministratie persoonsgegevens (GBA). In 1994 was de GBA een feit. Het computertijdperk

en de invoering van de GBA zorgden ervoor dat persoonsregistraties beter en nauwkeuriger verwerkt, aangepast, uitgebreid, geraadpleegd en toegepast konden worden (Holthuizen-Seegers & Wens 1993).

7.5 Huidige ontwikkelingen: voortschrijdende informatisering

De modernisering van de GBA en – recenter – de introductie van het burgerservicenummer (BSN) en de Digitale Identiteit (DigiD) geven vorm aan de gemeentelijke basisadministratie en identiteitsinfrastructuur van tegenwoordig. De gemoderniseerde GBA moet overheidsorganisaties efficiënter laten werken en beter laten samenwerken en de dienstverlening verbeteren (www.bzk.nl). Het hiervoor benodigde elektronisch verkeer tussen overheidsorganisaties onderling en met burgers wordt op steeds grotere schaal gerealiseerd.

De aandacht gaat daarbij vooral uit naar de technische vervolmaking en een efficiëntere inrichting van de overheid. Prins en Ham (2008, p. 10) zien het streven naar efficiëntie als dominant: "We streven alleen nog naar efficiëntie, voeren onze taken volledig gestandaardiseerd uit en technologische middelen zijn doelen op zich geworden." De mogelijkheden van ICT hebben dit streven alleen maar versterkt. De voortschrijdende informatisering heeft daarnaast grote invloed op de hoeveelheid verzamelde gegevens. In eerste instantie werden gegevens vooral vastgelegd om de toenemende wet- en regelgeving te kunnen uitvoeren, en maakte de invoering van de computer dit werk gemakkelijker. In hun onderzoek constateren Schermer en Wagemans (2009) echter dat tegenwoordig bij nagenoeg *alle* processen en handelingen in onze informatiemaatschappij persoonsgegevens worden vastgelegd.

Informatisering leidt dan ook tot versterking van de beheersingsdimensie waardoor de balans tussen overheid en burger dreigt door te slaan. Zuurmond (1994) betoogt dat de 'ijzeren kooi' van de klassieke bureaucratie meer en meer vervangen wordt door een 'virtuele vesting'. Elektronische databases zijn behalve veelomvattender ook dwingender dan klassieke kaartenbakken. De computer is tussen de ambtenaar en de burger komen te staan en laat nog minder ruimte voor persoonlijke interactie en 'afwijkende' gevallen.

Informatisering maakt het registreren van gegevens gemakkelijker en tegelijkertijd normaler, waardoor meer gegevens dan ooit worden vastgelegd. Alleen al in de periode van 1988 tot 2000 vertienvoudigde het aantal databases bij de overheid en semioverheid, van circa 3500 tot 30.000 (Schermer & Wagemans 2009). Zoals gezegd, kent de GBA alleen al honderden afnemers. Bovendien worden bestanden van instanties steeds vaker aan elkaar gekoppeld via verwijsindexen en inkijkfuncties als Suwinet en het elektronisch kinddossier. Overheidsinstanties krijgen daarmee een steeds completer beeld van de burger. De burger wordt in feite transparant voor de overheid.

7.6 Dynamiek in de basisregistratie

Zoals we in de vorige paragraaf hebben kunnen zien, maakt vandaag de dag het vastleggen van identiteiten deel uit van een schijnbaar ingesleten en vanzelfsprekende administratieve routine. In menig eerste contact met een overheidsinstantie worden als eerste formele handeling NAW-gegevens ofwel ter plaatse ingevoerd in een registratiesysteem of 'opgehaald' uit het bestaande systeem. Het is de vanzelfsprekendheid waarmee de burger wordt verzocht zijn 'klantnummer' of burgerservicenummer bij de hand te houden als deze een dienst van de overheid verlangt. Deze vanzelfsprekendheid blijft echter niet zonder gevolgen.

In het voorgaande hebben we betoogd dat het registreren van personen invloed heeft op de (machts)relatie tussen overheid en burger. Volgens Caplan en Torbey (2001) vormt identificatie een primaire bron van interactie en communicatie tussen burger en staat. Dit kan zowel beheersingsdoelen dienen – zoals het heffen van belasting – als de burger beschermen tegen de willekeur van machthebbers. Ook liggen persoonsregistraties ten grondslag aan de ontwikkeling van onze democratische rechtsstaat en de effectuering van klassieke, politieke en sociale rechten. Registraties zijn daarom niet zomaar een papieren of elektronische aangelegenheid, maar bij uitstek een politieke aangelegenheid. In dit licht kan de GBA dan ook worden beschouwd als een onderdeel van de moderne rechtsstaat, waarin de macht van de overheid wordt gereguleerd en beperkt. De GBA registreert immers niet alleen belastingbetalers maar ook uitkeringsgerechtigden en kiezers.

Tevens hebben we gezien dat in de loop van de twintigste eeuw de voortschrijdende informatisering het gebruik van registraties ingrijpend heeft veranderd. Daarbij valt op dat deze 'modernisering' vooral wordt beschouwd als een technische aangelegenheid, gericht op verbetering van efficiëntie en doelmatigheid. Door deze eenzijdige aandacht voor efficiëntie dreigt de balans tussen emancipatie en beheersing door te slaan naar het laatste. Caplan en Torpey (2001) omschrijven de continue spanning tussen beheersing en emancipatie als een kat-en-muisspel tussen staat en burger. Hun voorlopige conclusie is dat, ook al is het spel nooit van tevoren uitgemaakt, de kat (de overheid) vooralsnog de betere kaarten in handen heeft (Caplan & Torpey 2001, p. 7). Het evenwicht in de relatie tussen overheid en burgers dreigt te worden verstoord door een overmaat aan bureaucratisering en beheersingsdenken, dat vooral leidt tot nieuwe afhankelijkheden van de burger. Dit gevaar wordt alleen maar bestendigd door de discussie over de modernisering van registraties zoals de GBA alleen in termen van efficiëntie en techniek te blijven voeren, in plaats van ook het belang en de mogelijkheden die de modernisering biedt voor de emancipatie te onderkennen.

7.7 Conclusies: op zoek naar evenwicht

Voor de huidige discussie is het van belang de emancipatoire kant van registraties te blijven benadrukken en voldoende waarborgen te ontwikkelen voor een nieuw evenwicht tussen overheid en burger. Dat roept de vraag op hoe de positie van de burger ten opzichte van de overheid kan worden versterkt.
Het nog steeds groeiende informatieoverwicht dat de overheid heeft ontwikkeld ten opzichte van de burger behoeft een nieuw systeem van *checks and balances*. Bescherming van privacy beschouwen wij als een belangrijk onderdeel van deze checks and balances maar is vooral defensief van aard. Ze doet onvoldoende recht aan het emancipatoir potentieel dat persoonsregistraties van oudsher kenmerkt. Wij willen juist aandacht vragen voor de mogelijkheden die de modernisering van registraties biedt voor een verdere emancipatie van burgers. Ter afsluiting willen wij enkele 'openingszetten' in deze discussie doen, waarbij de terminologie al aangeeft dat we in dit stadium niet de pretentie hebben een 'winnende variant' op het bord te kunnen toveren. Regievoering door burgers over de eigen persoonsgegevens staat in onze aanzet centraal.

Regievoering betekent kort gezegd *inzicht* hebben in en *invloed* hebben op de verwerking van persoonsgegevens door de overheid. Regie door de burger gaat verder dan alleen inzicht geven in de gegevens die over hem of haar worden verwerkt en het voldoen aan wettelijke informatieplichten. Het gaat vooral om een bepaalde mate van zeggenschap van burgers over hun gegevens en om het kunnen uitoefenen van invloed op de wijze waarop gegevens worden verwerkt op basis waarvan door anderen (lees: de overheid) besluiten worden genomen die van invloed zijn op hun leven (N2L/Zenc 2002).

Inzicht in gegevensverwerking is vooral afhankelijk van de transparantie van die verwerking en de kennis die de burger heeft van het feit dat die verwerking plaatsvindt. Openbaarheid en transparantie vormen dan ook belangrijke voorwaarden voor regievoering door de burger. Hierbij gaat het grotendeels om in de Wet bescherming persoonsgegevens (WBP) opgenomen verplichtingen en daaraan gekoppelde rechten voor betrokkenen, zoals het inzage- en correctierecht. Het inzage- en correctierecht is echter vaak geen 'actief' recht. De burger heeft over het algemeen geen directe inzage, maar moet hiervoor een schriftelijk verzoek indienen. De site www.mijnoverheid.nl vormt hierop een uitzondering. Op deze site kunnen burgers inzicht krijgen in een aantal gegevens die de overheid over hen vastlegt. Het gaat vooralsnog om gegevens uit de GBA, het Digitaal Klantdossier, de Rijksdienst Wegverkeer en het Kadaster. In aanvulling hierop zou de overheid bij elke beschikking een bijlage kunnen toevoegen waarin staat op welke gegevens van de aanvrager de beslissing is gebaseerd. Ook dat biedt de aanvrager de mogelijkheid om te controleren of de overheid geen verkeerde gegevens heeft gebruikt. Dat voorkomt dat burgers een bijna kansloze gang door bureaucratische krochten moeten maken om onjuistheden over hun persoonlijke situatie te laten corrigeren.

Een balans tussen overheid en burger vraagt evenwel vooral om meer invloed van de burger op voor hem relevante gegevensverwerking. Hiervoor biedt de WBP geen mogelijkheden. Burgers kunnen immers niet zelf hun gegevens wijzigen. Toegepast op de GBA zou de site www.mijnoverheid.nl de burger meer mogelijkheden moeten bieden om (bepaalde) gegevens te kunnen wijzigen. Zo zou de mogelijkheid kunnen worden geschapen dat burgers zelf kunnen aangeven of ze met hun meisjesnaam willen worden aangesproken. Een andere mogelijkheid is om hen zelf in staat te stellen om op basis van eigen gegevens inkomensondersteunende voorzieningen aan te vragen.

Met deze voorbeelden willen we illustreren dat persoonsregistraties niet noodzakelijkerwijs *alleen* toegesneden hoeven te zijn op efficiëntieverhoging. Registraties kunnen ook zo worden ingericht dat ze het burgers gemakkelijker maken wijzigingen in hun registratie aan te brengen of in aanmerking te komen voor bepaalde rechten. Bestanden kunnen aan elkaar worden gekoppeld, waardoor bijvoorbeeld niet-gebruik van inkomensondersteunende voorzieningen inzichtelijk wordt. Zowel de overheid als de burger kunnen daarvan profiteren. Het zijn dus juist de ontwikkelingen in de ICT die uitgelezen mogelijkheden bieden voor het versterken van de positie van de burger. Aan de rechten en plichten die in de vorige paragrafen aan bod kwamen, kunnen dan ook informatierechten van de burger en informatieplichten van de overheid worden toegevoegd (zie ook Bovens 1998). Met behulp van ICT kunnen nieuwe checks and balances worden toegevoegd, waardoor de muis niet langer met huid en haar is overgeleverd aan de kat.

Literatuur

Databases in beeld

Algemene Rekenkamer (2007). *Lessen uit ICT-projecten bij de overheid. Deel A*. [z.p.]

Automatisering Gids (2010). 'Plan elektronische overheid dreigt faliekant te mislukken'. 12 februari 2010.

BB Digitaal Bestuur (2010). 'De zeven gevaren van datahonger'. Maart 2010.

Commissie-Brouwer (2009), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*. Den Haag: Rijksoverheid.

Eerste Kamer (2009-2010a). *Verslag van een rondetafelgesprek*. Vergaderjaar 2009-2010, 31 466, F.

Eerste Kamer (2009-2010b). *Verslag van de expertbijeenkomst over het elektronisch patiëntendossier van de vaste commissie voor Volksgezondheid, Welzijn en Sport/ Jeugd en Gezin van de Eerste Kamer op woensdag 9 december 2009*. Vergaderjaar 2009-2010, 31 466, E.

Hildebrandt, M. & S. Gutwirth (red.) (2008). *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer.

Hof, C. van 't, R. van Est & F. Daemen (red.) (2010). *Check in/Check uit. De digitalisering van de openbare ruimte*. Rotterdam: Rathenau Instituut/ NAi Uitgevers.

Leenes, R. (2010). *Harde lessen. Apologie van technologie als reguleringsinstrument*. Tilburg: Universiteit van Tilburg.

Munnichs, G. (2009). *Startnotitie Expertmeeting elektronisch patiëntendossier (EPD)*. Den Haag: Eerste Kamer der Staten-Generaal/Rathenau Instituut.

Nationale ombudsman (2009). *De burger in de ketens. Verslag van de Nationale ombudsman over 2008*. Den Haag: Nationale ombudsman.

NRC Handelsblad (2007). 'Stad zegt of u seksuele voorlichting moet geven'. 1 november 2007.

Schermer, B.W. & T. Wagemans (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*. Amsterdam: Considerati.

Vedder, A. et al. (2007). *Van privacy-paradijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*. Den Haag: Rathenau Instituut.

www.iederkindwint.nl. http://www.iederkindwint.nl/#pagina=1006.

De OV-chipkaart en de kilometerheffing: een elektronisch enkelbandje voor reizigers?

Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, Massachusetts: MIT.
Camenisch, J. & A. Lysyanskaya (2002). 'A Signature Scheme for Efficient Protocols'. In: Conference proceedings *Security in Communication Networks*, pp. 268-289.

College bescherming persoonsgegevens (2008). *Brief aan Staatsecretaris van Verkeer en Waterstaat Mevrouw J.C. Huizinga-Heringa (kenmerk z2008-01411)*. 6 november 2008.

Jonge, W. de & B. Jacobs (2008). 'Privacy-friendly Electronic Traffic Pricing via Commits'. In: Conference proceedings *Formal Aspects in Security and Trust*, pp. 143-161.

Kolman, S. & R. van Est (2010). 'De genetwerkte auto'. In: Hof, C. van 't, R. van Est & F. Daemen (red.). *Check in/Check uit. De Digitalisering van de openbare ruimte*. Rotterdam: Rathenau Instituut/ NAI Uitgevers, pp. 135-167.

Winter, B. de (2008). '7 jaar centrale opslag OV-reisgegevens niet nodig'. In: *Webwereld.nl*, 17 november 2008.

Het elektronisch patiëntendossier vanuit informatiebeveiligingsperspectief

Noordende, G. van 't (2010). *A Security Analysis of the Dutch Electronic Patient Record System*. Technical Report UVA-SNE-2010-01. Amsterdam: Universiteit van Amsterdam.

NOVA (2008). Elektronisch patiëntendossier part 1. 12 november 2008 (http://www.youtube.com/watch?v=ahkcA1PH7Mw).

Spaink, K. (2005). *Medische geheimen. De risico's van het elektronisch patiëntendossier*. Amsterdam: Nijgh & Van Ditmar.

Het elektronisch kinddossier: kansen en kanttekeningen

Nationale ombudsman (2009). *De burger in de ketens. Verslag van de Nationale ombudsman over 2008*. Den Haag: Nationale ombudsman.

Klantenprofielen: de onzichtbare hand van internet

Agre, P.E. & M. Rotenberg (red.) (2001). *Technology and privacy: The new landscape*. Cambridge, Massachusetts: MIT.

Ayres, I. (2007). *Super Crunchers: why thinking-by-numbers is the new way to be smart*. New York: Bantam Books.

Borking, J.J. & Ch.D. Raab (2001). 'Laws, PETs and Other Technologies for Privacy Protection'. In: *Journal of Information, Law and Technology,* 2001 (1).

Custers, B. (2004). *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen: Wolf Legal Publishers.

Dijk, N. van (2009). 'Intellectual Rights as Obstacles for Transparency in Data Protection'. In: Deuker, A. (red.), *Mobile Marketing in the Perspective of Identity, Privacy and Transparency.* FIDIS deliverable. 11 december 2009.

Dijk, N. van (2010). 'Auteursrecht in Profielen'. In: *Computerrecht*, Issue 2, pp. 53-61.

Dolinar, K. et al. (2009). 'Design Patterns for a Systemic Privacy Protection'. In: *IARIA International Journal of Advances in Security*, no. 2, pp. 267-287.

Hildebrandt, M. & S. Gutwirth (red.) (2008). *Profiling the European Citizen. Cross-disciplinary Perspectives*. Dordrecht: Springer.

Hildebrandt, M. & B.J. Koops (2010). 'The challenges of Ambient Law and legal protection in the profiling era'. In: *Modern Law Review*, 73(3), pp. 428-460.

Jernigan, C. & B.F.T. Mistree (2009). 'Gaydar: Facebook friendships expose sexual orientation'. In: *First Monday,* 14(10).

Stone, B. (2010). 'Sure, It's Big, but is that Bad? Google'. In: *New York Times*, 21 mei 2010.

The Economist (2010). 'Data, data everywhere. A special report on managing information', 27 februari 2010.

Zarsky, T.Z. (2002-2003). '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion'. In: *Yale Journal of Law & Technology*, 5(4), pp. 17-47.

De schaduwzijden van het Schengen Informatie Systeem

Brouwer, E. (2008). *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*. Leiden/Boston: Martinus Nijhoff.

College bescherming persoons-gegevens (2008). *Brief aan Minister van Justitie. Afronding onderzoek artikel 99 SUO*. 20 maart 2008.

Computable (2009). 'Vertraging SIS II kost ministerie miljoen extra'. 22 januari 2009 (http://www.computable.nl/artikel/ict_topics/overheid/2843704/1277202/vertraging-sis-ii-kost-ministerie-miljoen-extra.html).

Council of the European Union (2009). *Report on the further direction of SIS II*. Doc.nr. 10005/09, 20-05-2009.

European Data Protection Supervisor (2010). 'Opinions'. In: *Official Journal of the European Union*, C 70. 19 March 2010.

Europees Parlement (2003). *Verslag met een ontwerpaanbeveling van het Europees Parlement aan de Raad betreffende de tweede generatie van het Schengen-informatiesysteem (SIS II)*. A5-0398/2003.

House of Lords European Union Committee (2007). *9th Report of Session 2006-07. Schengen Information System II (SIS II). Report with Evidence*. HL Paper 49. London: The Stationary Office Limited.

Joint Supervisory Authority of Schengen (2005). *Article 96 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System*. 20 June 2005.

Joint Supervisory Authority of Schengen (2007). *Article 99 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System*. 18 December 2007.

Joint Supervisory Authority of Schengen (2009a). *Article 97 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 97 alerts in the Schengen Information System*. 13 October 2009.

Joint Supervisory Authority of Schengen (2009b). *Article 98 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 98 alerts in the Schengen Information System*. 13 October 2009.

Nationale ombudsman (2010). *Toegang verboden. Onderzoek naar de opname van vreemdelingen in het Schengen Informatie Systeem en de informatievoorziening hierover*. Rapportnummer 2010/115. Den Haag: Nationale ombudsman.

Tweede Kamer (1996-1997a). *Rapport Nationaal Schengen Informatie Systeem*. Vergaderjaar 1996-1997, 25 200, nrs. 1-2.

Tweede Kamer (1996-1997b). *Verslag van een Algemeen Overleg*. Vergaderjaar 1996-1997, 25 200, nr. 6.

Dynamiek in de gemeentelijke basisadministratie

Bovens, M.A.P. (1998). *De digitale rechtsstaat, beschouwingen over informatiemaatschappij en rechtsstaat*. Utrecht: Universiteit Utrecht.

Caplan, J. & J. Torpey. (2001). *Documenting individual identity. The development of state practices in the modern world*. Princeton: Princeton University Press.

Centraal bureau voor genealogie (2009). Persoonskaarten en persoonslijsten (http://www.cbg.nl/download/cbg_nl_persoonskaarten_200901.pdf).

Holthuizen-Seegers, G.H.J. & M.C.C. Wens (1993). *Persoonlijk gegeven, grepen uit de geschiedenis van bevolkingsregistratie in Nederland*. Amersfoort: Bekking.

Hoof, J. van & J. van Ruysseveldt (1996). *Sociologie en de moderne samenleving. Maatschappelijke veranderingen van de industriële revolutie tot in de 21ste eeuw*. Amsterdam: Boom.

Lütter, G. & R. van Troost (2008). *De dataloods en zijn machinekamer. Inleiding tot de GBA*. Deventer: Kluwer.

Net2Legal Consultants/Zenc (2002). *De betrokkene betrokken*. Onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijks-relaties, Directie Informatiebeleid Openbare Sector. [z.p.]

Prins, C. & M. Ham (2008). *In de greep van de technologie, Nieuwe toepassingen en het gedrag van de burger*. Amsterdam: Van Gennep.

Schermer, B.W. & T. Wagemans. (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*. Amsterdam: Considerati.

Weber, M. (1978). *Economy and society: an outline of interpretive sociology*. Berkeley: University of California Press. Vertaling van Weber, M. (1922). *Wirtschaft und Gesellschaft*.

www.bzk.nl. http://www.bzk.nl/actueel/nieuws--en/@117129/modernisering-gba.

Zuurmond, A. (1994). *De infocratie, Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk*. Den Haag: Phaedrus.

Verantwoording

Deze studie maakt gebruik van zes casestudies over het gebruik van databases. Hierbij is gekozen voor de volgende onderwerpen:
- de OV-chipkaart en de kilometerheffing
- het elektronisch patiëntendossier
- het elektronisch kinddossier
- klantenprofielen op internet
- het Schengen Informatie Systeem
- de gemeentelijke basisadministratie.

Bij deze keuze is rekening gehouden met een spreiding over diverse gebieden en een mix van publieke en private databases, met tevens aandacht voor het Europese gebruik van databases. Deze keuze vloeit mede voort uit oriënterende gesprekken die aan het begin van het project zijn gevoerd met tien deskundigen (zie voor de namen van de deskundigen bijlage 1). Deze keuze blijft uiteraard tot op zekere hoogte arbitrair. We hadden ook kunnen kiezen voor casestudies over de slimme energiemeter, de centrale opslag van biometrische paspoortgegevens, het Landelijk Informatiesysteem Schulden, het elektronisch leerdossier of de onstuimige groei van sociale netwerksites als Hyves of Facebook – om maar enkele andere voorbeelden te noemen. Deze variëteit aan onderwerpen geeft al aan hoe breed gebruik wordt gemaakt van gedigitaliseerde gegevensbestanden.

Voor de beschrijving van de cases is niet één strak stramien gehanteerd. In plaats daarvan is gewerkt met een lijst met aandachtspunten, als leidraad voor de auteurs (zie daarvoor de auteursinstructies in bijlage 2). Iedere case heeft weer zijn eigen bijzonderheden en werpt weer een net ander licht op het functioneren van databases.

In het essay 'Databases in beeld' presenteren de redacteuren Munnichs, Besters en Schuijff de belangrijkste uitkomsten van de casestudies. Hiervoor hebben zij gebruikgemaakt van de resultaten van een expertmeeting die het Rathenau Instituut op 19 maart 2010 heeft gehouden. Tijdens deze bijeenkomst zijn eerdere versies van de casestudies besproken (zie bijlage 3 voor de deelnemers aan de expertmeeting). De verantwoordelijkheid voor de inhoud van het essay ligt evenwel volledig bij de auteurs.

Project Databases in Beeld

Deze studie maakt deel uit van het project Databases in Beeld van het Rathenau Instituut. Dit project bouwt voort op een aantal eerdere publicaties van het instituut: *Van privacyparadijs tot controlestaat?* (Vedder et al. 2007), Bericht aan het Parlement *Opsporing behoeft 'checks and balances'* (Munnichs 2008), *De Migratiemachine* (Dijstelbloem & Meijer 2009) en *Check in/Check uit. De digitalisering van de openbare ruimte* (Van 't Hof, Van Est & Daemen 2010). Meer specifiek vormt de studie een uitwerking van de aanbeveling in *Opsporing behoeft 'checks and balances'* om de architectuur van datasystemen op de politieke agenda te zetten.

Parallel aan deze studie heeft het Rathenau Instituut twee focusgroepen georganiseerd over het elektronisch kinddossier en klantenprofielen op internet. De resultaten daarvan worden apart gepubliceerd. De belangrijkste resultaten van de studie en de focusgroepen zullen in 2011 worden gepresenteerd in een Bericht aan het Parlement.

Het Rathenau Instituut heeft in december 2009 en maart 2010 ter ondersteuning van en in samenwerking met de Eerste Kamercommissie Volksgezondheid, Welzijn en Sport/Jeugd en Gezin (VWS/JG) twee expertmeetings georganiseerd over het elektronisch patiëntendossier.

Over de auteurs

Michiel Besters
Michiel Besters is onderzoeker bij het Rathenau Instituut. Hij studeerde filosofie aan de Universiteit van Tilburg. Zijn onderzoek richt zich op medische technologie en veiligheidstechnologie (databases, politierobots). Michiel publiceerde eerder samen met Lotte Asveld het rapport *Medische technologie: ook geschikt voor thuisgebruik* (2009) bij het Rathenau Instituut. Per oktober 2010 treedt Michiel als promovendus politieke filosofie in dienst bij de Faculteit Geesteswetenschappen van de Universiteit van Tilburg.

Ellen Boschker
Ellen Boschker is bestuurskundige. Zij is cum laude afgestudeerd aan de Radboud Universiteit Nijmegen met als specialisatie goed bestuur. Vanuit deze achtergrond heeft Ellen een aanhoudende interesse voor de relatie tussen burger en overheid. Als adviseur bij Zenc zet zij zich in voor een krachtig bestuur en een krachtige samenleving. Zij is een expert op het gebied van basisregistraties.

Peter Castenmiller
Peter Castenmiller studeerde politicologie aan de Universiteit van Amsterdam. In 2001 is hij gepromoveerd op een onderzoek naar de relatie tussen burgers en lokaal bestuur. Peter is een expert op het terrein van het functioneren van het openbaar bestuur. Als adviseur bij Zenc combineert hij kennis van de inrichting en het functioneren van het openbaar bestuur met verschillende praktische functies in het openbaar domein. Naast zijn dienstverband bij Zenc is Peter lector aan BAZN, de bestuursacademie, op het thema 'Bestuurskracht en innovatie'.

Niels van Dijk
Niels van Dijk verricht promotieonderzoek aan de Vrije Universiteit Brussel binnen het onderzoeksproject *Law and Autonomic Computing. A mutual transformation process*. Hij studeerde rechten in Amsterdam en filosofie in Amsterdam en Barcelona. Zijn onderzoek richt zich op de confrontatie en wisselwerking tussen nieuwe informatietechnologieën en recht op het gebied van auteursrecht en dataprotectie.

Mireille Hildebrandt
Mireille Hildebrandt is Universitair Hoofddocent Rechtstheorie aan de Erasmus Universiteit Rotterdam en senior onderzoeker bij het centrum voor Law Science Technology and Society (LSTS) aan de Vrije Universiteit Brussel. Zij was projectleider van het deelproject inzake profileringstechnologie binnen het KP6-onderzoeksprogramma over de Future of IDentity in the Information Society (FIDIS) van de Europese Commissie. Zij redigeerde samen met Serge Gutwirth *Profiling the European Citizen. Cross-Disciplinary Perspectives* (2008). Binnenkort verschijnt bij Routledge *The philosophy of law meets the philosophy of technology. Autonomic computing and transformations of human agency*, dat zij samen met Antoinette Rouvroy redigeerde.

Simone van der Hof
Simone van der Hof is jurist en universitair hoofddocent regulering van ICT bij Tilburg Institute for Law Technology and Society (TILT) van de Universiteit van Tilburg. In haar onderzoek heeft zij zich de afgelopen jaren beziggehouden met de wijzen waarop de overheid identiteiten van burgers construeert voor uiteenlopende doeleinden (bijv. publieke dienstverlening, beleidsvorming, criminaliteits- en fraudebestrijding) en welke effecten dat heeft op de relatie burger-overheid. Verder bestudeert zij reguleringsvraagstukken rondom onlinerisico's, zoals cyberpesten en digitale kinderlokkerij, waarmee minderjarigen worden geconfronteerd.

Bart Jacobs
Bart Jacobs is hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen. Hij studeerde wiskunde en filosofie. Zijn publicaties betreffen zowel theoretisch onderzoek als praktisch werk met directe maatschappelijke relevantie: elektronisch stemmen, biometrische paspoorten, OV-chipkaarten en slimme elektriciteitsmeters. Hij verschijnt met enige regelmaat in de media, over deze en andere onderwerpen.

Geert Munnichs
Geert Munnichs werkt sinds 2002 bij de afdeling Technology Assessment van het Rathenau Instituut, als senior onderzoeker en (vanaf 2010) als coördinator. Behalve met het project Databases in Beeld heeft hij zich de afgelopen jaren beziggehouden met de onderwerpen veiligheid en privacy, voeding en gezondheid en dierenwelzijn. Hij promoveerde aan de Rijksuniversiteit Groningen op het proefschrift *Publiek ongenoegen en politieke geloofwaardigheid. Democratische legitimiteit in een ontzuilde samenleving* (2000). Vervolgens was hij als onderzoeker en medewerker Studium Generale verbonden aan Wageningen Universiteit. Geert studeerde milieuhygiëne, filosofie en geschiedenis aan de Landbouwuniversiteit Wageningen.

Mirjam Schuijff
Mirjam Schuijff werkt als onderzoeker bij de afdeling Technology Assessment van het Rathenau Instituut. Zij studeerde filosofie en bestuurskunde in Nijmegen. Naast haar onderzoek naar het gebruik van databases doet zij onderzoek naar technologie voor mensverbetering en ontwikkelingen in de neurowetenschappen.

Wouter Teepe
Wouter Teepe was tot augustus 2009 werkzaam als onderzoeker voor de Digital Security group van de Radboud Universiteit Nijmegen en was betrokken bij het ontdekken van cryptografische zwakheden in de Mifare Classic-chip die in de OV-chipkaart wordt gebruikt. Zijn bijdrage aan dit boek is vanuit die functie tot stand gekomen. Hij studeerde kunstmatige intelligentie in Groningen en is daar gepromoveerd op het maken en analyseren van cryptografische oplossingen voor enkele veelvoorkomende privacyproblemen. Momenteel is hij adviseur informatiebeveiliging voor diverse opdrachtgevers binnen de Rijksoverheid.

Arre Zuurmond
Arre Zuurmond heeft Bestuurskunde gestudeerd aan de Universiteit van Amsterdam. Sinds 1989 verricht hij onderzoek naar informatisering in het openbaar bestuur. In 1994 is hij cum laude gepromoveerd op het proefschrift *De Infocratie*, waarvoor hij de Van Poelje jaarprijs (voor de beste bestuurskundige publicatie van 1994) kreeg. Per 1 april 2000 is hij met een eigen adviesbureau begonnen, Zenc, waar hij zich richt op bestuurlijke innovaties en de rol van ICT. Als partner van Zenc adviseert Arre departementen, provincies en gemeenten op het terrein van organisatie-inrichting en informatievoorziening.

Bijlage 1: Oriënterende gesprekken

Sjaak Brinkkemper, hoogleraar informatie en softwaresystemen, Universiteit Utrecht

Paul ´t Hoen, voorzitter adviesraad, ICT Regie

Bart Jacobs, hoogleraar computerbeveiliging, Radboud Universiteit Nijmegen

Hadewych van Kempen, senior kennisadviseur, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Jacob Kohnstamm, voorzitter College bescherming persoonsgegevens

Martijn Kriens, zelfstandig ICT-consultant

Ronald Leenes, wetenschappelijk directeur TILT, Universiteit van Tilburg

Johan Louwers, Oracle consultant, Capgemini Outsourcing

Corien Prins, hoogleraar recht en informatisering, Universiteit van Tilburg en raadslid WRR

Arre Zuurmond, Zenc en bestuurslid Rathenau Instituut

Bijlage 2: Auteursinstructies casestudies

Voor het schrijven van de casestudies voor het project Databases in Beeld gelden de volgende richtlijnen. Deze richtlijnen moeten niet als een strak stramien worden beschouwd. De lijst is niet uitputtend. Daarnaast zijn niet alle aspecten even relevant voor alle casestudies. Ook kan het zijn dat in de loop van het traject, in wisselwerking tussen projectleiding en auteurs, de accenten verschuiven.

Centrale vragen

Centrale vragen bij iedere casestudie luiden:
- Welke keuzes zijn gemaakt op het gebied van de architectuur van databases?
- Welke (onbedoelde) gevolgen hebben die keuzes?
- Welke alternatieve keuzes zijn mogelijk?
- Dwingen de gevolgen tot herbezinning op de oorspronkelijke doelstellingen?

Nota bene: het gaat ons niet om een technische beschrijving van ICT-informatie-systemen, maar om de functies die ze (moeten) vervullen en de risico's die verbonden zijn aan het gekozen ontwerp.

Relevante aspecten casestudies

Inleiding
- Wat is de aanleiding voor invoering van de database/het informatiesysteem?
- Wat is de doelstelling: wat moet het systeem doen?

Vormgeving
- Welke gegevens worden verzameld?
- Welke verwerking, uitwisseling, koppeling en analyse van gegevens vindt plaats?
- Hoe lang worden gegevens bewaard?
- Welke partijen hebben toegang tot de gegevens?
- Hoe zijn de gegevens beveiligd, bijvoorbeeld tegen identiteitsdiefstal?
- Welke controle vindt plaats op de invoer, kwaliteit, verwerking, toegang en vernietiging van gegevens?

Werking in de praktijk
- Is het systeem werkbaar voor de betrokken professionals?
- Werkt het systeem effectief: draagt het daadwerkelijk bij aan de doelstellingen?

- Welke risico's doen zich voor? Denk hierbij aan interpretatieproblemen doordat data van hun context zijn ontdaan, foutieve koppelingen, misinterpretaties als gevolg van bestandsvervuiling of identiteitsdiefstal.
- Welk effect heeft het systeem op het werk van de professionals?
- Is de controle op de invoer, kwaliteit, verwerking, toegang en vernietiging van gegevens voldoende?

Positie van de burger
- Welk effect heeft het systeem op de positie van de burger (als klant, cliënt, patiënt, et cetera)?
- Hoe is het inzage- en correctierecht geregeld? Welke controlemogelijkheden heeft de burger? Volstaan deze?
- Bij wie kunnen burgers aankloppen als er iets fout gaat?
- Hebben burgers een 'opt out'-mogelijkheid?

Bredere issues
- Welk effect heeft het systeem op bestaande machtsverhoudingen?
- Kunnen de opgeslagen gegevens worden gebruikt voor andersoortige doeleinden? Is bij het ontwerp van het systeem bewust gekozen voor deze (extra) mogelijkheden?
- Leidt profilering tot praktijken van *social sorting* en aangepast, 'wenselijk' gedrag van burgers?

Alternatieven
- Welke alternatieve ontwerpkeuzes zijn mogelijk? Met wat voor gevolgen?
- Wat zou er gebeuren als er geen database/informatiesysteem zou zijn ingevoerd?

Over de historische casestudie over de gemeentelijke basisadministratie (GBA) wordt nader overleg gevoerd met de auteurs, omdat deze afwijkt van de overige cases.

Bijlage 3: Deelnemers expertmeeting Rathenau Instituut 19 maart 2010

Michiel Besters, onderzoeker afdeling Technology Assessment, Rathenau Instituut

Guus Bronkhorst, hoofd cluster Informatiebeleid Basisvoorzieningen Overheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Frans Brom, hoofd afdeling Technology Assessment, Rathenau Instituut

Alex Commandeur, hoofd afdeling toezicht publieke sector, College bescherming persoonsgegevens

Egbert Dommering, hoogleraar theorie van informatierecht, Instituut voor Informatierecht (IViR), Universiteit van Amsterdam

Bart Jacobs, hoogleraar computerbeveiliging, Radboud Universiteit Nijmegen

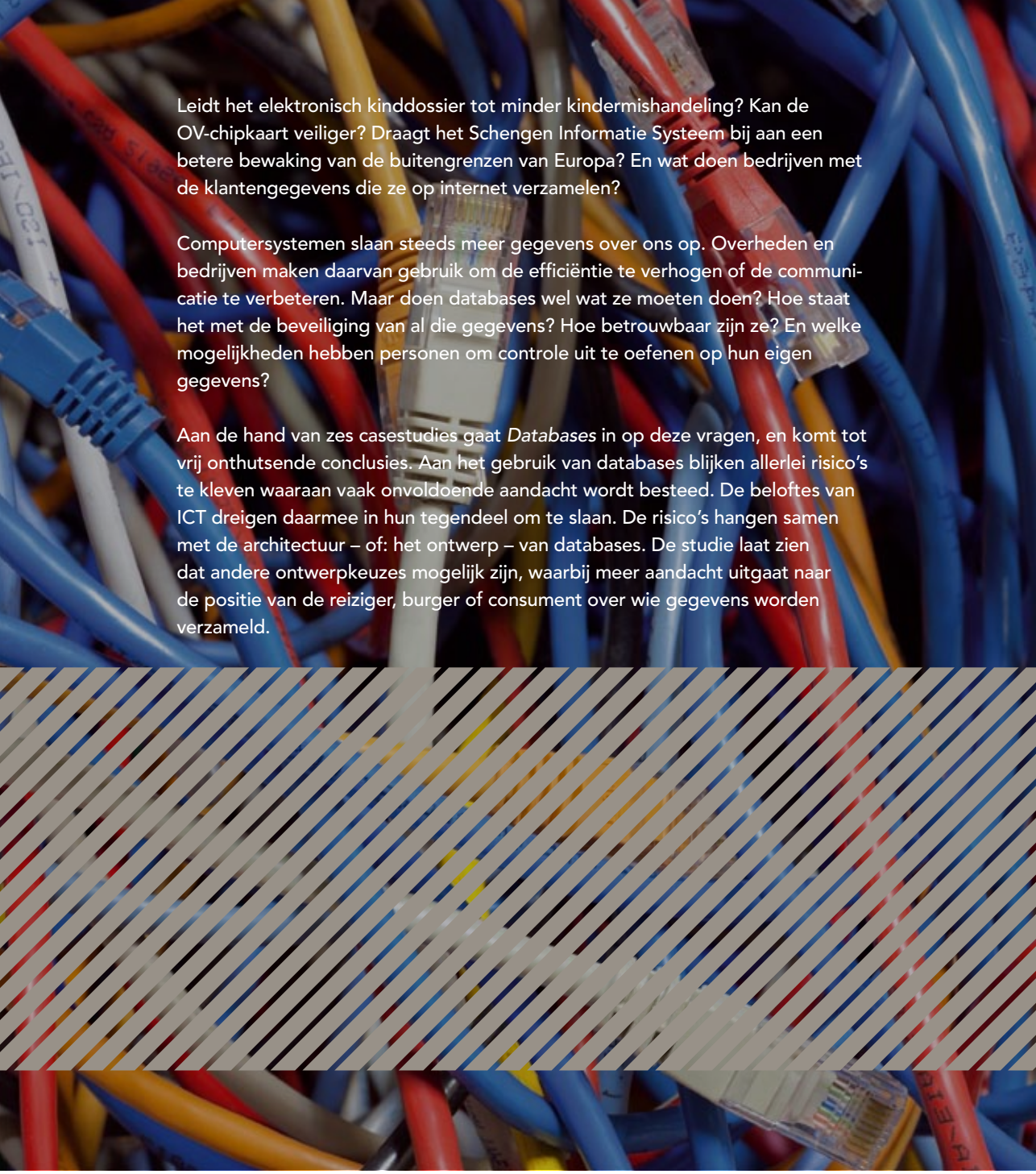
Ronald Leenes, hoogleraar regulering door technologie, Universiteit van Tilburg

Xander van der Linde, adviseur Burgerlink, ICTU

Geert Munnichs, coördinator afdeling Technology Assessment, Rathenau Instituut

Matt Poelmans, directeur Burgerlink, ICTU

Wie was Rathenau?
Het Rathenau Instituut is genoemd naar professor dr. G.W. Rathenau (1911-1989). Rathenau was achtereenvolgens hoogleraar experimentele natuurkunde in Amsterdam, directeur van het natuurkundig laboratorium van Philips in Eindhoven en lid van de Wetenschappelijke Raad voor het Regeringsbeleid. Hij kreeg landelijke bekendheid als voorzitter van de commissie die in 1978 de maatschappelijke gevolgen van de opkomst van micro-elektronica moest onderzoeken. Een van de aanbevelingen in het rapport was de wens te komen tot een systematische bestudering van de maatschappelijke betekenis van technologie. De activiteiten van Rathenau hebben ertoe bijgedragen dat in 1986 de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA) werd opgericht. NOTA is op 2 juni 1994 omgedoopt in Rathenau Instituut.



Leidt het elektronisch kinddossier tot minder kindermishandeling? Kan de OV-chipkaart veiliger? Draagt het Schengen Informatie Systeem bij aan een betere bewaking van de buitengrenzen van Europa? En wat doen bedrijven met de klantengegevens die ze op internet verzamelen?

Computersystemen slaan steeds meer gegevens over ons op. Overheden en bedrijven maken daarvan gebruik om de efficiëntie te verhogen of de communicatie te verbeteren. Maar doen databases wel wat ze moeten doen? Hoe staat het met de beveiliging van al die gegevens? Hoe betrouwbaar zijn ze? En welke mogelijkheden hebben personen om controle uit te oefenen op hun eigen gegevens?

Aan de hand van zes casestudies gaat *Databases* in op deze vragen, en komt tot vrij onthutsende conclusies. Aan het gebruik van databases blijken allerlei risico's te kleven waaraan vaak onvoldoende aandacht wordt besteed. De beloftes van ICT dreigen daarmee in hun tegendeel om te slaan. De risico's hangen samen met de architectuur – of: het ontwerp – van databases. De studie laat zien dat andere ontwerpkeuzes mogelijk zijn, waarbij meer aandacht uitgaat naar de positie van de reiziger, burger of consument over wie gegevens worden verzameld.

9 789077 364338 >