Telematica
Instituut

Persoonsinformatie- of identiteitsbeleid?

Identiteitsvaststelling en elektronische dossiers in het licht van maatschappelijke en technologische ontwikkelingen

Auteurs:

Rogier Brussee
Lex Heerink
Ronald Leenes
Sjaak Nouwt
Martin Pekarek
Annemarie Sprokkereef
Wouter Teeuw

Telematica
Instituut

TELEMATICA INSTITUUT, ENSCHEDE, REPORT TI/RS/2008/034

Inhoudsopgave

Afkortingen **5**
1 Inleiding **7**
1.1 Opdrachtformulering 7
1.2 Interpretatie van de vraagstelling 8
2 Belangrijke ontwikkelingen voor het persoonsinformatiebeleid **11**
2.1 Nieuwe noties van privacy 11
2.1.1 Connect & share 11
2.1.2 Personalisatie 12
2.2 Transparantie en vertrouwen 14
2.2.1 Good governance 14
2.2.2 Diensten via elektronische kanalen 15
2.3 Technologie 16
2.3.1 Identiteit 16
2.3.2 Identiteitsfraude 17
2.3.3 Privacy Enhancing Technologies (PET) 18
2.3.4 Overige technologie gerelateerde trends 20
2.3.5 E-overheid / service oriëntatie 20
2.4 Conclusies 22
3 Effecten in de praktijk bij Justitie, basisregistraties en elektronische dossiers **23**
3.1 Cases op het terrein van Justitie 23
3.1.1 Identiteitsvaststelling in de strafrechtketen (bestaande casus) 23
3.2 Cases rond persoonsdossiers 33
3.2.1 Elektronisch patiëntendossier EPD (casus in ontwikkeling) 33
3.2.2 Elektronisch kinddossier Jeugdgezondheidszorg EKD-JGZ (casus in ontwikkeling) 45
3.3 Cases rond e-overheid processen 53
3.3.1 Digitaal klantdossier DKD (bestaande casus) 53
3.3.2 Omgevingsvergunning (casus in ontwikkeling) 61
4 Ontwikkelingen in het persoonsinformatiebeleidsdomein in het licht van het juridisch kader **67**
4.1 Noties van privacy 67
4.2 Transparantie en vertrouwen 68
4.3 Technologie 68
4.4 Tot slot 70
5 Samenvatting en conclusies **73**
5.1 Terugblik op maatschappelijke en technologische trends 73
5.2 Casus specifieke conclusies 73
5.2.1 Kansen 74
5.2.2 Bedreigingen 75
5.3 Spanningsveld databescherming versus nieuwe noties privacy 76
5.3.1 Risicobewustzijn 77
5.3.2 Persoonsgegevens en identiteit 77
5.4 Spanningsveld vertrouwen versus uitwisselen 79
5.4.1 Risicoklassen van persoonsgegevens 79
5.4.2 Verantwoordelijkheid 80
5.4.3 Burgerservicenummer (BSN) 81
5.5 Technologie als kans of bedreiging 82
5.5.1 Identiteitsfraude 82

5.5.2 Macromyopia 83
Referenties 85
Appendix A: Begeleidingscommissie 89
Appendix B: Geïnterviewden 91
Appendix C: Case study protocol 93
Appendix D: Brief SZW over beveiligingsplannen Suwi-net gemeenten 95
Appendix E: Wet bescherming persoonsgegevens 97
E.1 Wanneer is de Wbp van toepassing? 97
E.2 Relevante begrippen uit de Wbp 98
E.3 Relevante bepalingen uit de Wbp 100

Afkortingen

BIG	Wet Beroepen in de Individuele Gezondheidszorg
BSN	Burgerservicenummer
BKWI	Bureau Keteninformatisering Werk en Inkomen
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CBP	College bescherming persoonsgegevens
CIBG	Centraal Informatiepunt Beroepen Gezondheidszorg
CJD	Centrale Justitiële Documentatiedienst
CJG	Centrum voor Jeugd en Gezin
CP-ICT	Coördinatiepunt ICT Gemeenten
CWI	Centrum voor Werk en Inkomen
DKD	Digitaal Klant Dossier
EKD	Elektronisch Kind Dossier
EMD	Elektronisch Medicatie Dossier
eNIK	Elektronische Nationale IdentiteitsKaart
EPD	Elektronisch Patiënten Dossier
GBA	Gemeentelijke basisadministratie Persoonsgegevens
GBZ	Goed Beheer Zorgsystemen
GGD	Gemeentelijke Gezondheidsdienst
GSD	Gemeentelijke Sociale Dienst
HIS	Huisartsinformatiesysteem
IBG	Informatie Beheer Groep
IGZ	Inspectie voor de Gezondheidszorg
JGZ	Jeugdgezondheidszorg
LSP	Landelijk SchakelPunt
NAW	Naam Adres Woonplaats gegevens
Nictiz	Nationaal ICT Instituut in de Zorg
NFI	Nederlands Forensisch Instituut
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
PET	Privacy Enhancing Technology
PIB	Persoonsinformatiebeleid
PIP	Persoonlijke Internet Pagina
PKI	Public Key Infrastructure
PPS	Publiekprivate samenwerking
RDW	Dienst Wegverkeer

SKN	StrafrechtsKetenNummer
SBV-z	Testtool Sectorale Berichten Voorziening in de Zorg
SVB	Sociale Verzekering Bank
SZW	Ministerie van Sociale Zaken en Werkgelegenheid
UWV	Uitvoeringsinstituut WerknemersVerzekeringen
UZI	Unieke Zorgverlener Identificatie
VIP	VerwijsIndex Personen strafrechthandhaving
VIR	Verwijsindex Risicojongeren
VNG	Vereniging van Nederlandse Gemeenten
VROM	Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
VWS	Ministerie van Volksgezondheid Welzijn en Sport
Wabo	Wetsvoorstel algemene bepalingen omgevingsrecht
Wbp	Wet bescherming persoonsgegevens
Wbsn-z	Wet gebruik BSN in de zorg
Wcpv	Wet collectieve preventie volksgezondheid
WDH	Waarneemdossier Huisartsen
Wet pg	Wet publieke gezondheid
WEU	Wet eenmalige uitvraag werk en inkomen
Wgbo	Wet geneeskundige behandelingsovereenkomst
WIA	Wet Werk en Inkomen naar Arbeidsvermogen
Wjz	Wet op de jeugdzorg
WW	Werkloosheidswet
WWB	Wet werk en bijstand
ZIS	Ziekenhuisinformatiesysteem

1 Inleiding

1.1 Opdrachtformulering

Het huidige persoonsinformatiebeleid is vastgelegd in 1991 en kent vier (principiële) uitgangspunten:
1. Persoonsgegevens worden decentraal beheerd (gemeenten).
2. Gegevens worden enkelvoudig uitgevraagd.
3. Gegevens worden niet langer dan noodzakelijk opgeslagen (tijdelijk).
4. Gegevens worden multifunctioneel gebruikt.

Ondertussen is de wereld veranderd met ontwikkelingen als de *elektronische overheid*. Ook speelt de vraag hoe het persoonsinformatiebeleid zich verhoudt tot de Wet bescherming persoonsgegevens. Dit geeft aanleiding het persoonsinformatiebeleid te evalueren en/of te herijken. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) wenst in 2009 te komen tot een beleidsrapportage aan de Ministerraad en aan de Tweede Kamer ten aanzien van persoonsinformatiebeleid (PIB).

> *"Persoonsinformatiebeleid is de zorg voor een doeltreffend en doelmatig gebruik van persoonsgegevens door overheidsinstellingen voor het uitvoeren van hun taken, dit met inachtneming van het wettelijk kader."*

In deze context heeft eLaw Leiden een eerste evaluatie uitgevoerd van de Wet bescherming persoonsgegevens (Wbp) en zijn een aantal knelpunten geïdentificeerd (Zwenne e.a., 2007). Daarnaast heeft Zenc een onderzoek naar de toekomst van persoonsinformatiebeleid uitgevoerd (Azouz e.a., 2007). Uit deze rapporten en de daarover gevoerde discussie zijn actiepunten gekomen die zich lenen tot het doen van onderhavig vervolgonderzoek. De volgende probleemstelling dient als uitgangspunt voor dit vervolgonderzoek:

> *Moet het persoonsinformatiebeleid worden herijkt op de belangrijkste terreinen waar de overheid beleid entameert om informatievoorziening te stroomlijnen, in het licht van de kansen en bedreigingen van ICT voor overheid en burger?*

Het onderzoek geeft specifiek antwoord op de volgende vier deelvragen:
1. Welke technische, bestuurlijke en organisatorische ontwikkelingen zijn van belang in het kader van het persoonsinformatiebeleid?
2. Welke effecten zien we hiervan in praktijk van Justitie, basisregistraties en elektronische dossiers zoals EKD, EPD, EMD en DKD?
3. Hoe verhouden de ontwikkelingen zich tot de het juridische kader zoals dit wordt vorm gegeven door de Wbp?
4. Welke conclusies zijn te trekken uit mogelijke spanningen tussen uitvoeringspraktijk en juridisch kader?

1.2 Interpretatie van de vraagstelling

Het rapport 'De toekomst van persoonsinformatiebeleid' (Azouz e.a., 2007) gaat in op de vraag of het wenselijk is te komen tot een herijking van het persoonsinformatiebeleid van het ministerie van BZK, gezien de hoeveelheid maatschappelijke, internationale, bestuurlijke, organisatorische, technologische en juridische ontwikkelingen. Hoofdconclusies van het onderzoek zijn:

- Het is noodzakelijk om het gebruik van gegevens altijd in de context van het gebruik te zetten.

- Persoonsinformatiebeleid kan zich niet beperken tot afzonderlijke organisaties, informatie verspreidt zich in een netwerk van organisaties.

- Afwegingen over het gebruik van gegevens moeten dus altijd in dit netwerk plaatsvinden.

- Belangen ten aanzien van het persoonsinformatiebeleid moeten evenwichtig worden afgewogen, doelbinding staat voorop.

Wij gebruiken het rapport 'De toekomst van persoonsinformatiebeleid' (Azouz e.a., 2007) als uitgangspunt, maar willen de volgende gezichtspunten toevoegen:

- Nieuwe noties van privacy. Traditioneel heeft informationele privacy te maken met bescherming van persoonsgegevens en inzage in wat er over jou is vastgelegd en wat daarmee gebeurt. In de huidige praktijk is het al de vraag in hoeverre het inzagerecht daadwerkelijk kan worden uitgeoefend (denk bijvoorbeeld aan cameratoezicht). We gaan toe naar een informatiemaatschappij waarin gigantisch veel informatie wordt verzameld en door koppeling van informatiebronnen nieuwe, afgeleide informatie ontstaat. Daarbij is het de vraag of je redelijkerwijs nog kan weten waar wat over je is vastgelegd, en in welke mate het inzagerecht in de praktijk wel is uit te oefenen. Dit vereist mogelijk een andere, minder traditionele kijk op privacy.

  Nieuwe noties van privacy kunnen ook betrekking hebben op bescherming van de eigen identiteit. De notie van privacy verandert dan bijvoorbeeld in die zin, dat het niet (alleen) een zelfstandig te beschermen waarde is, maar (ook) een middel ter bescherming van de eigen identiteit. Denk hierbij bijvoorbeeld aan een kwaadwillende persoon die gebruik maakt van de identiteit van een ander (identiteitsdiefstal) en daardoor deze identiteit in relatie brengt met bijvoorbeeld terrorisme of pedofilie.[1]

- Transparantie en vertrouwen gezien vanuit ICT als bedreiging en/of als oplossing. Naast dreiging van buiten de overheid kan er ook dreiging zijn van binnenuit. Vertrouwen van de burger heeft te maken met in transparantie over wat er wordt vastgelegd (in basisregistraties, in dossiers, of in andere meer informele systemen), wie zijn gegevens kan inzien, wie ze ook mag inzien en voor welke doelen, en wie ze eventueel zou kunnen opvragen, nu of in de toekomst. Tevens heeft het te maken met hun zorgvuldig er met hun gegevens worden omgesprongen (voorbeelden: verloren

[1] Zie bijvoorbeeld Charles den Tex, 'Straks wordt ik nog gezocht voor pedofilie'. NRC Handelsblad, 2 september 2008.

USB sticks bij justitie en defensie). Onzekerheid over de vraag wie toegang heeft tot medische gegevens kan, bijvoorbeeld, effect hebben op het wel of niet naar een arts gaan of het opnemen van telefoongesprekken kan uitmaken voor wat er wordt gezegd.

Transparantie en vertrouwen heeft niet alleen betrekking op vertrouwen van burgers in de overheid, maar werkt ook de andere kant op. Het is voor burgers immers makkelijker geworden om de communicatie met ambtenaren te loggen, bijvoorbeeld door telefoongesprekken op te nemen. Ambtenaren zullen wellicht meer op hun woorden moeten gaan letten en erop moeten vertrouwen dat datgene wat ze zeggen niet in een later stadium tegen ze gebruikt gaat worden. Met het oog hierop zou het begrip ‘vertrouwen’ wellicht meer inzichtelijk moeten worden gemaakt.

- Technologie. Technologische ontwikkelingen kunnen een bedreiging vormen voor de privacy (denk aan cybercrime), maar tegelijkertijd kan technologie ook een oplossing zijn (*privacy enhancing technologies*). De informatisering in diverse ketens maakt dat processen automatisch worden afgehandeld, zonder menselijke tussenkomst. Welke relevante technologische ontwikkelingen spelen? En hoe realistisch zijn ze? En wat is hun mogelijk effect op het persoonsinformatiebeleid?

- Concretiseren via cases. Aan de hand van cases kijken we hoe beleidsprincipes zich vertalen naar de concrete praktijk of concrete handvaten. Krijgt de burger wat hij wil? Wat zijn tastbare gevolgen voor burgers? Het rapport ‘De toekomst van persoonsinformatiebeleid’ (Azouz e.a., 2007) bekijkt al een aantal cases, wij voegen cases toe op met name het gebeid van justitie en de elektronische dossiers.

2 Belangrijke ontwikkelingen voor het persoonsinformatiebeleid

Nieuwe technologie heeft in de laatste jaren veel zaken binnen bereik gebracht, die daarvoor niet mogelijk of niet kosteneffectief waren. Voorbeelden hiervan zijn het koppelen van gegevensbestanden ter bestrijding van fraude, of cameratoezicht. In de context van de privacybalans is niet zozeer de technologie op zich interessant, maar eerder het gebruik en de mogelijkheden die met nieuwe technologie binnen bereik komen. Het is van belang dit gebruik te plaatsen in de organisatorische en bestuurlijke ontwikkelingen. Hierbij kan men denken aan internationalisatie, centralisatie en decentralisatie, horizontalisering van toezicht en privatisering.

In dit hoofdstuk zullen wij ontwikkelingen in kaart brengen en daarbij beschrijven hoe deze ontwikkelingen de privacybalans beïnvloeden en zouden kunnen beïnvloeden. In het rapport 'De toekomst van persoonsinformatiebeleid' staan al een groot aantal ontwikkelingen beschreven (Azouz e.a., 2007; hoofdstuk 4). Conclusie is dat de maatschappelijke, juridische en internationale ontwikkelingen laten zien dat informationele privacy de afgelopen jaren onder druk is komen te staan. Wij doen deze inventarisatie van ontwikkelingen niet over, maar voegen onze visie toe vanuit de gezichtspunten als genoemd in sectie 1.2: nieuwe noties van privacy, transparantie en vertrouwen van de burger, en technologische ontwikkelingen.

Het resultaat is een overzicht van relevante trends. Vervolgens zal in hoofdstuk 3 de impact van deze trends worden geïnterpreteerd in de context van de privacygevoelige toepassingen zoals geselecteerd via een aantal casussen.

2.1 Nieuwe noties van privacy

2.1.1 Connect & share

De menselijke behoefte aan communicatie is basaal. Nieuwe technologische ontwikkelingen hebben ook nieuwe vormen van communicatie mogelijk gemaakt. In het bijzonder zijn burgers altijd bereikbaar (*always connected, on-line*), en zetten hun –soms privacy gevoelige– informatie op Internet (*Hyves, LinkedIn*) of delen die via *communities* of *blogs*. Dit heeft invloed op zowel de communicatie met de overheid als het privacy beleid. Mogelijk zijn nieuwe noties van privacy nodig. Ontwikkelingen zijn:

- Waar gebruikers altijd *connected* zijn verwacht men dat ook van de overheid. Staatsecretaris Heemskerk spreekt in zijn ICT-agenda over "Veel diensten, zowel van overheid als bedrijfsleven, zijn 24 uur per dag digitaal beschikbaar en toegankelijk en worden gebruikt op momenten dat de gebruiker het wil. Ook professionals binnen de overheid kunnen beschikken over relevante informatie en diensten. (EZ, 2008)" Om dit te realiseren zullen heel veel zaken automatisch, zonder menselijke tussenkomst, moeten kunnen worden afgehandeld.

- De notie van privacy verandert ook doordat steeds meer burgers via hun virtuele identiteit (soms zelfs zeer persoonlijke) informatie over zichzelf op internet

publiceren. Personen blijken bereid om, via bijvoorbeeld *Hyves* of *MySpace*, heel veel informatie over zichzelf met de buitenwereld te delen. Dit roept een aantal vragen op. Gegevens die de overheid zorgvuldig beschermt zijn mogelijk allang publiek beschikbaar. Uiteindelijk heeft de burger het recht om zelf te beslissen wat hij of zij over zich zelf prijsgeeft maar wellicht moeten burgers ook tegen zichzelf worden beschermd, want data die eenmaal op Internet staat gaat er 'nooit' meer af. Tevens wordt er data gedeeld over "de buren", of in ieder geval is heel veel informatie af te leiden door bronnen te combineren. Ook (kleine) blunders van de overheid of een ambtenaar kunnen op Internet uitvoerig worden uitgemeten, met alle gevolgen van dien.

- Burgers willen meedenken en meepraten[2]. Men wil zich uiten en deel uitmaken van de groep. Op de site www.privacyproject.nl, bijvoorbeeld, kunnen burgers zelf filmpjes, foto's, audio en tekst plaatsen waarin ze vertellen wat hun visie op privacy is. Een ander voorbeeld is de stijging van het aantal buurtportals die vaak een overzicht geven van wat leeft in de wijk. Dergelijke discussiegroepen richten zich mede op onderwerpen die direct relateren aan het overheidsbeleid of overheidsdienstverlening waarin persoonsinformatie een rol kan spelen. Verschillende gemeenten zijn al aan de slag gegaan met het *web 2.0* concept, dat zich kenmerkt door een meer actieve rol van gebruikers (Frissen e.a., 2008).

- Koppelen van (elektronische) informatiebronnen gebeurt al heel lang, maar de schaal waarop dit gebeurt en de mogelijkheden om informatie (semantisch) te relateren zijn veranderd door de technologieontwikkelingen. De koppeling van informatiebronnen en het gebruik van uniforme identifiers, zoals het BSN[3], kan van invloed zijn op de identiteit van de burger (die tegelijkertijd een ouder kan zijn, wetenschapper, sporter, activist, belastingbetaler, patiënt, etc.). Door het gemis van contextinformatie kan vervolgens een onjuist samengestelde identiteit ontstaan[4]. De digitale identiteit kan de sociale identiteit van de burger onder druk zetten.

2.1.2 Personalisatie

Informatietechnologie maakt het mogelijk de juiste informatie op de juiste tijd op de juiste plaats af te leveren. Profielen spelen hier vaak een onderliggende rol. Gebruikers hebben zelf aangegeven wat hun voorkeuren zijn, of deze zijn afgeleid van hun gedrag (surfgedrag op Internet). Hierdoor kunnen diensten op maat worden aangeleverd. Dit zal zich ook doorzetten richting overheidsdiensten. Zo wordt er binnen MijnOverheid.nl aan gedacht om nieuwsfeeds met nieuws uit de gemeente van de betreffende burger te tonen. Tevens is het mogelijk bij een aantal gemeenten om je als burger te abonneren op een informatiedienst over vergunningen waardoor je op de hoogte wordt gesteld van vergunningsaanvragen in je eigen en aanpalende postcodegebieden. Ontwikkelingen met betrekking tot personalisatie zijn:

---

[2] Hoewel: "Slechts 28% van de burgers hecht belang aan participeren in maatschappelijke discussies en debatten." Bron: InOverheid.nl, Overheid heeft te hoge verwachtingen van burgers. Nieuwsbericht, 22 september 2008.

[3] Merk op dat ook al kunnen 'technisch gezien' bestanden eenvoudig gekoppeld worden (door bijvoorbeeld standaardisatie of een BSN), een feitelijke koppeling zelf nog steeds gebonden is aan het wettelijk kader dat bepaalt wat wel of niet mag worden gekoppeld.

[4] Aan de andere kant is het ook weer zo dat het kiezen voor één persoonsnummer de foutmarge in gegevensbestanden kan verkleinen. Dit is er de reden van dat er in de zorg niet is gekozen voor een eigen persoonsnummer (zie ook sectie 3.2.1.8).

- *Ambient Intelligence* is een visie op de toekomst waarin de mens wordt omringd door een 'slimme omgeving' die niet alleen weet dat er mensen aanwezig zijn, maar ook wie, met welke eigenschappen, en mogelijk zelfs met een inschatting van emoties, behoeften en intenties. De intelligente omgeving kan zich daaraan aanpassen, erop reageren of erop anticiperen. Het is duidelijk dat hier privacy aspecten spelen, in het bijzonder rond het koppelen van omgevingsinformatie aan persoonsinformatie, en rond het feit dat in deze visie apparatuur zodanig in de omgeving van de persoon wordt verwerkt dat hij er nauwelijks iets van merkt (fysieke inbedding) en hij er op een 'natuurlijke' manier mee kan communiceren (sociale inbedding). Een van de potentiële toepassingen van Ambient Intelligence is de zorg (Schuurman e.a., 2007). Het gebruik van velerlei sensoren in de zorg roept ook weer vragen op, bijvoorbeeld (denk ook aan dementie) wie aan wie toestemming moet vragen om welke sensorinformatie te mogen gebruiken.

- Personalisatie is mede mogelijk door verbeterde technologie om personen of hun gedrag te monitoren. Als voorbeeld binnen Justitie beschrijven Kruissink e.a (2007) hoe op experimentele basis gevangenen bij de DJI in Lelystad worden voorzien van een elektronisch label (RFID polsband) om hen te kunnen monitoren. Naast gebruik voor identificatiedoeleinden of om te zien wie waar is, is uiteindelijke de doelstelling recidive vermindering: door te individualiseren kunnen effectievere, op maat gesneden programma's worden geleverd. Het individueel herkennen van gedetineerden en het aanmaken en koppelen van digitale dossiers geeft inzicht in wie met wie omgaat, wat men doet, etc., en vergroot zo het voorspellende vermogen. Ook gedrag op Internet kan hierin worden meegenomen[5]. Ook spelen efficiëntie en kosten een rol (minder personeel nodig).

  Teeuw en Vedder (2008) beschrijven mede naar aanleiding van deze casus hoe convergerende technologieën het mogelijk maken dat vele variabelen online worden bijgehouden of gestuurd, en vertalen dit naar toekomstige scenario's rond monitoring. Te denken valt aan sensoren of actuatoren in het lichaam of op de huid die inzicht geven in de fysieke gesteldheid (bijvoorbeeld voor doeleinden van leugendetectie) of lab-on-a-chip ontwikkelingen (nano- en biotechnologie) die snelle analyses mogelijk maken. Men zou, bijvoorbeeld urine in een (scheidings)toilet kunnen analyseren op drugsgebruik. Ook kan uit DNA steeds meer worden afgeleidt[6]. De vraag speelt wat je allemaal kan of mag monitoren, wat hieruit allemaal af te leiden is, en in hoeverre de betrokkenen hiervan wel of niet expliciet op de hoogte moeten worden gebracht.

- Gepersonaliseerde communicatie wordt mogelijk. Een voorbeeld is Lonely Planet[7] die een online tool heeft ontwikkeld waarmee je een compleet eigen reisgids kan samenstellen, als alternatief voor de standaard reisgidsen. Een ander voorbeeld is *narrowcasting*, het door middel van audiovisuele displays benaderen van een of meer

[5] Hierbij speelt (wetenschappelijk gezien) de vraag rond de betrouwbaarheid van de analyses van de waargenomen data: Vanuit afgeleide data (mogelijk verzameld zonder dat iemand het weet, of gedrag op Internet) wordt een beeld bepaald, maar in hoeverre is dat beeld nog congruent met de werkelijke persoon?

[6] Recent hebben onderzoekers uit IJsland en Nijmegen in het DNA van mensen van Europese origine genvarianten gevonden die duidelijk verband houden met oog-, haar- en huidskleur (Sulem e.a., 2007). Dit maakt het mogelijk om op basis van uitsluitend iemands DNA steekhoudende uitspraken te doen over de kleur van zijn haar, huid of ogen.

[7] http://www.lonelyplanet.com/

specifieke doelgroepen, op een specifieke plaats en op specifieke momenten. De inhoud is daarbij op maat gesneden voor de (op dat moment aanwezige) ontvangers. De overheid weet veel van haar burgers, en zou dit kunnen gebruiken om persoonlijke (pro-actieve) dienstverlening richting haar burgers tot stand te brengen. Hoe ver je hierin kunt en wilt gaan hangt af van de notie van privacy. Een middel om dit realiseren is het gebruik van portlet technologie[8]. Hiermee kunnen gebruikers, net zoals bij iGoogle, de voor hun situatie relevante overheidsdiensten kiezen. Bedrijvenloket experimenteert reeds met portlet technologie, en ook het Digitaal Klant Dossier maakt gebruik van portlettechnologie.

2.2 Transparantie en vertrouwen

2.2.1 Good governance

Het rapport 'De toekomst van persoonsinformatiebeleid' (Azouz e.a., 2007) geeft al aan dat afwegingen over het gebruik van gegevens altijd in een netwerk plaatsvinden. Technologie speelt hierbij een ondersteunende rol: Enerzijds door het koppelen van gegevensbestanden, anderzijds door samenwerking in teams of tussen organisaties te ondersteunen (*Microsoft Sharepoint*, etc.). Belangrijke ontwikkelingen zijn:

- We observeren, vanuit de doelstelling tot betere dienstverlening (kwaliteit), administratieve lastenverlichting (efficiëntie), of handhaving en toezicht (veiligheid) een toenemende koppeling van informatiebestanden. Een voorbeeld hiervan is de Dienst Werk en Inkomen (DWI) van de gemeente Amsterdam die haar gegevens van werkzoekenden koppelt aan de vacaturebank van het Centrum voor Werk en Inkomen (CWI) opdat werkzoekenden sneller aan een baan komen[9]. Een ander voorbeeld is de vooringevulde aangifte inkomstenbelasting, waarin loongegevens en WOZ-waarde al zijn verwerkt. Weer andere voorbeelden zijn de verstrekking van vlieggegevens aan VS in het kader van terreurdreiging, of het gebruik van nuts gegevens zoals watergebruik per huishouden om sociale fraude op te sporen.

  Deze trend lijkt onomkeerbaar, maar er kunnen wel een aantal kanttekeningen bij worden geplaatst. De burger heeft geen goed beeld welke informatie van hem/haar waar terecht komt en voor welk doeleinde. Burger kan gevoel krijgen dat 'niets meer veilig is voor de handen van de overheid'. Als het gaat om de betrouwbaarheid van informatie, is het vertrouwen in de overheid betrekkelijk gering (Dekker, 2001)[10]. En als een vooringevuld formulier de basis voor de aanslag wordt, moet de burger aantonen dat er een fout zit in de gegevens van de fiscus (omkering 'bewijslast'). Het zou ook onduidelijk voor de burger kunnen zijn waar hij moet klagen als bepaalde informatie incorrect is volgens hem/haar. Het wettelijk kader bepaalt welke gegevens over een persoon al of niet direct kunnen worden gekoppeld. Dit is niet noodzakelijkerwijs ook de perceptie van de burger. Immers, de telecom operator

[8] *Portlets* zijn toepassingen (componenten) die op basis van bepaalde afspraken (open standaarden) eenvoudig kunnen worden toegevoegd aan / samengesteld tot een website binnen een web portal. In tegenstelling tot een traditionele web service omvat een portlet niet alleen de functionaliteit van de toepassing, maar ook de presentatie ervan en de interactie ermee.
[9] http://www.computable.nl/artikel/ict_topics/overheid/2675739/1277202/sociale-dienst-sluit-aan-op-vacaturebank-cwi.html
[10] Zie ook ontwikkelingen als http://www.wijvertrouwenstemcomputersniet.nl/

weet waar ik ben, belastingdienst wat ik verdien, de arts wat ik mankeer, etc. Zo is er al met al heel veel bekend (ook al mag dat niet gekoppeld worden).

- Er is een toenemende publiekprivate samenwerking (PPS). Een voorbeeld hiervan is de WMO, waar gemeenten contacten onderhouden met, en doorverwijzen naar, particuliere thuiszorgorganisaties. Een ander voorbeeld is re-integratie, waar commerciële re-integratiebedrijven vaak bij de re-integratie van een klant zijn betrokken. Het lijkt een trend te zijn dat de overheid steeds meer van haar oorspronkelijke taken afstoot, deels onder invloed van de roep om meer marktwerking. In tegenstelling tot publieke aanbesteding bemoeit de overheid zich bij PPS-constructies niet met de inhoud en stuurt volledig op het gewenste einddoel. Op deze wijze hebben de marktpartijen alle vrijheid om naar eigen inzicht de uitvoering vorm te geven. Meeste PPS-constructies zie je in de bouw (grote infrastructurele projecten), maar ook andere terreinen zijn in opkomst. Hierbij zouden ook persoonsgegevens een rol kunnen gaan spelen, bijvoorbeeld rond de medische of sociale ketens. Een ander voorbeeld is ook de uitwisseling van camerabeelden tussen de publieke en private sector. Denk bijvoorbeeld aan de beveiliging van semi-publieke ruimtes als winkelcentra en stations.

- Identiteitsmachtiging zal toenemen. Soms zal een burger of bedrijf niet zelf diensten afnemen bij de overheid, maar laat men zich vertegenwoordigen door een derde partij die namens de burger of het bedrijf optreedt. Deze situaties ontstaan als burgers of bedrijven zelf geen diensten kunnen, willen of mogen afnemen, bijvoorbeeld bij wilsonbekwaamheid, bij het uitbesteden van handelingen (zoals bij de accountant), of bij het van rechtswege gedwongen uitbesteden van handelingen (bijvoorbeeld een ondercuratelestelling). De overheid is bezig met het opzetten een van een Gemeenschappelijke Machtigings Voorziening (GMV)[11]. De GMV stelt burgers en bedrijven in staat zich bij elektronische dienstverlening door de overheid door een ander te laten vertegenwoordigen. Voorbeelden zijn het aanvragen van zorg door een kleinkind, of het uitbesteden van de belastingaangifte door een assurantiekantoor. De GMV is een aanvullende functionaliteit op DigiD. GMV is een programma dat uitgevoerd wordt door ICTU, de beoogde beheerder is GBO.overheid. In de huidige planning wordt er vanaf 1 april 2009 gestart met proeven bij de belastingdienst. Vanaf 2010 wordt GMV ingezet als overheidsbrede voorziening.
  De mogelijkheid je te laten vertegenwoordigden bij het doen van overheidszaken roept allerlei vragen op met betrekking tot persoonsinformatiebeleid, met name betreffende de toegang tot, en het gebruik van de persoonsgegevens van de machtiger door de vertegenwoordiger. In dit rapport zal niet nader worden ingegaan op persoonsinformatiebeleid ten aanzien van machtigingssituaties..

2.2.2 Diensten via elektronische kanalen

Naast meer betrokken organisaties zie we ook de ontsluiting van gegevens via meerdere kanalen, zoals post, telefoon, balie, e-mail, website, chat, etc. Dit hangt deels ook samen met het feit dat burgers ‘gemak’ willen. Voorbeelden zijn:

- Multi-channeling op zichzelf betekent dat dezelfde functionaliteit via meerdere ontsluitingsmogelijkheden wordt aangeboden zoals via Internet, de balie of

[11] Zie http://www.e-overheid.nl/e-overheid/projecten/gmv/

telefonisch. Het project Kanalen in Balans[12] houdt zich met de effecten van multichanneling voor de publieke dienstverlening. Uit studies van Jan van Dijk cs[13] blijkt dat

- de kanaalkeuze van burgers afhankelijk is van het type dienst, de situatie waarin de burger zich bevindt, en de kanaalkenmerken (telefoon → snelheid, balie→ zekerheid, website → goedkoop)

- het gebruik van elektronische kanalen toeneemt, met name voor simpele diensten zoals het invullen van een formulier. Voor complexe diensten hebben de traditionele kanalen zoals balie en telefoon nog steeds voorkeur

- elektronische kanalen beter scoren op wachttijd en bereikbaarheid, terwijl traditionele kanalen juist beter gewaardeerd worden op het gebied van persoonlijkheid, duidelijkheid en volledigheid.

Binnen het project Kanalen in Balans is geen onderzoek gedaan naar de relatie tussen kanaalgebruik en de invloed ervan op privacy. Wel is het aannemelijk dat er een relatie bestaat tussen de gehanteerde authenticatie strategie en het kanaal: hoe zwakker de authenticatie van het kanaal, hoe minder persoonsgegevens ontsloten zullen worden over dit kanaal. Deze stelling is echter niet door onderzoek onderbouwd. De kernvraag is welke informatie veilig over welk kanaal kan worden verstrekt. Dit speelt ook vanuit een beveiligingsperspectief.

- Een andere trend is de gegevensontsluiting door middel van heel veel portalen op Internet. Voorbeelden zijn MijnOverheid.nl, DKD, gemeentelijke portalen, Bedrijvenloket, themaportalen zoals ‘onderwijs en bijverdienen’ of ‘expats’, IBG, etc. Veel overheidsorganisaties ontsluiten gegevens via portalen niet alleen omdat het handig is voor de burger, maar ook om zichtbaarheid te zijn voor de burger. Vanuit persoonsinformatiebeleid spelen vragen rondom authenticatie (via DigiD). Tevens is er het gevaar van privacyinbreuk door onveilige computeromgevingen van gebruiker zelf (zie ook sectie 2.3.1).

2.3 Technologie

2.3.1 Identiteit

De overheid wil dat burgers veilig en vertrouwd bij haar terecht kunnen. Hierbij speelt het een belangrijke rol of de toegang via Internet veilig is. Rond het zogenaamde *identity management* zijn de volgende ontwikkelingen belangrijk:

- Er ontstaan nieuwe manieren voor authenticatie, het verifiëren van iemands identiteit. Authenticatie is nodig bij het op elektronische wijze toegang krijgen tot

[12] Zie www.kanaleninbalans.nl
[13] Wikken en Wegen van Burgers op een Balans van Kanalen, zie https://doc.telin.nl/dsweb/Get/Document-86759/2-KiB-seminar-20080424-Wikken%20en%20Wegen%20-%20van%20Dijk%20UT.pdf

(overheids)diensten en kan op drie verschillende manieren plaatsvinden, al of niet gecombineerd:
- gebruik van een biometrisch kenmerk (vingerafdruk, irisscan, gelaatscan, stemherkenning, DNA, etc.);
- gebruik van een token dat iemand bij zich heeft (smart card, USB stick, bankpas, digitaal certificaat, etc.);
- vragen naar wat iemand weet (in het algemeen een wachtwoord).

Rond biometrie vinden continu technologische innovaties plaats zoals verbeteringen in (3D)gezichtsherkenning of de opkomst van DNA profielen. Daarnaast maken de ontwikkelingen richting *ambient intelligence* (zie sectie 2.1.2) het mogelijk dat er ook geheel nieuwe manieren van identificatie ontstaan, zoals identificatie op basis van locatie (omgevingsinformatie). Als je bijvoorbeeld nu in Amsterdam pint, kun je niet over een uur in Groningen zijn; of als je telefoon aanwezig is (persoonlijk apparaat), is de kans groot dat jij er ook bent.

- We observeren de opkomst van digitale identiteiten en authenticatie mechanismen, zoals OpenID[14], waarbij niet voor elke functionaliteit op het internet een apart gebruikersaccount wordt aangemaakt, maar waarbij iemand een digitaal identiteitsbewijs verkrijgt van een Identity Provider. De authenticatie van openID en de bijbehorende digitale identiteit kan worden gebruikt voor verschillende diensten om in te loggen op een server[15].

- Cameratoezicht ontwikkelt zicht richting intelligent cameratoezicht, waarin bijvoorbeeld personen kunnen worden geïdentificeerd of gedrag kan worden herkend. Gezichtsherkenning werkt bijvoorbeeld goed voor verificatie (ben je wie je zegt dat je bent). Identificatie (een persoon herkennen in de massa) is moeilijker en vereist conditionering, maar ontwikkelingen gaan snel[16]. Feitelijk is dit een bijzondere vorm van biometrie.

2.3.2 Identiteitsfraude

Identiteitsfraude kan op meerdere, ook niet-elektronische wijze worden gepleegd. Echter, communicatie in de digitale wereld (Internet) geeft een verhoogd risico met betrekking tot identiteitsdiefstal. Daardoor zouden kwaadwillende personen ten onrechte gebruik kunnen maken van iemands identiteit. Tegen verschillende vormen van identiteitsfraude zijn er adequate oplossingen, maar waakzaamheid blijft niettemin geboden[17]. Via de zoekmachine Google, bijvoorbeeld, zou heel veel informatie over een persoon kunnen worden gevonden. In principe kan dit al bijdragen aan identiteitsdiefstal. Verschijnselen op Internet die het risico op identiteitsdiefstal verhogen zijn:

- *Phishing* bestaat uit het oplichten van personen door deze te lokken naar een valse (bank)website, die een kopie is van de echte website, en ze daar nietsvermoedend te laten inloggen met hun inlognaam en wachtwoord. Hierdoor krijgt een fraudeur de beschikking over authenticatiegegevens die kunnen worden gebruikt voor

[14] http://openid.net/
[15] Merk op dat rond digitale identiteit iets anders is als een ‘virtuele identiteiten’, waarmee doorgaans een (aangenomen) identiteit (‘alias’) in de digitale wereld (of Second Life) wordt aangeduid.
[16] Zie bijvoorbeeld http://www.eenveiligamsterdam.nl/nieuws/nieuwsoverzicht_2008/8/6972/
[17] http://www.3xkloppen.nl/

identiteitsfraude. De slachtoffers worden vaak via e-mail naar deze valse website gelokt.

- *Pharming* is het misleiden van internetgebruikers door hun verkeer om te leiden naar een andere server. Internet gebruikt zogenaamde DNS-servers die domeinnamen (zoals www.minbzk.nl) omzetten in werkelijke IP-adressen die bestaan uit vier getallen (zoals “62.112.230.131”). Bij pharming wordt een DNS-server aangevallen en wordt het internetadres van een bepaalde domeinnaam gewijzigd. De nietsvermoedende internetgebruiker typt het bekende webadres in, maar komt op een nagebootste site terecht (o.a. op phishing sites). De internetgebruiker merkt hier niets van, ook anti-virus programma's of anti-spyware software beschermen niet tegen pharming. De bescherming moet komen van de beheerder van de website.

- *Skimmen* betreft het kopiëren van kaartgegevens (PIN-pas of creditcard) en opslaan van de pincode bij kaartgebruik in winkel of geldautomaat. Met een gekopieerde PIN-Pas en pincode kunnen kwaadwillende personen zich valselijk authenticeren en betalingen doen uit naam van een ander.

- *Man-in-the-middle* is het verschijnsel waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. De berichten kunnen daarbij mogelijk gelezen en/of veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. Voorbeelden hiervan zijn het onderscheppen van e-mail(s) of ander dataverkeer tussen twee of meerdere computers. Ook het onderscheppen van brieven of telefoongesprekken kan men zien als een man-in-the-middle-aanval.

- Er wordt steeds meer gelogd. Op Internet laat je sporen na. Er worden steeds meer gegevens opgeslagen, zowel inhoudelijk als betreffende de frequentie van gebruik (verkeersgegevens). Technologieontwikkelingen (dataopslag, communicatie, mens-machine interfaces) maken het ook mogelijk dat er steeds meer wordt verzameld. Dit maakt het enerzijds lastig om alle persoonsinformatie of privacygevoelige informatie onder controle te houden, te beschermen. Anderzijds is juist te traceren wie bepaalde gegevens inziet, waardoor het mogelijk is betrokkenen hierop aan te spreken.

2.3.3 Privacy Enhancing Technologies (PET)

Waar enerzijds technologieontwikkelingen een bedreiging kunnen zijn, kunnen ze anderzijds de oplossing zijn die het mogelijk maakt om je te beschermen tegen digitale bedreigingen. In het bijzonder wordt de term *privacy enhancing technologies* gebruikt om technologieën aan te duiden die de privacy beschermen. We observeren de volgende ontwikkelingen:

- Technologieën die communicatie anoniem maken door iemands stabiele identificator (gebruikersnaam, email of IP adres.) te vervangen door een niet-traceerbare identificator (eenmalig email adres, random IP adres van een verzameling deelnemende computers, etc.), of alternatieve oplossingen waarbij één digitale identiteit wordt gebruikt door meerdere ‘echte identiteiten’ waardoor er geen persoonlijk gebruikersprofiel kan worden opgebouwd.

- Het gebruik van biometrie als PET. De mate waarin biometrie gebruikt kan worden om privacy te beschermen hangt sterk af van het doel waarvoor het wordt toegepast: authenticatie of identificatie. Veiligheid is bij de overheid meestal de hoofdreden om

biometrie in te zetten. Dit resulteert in het gebruik van biometrie ter identificatie dat gepaard gaat met het opzetten en onderhouden van grote databestanden. Deze toepassing van biometrie is intrinsiek privacy aantastend. Om deze aantasting te minimaliseren zijn nieuwe PET technologieën in ontwikkeling die niet alleen interoperabiliteit maar ook revocabiliteit van biometrische gegevens kunnen garanderen. In de private sector is het doel van het gebruik van biometrie veelal gebruikersvriendelijke authenticatie en verhoogde efficiency. Er ligt hier een spanningsveld daar eventuele PET maatregelen juist vaak in strijd zijn met de laatste twee doelstellingen. PET technologieën die op dit moment nog volop in ontwikkeling zijn maar al betere garantie van privacy kunnen bieden zijn 'match on card' of 'sensor on card'. Omdat de houder dan de biometrische gegevens bij zich draagt is er geen centrale opslag (er blijven geen gegevens achter, een ander kan er niet bij). De biometrische gegevens die worden gebruikt voor authenticatie zijn daarmee beter beveiligd.

Door De Leeuw (2007) is bovendien gewezen op de onbedoelde effecten die het gebruik van biometrie kan hebben. Ten eerste kan het leiden tot ongemak bij goedwillende burgers. Ten tweede zal een aantal categorieën van personen, zoals ouderen, gehandicapten, vrouwen en raciale minderheidsgroepen, zich ongelijk behandeld kunnen voelen.[18] Ten derde is biometrische identiteitsdiefstal mogelijk doordat biometrische kenmerken (gelaatscan, iris, vingerafdruk) gekopieerd of vervalst kunnen worden. Biometrische identiteitsdiefstal is bijzonder aantrekkelijk voor de dader en bijzonder schadelijk voor het slachtoffer. Ten vierde biedt biometrische technologie nooit volledige zekerheid over de authenticiteit van een identiteitsclaim. Tot slot kan de vingerafdruktechnologie de bewijskracht van vingerafdrukken in het strafrecht ondermijnen als gevolg van een verwachte toename van vervalste en gekopieerde vingerafdrukken.

- Beveiliging op architectuurniveau. Het concept 'privacy by design' dat in theorie zo aantrekkelijk lijkt wordt in de praktijk relatief weinig tot uitvoering gebracht. Bij de ontwikkeling van het DKD en andere grootschalige projecten waarbij persoonsgegevens worden uitgewisseld is gekozen voor eenvoudige PET maatregelen. Meer complexe maatregelen zoals pseudonimisering (bijvoorbeeld door 'one-way' versleuteling van het BSN[19]) en anonimisering worden nauwelijks of niet toegepast. Het gebruik van PETs op architectuur niveau wordt doorgaans als duur, complex en moeilijk inzetbaar ingeschat. Deze perceptie wordt ten dele verklaard door de afwezigheid van duidelijke voorlichting, enorme diversiteit aan typen informatiesystemen, gebrek aan duidelijk overheidsvoorkeursbeleid voor PETs, gebrek aan centrale coördinatie en aan PET aanbod op maat (Bos, 2007). Een duidelijker en pro-actiever overheidsbeleid ten aanzien van PETs wordt sinds kort ook door de EU gestimuleerd en gesubsidieerd (COM, 2007).

[18] Volgens De Leeuw kunnen gehandicapten bijvoorbeeld problemen ondervinden bij gelaatsherkenning en iristechnologie. Voorts zijn technologische varianten van seksisme en racisme niet uit te sluiten bijvoorbeeld als gevolg van systematische ondervertegenwoordiging van vrouwen en vertegenwoordigers van raciale minderheidsgroepen in de groepen proefpersonen bij laboratoriumproeven waarin de technologieën worden getest. Een mogelijk gevolg daarvan is een relatief hoog aantal onterechte acceptaties of weigeringen binnen die groepen.
[19] One-way versleuteling (hashing) betekent het onomkeerbaar versleutelen van het BSN nummer.

2.3.4 Overige technologie gerelateerde trends

Rond technologie speelt ook de perceptie van wat met technologie kan. Drie 'trends' willen we hier in het bijzonder noemen:

- *Macromyopia* is het verschijnsel dat ontwikkelingen op korte termijn worden overschat en op lange termijn worden onderschat. Voorbeelden van hoge verwachtingen van technologie observeren we momenteel rond DNA of nanotechnologie. De praktijk kan echter weerbarstiger zijn. Toch zouden de lange termijn consequenties kunnen worden onderschat, simpelweg omdat deze op dit moment nog niet zijn voor te stellen. Een voorbeeld van het onderschatten van de impact van technologie op de lange termijn zien we rond het succes van SMS en mobiele communicatie. Ook zien we dit verschijnsel terug in uitspraken door gewaarde personen zoals '*Radio has no future*[20]', '*By 1985, machines will be capable of doing any work Man can do*[21]', of '*There is no reason anyone would want a computer in their home*[22].' Macromyopia is gerelateerd aan de zogenaamde *Gartner Hype Cycle* voor de introductie van nieuwe technologie[23].

- Bij technologie speelt heel vaak de zogenaamde *function creep*. Dit is het verschijnsel dat de technologie voor andere doelen wordt gebruikt dan waarvoor hij aanvankelijk is ontwikkeld of ingevoerd. Een voorbeeld is het invoeren van cameratoezicht voor openbare orde, waarbij opsporing als 'bijvangst' is toegestaan. Verschuivingen kunnen optreden in verschillende richtingen, met name het gebruik voor andere (meerdere) doelen dan aanvankelijk de bedoeling, het gebruik door andere gebruikersgroepen, het gebruik in andere toepassingsdomeinen, of het toepassen op andere informatiebestanden.

- Er is een wisselwerking tussen technologische ontwikkelingen en maatschappelijke trends. We spreken ook wel van *co-evolutie*. Dit verschijnsel speelt bij ontwikkelingen over langere termijn. Nanotechnologie is een voorbeeld van hoe een positief beeld en hoge verwachtingen de ontwikkelingen enorm kunnen versnellen en industrie en overheid (subsidie) zich er vol op richten. Als zou blijken dat nanodeeltjes gevaarlijk zijn, de opinie omslaat, de overheid met regelgeving komt, industrie geen risico's wil nemen, etc., kan een technologische ontwikkeling zo weer vertraagd worden.

2.3.5 E-overheid / service oriëntatie

Een aantal trends, ten slotte, zijn gerelateerd aan het domein van de overheid. Op het gebied van de overheidsdienstverlening observeren we de volgende trends:

- We zien een toenemende druk van de overheid op burgers om persoonlijke informatie over zichzelf prijs te geven. Een voorbeeld hiervan is de minister van Justitie Ernst Hirsch Ballin (CDA) die in de Tweede Kamer zegt dat het afstaan van DNA-

[20] Lord Kelvin, Schotse wis- en natuurkundige, president van de Royal Society, 1897.
[21] Herbert A. Simon, Carnegie Mellon University, beschouwd als een van de grondleggers van de kunstmatige intelligentie, 1965.
[22] Ken Olson, directeur, voorzitter en oprichter van Digital Equipment Corp. (DEC), 1977.
[23] Zie http://www.gartner.com/.

materiaal voor een grootschalig onderzoek naar de dader van een misdaad een burgerplicht is[24].

- Er is een trend richting centralisatie van het beheer van basisgegevens. Voorbeelden hiervan zijn de diverse basisregistraties (GBA, Handelsregister, BAG, Kadaster en topografie, RDW, BRI, BLAU, WOZ)[25]. De basisregistratie als unieke houder van brongegevens heeft op een aantal manieren impact op het persooninformatiebeleid. Overheidsinstanties putten uit basisregistraties (indien nodig) en er kan kwetsbaarheid voor inbreuk ontstaan omdat het gebruikt wordt door veel instanties.

- We observeren een toenemende samenwerking tussen overheidspartijen via het gezamenlijk inkopen (en uitbesteden) van (ICT) dienstverlening. Voorbeelden zijn DIMPACT en GovUnited, die onderling ook weer samenwerken, en Wigo4it, waarin de sociale diensten van de vier grote steden samenwerken. Op inkoopgebied ontstaat dus een zekere mate van centralisatie.

- Elektronische dossiervorming lijkt een trend te zijn, zoals Elektronisch patiëntendossier (EPD), Digitaal klantdossier (DKD), burgerdossier, fiscaal dossier, etc. Bij alle dossiers spelen vragen als dat elektronische dossiers sneller zijn te vermenigvuldigden en te verspreiden dan papieren dossiers, en gemakkelijker zijn te koppelen. Het is daarom eigenlijk ook een vorm van centralisatie. Daarnaast spelen vragen als: Wie is eigenlijk eigenaar van het dossier, en wie is eigenaar van de informatie in het dossier? Hoe zit het met inzagerecht / correctierecht / recht op maken van aanmerkingen? Voor medisch personeel geldt een geheimhouding (als je inbreuk maakt kun je vervolgd worden), geldt dit ook voor een ambtenaar?

- Toenemend gebruik van open standaarden bij de overheid. Open standaarden[26] zijn publiek beschikbare specificaties (veelal bij hard- en software) voor het uitwisselen van gegevens. Doordat iedereen de standaard mag gebruiken, neemt de uitwisselbaarheid van gegevens tussen de verschillende soorten hardware- en softwareonderdelen toe. Voorbeelden van open standaarden die gebruikt worden bij de overheid zijn de overheidsservicebus (OSB), XBRL, en ebMS. De Nederlandse Overheid Referentie Architectuur (NORA)[27] moedigt het gebruik van open standaarden aan. Bij het uitwisselen van gegevens, en dan in het bijzonder persoonsgegevens, dient altijd rekening te worden gehouden met het privacyaspect. Men dient ervoor zorg te dragen dat onbevoegde partijen niet kunnen meekijken met de communicatie en dat de uitgewisselde informatie goed wordt versleuteld. Dit kan prima met behulp van open standaarden, zoals de overheidsservicebus. Zelfs voor kwaadwillende personen die kennis nemen van de betreffende open standaard is toegang tot gegevens nagenoeg onmogelijk zolang ze niet beschikken over de juiste sleutels.

[24] http://frontpage.fok.nl/nieuws/98720/-Hirsch-Ballin:-afstaan-DNA-is-burgerplicht.html
[25] http://www.e-overheid.nl/sites/stelselbasisregistraties/de_basisregistraties/de_basisregistraties.html
[26] Merk op dat open standaarden niet gelijk zijn aan open source software. Open source software is software waarvan de broncode is in te zien en te veranderen. Vaak maakt deze software wel gebruik van open standaarden. Na aanleiding van de zogenoemde motie-Vendrik is in Nederland het gebruik van Open Standaarden en Open Source via een overheidsprogramma gestimuleerd.
[27] http://www.e-overheid.nl/atlas/referentiearchitectuur/nora/nora.html

- Er is een trend om gegevens langer te bewaren. Dit gaat niet alleen om overheidsgegevens. De overheid speelt wel een rol in het bepalen van bewaartermijnen. Uitgangspunt bij persoonsinformatiebeleid is altijd dat gegevens niet langer worden bewaarde dan nodig. Echter, veel gegevens zouden voor opsporingsdoeleinden nuttig kunnen zijn en dan gelden andere wetten. Hier speelt de balans privacy versus veiligheid, maar ook de invloed van Europese wet- en regelgeving. De technologie maakt het ook mogelijk om gegevens massaal te bewaren. Zo is bijvoorbeeld door de miniaturisatie van massa-opslag het Besluit Verstrekking Gegevens Telecommunicatie uitvoerbaar geworden. Daarbij wordt het ook steeds eenvoudiger en goedkoper om te registreren wie welke gegevens gebruikt. Hierdoor komt controle achteraf van gegevensgebruik steeds eenvoudiger. Dit beïnvloedt de manier waarop toezicht kan worden uitgevoerd.

2.4 Conclusies

De (technologische) trends geven enerzijds kansen en vormen anderzijds bedreigingen voor de privacy. We kunnen dit concluderend samenvatten in een aantal afwegingen om mee te nemen bij het evalueren van de cases:

- De balans tussen het (via technologie) voorkomen van data-toegang versus het traceerbaar en transparant maken van wie wat ziet of heeft gezien (en het zo nodig ter verantwoording roepen). Technologie maakt dergelijke nieuwe privacy modellen mogelijk of zelfs noodzakelijk. Waar je alle normen rond data inzage mogelijk niet meer bij voorbaat kunt afdwingen (door dataprotectie) moet je wellicht naar modellen waarin je achteraf misbruik strafbaar stelt (via traceerbaarheid). Tegelijkertijd hebben we te maken met het bestaande wettelijk kader dat bepaalde modellen oplegt.

- De balans tussen technologie als bedreiging en technologie als oplossing. Enerzijds is er het gevaar van identiteitsdiefstal, identiteitsfraude, of identiteitgerelateerde imagoschade door de genoemde trends. Anderzijds kan (*privacy enhancing*) technologie een oplossing zijn voor bedreigingen rond persoonsinformatie.

- De balans tussen het vertrouwen van de burger en het binnen de (semi-)overheid uitwisselen van gegevens. Enerzijds is er een merkbaar toenemende behoefte bij de (semi-)overheid aan verkrijging/uitwisseling van persoonsinformatie (bijvoorbeeld uitwisseling door hulpverlenende instanties bij huiselijk geweld/kindermishandeling), maar anderzijds kan dat de toegang tot (in dit geval) de gezondheidszorg bedreigen. Als je er niet op kunt vertrouwen dat je HIV-besmetting of SOA geheim blijft bij je huisarts, zul je niet meer zo gemakkelijk naar de huisarts gaan.

Deze drie punten worden bij de casusbeschrijvingen steeds meegenomen.

3 Effecten in de praktijk bij Justitie, basisregistraties en elektronische dossiers

De ontwikkelingen en trends bieden inzicht in hoe bijvoorbeeld technologie de privacybalans kan beïnvloeden. In dit hoofdstuk vertalen we deze ontwikkelingen naar cases. Het gaat daarbij enerzijds om bestaande cases, die al zijn ingevoerd in de praktijk, en waarin we ons richten op hoe de mogelijkheden tot nu toe in de praktijk vorm hebben gekregen. Anderzijds zijn er ook nog in ontwikkeling zijnde (toekomstige) cases, zoals het Elektronisch Patiënten Dossier, waartoe al wel beleid is ontwikkeld, maar dat nog niet in de praktijk is ingevoerd. De volgende cases komen aan de orde:

- Case studie die ligt op het terrein van Justitie, in het bijzonder de identiteitsvaststelling in de strafrechtketen. Bij deze cases spelen vaak ‘ruimere mogelijkheden’ in het kader van opsporing. Ook speelt technologie een grote rol.
- Case studies rond drie gerelateerde elektronische dossiers met persoonsinformatie: Elektronisch Medicatie Dossier (EMD), Elektronisch Kind Dossier (EKD), en Elektronisch Patiënten Dossier (EPD). Bij deze cases speelt vooral het opslaan van privacygevoelige data en de toegang hiertoe.
- Case studies van twee elektronische dossiers die gerelateerd zijn aan e-overheid ketens: Digitaal Klant Dossier (DKD) en de omgevingsvergunning. Bij deze cases speelt de dienstverlening van de overheid sterk, en de interacties tussen burger en overheid.

Aan de hand van de trends uit hoofdstuk 2 kan gericht worden gezocht naar kansen of bedreigingen van de nieuwe mogelijkheden. Zo kan bijvoorbeeld worden gecontroleerd of federatieve identiteiten worden gebruikt bij elektronische dossiers, of dat minimale datasets worden geregistreerd, of er bewust wordt omgegaan met de toestemming van personen, of er centrale versus decentrale gegevensopslag is, etc. Aan de hand van deze constateringen, kan een indicatie worden verkregen in hoeverre de privacybalans is verschoven. Dit laatste doen we steeds onder het kopje “analyse door projectteam”.

3.1 Cases op het terrein van Justitie

3.1.1 Identiteitsvaststelling in de strafrechtketen (bestaande casus)

3.1.1.1 Algemene beschrijving van de casus

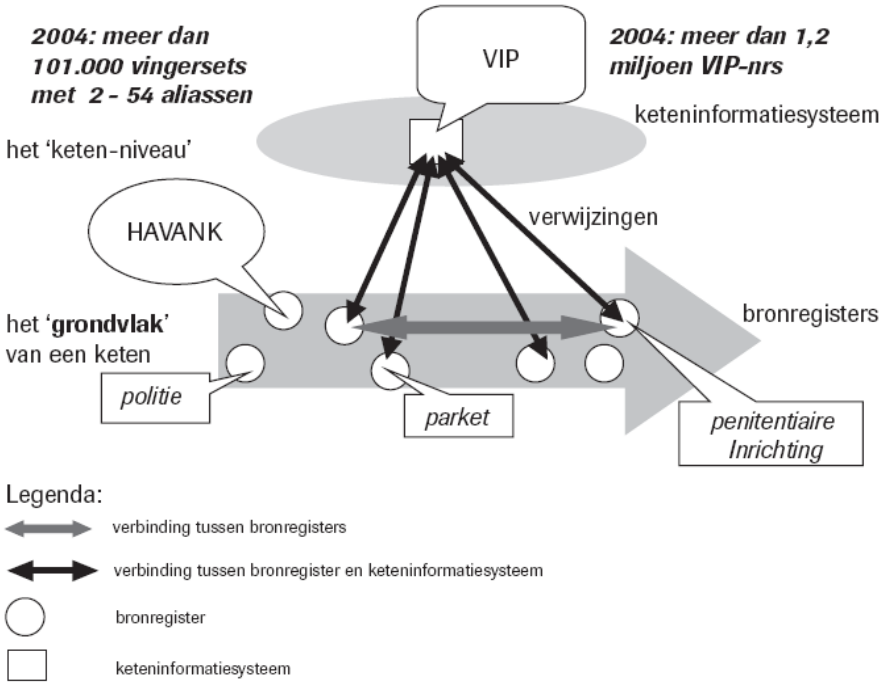
Identiteitsfraude, het ten onrechte gebruik maken van iemands identiteit (zie sectie 2.3.2), speelt in alle sectoren. In deze casus, de strafrechtketen, gaat het erom dat de juiste persoon wordt berecht en de betreffende gegevens worden geregistreerd in het juiste strafblad. Daarmee gaat het om de identiteitsvaststelling van personen en de kwaliteit van gegevens in de diverse registers.

De strafrechtketen, zoals beschreven door Grijpink (2006b), bestaat uit de fases van opsporing, vervolging, berechting en tenuitvoerlegging vonnis/detentie (gevangeniswezen, reclassering, advocatuur). Bij iedere stap zijn identificerende persoonsgegevens cruciaal. Daartoe is in de periode 1993-1995 het informatiesysteem

‘VerwijsIndex Personen strafrechthandhaving (VIP)’ ingevoerd. Dit systeem kent een uniek VIP-nummer toe aan iedereen die voor het eerst wordt geregistreerd in de systemen van het Openbaar Ministerie. Het informatiesysteem registreert de opgegeven identificerende persoonsgegevens en verwijst naar bronregisters van aangesloten ketenpartners.

Daarnaast is er een gegevensbank met sets van tien vingerafdrukken van veel misdrijfverdachten, het HAVANK-systeem van de Nederlandse politie. Elke unieke set van tien vingerafdrukken heeft een eigen HAVANK-nummer en daaraan gekoppeld de identificerende persoonsgegevens (naam, voornamen, geslacht, geboortedatum, geboorteplaats) waaronder de set vingerafdrukken ter registratie of controle is aangeboden. Aan één HAVANK-nummer kunnen meerdere namen (aliassen) gekoppeld zijn waaronder deze set vingerafdrukken is aangeboden. Ook kunnen aan één naam meerdere vingerafdruksets (HAVANK-nummers) gekoppeld zijn (een identiteit die door meerdere personen wordt gebruikt).

Tenslotte beheert het Nederlands Forensisch Instituut (NFI) een DNA-databank voor strafzaken met daarin DNA-profielen van sporen, verdachten en veroordeelden (Meulenbroek, 2008). Opname en verwijdering van DNA-profielen is strikt gereguleerd en geschiedt uitsluitend nadat het NFI hiertoe een schriftelijke opdracht van de bevoegde autoriteit heeft ontvangen. Het NFI mag alleen die DNA-profielen in de Nederlandse DNA-databank voor strafzaken opnemen die zijn verkregen in een zaak waarbij voor het misdrijf voorlopige hechtenis is toegestaan. Dit komt over het algemeen neer op misdaden waarvoor een gevangenisstraf van vier jaar of meer is gesteld. Matchende DNA-profielen geven vaak belangrijke tactische informatie voor de opsporing.



Figuur 1: HAVANK en VIP in de strafrechtketen (overgenomen uit Grijpink (2006a)).

In de strafrechtketen kan niet worden gerekend op de medewerking van verdachten. Dit kan zich uiten in identiteitsfraude, dat wil zeggen dat iemand met kwade bedoelingen gebruik maakt van de identiteit van een ander. De verdachte heeft, bijvoorbeeld, een

identiteitsbewijs dat niet van zichzelf is of gebuikt een naam of BSN dat niet bij hem hoort. Identiteitsfraude wordt niet altijd op het moment van controle opgemerkt (de gegevens komen immers overeen met wat is opgenomen in de GBA), maar pas later. Sporen leiden vervolgens naar het slachtoffer (een onschuldige of iemand die, bijvoorbeeld, tegen betaling meewerkt) in plaats van naar de dader.

Hoewel alomvattende gegevens over identiteitsverwisseling in de strafrechtketen niet beschikbaar zijn, zijn er wel duidelijke aanwijzingen voor problemen rond de identiteitsvaststelling van verdachten en veroordeelden en de juistheid van gegevens in de registers. Op basis van cijfermateriaal van de Dienst Nationale Recherche-informatie (DNRI) van het KLPD is in 2004 vastgesteld dat ruim bij 92.000 (van de circa 1,26 miljoen) administratieve identiteiten in het HAVANK vingerafdrukkenbestand van de Nederlandse Politie sprake was van verschillende namen voor éénzelfde persoon (dit betreft zowel op strafrechtelijke als op vreemdelingenrechtelijke titel afgenomen vingerafdrukken)[28]. Het gaat dan om twee tot 51 administratieve identiteiten die zijn gekoppeld aan een (identieke) vingerafdrukset. Welk deel hiervan berust op bewuste identiteitsfraude en welk deel berust op administratieve verschrijvingen valt niet te bepalen. Merk op dat een deel van de andere vingerafdrukken, gekoppeld aan slechts één set identificerende persoonsgegevens, mogelijk ook op een alias zouden kunnen zijn geregistreerd.

Het grote aantal VIP-nummers dat werd uitgegeven was in 2004 tevens aanleiding voor een steekproef waarbij VIP- en HAVANK-gegevens werden vergeleken. Bij de steekproef in een drietal penitentiaire inrichtingen begin 2006 werden van alle 707 gedetineerden vingerafdrukken afgenomen. Deze werden vergeleken met het bestand HAVANK en de VIP. Daarbij bleek dat 22% van de geregistreerde identiteiten niet goed is. Bij 15% lijkt sprake van administratieve missers. In 46 gevallen (= 7%) lijkt sprake van identiteitsfraude[29]. Grijpink (2006a) noemt dat aan een persoon, gerelateerd aan een HAVANK-nummer met 27 aliassen, in totaal dertien verschillende VIP-nummers waren toegekend, waarvan er vijf overeenstemden met de gegevens als opgenomen in de GBA. Tevens werd zichtbaar dat deze persoon op enig moment op twee plaatsen in de gevangenis zat. Ook zou in een aantal gevallen de DNA-gegevens niet op de juiste persoon zijn geregistreerd. Tevens is een bekend gegeven dat het aantal vermiste Nederlandse paspoorten en rijbewijzen in de honderdduizenden loopt[30].

Merk op dat al is het mogelijk dat de identiteitsgegevens niet kloppen of personen onder een alias kunnen opereren, dit nog niet betekent dat de betrokkenen niet terecht gedetineerd zouden zijn. Het betekent wel dat registers ‘vervuild’ zijn: de straf wordt op een andere naam vastgelegd.

[28] Zie de brief van de Minister van Justitie aan de Tweede Kamer over identiteitsvaststelling in de strafrechtketen, kenmerk 5451389/06, d.d. 6 december 2006.
[29] Zie memorie van toelichting bij wetsvoorstel *Kamerstukken II*, 2007/08, 31 436, nr. 3, par. 3.
[30] Het aantal als vermist of gestolen opgegeven reisdocumenten (paspoort of identiteitskaart) bedroeg in 2006 circa 190.000, waarbij sprake was van een stijgende lijn t.o.v. voorgaande jaren (TK 31436), en in 2007 circa 185.000 (zie brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer, kenmerk BPR2008/57314, d.d. 19 augustus 2008, http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/95439/bzk57314.pdf).

3.1.1.2 Beleidsontwikkeling

Om identiteitsvaststelling te verbeteren ligt er momenteel een wetsontwerp bij de Tweede Kamer dat er onder andere op inzet dat aan het begin van de keten iemand deugdelijk wordt geïdentificeerd (identiteitsdocument plus foto plus vingerafdrukken), en in latere fases (via o.a. biometrie) kan worden geverifieerd of nog steeds dezelfde persoon zich meldt. Tevens is een proces in gang gezet om een wederzijdse koppeling te leggen tussen HAVANK-nummers enerzijds en VIP-nummers –dat wil zeggen strafrechtketennummers (zie sectie 3.1.1.3)– anderzijds. Deze koppeling maakt het mogelijk om te traceren of er in het verleden sprake is geweest van aliasmisbruik, en eventuele dossiervervuiling te corrigeren.

3.1.1.3 Juridische setting

Er ligt een wetsvoorstel bij de Tweede Kamer tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten in verband met het verbeteren en versterken van de vaststelling van de identiteit van verdachten, veroordeelden en getuigen (Wet identiteitsvaststelling verdachten, veroordeelden en getuigen). Blijkens de memorie van toelichting bij dit wetsvoorstel is het voor het rechtmatig en doeltreffend handelen in relatie tot de burgers in veel gevallen nodig dat de overheid de identiteit van de betrokkene kent.[31] Dat is mogelijk als een aantal identiteitsgegevens op zorgvuldige wijze wordt vastgesteld en voor verificatie beschikbaar is. Een terrein waar dit in bijzondere mate van belang is, is de strafrechtspleging. Een zorgvuldige vaststelling van de identiteit van de verdachte of veroordeelde is een fundamentele eis en een elementaire voorwaarde voor de rechtmatigheid en doeltreffendheid van het justitieel overheidsoptreden. Strafrechtelijke interventies, zoals de toepassing van dwangmiddelen of de tenuitvoerlegging van straffen of maatregelen, zijn, als zij de verkeerde persoon treffen, ondoelmatig, ondoeltreffend en kunnen ook onrechtmatig zijn. De overheid dient zich er dan ook voor in te spannen dat aan iedere interventie – zeker als zij de rechten of vrijheden van burgers raakt – een zorgvuldige identiteitsvaststelling voorafgaat. Zoals in de memorie van toelichting wordt betoogd, behoeft die identiteitsvaststelling in de strafrechtsketen verbetering en versterking. Hoofddoelstelling van het wetsvoorstel is dan ook het versterken van een juiste, betrouwbare en zorgvuldige vaststelling van de identiteit van verdachten en veroordeelden in de strafrechtsketen. Dit houdt onder andere in dat de identificerende persoonsgegevens die nodig zijn voor de uitvoering van de werkprocessen in de strafrechtsketen, betrouwbaar zijn en voor alle partners in die keten op een effectieve en efficiënte manier beschikbaar moeten zijn. Om dat te bewerkstelligen kent het wetsvoorstel zes maatregelen:

[31] Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten in verband met het verbeteren en versterken van de vaststelling van de identiteit van verdachten, veroordeelden en getuigen (Wet identiteitsvaststelling verdachten, veroordeelden en getuigen). *Kamerstukken II*, 2007/08, 31 436, nr. 3.

1. Het invoeren van een strafrechtsketennummer (SKN) als persoonsnummer voor de gehele strafrechtsketen, en het verplicht gebruik daarvan door alle partijen in de strafrechtsketen.
   Dit nummer is feitelijk de opvolger van het VIP-nummer en wordt gebruikt om verdachten en veroordeelden eenduidig te kunnen identificeren en registreren en gegevensuitwisseling tussen de partijen te faciliteren.
   Merk op dat daarnaast tevens het burgerservicenummer mag worden gebruikt, en dit is zelfs noodzakelijk indien wordt gecommuniceerd met partijen buiten de strafrechtketen (bijvoorbeeld controle bij GBA).
   Het SKN is, net als het BSN, informatieloos, rechtenvrij, uniek en persoonsgebonden.
2. Het verruimen van de mogelijkheden van de afname en het gebruik van foto's en vingerafdrukken voor het vaststellen van de identiteit van verdachten en veroordeelden.
   Merk op dat het disproportioneel wordt geacht het DNA-profiel van een verdachte of veroordeelde vast te stellen omwille van de bepaling van zijn identiteit.
3. De introductie van een identificatieplicht voor een verdachte ten opzichte van een rechterlijk ambtenaar en voor een gedetineerde verdachte of een veroordeelde ten opzichte van de directeur of hoofd van een inrichting of psychiatrisch ziekenhuis waar hij zijn straf of maatregel ondergaat.
4. Het opleggen van de verplichting aan de functionarissen in de strafrechtsketen om de identiteit van een verdachte of veroordeelde vast te stellen en het regelen van de momenten waarop die verplichting geldt. Hierop bestaat een uitzondering voor de rechterlijk ambtenaar aan wie de bevoegdheid wordt toegekend om de identiteit van een verdachte alleen vast te stellen als over zijn identiteit twijfel bestaat.
   Merk op dat in een aantal gevallen verificatie van identiteit ook niet wordt opgelegd, omdat fraude onwaarschijnlijk wordt geacht (in verband met aanwezigheid ouders of begeleiders) of disproportioneel. Het betreft dan bijvoorbeeld momenten rond psychiatrie, tbs-klinieken of jeugdigen.
5. Het aanwijzen van de Minister van Justitie als ID-autoriteit voor de strafrechtsketen.
6. Het oprichten van de strafrechtsketendatabank en het stellen van regels over het verwerken van de identificerende persoonsgegevens die daarin zullen worden opgeslagen, en van de vingerafdrukken die in het vingerafdrukkenbestand van de politie, HAVANK, worden opgeslagen.
   Net als de huidige VIP valt de strafrechtsketendatabank onder het regime van de Wet bescherming persoonsgegevens als bijzondere (strafrechtelijke) persoonsgegevens. De strafrechtsketendatabank bevat ook foto’s, aangeleverd via politie of de Koninklijke marechaussee, of via penitraire- en tbs-inrichtingen. Op HAVANK is de Wet politiegegevens van toepassing, en via het nieuwe wetsvoorstel verwijst ook het Wetboek van Strafvordering naar HAVANK.

Het wetsvoorstel heeft tevens tot doel getuigen de verplichting op te leggen zich desgevraagd tegenover de rechter te legitimeren omdat er in de praktijk behoefte bestaat om, indien er twijfel bestaat over hun identiteit, ook hun identiteit te kunnen controleren.

Thans bestaat al de bevoegdheid tot identiteitsvaststelling van verdachten door middel van foto’s en vingerafdrukken in het Wetboek van Strafvordering, de Penitentiaire Beginselenwet, de Beginselenwet verpleging ter beschikking gestelden en de Beginselenwet justitiële jeugdinrichtingen. Het wetsvoorstel voorziet in een integrale en systematische benadering van het vaststellen van de identiteit van verdachten en veroordeelden. Via dit wetsvoorstel wordt voorts een strafrechtsketendatabank in het leven geroepen die het informatiesysteem Verwijsindex Personen moet vervangen. De invoering middels dit wetsvoorstel, van een identificatieplicht voor een verdachte ten

opzichte van een (verhorend) rechterlijk ambtenaar en voor een veroordeelde in het kader van de tenuitvoerlegging van zijn straf of maatregel, ligt in het verlengde van de Wet op de uitgebreide identificatieplicht (Stb. 2004, 300), waarin een identificatieplicht is geïntroduceerd voor iedereen vanaf 14 jaar. Het wetsvoorstel zoekt tevens aansluiting bij de introductie van het gebruik van biometrische kenmerken ten behoeve van de identiteitsvaststelling op reisdocumenten, vreemdelingendocumenten en rijbewijzen, alsmede de invoering van het burgerservicenummer (BSN) als uniek registratienummer voor iedere burger ten behoeve van alle overheidsorganen.[32]

Foto's en vingerafdrukken dienen, behalve voor identiteitsvaststelling, ook voor opsporing. In die zin dienen zij hetzelfde doel als DNA-profielen. Met betrekking tot bewaartermijnen is het voorstel zoveel mogelijk te harmoniseren met de wetgeving rond DNA.

3.1.1.4 Institutionele setting

Bij de verschillende fases in de strafrechtketen zijn een veelheid aan partijen betrokken:
- Opsporing: politie, bijzondere opsporingsdiensten, marechaussee;
- Vervolging: Openbaar Ministerie, advocatuur, rechter-commissaris;
- Berechting: rechter, Openbaar Ministerie, advocatuur, reclassering;
- Tenuitvoerlegging vonnis/detentie: gevangeniswezen, reclassering, advocatuur, raad voor de kinderbescherming, etc.

Daarmee is de strafrechtsketen is een zeer complexe keten met een groot aantal partners. Om de informatievoorziening over personen en de gegevensuitwisseling tussen de ketenpartners te optimaliseren is in december 2004 het Programma Informatievoorziening Strafrechtsketen (Progis) door de Bestuursraad van het ministerie van Justitie ingesteld.

Het gegevensbeheer van VIP en Justitiële Documenten vindt plaats bij de Justitiële Informatiedienst (JustID). De Justitiële Informatiedienst heeft als primaire taak het verstrekken van een integer en een integraal persoonsbeeld van justitiabelen aan daartoe gerechtigden. Om dit beeld samen te stellen, worden in samenwerking met de ketenpartners gegevens op een efficiënte en effectieve manier verzameld, bewerkt en beheerd. Binnen de JustID zijn de organisaties rond de Verwijsindex Persoonsgegevens strafrechthandhaving (VIP) in Leeuwarden en de Centrale Justitiële Documentatie (CJD) in Almelo samengevoegd. Het strafrechtelijk verleden van personen wordt vastgelegd in het Justitiële Documentatie Systeem ('strafbladregister')..

3.1.1.5 Elektronische dienstverlening aan de burger

In het nieuwe wetsvoorstel is identificatie 'modulair' opgebouwd waarbij technologie een ondersteunende rol speelt. De modules zijn:
1. Controle van identiteit op basis van een identiteitsdocument. Bij het staande houden van personen "op straat" wordt volstaan met visuele controle. Wordt de verdachte aangehouden en overgebracht naar een plaats van verhoor, dan wordt de controle ondersteund met technische apparatuur (stap 2 of 3).
   Indien de verdachte geen identiteitsdocument toont, of dit document niet echt, eigen of geldig is, vindt eveneens stap 2 (bij verificatie) of 3 (bij identificatie) plaats.

[32] *Kamerstukken II*, 2007/08, 31 436, nr. 3, p. 3.

2. Verificatie met behulp van een enkele vingerafdruk. Dit gebeurt digitaal. Er is inmiddels al een traject gestart voor een nieuw HAVANK-systeem om het digitaal afnemen, verzenden en vergelijken van vingerafdrukken te ondersteunen.
3. Identificatie met behulp van tien vingerafdrukken en een foto. Dit wordt digitaal ondersteund. Als een persoon nog niet bekend is in het systeem, wordt opgeschaald naar stap 4.
4. Afnemen van vingerafdrukken met inkt en papier. Als er geen echt, eigen, geldig en gekwalificeerd identiteitsdocument voor handen is wordt bovendien opgeschaald naar stap 5.
5. Rechercheonderzoek. Technologie speelt hier een rol bij het raadplegen van gegevensverzamelingen als GBA.

3.1.1.6 Identity management

In de strafrechtketen is wettelijk geregeld welke organisaties toegang hebben tot bepaalde gegevens. De systemen en verbindingen worden ook zorgvuldig beveiligd. Bij de implementatie van de nieuwe wetgeving wordt zoveel mogelijk aangesloten bij bestaande systemen en/of organisatie die deze beheren (HAVANK, JustID, etc.). Daarmee wordt bij nieuwe ontwikkelingen aangesloten en vertrouwd op de al bestaande en solide toegangsmechanismen. Een en ander garandeert nog niet dat personen onrechtmatig toegang krijgen tot bepaalde gegevens. De bevoegdheid om gegevens in te zien is gekoppeld aan iemands functie en iemands taak. Het kan zijn dat iemand vanuit zijn functie wel het recht heeft gegevens in te zien, maar dat zijn taak dit nog niet rechtvaardigt, zoals geïllustreerd wordt door de ‘casus Van Persie’ (juridische waarborg versus praktijk)[33].

3.1.1.7 Veranderingen ingevolge (het gebruik van) ICT

Het gebruik van gelaatscan (foto) en dactyloscopie (vingerafdrukherkenning) neemt snel toe. Ook los van deze casus –identiteitsvaststelling in de strafrechtketen– observeren we een toenemend gebruik van biometrische technieken. Zoloopt er een pilot rond elektronische meldingsplicht door stemherkenning met betrekking tot het handhaven van stadionverboden[34]. In het algemeen lijkt er in het veld –in het bijzonder bij politie– een zekere drang nieuwe technologie toe te passen: men ziet de potentie en wil deze benutten. De technologie wordt dan (door Justitie) getoetst aan het wettelijk kader en ingevoerd. De veranderingen betreffen vooral verbeteringen van kwaliteit (minder fouten) en efficiëntie (snellere controle) in bestaande processen. De processen (werkwijzen) zelf veranderen bijvoorbeeld via de nieuwe procedures zoals vastgelegd in het wetsvoorstel als beschreven in sectie 3.1.1.3.

3.1.1.8 Relevante kwesties die rijzen/zijn gerezen in de betreffende case

Wat opvalt, is dat er veel initiatieven van onderaf opkomen (de Korpsen). Men experimenteert met technologie, ziet de mogelijkheden, en wil dit toepassen. Vervolgens komen er oplossingen naar boven (opschaling), deze worden getoetst aan de wet en vervolgens wel of niet ingevoerd. Indien noodzakelijk kan worden gewerkt aan een aanpassing van de wet. Initiatieven van onderaf kunnen heel krachtig zijn, vooral als het

[33] http://www.nu.nl/news/607303/14/Agenten_probeerden_dossier_Van_Persie_in_te_zien.html
[34] http://www.om.nl/onderwerpen/voetbalvandalisme_en/@125938/stemherkenning_nieuw/

om draagvlak gaat. Aan de andere kan betekent de late betrokkenheid van met Ministerie van Justitie ook dat er weinig regie is op het ontwikkelen van de oplossingen zelf, en dus ook op het meenemen van privacyaspecten tijdens het ontwerpproces: er worden kant-en-klare oplossingen voorgesteld. Justitie heeft aangegeven hier zelf meer greep op te willen hebben.

De vraag rijst of er in deze gevallen geen sprake is van 'technology push': de technologie is beschikbaar *dus* wordt hij toegepast. Als voorbeeld is tijdens een interview het gebruik van elektronische labels rond open inrichtingen genoemd. Voorheen had men bewegingsvrijheid terwijl nu een enkelband wordt gebruikt. De argumentatie hiervoor lijkt vooral te komen vanuit de beschikbaarheid van technologie.

Naast het registeren van gegevens van gedetineerden vindt er ook registratie van bezoekers van Penitentiaire Inrichtingen plaats. Dit zijn vaak lokale registers. Wettelijk gezien is hier veel minder geregeld over wie toegang heeft tot deze gegevens (dit valt onder de Wbp). De indruk bestaat dat op dit punt de hoeveelheid geregistreerde persoonsinformatie vrij moeiteloos toeneemt en er weinig toezicht is op de toegang, de verstrekking en bewaartermijnen ervan. Een bezoekersregistratie geeft tevens inzicht in wie met wie omgaat in het potentieel criminele circuit. Hier ligt een spanningsveld tussen privacy en opsporing: bezoekers kunnen zich belemmerd voelen of dit ervaren als inbreuk op hun privacy. Hetzelfde geldt voor telefonisch contact, waar digitale technieken het (stelselmatig?) opnemen van gesprekken vereenvoudigen.

Een laatste vraag die rijst is dat, als het in de strafrechtketen al zo slecht is gesteld met de kwaliteit van identiteitsgegevens, hoe het dan zit in andere ketens, zoals de zorg. Daar zouden bijvoorbeeld ook (medische) dossiers vervuild kunnen raken als er sprake is van identiteitsfraude, wat weer gevolgen kan hebben als (via Internet) dossiers minder plaatsgebonden worden. In de strafrechtketen lijkt het maatschappelijk belang –dat de juiste persoon gestraft wordt– en daarmee de urgentie van deze problematiek vooralsnog groter.

3.1.1.9 Dilemma's waar men in de case tegenaan is gelopen

Grijpink (2006a) geeft als oorzaak van identiteitsfraude aan dat de focus teveel ligt op het identiteitsbewijs in plaats van de persoon die zich ervan bedient. Bij digitale identificatiemiddelen vertrouwt de controleur bovendien teveel op het resultaat van de elektronische verificatie en kan de gecontroleerde de regie in handen nemen door bijvoorbeeld pasjes onbruikbaar te maken. Het hele proces van controle is bovendien te voorspelbaar. Ook het op de identiteitsbewijzen zelf aanbrengen van (biometrische) gegevens maakt het voor fraudeurs alleen maar makkelijker, zeker als je bedenkt dat deze(reis)documenten ook worden gebruikt in minder betrouwbare omgevingen in het buitenland. Het gaat niet om het identiteitsbewijs, maar het proces van controle, vooral aan het begin en eind van de (strafrecht)keten. Elders (Grijpink, 2008) wijst Grijpink op het Oostenrijkse model van het gebruik van persoonsnummers. In het Oostenrijkse model heeft iedere burger een uniek identificatienummer dat de sourcePIN wordt genoemd (Hayat e.a., 2005). Deze sourcePIN is alleen bekend bij de eigenaar, het is bij wet zelfs aan de uitgevende autoriteit niet toegestaan om een kopie te bewaren. In elke overheidssector wordt een eigen sectorspecifieke PIN (ssPIN) gebruikt. Deze wordt afgeleid uit de sourcePIN, maar omgekeerd kan de sourcePIN niet uit een ssPIN worden afgeleid, en kunnen ssPINs ook niet van elkaar worden afgeleid. Volgens Grijpink toont het Oostenrijkse model aan dat een combinatie van vervormde persoonsnummers met

afgeschermde en vervormde biometrische kenmerken tot veilige en betrouwbare grootschalige biometrietoepassingen kan leiden.

3.1.1.10 Analyse door projectteam

Identiteitsfraude heeft betrekking op het (frauduleus) verkrijgen van de persoonsgegevens van een ander, en vervolgens deze gegevens te gebruiken om in andermans naam activiteiten (bijvoorbeeld delicten) uit te voeren. Daarnaast kan deze ander vrijwillig (tegen betaling bijvoorbeeld) zijn persoonsgegevens afstaan. Ook kan het zijn dat deze ander zich op verzoek van iemand voor iemand uitgeeft (bijvoorbeeld het tegen betaling uitzitten van de straf van een ander). Het tegengaan van deze identiteitsfraude vertaalt zich in de strafrechtketen vooral in een goede identiteitsvaststelling en verhoging van de kwaliteit van gegevens. Hier zien we de onderstaande kansen en bedreigingen.

Kans: Het toepassen van biometrie (vingerafdruk, gelaatscan) maakt het stelen van een identiteit moeilijker. Authenticatie (bij diensten) vind immers plaats op basis van biometrie (wie je bent), persoonsgegevens (wat je weet) en tokens/pasjes (wat je hebt); en hoe meer van deze factoren gecombineerd worden hoe kleiner de kans op identiteitsfraude. Daarnaast is het zo dat als bij een heterdaad biometrische kenmerken (vingerafdruk) worden vastgesteld, er in het vervolg van de strafrechtketen met hoge mate van zekerheid kan worden vastgesteld dat het om dezelfde persoon gaat.

Kans: Als verkeerde personen een straf uitzitten heeft dat grote impact op het beeld van een betrouwbare overheid. De verbetering van de kwaliteit van identiteitsvaststelling kan dus leiden tot een groter vertrouwen in de overheid.

Kans: Ook kan in de toekomst context informatie (waar is iemand, met wie is hij samen, etc.) technologisch gezien identificatie betrouwbaarder maken. De toepassing van deze technologie dient uiteraard te vallen binnen de grenzen van de wet (vooral Wbp).

Bedreiging: De zwakke schakel blijft echter de controle van identiteitsdocumenten. Ergens in het proces zal een koppeling moeten plaatsvinden tussen enerzijds een persoon (die zich meldt) en anderzijds een identiteit (vast te stellen via in eerste instantie een identiteitsdocument). Zelfs bij een heterdaad bestaat altijd de mogelijkheid van ‘alias fraude’. Door de koppeling van strafrechtsketennummers met HAVANK-nummers (gerelateerd aan één set vingerafdrukken) vallen wel de personen door de mand die zich bijvoorbeeld willen bedienen van meerdere aliassen (verschillende identiteitsbewijzen). Maar voor nieuwe, nog niet in de strafrechtketen geregistreerde personen blijft het voor de koppeling tussen persoon en identiteit nog steeds gaan het om de controle van identiteitsbewijzen.

Bedreiging: Er zitten tevens risico’s in het teveel vertrouwen op de techniek (in plaats van het proces van identificatie). Het vertrouwen op de techniek leidt er tegelijkertijd toe dat biometrische identiteitsdiefstal interessanter wordt voor kwaadwillende personen. Het is moeilijker om een vingerafdruk te kopiëren maar niets is onmogelijk[35]. Tevens is het lastiger diefstal van biometrische gegevens ongedaan te maken: je kunt je eigen

[35] Denk aan (digitale) diensten of toegangssystemen waarbij alleen een vingerafdruk wordt gebruikt voor authenticatie. Een kopje waaruit gedronken is kan in principe al worden gebruikt voor het achterhalen van een vingerafdruk.

biometrische kenmerken niet vervangen. Ook zijn de vingerafdrukken van kinderen onder de zes jaar en van ouderen (te droge of te dunne huid) onbetrouwbaar of van mindere kwaliteit (Bzk, 2005). De Britse wetenschapper John Daugman, specialist op het gebied van irisherkenning, voorspelt dat de Britse id-kaart ten onder gaat omdat er teveel verkeerde identificaties zullen zijn als er met vingerafdrukken en gezichtsherkenning wordt gewerkt[36].

Bedreiging: Inbreuk op privacy en belemmeringen in de persoonlijke levenssfeer vloeien ook voort uit bezoekersregistraties bij Penitentiaire Inrichtingen. Deze systemen zijn vaak lokaal voor instellingen en vallen onder de Wbp. Het risico hier is echter dat bij niet alle gebruikers duidelijk is in hoeverre deze registraties gekoppeld mogen worden aan gegevens uit de strafrechtketen, of mogen worden opgevraagd door politiekorpsen, of mogen worden uitgewisseld tussen instellingen. Tevens spelen bewaartermijnen, die uiteraard wel moeten worden nageleefd.

Bedreiging: Als bestanden eenmaal zijn vervuild, bijvoorbeeld iemand die als gevolg van identiteitsfraude ten onrechte een strafblad heeft gekregen, dan is correctie lastig omdat sporen vooral naar het slachtoffer leiden, en mogelijk ook de bewijstlastbewijslast daar ligt.

[36] http://webwereld.nl/articles/52925/-britse-id-kaart-gaat-ten-onder-aan-mismatches-.html

3.2 Cases rond persoonsdossiers

3.2.1 Elektronisch patiëntendossier EPD (casus in ontwikkeling)

3.2.1.1 Algemene beschrijving van de casus

Het elektronisch patiënten dossier (EPD) zoals dat per 1 juni 2008 geleidelijk wordt ingevoerd, is een landelijke infrastructuur voor geregistreerde zorgverleners waarmee patiëntinformatie uit verschillende informatiesystemen kan worden uitgewisseld[37]. Het Elektronische Medicatie Dossier (EMD) en het Waarneem Dossier Huisartsen (WDH) zijn deel van het EPD en als eerste operationeel. Per september 2008 komen de eerste praktijken vanuit een pilot fase in regulier gebruik. Hierbij worden gegevens uitgewisseld tussen apotheken, ziekenhuizen, huisartspraktijken en huisartsposten. Het landelijk EPD moet geleidelijk aan toegang geven tot alle gegevens die van belang zijn voor de behandeling van patiënten, zoals allergieën, laboratoriumuitslagen en röntgenfoto's.

- *Landelijk schakelpunt*

Het landelijk schakelpunt (LSP), maakt elektronische uitwisseling van patiëntinformatie tussen zorgverleners onderling en zorgverleners en zorginstellingen mogelijk. Keurings- en bedrijfsartsen zijn uitgesloten van toegang, net als de zorgverzekeraars. De belangrijkste dienst van het LSP is de verwijsindex ook wel verwijs- en routeringsdienst genoemd. Het is de ‘Internet Exchange’ van de informatie infrastructuur in de zorg. Het landelijk schakelpunt bewaart geen gegevens van de patiënt maar gegevens over de plaats waar gegevens van patiënten zijn opgeslagen. De gegevens zelf blijven beheerd bij de verantwoordelijke zorgverlener. Een geautoriseerde zorgverlener kan de gegevens via een zoekmachine opzoeken en ze dan via het LSP opvragen uit dossiers elders in het land op basis van het burgerservicenummer (BSN) van de patiënt.

De informatie in patiëntendossiers is vertrouwelijk en de zorgverlener moet een geldige reden hebben om gegevens op te vragen. Alleen zorgverleners die zijn geregistreerd in het UZI-register (zie onder) en zich geauthenticeerd hebben met hun UZI-pas kunnen het dossier via het landelijk schakelpunt raadplegen. Daarvoor moeten zij wel de toestemming van de desbetreffende patiënt hebben. Ook kan een patiënt bezwaar maken tegen gegevensuitwisseling via het LSP en deze (laten) blokkeren. Het LSP zorgt daarnaast voor de feitelijke autorisatie. Het systeem logt alle toegangen zodat het mogelijk is om achteraf te controleren of ook daadwerkelijk een noodzaak bestond voor het inzien van gegevens en een behandelingsrelatie bestaat zodat er eventueel (tucht)rechtelijk kan worden opgetreden.

Uiteindelijk moeten via het LSP ook patiënten toegang krijgen tot hun eigen patiëntinformatie, waarmee zij het recht op inzage in hun gegevens (op grond van de Wgbo en Wbp) direct kunnen uitoefenen. De toegang door patiënten kan echter tegelijkertijd worden gezien als een potentieel veiligheidsrisico van het systeem.

[37] Zie http://www.infoepd.nl/informatiepunt_com/za_epdepd.php

- *Goed beheerd zorg systeem*

Voordat zorgverleners op het LSP mogen aansluiten moeten hun systemen voldoen aan de eisen van een Goed Beheerd Zorgsysteem (GBZ)[38]. De belangrijkste eisen van het GBZ zijn gericht op het transparant houden van de verantwoordelijkheid van de behandelende zorgverlener voor patiëntendata, procedures om er voor te zorgen dat patiëntdossiers daadwerkelijk aan de goede patiënt worden gekoppeld en het handhaven van de privacy van de patiënt. Verder zijn er technische eisen zoals het gebruik van HL7 voor berichtenuitwisseling. Deze eisen liggen vast in de NEN normen 7510[39] en als aanvulling daarop NEN 7511/7512. In de praktijk zullen de eisen voor een GBZ wat betreft de technische infrastructuur worden afgedekt door het gebruik van een gecertificeerd zorgsysteem van een gecertificeerd productleverancier.

Voor het koppelen van patiënten aan hun dossiers moet het BSN van de patiënt aan de dossiers worden toegevoegd en worden geverifieerd (zie sectie 3.2.1.6). Nieuwe dossiers worden alleen onder het BSN opgeslagen.

Zorgverleners kunnen alleen patiëntendata invoeren, veranderen of opvragen via het LSP na zich te hebben geauthenticeerd met behulp van een pincode en een z.g. UZI-pasje. Het valt binnen de professionele verantwoordelijkheid van zorgverleners dat ze hun pasje niet uitlenen en hun pincode geheimhouden met uitzonderingen voor laag veiligheidsniveau anonieme pasjes voor een groep medewerkers. Uit pilots is gebleken dat er situaties zijn waar dit praktische problemen oplevert zoals bij het opvragen van dossiers door medische assistenten voor de eigenlijke zorgverlener waarvoor een mandateringssysteem zal worden opgezet. Binnen een goed beheerd zorgsysteem kan de verantwoordelijkheid voor en het opvragen van gegevens door het systeem worden bijgehouden, mits iedereen zich aan de procedures houdt. De mate waarin dit volgens de letter zal gebeuren hangt af van de praktische werkbaarheid.

3.2.1.2 Beleidsontwikkeling

Volgens het plan van aanpak van het EPD van het ministerie van VWS moet: “Kwaliteit, doelmatigheid en doeltreffendheid van de zorg moeten verbeterd worden. Een van de aandachtspunten daarbij is het tijdig en op eenduidige wijze beschikken over de gegevens van een patiënt. Helaas blijkt dat door gebrek aan informatie of door onjuiste informatie niet altijd optimale zorg verleend wordt.”[40] Het elektronisch patiëntendossier ontstond vanwege de steeds mondiger wordende patiënt, en de wens van overheid en het veld om zorggegevens beter toegankelijk te maken. Met behulp van ICT zouden kwaliteit, doelmatigheid en doeltreffendheid moeten worden aangepakt.

Hoewel er op regionaal en individueel niveau al veel initiatieven waren om gegevens uit te wisselen, was de Nederlandse overheid er niet van overtuigd dat de zorgorganisaties zelf een EPD voor elkaar konden krijgen. Omdat optimale benutting van ICT-initiatieven niet bestond was sprake van zowel technologische als organisatorische fragmentatie en een gebrek aan snelheid. Op verzoek van de Kamer is de overheid daarom ingesprongen om lokale initiatieven op te schalen naar landelijk niveau. Om dit te bereiken werd het

[38] https://www.nictiz.nl/?mid=132&pg=167&doc=120&download&ext=pdf
[39] http://www.nen7510.org/
[40] Ministerie van VWS, ‘ICT in de zorg. Van Elektronisch Medicatie Dossier naar Elektronisch Patiënten Dossier. Plan van aanpak’, 1 maart 2005, p. 2

Elektronisch Patiëntendossier ingericht, welke in verschillende zogenaamde 'hoofdstukken' geïmplementeerd gaat worden. Het uiteindelijk EPD bevat alle relevante medische gegevens over de patiënt, inzichtelijk voor alle daartoe bevoegde zorgverleners in heel Nederland. Regionale ontwikkelingen zoals de OZIS regio's kunnen wel naast en in samenwerking met het landelijke EPD blijven bestaan.

De eerste initiatieven die uiteindelijk leiden tot een landelijk EPD zijn al gestart in 2001, waaronder de opzet van een BSN in de zorg en de inrichting van het Nationaal ICT Instituut in de Zorg (NICTIZ). Hoewel de voorspelling was dat al in 2004 een landelijk EPD zou bestaan[41], is pas per januari 2006 de infrastructuur voor het eerst uitgerold en is men nu (september 2008) bezig met opschalen naar landelijke pilots op het gebied van het EMD en WDH. De landelijke vereniging van huisartsen vreest echter een administratieve lastenverzwaring. Zij heeft haar leden geadviseerd alleen aan de WDH mee te doen als de huisartsen waarneempost is aangesloten ondanks dat er tot eind 2009 subsidie beschikbaar is voor het aansluiten.

- *Beleidskeuzen*

De algehele regie wordt niet gevoerd door de overheid, maar bestaat uit een balans tussen overheid en veld. De overheid draagt slechts zorg voor de invulling van de communicatie randvoorwaarden en de centrale voorzieningen. Het veld zorgt voor implementatie, financiering en uitvoering. Op basis van de NICTIZ basisinfrastructuur wordt er uitgegaan van een aantal kernpunten in het beleid rondom het EPD:

- De zorgverlener is autonoom en zelf verantwoordelijk voor zijn informatie en ter beschikking stelling daarvan.
- Gegevens blijven bij de zorgverlener en worden decentraal opgeslagen. De verwijsindex regelt de communicatie tussen decentrale databases. Dit in het kader van veiligheid en bescherming van persoonsgegevens.
- Aansluiten bij bestaande wet- en regelgeving. Waar nieuwe wetgeving nodig is wordt geprobeerd binnen bestaande wetgeving van start te gaan.
- Aansluiten bij de speciaal ontwikkelde NEN-norm 7510 voor veilig en betrouwbaar communiceren.

3.2.1.3 Juridische setting

De juridische setting kan worden verdeeld in twee delen; context specifieke wetgeving en algemene wetgeving. De context specifieke wetgeving (lex specialis) richt zich op wetgeving voor medische professionals en organisaties (Wet BIG, Wgbo, Kwaliteitswet zorginstellingen (Kzi)) en op de constructie van een EPD (Wet op het EPD). De algemene wetgeving (lex generalis) die integraal toepasbaar is, bestaat met name uit de Wet bescherming persoonsgegevens (Wbp) en de Wet gebruik burgerservicenummer in de Zorg (Wbsn-z).

Het landelijke EPD heeft tot doel de goede behandeling en verzorging van patiënten te ondersteunen. Op de behandeling en verzorging van patiënten is boek 7, afdeling 5, titel 5 van het Burgerlijk Wetboek (Wet geneeskundige behandelingsovereenkomst: Wgbo) van toepassing. Deze wet legt aan hulpverleners o.a. een dossierplicht en een geheimhoudingsplicht op.

[41] Ton Smit, 'Borst voorspelt: 'Zorg heeft landeljk EPD in 2004', Automatiseringsgids, week 43, 2001

Naast de Wgbo, die dus o.a. een dossierplicht kent, is ook de Wbp van toepassing op de verwerking van persoonsgegevens over iemands gezondheid. Zodanige verwerking is slechts toegestaan als aan de voorwaarden uit de Wbp is voldaan.

Sinds de invoering van de Zorgverzekeringswet (Zvw), op 1 januari 2006, bestaat er in de gezondheidszorg een wettelijke identificatieplicht. Artikel 118 Zvw luidt als volgt:

> *"1. Een verzekerde die voor rekening van zijn zorgverzekering bij ministeriële regeling aan te wijzen zorg of andere diensten als bedoeld in artikel 11 wenst te genieten, verstrekt aan de persoon of instelling die die zorg of dienst verleent ter inzage een identiteitsbewijs als bedoeld in artikel 1, eerste lid, van de Wet op de identificatieplicht, of een ander bij ministeriële regeling aan te wijzen document waarmee zijn identiteit kan worden vastgesteld.*
>
> *2. Indien het identiteitsbewijs niet onmiddellijk ter inzage kan worden verstrekt, kan de persoon of instelling toestaan dat uiterlijk binnen een termijn van veertien dagen aan deze verplichting wordt voldaan."*

Sinds de inwerkingtreding van de Wbsn-z, bepaalt het derde lid van art. 118 Zvw dat de hulpverlener (persoon of instelling) het BSN van de patiënt/verzekerde in zijn administratie opneemt na verificatie bij de SBV-Z.

- *Wbsn-z*

Een aparte wet, de Wet gebruik burgerservicenummer in de zorg (Wbsn-z), regelt het gebruik van het BSN in de gezondheidszorg. Behalve de overheid mag ook de zorgsector het BSN gebruiken bij het uitwisselen van gegevens met andere zorgaanbieders, indicatieorganen en in het declaratieverkeer. Zorgaanbieders en indicatieorganen mogen het BSN gebruiken vanaf 1 juni 2008. Een jaar daarna is gebruik van het BSN verplicht. Het BSN moet in de zorgsector een eind maken aan de verschillende persoonsnummers die zorgaanbieders, indicatieorganen en zorgverzekeraars nu nog gebruiken. De invoering van het BSN in de zorg heeft de volgende voordelen:

- Het vermindert het aantal fouten bij het uitwisselen van patiëntgegevens.
- Het voorkomt persoonsverwisseling.
- Het maakt declareren eenvoudiger.
- Het geeft betere bescherming tegen identiteitsfraude.

Het BSN is ook een voorwaarde om op een betrouwbare en veilige manier patiëntgegevens uit te wisselen via het landelijk elektronisch patiëntendossier (EPD).[42]

[42] Bron: Informatiepunt BSN in de zorg en landelijk EPD. Op internet: <http://www.infoepd.nl/informatiepunt_com/achtergrondinformatie_bsn_in_de_zorg.php> (laatst geraadpleegd op 23 september 2008).

- *Kaderwet elektronische zorginformatieuitwisseling (Wet EPD)*

Bij het parlement is momenteel aanhangig de Wet tot wijziging van de Wbsn-z ivm de landelijke elektronische informatieuitwisseling in de zorg (Wet EPD).[43] Deze wet zal gaan heten: Kaderwet elektronische zorginformatieuitwisseling. Het wetsvoorstel betreft de elektronische uitwisseling tussen zorgaanbieders van medische persoonsgegevens van hun patiënten: het regelt de beschikbaarheid van de gegevens alsmede de infrastructuur en de randvoorwaarden voor de uitwisseling. Het wetsvoorstel schept daarmee de kaders voor het landelijk elektronisch patiëntendossier (EPD). Het EPD is een stelsel waarin de medische dossiers van alle zorgaanbieders van een patiënt overzichtelijk geordend worden zodat ze geraadpleegd kunnen worden. Het dossier van een patiënt blijft bij de zorgaanbieder zelf, maar een andere zorgaanbieder van die patiënt kan de relevante gegevens, eventueel na daarop geattendeerd te zijn, wel inzien. Het gegevensverkeer wordt in goede banen geleid door op een centraal punt bij te houden waar zich welke dossiers bevinden. Via dat centrale punt wordt ook de verbinding tot stand gebracht tussen de zorgaanbieder die de medische gegevens van de patiënt heeft en de zorgaanbieder die ze wenst te raadplegen. Deze wet regelt o.a. de instelling van een Landelijk Schakel Punt (LSP), verplichtingen voor zorgaanbieders (o.a. verplichting tot aansluiting op het landelijke EPD), verplichtingen voor het LSP en delegatie via lagere regelgeving. Waar de zorgaanbieder verplicht is om mee te doen aan het EPD is de patiënt niet tot deelname verplicht.

Er is op dit moment nog geen wettelijke verplichting tot het gebruik van de UZI-pas. Na de invoering van de Wbsn-z op 1 juni 2008 en het verplichte gebruik daarvan na 1 juni 2009 is er echter wel een feitelijke indirecte verplichting tot gebruik van de UZI-pas. Het BSN van een patiënt moet in verband met de administratieve verplichtingen van een ziekenhuis gecontroleerd worden. De zorgverlener of zorginstelling moet dit nummer controleren bij de SBV-Z (zie sectie 3.2.1.6) en om hierop aansluiting te krijgen is een UZI-pas / UZI-servercertifiaat nodig.[44] Ook voor alle interactie met het landelijk schakelpunt is een UZI pas noodzakelijk.

3.2.1.4 Institutionele setting

De verantwoordelijkheid voor de patiëntendata ligt en blijft liggen bij de behandelende zorgverlener (en daarvan afgeleid, degene die de gegevens heeft ingevoerd, of degene die gegevens expliciet onder de verantwoording van een andere zorgverlener heeft gebracht).

Het Nationaal ICT Instituut in de Zorg (Nictiz) is de opdrachtgever en verantwoordelijke voor het Landelijk schakelpunt op verzoek van het Ministerie van VWS en de zorgsector. Ontwikkeling en beheer van het LSP is, na een Europese aanbesteding, in handen gegeven van CSC Computer Sciences B.V.

Het UZI register valt onder de verantwoordelijkheid van de CIBG een uitvoeringsorganisatie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Ook het SBV-z valt onder de verantwoordelijkheid van het CIBG. Voor het beheer van de PKI-infrastuctuur is Pink Roccade verantwoordelijk (althans volgens de naam op de certificaten).

[43] *Kamerstukken II*, 2007/08, 31 466, nr. 2.
[44] <www.uzi-register.nl> veelgestelde vragen, juridisch

3.2.1.5 Elektronische dienstverlening aan de burger

Op termijn (eind 2009) moet ook de individuele burger toegang krijgen tot zijn eigen gedistribueerde patiëntendossiers waarmee zij het recht op inzage in hun gegevens (op grond van de WGBO en Wbp) direct kunnen uitoefenen. Op het moment is echter nog geen middel beschikbaar waarmee een patiënt zich met voldoende zekerheid kan authenticeren aangezien DigiD+ niet als voldoende zeker wordt gezien. Er wordt gehoopt dat te zijner tijd de e-NIK (Elektronische Nationale IdentiteitsKaart) kan worden gebruikt. Deze kaart en de bijbehorende infrastructuur bestaat echter nog niet. Als miljoenen burgers toegang tot hun eigen dossier krijgen zal toegangscontrole met strikt technische middelen moeten worden afgedwongen.

De belangrijkste beoogde verandering voor de burger is echter grotere (medische) patiëntveiligheid doordat medische zorg van verschillende aanbieders beter op elkaar is afgestemd (bijvoorbeeld dat gevaarlijke combinaties van medicijnen niet meer worden voorgeschreven).

3.2.1.6 Identity management

- *Het BSN in de zorg en de SBV-Z*

Het kunnen koppelen van medische dossiers van een bepaald individu bij verschillende organisaties wordt vereenvoudigd wanneer ieder individu een landelijk uniek, persistent, persoonsgebonden nummer heeft dat binnen elk dossier wordt gebruikt.[45] Er is bij VWS voor gekozen hiervoor het BSN te gebruiken. Op grote hoeveelheden bestaande dossiers staat alleen naam adres en geboortedatum. Om deze dossiers van een BSN te voorzien worden apothekers en andere medische instellingen als ziekenhuizen geacht hun patiënten te vragen zich te legitimeren met een Nederlands identiteitsbewijs (paspoort, identiteitskaart of rijbewijs) waarop het BSN van de persoon is opgenomen. Deze plicht bestaat sinds de inwerkingtreding van de Zorgverzekeringswet op 1 januari 2006. Tot 1 juni 2008 bestond deze identificatieplicht, maar zonder dat het sofi-nummer of BSN mocht worden opgeslagen. Dat mag pas sinds de inwerkingtreding van de Wbsn-z. Huisartsen hebben een ontheffing hiervoor (motie Timmer[46]). Bovendien heeft het ministerie van VWS een aparte ICT-dienst in het leven geroepen, de SBV-Z (Sectorale Berichten Voorziening in de Zorg, die voor in het UZI register opgenomen partijen het BSN kan invullen op basis van naam geboortedatum en adres, dan wel voor een BSN ter vergelijking de naam geboortedatum en adres in de gemeentelijke basisadministratie kan teruggeven (verificatie of het betreffende BSN inderdaad aan die persoon is uitgegeven). Bij twijfel over een Nederlands identiteitsbewijs kan ook deze ook worden geverifieerd.

- *Het UZI-register en de UZI-pas*

Het unieke zorgverlener identificatie (UZI) register en de UZI-pas zijn een integraal onderdeel van het EPD. De door NICTIZ ontwikkelde basisinfrastructuur uit 2004 omvat een identificerend stelsel voor zorgverleners, met daarin een identificatieregister (UZI-

[45] Dat is overigens geen noodzakelijkheid. Het is ook mogelijk te werken met vertaaltabellen tussen de verschillende nummersystemen beheerd door schakelpunten of Kruispuntbanken, zoals dat bijvoorbeeld in België gebeurt.
[46] http://www.minvws.nl/kamerstukken/staf/motie_timmer__regionale_zorgvernieuwingsgelden.asp

register), en de UZI-pas als middel voor authenticatie en drager van een public en private key voor elektronische handtekening en beveiligde communicatie.

In het UZI-register wordt geregistreerd wie en op welk veiligheidsniveau toegang is verleend tot het EPD, in het bijzonder tot de LSP en de zogenaamde UZI-diensten. Om in het UZI register te kunnen worden ingeschreven dient een abonnee van het UZI-register een aanvraag te doen. Abonnees zijn meestal werkgevers, hetzij organisaties als ziekenhuizen, hetzij vrijgevestigde zorgverleners als huisartsen. Om als abonnee toegelaten te worden dient men (kopieën van) een paspoort op te sturen. Of iemand daadwerkelijk zorgverlener is, wordt getoetst in een van de door het ministerie van VWS erkende toetsingsregisters. Voor de artikel 3 beroepsgroepen is dit het BIG register. Toetsing van artikel 34 beroepsgroepen vindt plaats in het Kwaliteitsregister Paramedici of door een diplomatoets[47]. Om in de toetsingsregisters te worden opgenomen moet een diploma worden overlegd en regelmatig worden bijgeschoold.

Eenmaal ingeschreven in het register kan men een UZI pas aanvragen. Veranderingen in de toelatingsstatus worden automatische doorgegeven aan het UZI-register. UZI-Passen worden persoonlijk afgehaald en op het moment van afhalen wordt gecontroleerd of pas en legitimatie bewijs met elkaar overeenstemmen. Deze UZI pas werkt op basis van een PKI infrastructuur. Met de pas en een wachtwoord kan de gebruiker zich authenticeren en kunnen berichten worden versleuteld. Het zorgsysteem dient daarvoor een kaartlezer te hebben. Het LSP –of een UZI service provider als de SBV-Z– kan daarom nagaan welke persoon het systeem gebruikt, en nagaan of de desbetreffende persoon op grond van zijn professionele capaciteit volgens de Wet BIG gerechtigd is tot het opvragen van de informatie en het gebruik van de infrastructuur. Om controle op toegelaten gebruik achteraf mogelijk te maken houdt het systeem bovendien bij wie welke informatie waarvandaan heeft opgevraagd dan wel dat geprobeerd heeft.

Deze beveiliging vooraf en controle achteraf staat of valt er wel bij dat iedereen zich professioneel gedraagt en geen pasjes met pincode uitleent. Dit vergt een serieuze omslag in het denken (risicobewustzijn) binnen de gezondheidszorg. Uit een recent onderzoek van het College bescherming persoonsgegevens (CBP) en de Inspectie voor de Gezondheidszorg (IGZ) blijkt dat geen van de twintig onderzochte ziekenhuizen aan de norm voor informatiebeveiliging voldoet (IGZ/CBP, 2008). Zo wordt informatiebeveiliging niet systematisch geregeld, is de verantwoordelijkheid voor de beveiliging onvoldoende ingebed in de organisatie en is de toegang tot patiëntgegevens onvoldoende afgeschermd. Hele afdelingen blijken gebruik te maken van dezelfde inloggegevens en computers blijken onbeschermd toegankelijk te zijn voor derden. In vergelijking met een in 2004 uitgevoerd onderzoek blijkt er weinig te zijn verbeterd.

Voor zorgverleners in verschillende rollen heeft het UZI-register verschillende typen UZI-passen. Naast de UZI-pas voor de zorgverlener abonnee, kent het UZI-register de passen ‘medewerker op naam’ en ‘medewerker niet op naam’. De pas voor de medewerker op naam wordt door het UZI-register aan de medewerker zelf uitgereikt. De pas voor de medewerker niet op naam, wordt door het UZI-register aan de zorginstelling of zorgverlener uitgereikt. Op de UZI-passen voor de zorgverlener en de medewerker op

[47] Zie http://www.uziregister.nl/Images/Algemene_brochure_UZI-pas_tcm38-17176.pdf , http://www.uziregister.nl/ikwileenuzipas/voorwie/default.asp , http://www.infoepd.nl/ufc/file2/informatiepunt_sites/marjan/6f0a022dc96a561052e2b3915df61dcb/pu/Het_UZI_register_en_de_UZI_pas.pdf

naam staat een foto van de pashouder. De zorginstelling of zorgverlener geeft de pas aan een medewerker en houdt bij welke medewerker over deze pas beschikt. UZI passen kunnen een verschillend veiligheidsniveau hebben, waarbij passen op het hoogste veiligheidsniveau, nodig voor de toegang tot het LSP, altijd op naam moeten zijn gesteld. Technisch gezien is het UZI-register ook verantwoordelijk voor een zogenaamde Certificaat Dienstverlener of Certification Service Provider (CSP)[48], welke is opgenomen in de vertrouwenshiërarchie van de PKI overheid. Het UZI register publiceert op het web een lijst van geldige en ingetrokken certificaten. Het UZI register geeft ook certificaten uit voor informatie systemen en applicaties van zorgaanbieders. Deze worden aangeduid als services.

3.2.1.7 Veranderingen ingevolge (het gebruik van) ICT

Zorgverleners hebben het gevoel dat een gedeeld dossier voor een ander publiek wordt geschreven. Waar patiëntendossiers allereerst werden gezien voor eigen gebruik, speelt voor een gedeeld dossier op de achtergrond dat dit kan worden opgevraagd door collega's en op termijn ook door patiënten. De verwachtingen aan de rapportage zijn daarbij hoger omdat ze buiten de eigen context kunnen worden gebruikt (bijvoorbeeld niet alleen meer voor vervangende huisartsen maar ook het ziekenhuis). Het landelijk EPD geeft daarnaast nog een verschuiving van een regionaal (deels bekend) - naar een landelijk publiek.

Een met bovenstaande samenhangend gevolg is een grotere nadruk op en begrip voor standaardisatie.

3.2.1.8 Relevante kwesties die rijzen/zijn gerezen in de betreffende case

- *Het gebruik van het BSN*

Het gebruik van een landelijk uniek nummer in plaats van persoonsgegevens als naam en geboortedatum moet de kans op fouten bij het combineren van dossiers verkleinen. In theorie zou het mogelijk geweest zijn iedereen een speciaal voor de zorg en het EPD bedoeld nummer uit te geven zoals dit in bijvoorbeeld België en Oostenrijk is gebeurd waar de koppeling met andere nummers op een gecentraliseerd punt wordt gedaan. Dit zou zeker bijdragen aan het opsluiten van medische gegevens binnen de medische sector en het EPD. Het ministerie van VWS heeft echter aangedrongen op het gebruik van het BSN omdat ze wilde aansluiten bij de bestaande infrastructuur voor het eenmalig uitgeven van nummers, en bij bestaande identiteitsbewijzen. Het gebruik maken van paspoort, identiteitskaart of rijbewijs als legitimatiebewijs zou in ieder geval ergens (bijvoorbeeld bij SBV-z) op eenduidige wijze een koppeling tussen patiëntnummers en het BSN van een persoon vereisen. Dit zou lastiger zijn te verifiëren en de toch al grote complexiteit van de EPD operatie vergroten. Voor het gebruik van de BSN in de zorg is een aparte wet ingevoerd (Wet gebruik burgerservicenummer in de zorg: Wbsn-z).

- *Gedistribueerd of centraal*

De keuze van een gedistribueerde architectuur voor het EPD is vooral ingegeven door de keuze voor het houden van de verantwoordelijkheid voor patiëntgegevens bij individuele

[48] http://www.uziregister.nl/

zorgverleners. Het laat ook een gefaseerde invoering van het EPD toe waarbij steeds meer onderdelen kunnen worden gedeeld (zoals in de eerste fase elektronische medicatie dossier (EMD) en waarneem dossier huisartsen (WDH) terwijl lokaal veel meer digitaal beschikbaar kan zijn. Het doet ook recht aan de onafhankelijkheid van de Nederlandse zorgverlener. In Engeland met zijn nationaal georganiseerde gezondheidszorg is echter voor een gecentraliseerd systeem gekozen.

3.2.1.9 Dilemma's waar men in de case tegenaan is gelopen

Het EPD moet steeds balanceren tussen het doel van toegankelijkheid en de privacy van de patiënt. Het beschermen van de patiëntgegevens maakt implementatie en omgang met het EPD wezenlijk moeilijker. Er zijn daarom soms werkbare compromissen gesloten. Binnen een behandelingsrelatie is redelijk veel toegestaan, daarbuiten is geprobeerd toegang dicht te timmeren. Om dit onderscheid te handhaven is gekozen voor een mengsel van procedurele regels en afdwingen met technische maatregelen. Een dilemma is daarom wat beter door procedurele regels en wat door technische maatregelen kan worden afgedwongen. Technisch afdwingen forceert het handhaven van regels, maar maakt systemen inflexibel en kan zelfs tot onwerkbare situaties leiden.

In dit kader is het van belang goed oog te hebben op de sociale dynamiek binnen het veld. Wanneer beveiliging het werken lastiger maakt bestaat al snel de neiging om de beveiliging te negeren. "People make secure systems insecure. Not out of malice, or even out of laziness. People make secure systems insecure because insecure systems do what people want and secure systems don't." (Grimmelmann , 2008). Het lijkt overigens niet waarschijnlijk dat de beveiliging bij kleine huisartsenpraktijken en andere zorgverleners beter is geregeld dan in ziekenhuizen die veel meer middelen kunnen toewijzen aan deugdelijk ICT beleid.

3.2.1.10 Analyse door projectteam

Het Nederlandse EPD is zorgvuldig en doordacht opgezet. Er is veel aandacht besteed aan het op zetten van een "hek" om medische gegevens, om er voor te zorgen dat deze binnen de medische sector blijven. Daarbinnen zal op routine matige wijze informatie worden uitgewisseld vergelijkbaar met de manier waarop binnen een ziekenhuis informatie tussen medici wordt uitgewisseld. Er is de afweging gemaakt om zorgverleners een professioneel vertrouwen te geven en organisatorische regels op te stellen om er voor te zorgen dat uitwisseling plaats vindt binnen een behandelingsrelatie. Technische infrastructuur dwingt deze regels gedeeltelijk af. Waar dat onwerkbaar is, maakt de opzet controle achteraf mogelijk. Patiënten kunnen bovendien onderdelen van hun dossier voor bepaalde, of alle zorgverleners ontoegankelijk maken. Het is echter aan te nemen, en de ervaring in pilots leert, dat mensen er mee kunnen leven dat zorgverleners uit hoofde van hun functie privacygevoelige details te weten komen.

Kans: Het EPD wordt ingevoerd ter verbetering van de kwaliteit van de zorg aan patiënten[49].

- De kans op medische fouten wordt kleiner.
- De specialist, apotheker of (waarnemend)huisarts weet welke medicijnen worden gebruikt. Of voor welke medicijnen er een allergie is.

[49] http://www.infoepd.nl/informatiepunt_com/zorgconsument_landelijk_epd.php

- De patiënt hoeft niet steeds opnieuw te vertellen wat al in het medisch dossier staat (eenmalige uitvraag).
- Via het EPD informeert de waarnemend huisarts de eigen huisarts over de behandeling.

Bedreiging: Het EPD kan leiden tot een schaduw dossier van artsen voor eigen gebruik dat niet wordt gedeeld. Artsen kunnen in verband met verantwoordelijkheidsvragen terughoudend zijn rond het EPD. De landelijke vereniging van huisartsen stelt dat het gemiddeld 20 minuten per patiënt kost om het dossier te uniformeren en op een niveau te brengen dat het landelijk gedeeld kan worden[50].

Kans: Het EPD zou moeten leiden tot een meer gestructureerde en uniforme dossiervorming. Dat maakt aggregatie van data voor onderzoek ten behoeve van *evidence-based medicine*, mogelijk. Merk hierbij wel op dat epidemiologie en evidence-based medicine (bewust) geen designdoel van het EPD zijn. Voor het gebruik van de AORTA infrastructuur voor het elektronisch kind dossier (EKD) moeten hiervoor echter faciliteiten worden gecreëerd, aangezien anonieme analyse van de EKD gegevens tot de vereisten behoort waarop is ingezet.

Bedreiging: De grootste uitdaging op privacy gebied is om het "hek" om de medische sector overeind te houden en druk om het hek doorlaatbaar te maken voor partijen buiten de medische sfeer te weerstaan. De technische mogelijkheden om (delen van) patiëntendossiers beschikbaar te stellen voor andere doeleinden zijn immers door het EPD eveneens veel groter geworden. Ook al kan dit uitwisselen wettelijk gezien niet, hier speelt wel het vertrouwen en de perceptie van de burger.

Kans: De invoering van het EPD kan leiden tot betere technische informatiebeveiligingsmaatregelen en een groter bewustzijn voor het probleem.

Bedreiging: Op dit moment komt een groter risicobewustzijn ruim onvoldoende uit de verf. Het eerder aangehaalde rapport (IGZ/CBP, 2008) laat zien dat ziekenhuizen nog steeds niet voldoen aan de norm ter beveiliging van patiëntengegevens: “Uit het onderzoek blijkt dat er vooral op technisch gebied in vergelijking met vier jaar geleden veel is verbeterd. Echter, zowel de leiding als de medewerkers zijn zich nog steeds onvoldoende bewust van de risico’s die gebruik van ICT in ziekenhuizen met zich meebrengt. […] Een andere belangrijke bevinding is het ontbreken van bewustzijn bij medewerkers van het belang van informatiebeveiliging. Informatiebeveiliging staat of valt met het gedrag van medewerkers en effectieve controle op gedrag ontbreekt nog te vaak.”
Een te onzorgvuldige omgang met medische dossiers is ook zichtbaar geworden in een onderzoek van RTV West van november 2008. Een journalist van de omroep deed zich voor als coassistent en belde naar de ziekenhuizen met de vraag of ze medische dossiers van patiënten konden faxen naar hem. Zes ziekenhuizen vroegen alleen de naam en geboortedatum van de patiënt en faxten de gegevens toe. [51]

Bedreiging: De omvang van de schade door aanvallen van cybercriminelen wordt door het EPD in potentie vergroot (Spaink, 2005). Binnen de EPD architectuur en

[50] Brief van het LHV aan al haar leden d.d. 14 oktober 2008 over het EPD naar aanleiding van de brief van VWS aan alle huisartsen met de uitnodiging aan te sluiten op het LSP.
[51] http://www.ad.nl/binnenland/2765982/Ziekenhuizen_slordig_met_medisch_dossier.html

implementatie is veel aandacht voor beveiliging, maar met zijn gedistribueerde architectuur is het Nederlands EPD technisch wel vrij complex. Er lijkt ondertussen een criminele business case te bestaan voor de ontvreemding van medische gegevens, althans in de VS.[52]

Kans en bedreiging: Het lijkt er op of marktdruk en de eisen voor een goed beheerd zorgsysteem die het EPD stelt er voor zal zorgen dat er slechts een klein aantal aanbieders van zorgsystemen over blijft. Een fijnmazig gedistribueerd systeem van verantwoordelijkheden staat dit niet in de weg en een koppeling via een landelijk schakelpunt maakt het eenvoudiger. Wanneer daadwerkelijk een consolidatie optreedt binnen de markt voor zorgsystemen, vergroot dit de kwetsbaarheid van het systeem. Een fundamenteel lek in een systeem betekent dan namelijk een probleem op grote schaal. Diversiteit in aanbieders en een gedistribueerde architectuur leveren intrinsiek meer veiligheid op. Daar tegenover staat echter een grotere complexiteit.

Bedreiging: Het gebruik van technologie, zoals de UZI-passen, valt of staat met de discipline in het gebruik ervan. UZI-passen zijn op naam, en de druk (via sancties) is hoog om deze niet uit te lenen, maar werkbaarheid in de praktijk zou hier toch toe kunnen leiden (bijvoorbeeld artsen die uitlenen aan hun assistenten omdat assistentenpasje niet de bevoegdheden geven die nodig zijn). Hier ligt een balans van efficiëntie versus risico's.

Kans: Technische maatregelen zoals een mandateringsinfrastructuur kunnen veel voorkomende problemen op lossen binnen de letter of de geest van de wet.

Bedreiging: Waar op termijn patiënten toegang krijgen tot het EPD, heeft 'in principe' iedereen toegang tot het EPD. Dit wil zeggen, de beveiliging van het dossier wordt hiermee afhankelijk van hoe goed derden hun beveiliging hebben geregeld (externe factoren). Aangezien Nederland momenteel geen sterke identiteitsinfrastructuur kent (DigiD is momenteel het enige beschikbare authenticatiemiddel, terwijl de aanvraag van een DigiD geen fysieke presentatie van een deugdelijk identiteitsbewijs vereist – in sectie 0 gaan we hier nader op in) is hier een fundamenteel zwakke schakel in de beveiliging van persoonsinformatie die zich in dit veld nadrukkelijker manifesteert dan in andere publieke domeinen (zoals belastingen). Misbruik van een digitale identiteit om medische gegevens te achterhalen lijkt waarschijnlijker dan misbruik in het kader van belastingaangifte. Sterke authenticatie voor burgers, gelijk aan de UZI-passen voor zorgverleners, kan een groot deel van de risico's op dit punt verminderen. Nieuwe, hogere niveaus van DigiD, zoals beoogd met de elektronische Nederlandse identiteitskaart (eNIK[53]), zouden dit kunnen realiseren (Jacobs et al, 2008).

Kans: De AORTA EPD architectuur maakt co-creatie van dossiers, en patiënten die zelf informatie gaan bijhouden (via bijvoorbeeld Google Health) mogelijk of in elk geval niet onmogelijk. Hier speelt wederom de vraag van verantwoordelijkheid voor de juistheid van de gegevens. Tien ziekenhuizen hebben zelfs belangstelling getoond het landelijk

[52] In de VS is duidelijk geworden dat er ook een criminele business case bestaat voor de ontvreemding van medische gegevens. Elektronische patiëntendossiers van miljoenen Amerikanen zijn in handen gekomen van hackers. Die eisen een onbekend geldbedrag om af te zien van openbaarmaking van de zeer gevoelige informatie, aldus een bericht in de New York Times, zie http://www.nytimes.com/2008/11/07/business/07data.html.
[53] http://www.e-overheid.nl/thema/basisvoorzieningen/domeinbeauthenticatie/enik

elektronisch patiëntendossier (EPD) terzijde te schuiven en in plaats daarvan Google Health of Microsoft's Health Vault te gebruiken[54].

Bedreiging: Initiatieven zoals Google Health betekenen een centralisatie van medische gegevens wat inherent meer veiligheidsproblemen betekent dan een gedistribueerd systeem. Daarnaast is de vraag of het wenselijk is om medische gegevens onder te brengen bij een commerciële Amerikaanse partij gegeven het nagenoeg ontbreken van privacywetgeving in de VS.[55]

Bedreiging: Ook zien we binnen de medische sector een verschuiving van hulpverlening naar dienstverlening. De patiënt wordt daarbij niet alleen mondiger, maar ook veeleisender. In die context kan het bijhouden van allerlei eigen dossiers (de arts had het kunnen weten), samen met inzage door de patiënt in het medisch dossier (de arts heeft dit niet gezegd want het staat niet in het dossier), plus het feit dat elk (telefonisch) woord van de arts wordt gelogd (en een ongelukkige formulering tegen hem kan worden gebruikt) leiden tot een claimcultuur als het resultaat van een medische behandeling tegenvalt. Dit kan weer het gedrag van medici (ongewenst) beïnvloeden en tot risico verzekeringskosten leiden. Het EPD roept vragen op rondom aansprakelijkheid. Artsen zijn verplicht te zorgen voor juiste en volledige gegevens in het EPD, maar het ontslaat ze als behandelend arts niet om door te vragen naar ontbrekende, relevante gegevens. Dit maakt de aansprakelijkheidspositie onduidelijk (Barendrecht e.a., 2008).

[54] Dit kondigde Hans Kedzierski, bestuursvoorzitter van het Medisch Centrum Alkmaar, in september 2008 aan op het Innovatie Congres van IBM in Rotterdam.
NB De wet EPD verplicht het gebruik van het EPD door zorgaanbieders.
[55] Aangetekend moet wel worden dat privacywetgeving omtrent medische gegevens wel bestaat in de VS. Zie <www.hipaa.org>.

3.2.2 Elektronisch kinddossier Jeugdgezondheidszorg EKD-JGZ (casus in ontwikkeling)

3.2.2.1 Algemene beschrijving van de casus

Het Elektronisch kinddossier (EKD) moet op geleidelijke basis de papieren dossiers en de bestaande lokale EKD-systemen in de jeugdgezondheidszorg (JGZ) gaan vervangen[56]. Alle Jeugdgezondheidszorginstellingen (JGZ instellingen) moeten begin 2009 bezig zijn met het invoeren van de digitale dossiers. Eind 2009 moet het alle instellingen mogelijk zijn met digitale dossiers werken. Vanaf eind 2009 krijgen alle kinderen van 0 tot 19 jaar een EKD op het moment dat zij in contact komen met de jeugdgezondheidszorg, dat wil zeggen meestal bij of nog voor de geboorte. Het EKD wordt ingevoerd in drie fases[57]:

1. Fase 1 betreft het digitaliseren van de JGZ-sector. Hiervoor moeten JGZ-instellingen zelf onder bestuurlijke regie van gemeenten een automatiseringspakket aanschaffen. Een digitaliseringsplicht is opgenomen in het wetsvoorstel Publieke Gezondheid.
2. Fase 2 betreft het mogelijk maken van landelijke uitwisseling van dossiers binnen de jeugdgezondheidszorg via een landelijke kop en het analyseren van geanonimiseerde gegevens. Het sluit aan bij de bestaande praktijk om alle kinderen te controleren en risicogroepen op lichamelijk, sociaal en cognitief gebied vroegtijdig op te sporen. Het EKD-JGZ is de digitalisering van de bestaande praktijk van het doorgeven van papieren dossiers van consultatiebureaus aan schoolartsen bij de GGD's. In een later stadium moeten ook verloskundigen worden betrokken. Het grootschalig anoniem analyseren van de gegevens is echter nieuw. Het EKD-JGZ zal worden opgezet via aansluiting bij het Landelijk SchakelPunt (LSP) van de AORTA zorginfrastructuur[58]. Het NICTIZ heeft aangegeven dit eind 2009 te kunnen realiseren. Deze infrastructuur wordt ook gebruikt voor het landelijk Elektronisch Patiënten Dossier (EPD) in de zorg zodat een stap wordt gezet om te zijner tijd het EKD-JGZ bij het landelijk EPD aan te kunnen sluiten.
3. De Tweede Kamer wil, net als bijvoorbeeld de gemeente Rotterdam, het gebruik van het EKD-JGZ graag verbreden tot buiten de jeugdgezondheidszorg. Voor zo'n EKD voor de brede jeugdsector is een haalbaarheidsstudie uitgevoerd naar een ketenbrede informatie-uitwisseling in de hele jeugdsector (Bremer e.a., 2008). Het zou in deze fase 3 echter niet meer gaan om een elektronisch dossier voor de jeugdgezondheidszorg. Naast een EKD-JGZ moeten ook elektronische dossiers binnen het onderwijs (EKD-O, het leerling volgsysteem), jeugdhulpverlening (EKD-JH), justitie (EKD-J) en politie (EKD-P) worden ontwikkeld[59]. Deze dossiers zouden worden geacht sectoroverstijgend te integreren. Betrokkenen uit verschillende sectoren zouden er toegang toe moeten

[56] Zie http://www.jeugdengezin.nl/dossiers/elektronisch-kinddossier/default.asp
[57] Zie Brief van Minister Rouvoet dd 17 juli 2008, beschikbaar op http://www.jeugdengezin.nl/includes/dl/openbestand.asp?File=/images/pg-2864093-2-_tcm21-169731.pdf
[58] Zie de brief van Minister Rouvoet aan de eerste kamer dd 29 september http://www.minvws.nl/kamerstukken/pg/2008/wet-publieke-gezondheid1.asp
[59] Deze afkortingen zijn hier ingevoerd om een helder onderscheid te kunnen maken tussen de verschillende dossiers.

toe krijgen en de nieuwe centra voor jeugd en gezin zouden een rol krijgen. De verwijsindex risico jongeren (VIR) heeft met het EKD voor een brede jeugdsector, de brede jeugdsector als gebruiksgroep gemeen maar heeft een veel beperkter doelgroep aan kinderen en jeugdigen (risicojongeren) en bevat alleen de beperkte informatie dat er een melding over een kind of jongere is geweest. Omdat de haalbaarheidsstudie aangeeft dat de jeugdsector niet klaar is voor een integratie binnen de hele sector wil de minister een EKD voor de brede jeugdsector niet invoeren en zich concentreren op een EKD-JGZ. Wel speelt in politiek en in de media een breed EKD en de VIR steeds op de achtergrond bij discussies over het EKD-JGZ.

Voor het EKD-JGZ is een uitgebreide dataset met informatie elementen ontwikkeld, de JGZ-BDS[60]. Deze vormen de neerslag van bestaande formulieren voor het kinddossier zoals die in de papieren versies, bijvoorbeeld vanuit het ziekenhuis naar consultatiebureaus en daarvandaan naar schoolartsen en GGD's worden overgedragen. Een aantal omvat uitgebreide NAW-gegevens, het BSN, schoolcodes en codes van betrokken hulpverleners. Veruit de meeste van deze elementen hebben echter een duidelijk medische aard, zoals groeicurven en de inentingen die een kind heeft gehad. Er zijn echter ook elementen waarmee alcohol- en drugsgebruik, het hebben van seksuele contacten, of psychische problemen kan worden aangegeven. Tenslotte zijn er elementen voor het vastleggen van de sociaal economische situatie van ouders en verzorgers en kind/jongere. Deze veelheid van elementen is bedoeld om de gegevens van de bestaande formulieren te *kunnen* uitdrukken. Het is niet de bedoeling dat alle informatie elementen ook voor alle kinderen daadwerkelijk worden ingevuld[61].

Het EKD-JGZ dossier is er voor alle kinderen, is inhoudelijk van aard en wordt voor lange tijd bewaard. Daarmee vervult het een wezenlijke rol in het continu, longitudinaal volgen van jeugdigen.[62] Samen met het EKD-JGZ dossier vormt de landelijke Verwijsindex Risicojongeren (VIR) een belangrijk instrument om het kind te kunnen volgen in de jeugdketen. In samenhang met elkaar creëren de Centra voor Jeugd en Gezin (CJG), het EKD-JGZ dossier en de VIR een infrastructuur voor lokaal jeugdbeleid dat het volgende mogelijk maakt:

- Signalering van risico's via de Verwijsindex.
- Zorgcoördinatie en zorgverlening.
- Monitoring van zorg via het EKD-JGZ dossier.
- Op basis van gegevens uit het EKD-JGZ dossier kan de gemeente een optimaal (preventief) jeugdbeleid ontwikkelen.

3.2.2.2 De Verwijsindex Risicojongeren

Hoewel de landelijke Verwijsindex Risicojongeren (VIR)[63] en het EKD vaak in een adem worden genoemd[64] gaat het bij de VIR om een heel ander dossier dan bij het EKD-JGZ.

60

http://www.rivm.nl/jeugdgezondheid/images/Basis%20Dataset%20JGZ%20v2.0%20mapping.xls

61 Vergelijk H.N. Dupuis en M.W. Duthler in hun artikel in de NRC van 22 09 2008 http://www.nrc.nl/opinie/article1992979.ece/Je_hebt_een_jaar_borstvoeding_gehad,_begrijp_ik

62 In hoeverre het noodzakelijk is dat van alle kinderen in Nederland 1185 gegevens per kind gedurende 23 jaar bewaard blijven omdat dat 'goed is voor de hulpverlening' wordt betwijfeld door H.M. Dupuis en A.W. Duthler (NRC Handelsblad, 22 september 2008, p. 7). Is die noodzaak er niet, dan levert het een onaanvaardbare inbreuk op de persoonlijke levenssfeer op.

63 Zie http://www.verwijsindex.nl/

De Verwijsindex Risicojongeren hoort bij een notificatie systeem dat risicomeldingen van een brede groep professionals uit de jeugdsector bij elkaar brengt over een beperkte groep ontsporende jongeren. De jeugdsector is hierbij breed op te vatten en omvat partijen als de eigenlijke jeugdhulpverlening, schoolartsen, schoolhoofden, centrum voor werk en inkomen, bureau krediet registratie, politie en justitie. Het doen van een melding moet aan richtlijnen worden ontworpen maar laat vrijheid voor de professional om te melden op basis van een algemeen "niet pluis gevoel".

Het systeem houdt alleen bij dat er een melding is geweest over een jongere, de contact informatie van de melder en de datum. Op het moment dat een nieuwe melding wordt gemaakt wordt gecontroleerd of er al eerder een melding over de jongere is geweest. Zo ja, krijgen alle melders via e-mail bericht over de eerdere meldingen. De eerste keer dat een match plaats vindt wordt ook de betrokken jongeren en het gezin een brief gestuurd. Hulpverleners kunnen na een notificatie, als ze daar behoefte aan hebben contact met elkaar opnemen. Het systeem werkt zowel binnen gemeenten als over gemeentegrenzen heen en kan worden gevoed door regionale systemen, hoewel meldingen in de praktijk vrijwel altijd binnen een regio plaats vinden.

De VIR is bedoeld als index met andere woorden het moet bijhouden dat er een melding over een jongere is geweest, ("DAT" informatie). Er is geen infrastructuur om gegevens over jongeren ("WAT" informatie) op te halen, te delen en aan toegangscontrole te onderwerpen. Toegang tot het VIR systeem gaat via gebruikersnaam en paswoord. Bestaande regionale systemen die de VIR voeden, kunnen bovendien meestal de overleggen tussen instanties uit een notificatie (kunnen) voortkomen structureren[65].

3.2.2.3 Beleidsontwikkeling

Vanaf eind 2009 moet ieder kind dat in Nederland wordt geboren een elektronisch kinddossier jeugdgezondheidszorg (EKD-JGZ) krijgen. Het dossier bevat net als het papieren dossier nu, informatie over de fysieke en psychosociale toestand van het kind, de gezinssituatie en de omgeving.

In relatie tot het EKD voor de brede jeugdsector (en daarmee onafhankelijk van het EKD-JGZ) volgt uit het haalbaarheidsonderzoek naar de informatie-uitwisseling in de brede jeugdsector dat de sector op dit moment nog niet klaar is voor een ketenbrede informatie-uitwisseling langs digitale weg en op landelijk niveau (Bremer e.a., 2008). Wanneer dat in de toekomst wel het geval zou zijn, is speciale wetgeving nodig.[66] Er ligt wel een voorstel bij de raad van state voor de juridische verankering van de VIR en er wordt onderzocht wat de juridische implicaties zijn van het uitbreiden van de gegevens in de VIR met informatie over de gezinssituatie en over de vraag welk deel van de hulpketen de jongere is ingegaan[67].

---

[64] Als anekdotisch materiaal: http://www.congresenstudiecentrum.nl/handouts/071115jeugd/ws14en19%20JawadVanGastelCuyvers%201,%208,%2015.ppt

[65] http://www.provis2.nl/files/veelvuldig_gestelde_vragen/vooronderzoek_signaleringssystemen__versie_6_februari_2.pdf

[66] Brief van minister Rouvoet voor Jeugd en Gezin aan de Eerste Kamer d.d. 30 september 2008. http://www.minvws.nl/kamerstukken/pg/2008/wet-publieke-gezondheid1.asp

[67] Brief van minister Rouvoet aan de Eerste en Tweede Kamer dd 9 oktober 2008. http://www.jeugdengezin.nl/includes/dl/openbestand.asp?File=/images/djg-2880085a-_tcm21-173355.pdf

3.2.2.4 Juridische setting

De wettelijke basis voor de dossiervorming en het overdragen van digitale dossiers in de jeugdgezondheidszorg is de Wet geneeskundige behandelingsovereenkomst (Wgbo). Kader voor de bescherming van privacy bij gegevensuitwisseling in de jeugdzorgketen geven in het bijzonder de Wet bescherming persoonsgegevens (Wbp), de Wet op de jeugdzorg (Wjz), de Wet geneeskundige behandelingsovereenkomst (Wgbo), de (toekomstige) Wet publieke gezondheid, de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens inclusief de daarbij behorende aanwijzingen en besluiten. Deze wet- en regelgeving geeft aan wie met wie onder welke condities welke informatie mag uitwisselen. De VIR richt zich uitsluitend op signalering, bevat geen inhoudelijke informatie en de meldingen mogen beperkt worden bewaard. Op de VIR is de Wbp van toepassing.

Ter verzekering dat de automatisering van de EKD-JGZ dossiers van de grond komt, is in de Wet publieke gezondheid (Wet pg) een wettelijke verplichting opgenomen tot digitalisering van de jeugdgezondheidszorg. De Eerste Kamercommissie voor VWS/JG heeft echter op 10 september 2008 een brief gestuurd naar de minister met het verzoek een schriftelijke toezegging van de minister te ontvangen inzake het niet inwerkingtreden van de digitaliseringsplicht betreffende de patiëntendossiers in de jeugdgezondheidszorg (artikel 5, derde lid). Om “misverstanden weg te nemen” heeft de minister voor Jeugd en Gezin in zijn brief van 30 september 2008 uiteengezet dat de digitaliseringsplicht er toe moet leiden dat zorgverleners in de jeugdgezondheidszorg bij het vastleggen van patiëntgegevens niet langer gebruik maken van papieren dossiers, maar van elektronische dossiers[68]. De Wet pg is momenteel aanhangig bij de Eerste Kamer en treedt naar verwachting op 1 januari 2009 in werking. De wet vervangt de Infectieziektenwet, de Quarantainewet en de Wet collectieve preventie volksgezondheid (Wcpv). Op grond van de Wcpv zijn gemeenten verantwoordelijk voor de jeugdgezondheidszorg.

Minister Rouvoet voor Jeugd en Gezin wil een wet voor het gebruik van het BSN in de jeugdsector voorbereiden[69]. Deze is echter niet nodig voor het EKD-JGZ aangezien deze als medisch dossier valt onder de Wgbo en de wet BSN in de zorg. Uiteindelijk moet het EKD-JGZ onder hetzelfde wettelijke kader gaan vallen als het landelijke EPD.[70]

3.2.2.5 Institutionele setting

Consultatiebureauartsen en verpleegkundigen van de jeugdgezondheidszorg houden het EKD-JGZ bij en zijn inhoudelijk verantwoordelijk. Zij gebruiken het EKD-JGZ bij elk contactmoment voor registratie en informatie net als zij dat nu doen met hun papieren dossiers.

[68] Brief van minister Rouvoet voor Jeugd en Gezin aan de Eerste Kamer d.d. 30 september 2008 http://www.minvws.nl/kamerstukken/pg/2008/wet-publieke-gezondheid1.asp
[69] Brief van minister Rouvoet aan de Eerste en Tweede Kamer dd 9 oktober 2008. http://www.jeugdengezin.nl/includes/dl/openbestand.asp?File=/images/djg-2880085a-_tcm21-173355.pdf
[70] Brief staatssecretaris Ross over het EKD december 2005, zie http://www.vng.nl/Documenten/Extranet/Sez/ZWS/Elektronisch_kinddossier_en_verwijsindex_brief_Ross_aan_TK_december_2005.pdf.

Binnen de toekomstige wet Publieke Gezondheid (artikel 5 lid 1) draagt het college van burgemeester en wethouder zorg voor de uitvoering van de jeugdgezondheidszorg en in het bijzonder voor de invoering van de EKD-JGZ.

Het Centrum voor Jeugd en Gezin (CJG) zou een grote rol moeten gaan spelen als het EKD voor de brede jeugdsector (EKD fase 3) zou worden ingevoerd. Gemeenten krijgen de wettelijke taak om zorg te dragen voor de organisatie van een CJG en in het verlengde daarvan zorg te dragen voor het organiseren van een sluitende jeugdketen, waarbij duidelijke afspraken zijn gemaakt over onder meer zorgcoördinatie. Binnen het CJG speelt informatie-uitwisseling, binnen de geldende professionele normen en privacyeisen, een grote rol. In het algemeen is het zorg- en hulpverleningsnetwerk rondom een probleemjongere complex en zijn er veel verschillende organisaties betrokken. Hoewel het duidelijk is dat de Jeugd Gezondheidszorg deel is van brede jeugdsector is het niet duidelijk of de bovengenoemde verantwoordelijkheden van burgemeester en wethouders voor het EKD-JGZ aan een CJG zullen worden gedelegeerd. Het EKD-JGZ wordt kennelijk wel als een instrument gezien voor het optuigen van een CJG[71]

3.2.2.6 Elektronische dienstverlening aan de burger

Het EKD-JGZ is in te zien door de burger. Ook is het zo dat jongeren of hun ouders kunnen verzoeken om een bepaald deel van het dossier te wissen (zij beschikken daartoe over de patiëntenrechten uit de Wgbo). Een ‘inkijkdienst’ is (nog) niet aanwezig. Bij verhuizing wordt het complete dossier overgedragen. Ook wordt het hele dossier overgedragen bij het bereiken van de vierjarige leeftijd van consultatiebureau naar GGD.

3.2.2.7 Identity management

Toegang tot het EKD-JGZ wordt in de toekomst geregeld volgens de regels en de infrastructuur van het EPD, dat wil zeggen, volgens de wet geneeskundige behandelingsovereenkomst (Wgbo) en met dezelfde toegangscontrole met UZI-pasjes, en goed beheerd zorgsysteem volgens NEN norm (zie hoofdstuk 3.2.1).

3.2.2.8 Veranderingen ingevolge (het gebruik van) ICT

Om te zorgen voor uitwisselbaarheid tussen pakketten van verschillende leveranciers zijn inhoudelijke standaarden nodig. Voor elektronische dossieruitwisseling binnen de JGZ gaat het om de Basisdataset[72] en het dossieroverdrachtsbericht. De basisdataset bevat een groot aantal gegevenselementen (in de versie 2: zo’n krappe 1000) die afhankelijk van de situatie wel of niet moeten worden ingevuld.

Het gebruik van centraal toegankelijke gestandaardiseerde gegevens maakt statistische analyse voor epidemiologisch onderzoek mogelijk.

---

[71] Zie Bogaart Slabbertje, handreiking invoering jeugd en gezin (mei 2008), Brochure in opdracht van ministerie van Jeugd en Gezin http://www.invoeringcjg.nl/nl/Overige_Content/Documenten/Handreiking_Onderdelen_CJG.pdf

[72] Hier is al in 2005 een document over verschenen http://www.nictiz.nl/uploaded/FILES/JGZ/Basis%20Dataset%20JGZ%20V1.0.pdf, De versie 2 is als Excel sheet http://www.rivm.nl/jeugdgezondheid/images/Basis%20Dataset%20JGZ%20v2.0%20mapping.xls

3.2.2.9 Relevante kwesties die rijzen/zijn gerezen in de betreffende case

Aandachtspunten die naar voren zijn gekomen zijn

- Het EKD-JGZ heeft een redelijk duidelijke gebruikersgroep (consultatie bureaus, GGD, en in een later stadium verloskundigen) en een grote doelgroep (alle kinderen). Het systeem bouwt voort op een lang bestaande grootschalige praktijk met een duidelijk protocol: routinechecks, doorvragen waar nodig, en het bijhouden van gestandaardiseerde formulieren. De VIR heeft een brede en niet bijzonder duidelijk omlijnde gebruikers groep (de hele jeugd sector) en een veel kleinere doelgroep (risico jongeren). Het systeem bouwt voort op een kleinschalige praktijk met individuele zorgverleners die individuele risico gevallen kunnen inschatten en aanspreken en onderling direct, vaak mondeling overleggen. Een eventueel EKD voor de brede jeugdsector en alle kinderen heeft geen duidelijk omlijnde gebruikersgroep en een grote doelgroep.
- Het kind centraal is niet voldoende, het gaat in veel gevallen om het kind in de context. Het meenemen van steeds meer context betekent echter een steeds grotere uitbreiding van de scope van een dossier en daarmee met complexiteit op organisatorisch, juridisch en technisch gebied.
- Harde informatie als persoonsgegevens zijn niet altijd correct. In het bijzonder is een BSN wel een precieze persoonsaanduiding maar niet noodzakelijk de correcte voor het kind dat is onderzocht. Identificatie is dus ook voor het EKD-JGZ een aandachtspunt. Voor de meldingen in de VIR geldt dit probleem waarschijnlijk zelfs in nog sterkere mate.
- Sommige kinderen zijn niet bekend bij de burgerlijke stand, en hebben in het bijzonder geen BSN. Ook ongeboren kinderen hebben geen BSN. Dit laatste is van belang is als het EKD-JGZ moet aansluiten op prenatale zorg.

3.2.2.10 Dilemma's waar men in de case tegenaan is gelopen

Het EKD-JGZ geldt als medisch dossier. Er zijn de zware privacy eisen en de zware beveiligingseisen van het EPD opgelegd, zodat het EKD_JGZ net als een hoofdstuk van het EPD binnen het medische domein wordt gehouden. Het meest privacy gevoelige deel van het dossier, namelijk de conclusie dat er "iets" mis is met een kind, kan echter worden doorgegeven aan de VIR. Het VIR notificatie systeem heeft echter de wezenlijk grotere gebruikersgroep van de brede jeugd sector en een minder zware gegevensbeveiligingsinfrastructuur.

Bij de Stichting Ouders Online heersten misverstanden over het EKD-JGZ, maar na een goede uitleg is die onrust weggenomen. De mediapresentatie en de verwarring over de relatie met de VIR en de EKD voor de brede jeugdsector zijn wat dat betreft niet gelukkig geweest.

De Verwijs Index Risicojongeren (VIR) is iets wezenlijk anders als het Elektronisch Kind Dossier Jeugd Gezondheidszorg (EKD-JGZ). Het is ongelukkig dat EKD-JGZ en VIR zo vaak in een adem worden genoemd in de media. Bij de VIR gaat het om beperkte notificatie-informatie voor een brede groep hulpverleners en over een kleine groep jongeren. De relatie tussen VIR en EKD-JGZ is dat de JGZ een van de instanties is die een melding kunnen maken in de VIR, en dat EKD-JGZ en VIR beiden betrekking hebben op jeugdigen en daarom de verantwoordelijkheid zijn van het ministerie van Jeugd en Gezin. In discussie over een EKD voor de brede jeugdsector, fase 3 lijkt het onderscheid in gebruikersgroep, doelgroep en schaalgrootte (zie boven) tussen beide

systemen niet voldoende duidelijk te zijn geworden. Worden dossiers eenmaal geïntegreerd dan lijkt de natuurlijke tendens om ze steeds verder op te schalen en ze blijken dan te raken aan steeds meer gebieden. De afweging is dan of zo'n dossier nog wel valt binnen de oorspronkelijke gebruikscontext en of een verandering van die context en de afhankelijkheden die dat met zich meebrengt nog opwegen tegen de meerwaarde van integratie.

3.2.2.11 Analyse door projectteam

Het EKD-JGZ is een grotendeels medisch dossier met belangrijke sociaal en cognitieve componenten. Het is bedoeld voor de jeugdgezondheidszorg.

Kans: Doel van het EKD-JGZ is om geen kinderen uit het oog te verliezen, bijvoorbeeld na een verhuizing of als dossiers worden meegenomen bij bezoeken. Daarnaast mag worden verwacht dat het EKD-JGZ op termijn enige efficiëntie voordelen oplevert zeker als pre en post natale dossier bij het EKD-JGZ wordt opgenomen.

Kans: Het EKD-JGZ vergemakkelijkt het doen van epidemiologisch onderzoek door dat het de gegevens voor anonieme statische analyse bijeenbrengt.

Kans: Het EKD-JGZ lijkt technisch erg veel op een hoofdstuk van het EPD. In het EPD zijn de meeste zaken technisch al geregeld. Opname van het EKD-JGZ in het EPD betekent ook dat een medisch dossier over een cruciale levensfase wordt opgenomen.

Bedreiging: Het medische veld heeft te maken met het beroepsgeheim. Hoewel naleving van de geheimhoudingsplicht soms pijnlijk of kostbaar kan zijn, vooral daar waar medische hulpverlening raakt aan andere sectoren van de maatschappij zoals justitie en verzekeringen, wordt deze noodzakelijk geacht binnen een behandelrelatie. In sommige gevallen is het echter moeilijk om een grens te trekken tussen medische data en niet-medische data, bijvoorbeeld bij verwaarlozing. Daar wringt het 'model' van gegevens opsluiten binnen de medische sector en ontstaan onduidelijkheden rond persoonsinformatiebeleid. Dit is heel duidelijk voor de meldingen aan de VIR die op basis van de onderzoeken van de JGZ gebeuren. Of dit al dan niet via een technische koppeling met het EKD-JGZ zou kunnen plaats vinden lijkt daarbij minder relevant.

Hoewel het EKD-JGZ en de VIR duidelijk verschillende dossiers zijn heeft de positionering t.o.v. elkaar wel tot verwarring geleid. Er is ook een roep vanuit gemeenten en Tweede Kamerleden om het EKD breder te trekken dan het EKD-JGZ. Rond het EKD in brede zin zien we de volgende kansen en bedreigingen als het gaat om persoonsinformatiebeleid.

Kans: De Jeugd Gezondheidszorg is grotendeels bedoeld om grootschalig (vroegtijdig) probleemgevallen te signaleren, d.w.z. alle kinderen te onderzoek en de groep op te sporen waarbij de lichamelijke, cognitieve of sociale ontwikkeling niet in orde is. Via het EKD-JGZ wordt dit voor alle kinderen grootschalig bijgehouden. Vanuit een kleinschalige context vervult de VIR ook een dergelijke functie, voor individuele hulpverleners die individuele probleem jongeren melden en eventueel direct contact met elkaar op kunnen nemen. Het EKD-JGZ en de VIR vervullen daarom twee uiteinden van het spectrum.

Bedreiging: De (potentiële) betrokkenheid van heel veel actoren geeft inherent een risico op *function creep*. Omdat technische uitwisseling mogelijk is kan de neiging ontstaan

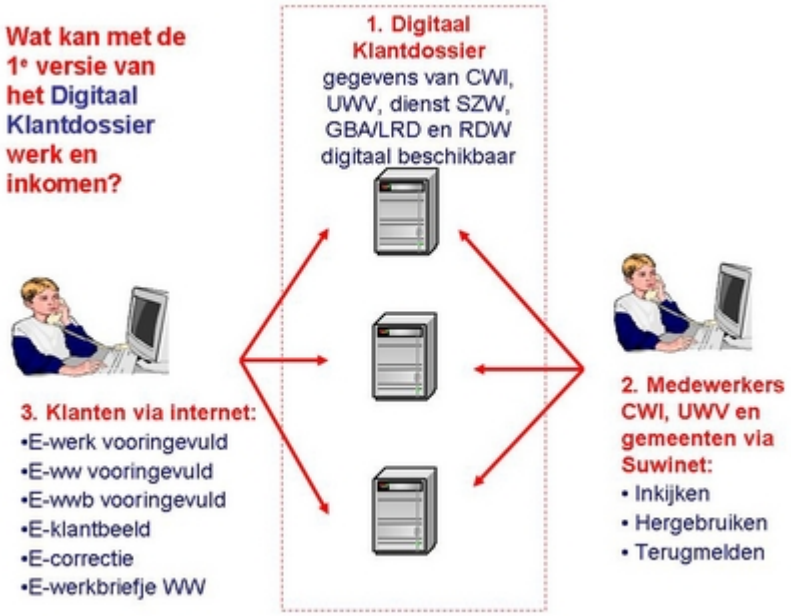
gegevens te gebruiken voor andere doeleinden dan waar ze voor zijn vastgelegd. Om te voorkomen dat de rechter de informatie uitwisseling via het EKD te wijd verbreid acht en vervolgens verbiedt, zullen sterke argumenten nodig zijn die de noodzaak tot een breed gebruik van een dergelijk informatiesysteem kan rechtvaardigen.
Gerelateerd speelt de vraag of informatie is te interpreteren door andere beroepsgroepen dan de professionals die deze data hebben vastgelegd. Dit raakt aan het dilemma van met elkaar om tafel zitten versus elektronisch communiceren dat een verhoogd risico op misverstanden inhoudt.

3.3 Cases rond e-overheid processen

3.3.1 Digitaal klantdossier DKD (bestaande casus)

3.3.1.1 Algemene beschrijving van de casus

Het Digitaal Klant Dossier (DKD)[73] is een virtueel dossier binnen de keten Werk en Inkomen waar klanten en medewerkers relevante gegevens kunnen raadplegen voor het recht op uitkering of toeleiding tot werk. Sinds 3 januari 2008 is het DKD landelijk operationeel. Het DKD maakt het mogelijk dat gegevens eenmalig worden uitgevraagd en worden hergebruikt[74]. Het DKD wordt elektronisch ontsloten voor klanten door middel van Internet en een Web browser. Voor geautoriseerde medewerkers wordt DKD elektronisch ontsloten door middel van de inkijkfunctie van Suwinet, het zgn. Suwinet Inkijk. Suwinet is een uitwisselingsnetwerk dat toegankelijk is voor partijen in de keten Werk en Inkomen en beheerd wordt door BKWI[75]. De burger kan zijn/haar klantbeeld bekijken via Werk.nl.



Figuur 2: Het Digitaal Klant Dossier (bron: http://dkd.nl/digitaal_klantdossier_in_het_kort/).

Binnen DKD werken CWI, UWV en gemeenten (GSD's) nauw samen. CWI en UWV gaan fuseren en vormen straks één organisatie. Tevens zijn er koppelingen met relevante basisregistraties zoals GBA en RDW. GBA[76] is de benaming voor de boekhouding van gegevens die gemeenten bijhouden over alle ingezetenen die in de betreffende gemeente woonachtig zijn of waren. GBA-Verstrekkingen (GBA-V) is de toepassing waarmee GBA gegevens digitaal toegankelijk gemaakt worden. De voorloper van GBA-V is de Landelijk Raadpleegbare Deelverzameling (LRD). RDW is een zelfstandig

[73] http://www.dkd.nl/
[74] Zie http://dkd.nl/digitaal_klantdossier_in_het_kort/
[75] Zie http://www.bkwi.nl/
[76] Zie http://www.gba.nl/

bestuursorgaan dat onder meer de ‘basisregistratie voertuigen’ voor de Nederlandse overheid beheert[77].

Dossierinkijk in DKD wordt onder meer gerealiseerd door middel van Suwinet-inkijk, waardoor naast medewerkers van CWI en UWV ook gemeentelijke sociale diensten toegang tot het dossier van klanten hebben. Suwinet-Inkijk is een toepassing waarmee geregistreerde gegevens kunnen worden getoond.

Een demonstratievideo waarin DKD nader wordt uitgelegd is beschikbaar op http://uitleg.operatiedkd.nl/video.htm.

3.3.1.2 Beleidsontwikkeling

Het DKD is opgezet volgens een groeimodel en heeft de ambitie integrale dienstverlening te bevorderen met o.a. een klantvolgfunctionaliteit door de keten Werk en Inkomen heen. Gemeenten worden ondersteund door een landelijke overheidsinstelling genaamd Operatie DKD[78] die invoering van DKD bij gemeenten ondersteunt. Dit wordt uitgevoerd door het Coördinatiepunt ICT Gemeenten (CP-ICT).

Naast uitbreiding van het DKD ligt ook koppeling met de Persoonlijke Internet Pagina (PIP) voor de hand. PIP[79] wordt ontwikkeld in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en beoogt hét loket te zijn waarmee burgers hun overheidszaken kunnen regelen in een persoonlijke en veilige omgeving. PIP heeft als doelstelling om een startpagina voor gepersonaliseerde overheidsdienstverlening aan burgers te verschaffen.

3.3.1.3 Juridische setting

De wettelijke basis voor de uitwisseling en samenwerking in het kader van DKD vormen onder andere de Suwi-wetgeving en de Wbp. De Wet eenmalige uitvraag werk en inkomen (WEU) is op 1 januari 2008 ingevoerd met het doel dat klantgegevens onderling tussen overheidspartijen beschikbaar worden voor hergebruik zodat de burger niets steeds lastig gevallen wordt met dezelfde vragen.

- *Wet eenmalige gegevensuitvraag werk en inkomen (WEU)*

Met de Wet eenmalige gegevensuitvraag werk en inkomen (WEU)[80] is beoogd de dienstverlening aan burgers te verbeteren door o.a. een wettelijk verbod op dubbele gegevensuitvraag in de Suwi-keten in te voeren. Een Digitaal Klantdossier (DKD) zou dat moeten ondersteunen. Om de eenmalige gegevensuitvraag en gegevenshergebruik te bevorderen is aansluiting gezocht bij het stelsel van basisregistraties (Gemeentelijke Basisadministratie, Nieuwe Handelsregister, Basis Gebouwen Registratie, Basisregistratie Kadaster, Basisregistratie Topografie en Basisregistratie Adressen). De

[77] Zie http://www.rdw.nl/
[78] Zie http://uitleg.operatiedkd.nl/operatieDkd.htm
[79] Zie http://www.e-overheid.nl/sites/pip/
[80] Wijziging van de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wet werk en bijstand, de Werkloosheidswet en enige andere wetten in verband met eenmalige gegevensuitvraag aan burgers (Wet eenmalige gegevensuitvraag werk en inkomen). *Kamerstukken II*, 2006/07, 30 970. De WEU is op 1 januari 2008 in werking getreden en zal komen te vervallen op 1 januari 2010.

overheid – inclusief organisaties in het Suwi-domein – is wettelijk verplicht gebruik te maken van deze basisregistraties. Omdat in het Suwi-domein meer informatie over burgers nodig is dan beschikbaar is via deze basisregistraties, is de eenmalige gegevensuitvraag uitgebreid tot de intake Werkloosheidswet (WW) en Wet werk en bijstand (WWB). De wet regelt nu dat gegevens die uit de polisadministratie van het UWV, de verzekerdenadministratie van de SVB of de GBA verkregen kunnen worden in beginsel niet mogen worden uitgevraagd bij de burger (art. 28 Wet Suwi).

Het verbod op dubbele gegevensuitvraag geldt voor UWV, CWI, SVB en gemeenten bij de uitvoering van wetgeving rond werk en inkomen. Die wetten zijn: Wet Suwi, WWB, IOAW (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen), WWIK (Wet werk en inkomen kunstenaars), WW, TW (Toeslagenwet), ZW (Ziektewet), WIA (Wet werk en inkomen naar arbeidsvermogen), de WAO (Wet op de arbeidsongeschiktheidsverzekering), de WAJONG (Wet arbeidsongeschiktheidsvoorziening jonggehandicapten), de AKW (Algemene Kinderbijslagwet), de AOW (Algemene Ouderdomswet) en de ANW (Algemene nabestaandenwet). Een overzicht van de gegevens die niet van de burger mogen worden uitgevraagd is te vinden in Bijlage II bij art. 5.2a van het Besluit Suwi.

- *Wet bescherming persoonsgegevens*

Op het digitaal klantdossier (DKD) is de Wet bescherming persoonsgegevens (Wbp) van toepassing. Het DKD is omschreven als een 'representatie van alle relevante (zowel actuele als historische) gegevens omtrent een klant binnen het Suwi-domein'.[81] Het DKD bevat basisgegevens (gestructureerde klantgegevens, inkomensgerelateerd en werkgerelateerd) en statusinformatie (plaats van de klant in de keten, status van dienstverlening). Het DKD is geen gegevensverzameling die op één plaats wordt aangelegd en bijgehouden, maar de gegevens die bij verschillende organisaties en in aparte registraties zijn vastgelegd worden in het DKD op een samenhangende wijze bijeengebracht en gepresenteerd.

Die uitwisseling van gegevens dient o.a. te voldoen aan de vereisten van doelbinding en proportionaliteit uit de Wbp. De noodzaak tot deze uitwisseling van gegevens is reeds gemaakt in de bijzondere wetten die de bevoegdheid en verplichting regelen tot het inwinnen en verstrekken (gesloten verstrekkingenregime) daarvan.

- *Regeling Suwi*

Als gevolg van de inwerkingtreding van de WEU, is op 30 mei 2008 de Regeling Suwi gewijzigd.[82] Deze wijziging betreft een aantal technische aanpassingen als gevolg van enige deregulering. Daarnaast is de regeling inhoudelijk op de volgende onderdelen aangepast:

- de verantwoording over de gegevensverwerking is gewijzigd (de artikelen 5.22 en 6.4);
- een bijlage is toegevoegd met daarin opgesomd de gegevens die voor eenmalige gegevensuitvraag in aanmerking komen;

[81] *Kamerstukken II*, 2006/07, 30 970, nr. 3, p. 8.
[82] Regeling van de Staatssecretaris van Sociale Zaken en Werkgelegenheid van 30 mei 2008, nr. UB/S/2008/14903, tot wijziging van de Regeling SUWI in verband met eenmalige gegevensuitvraag werk en inkomen. *Stct.* 11 juni 2008, nr. 110 / pag. 20 (Bijlage II gerectificeerd in *Stct.* 25 augustus 2008, nr. 163 / pag. 9).

- de bijlage met daarin opgenomen het gegevensregister Suwi is opnieuw vastgesteld;
- een bijlage is toegevoegd met daarin het Stelselontwerp en Beveiliging Gezamenlijke elektronische Voorzieningen Suwi (GeVS);
- een bijlage is toegevoegd met aansluitvoorwaarden niet Suwi-partijen op de GeVS;
- de bijlagen inzake de planning en control producten van het IB en het BKWI zijn vervangen door geactualiseerde bijlagen;
- de Stichting Inlichtingenbureau is aangewezen als de instelling bedoeld in artikel 1, onderdeel p, van de Wet Suwi.

3.3.1.4 Institutionele setting

DKD wordt in opdracht van de staatssecretaris van SZW uitgevoerd. DKD is formeel een programma van CWI, UWV, SVB, VNG en de vereniging Divosa. DKD wordt bestuurd door een stuurgroep waarin de deelnemende partijen zijn vertegenwoordigd en wordt beheerd door BKWI.

3.3.1.5 Elektronische dienstverlening aan de burger

DKD biedt momenteel verscheidene diensten aan klanten, waaronder
- Aanvragen van een uitkering (WW, WWB) middels e-intake en voorinvulling van formulieren
- Inschrijven voor werk
- Inzien van registratiegegevens
- Verzoek indienen tot correctie van geregistreerde gegevens

In de toekomst liggen koppelingen met de Sociale Verzekering Bank (SVB) en mogelijk Belastingdienst in het verschiet[74]. Indien de betrokken partijen beter en nauwgezetter registreren kan de volledigheid en betrouwbaarheid van de gegevens toenemen. Met het breder tonen van de gegevens en de afhankelijkheid van grotere groepen gebruikers zal meer druk uitgeoefend worden op partijen om de registratie bij te werken en bij te houden.

3.3.1.6 Identity management

Burgers kunnen met behulp van DigiD[83] gebruik maken van DKD. Voor DKD is DigiD op basisniveau vereist, dat wil zeggen dat gebruiken zich moeten authenticeren door middel van een gebruikersnaam en een wachtwoord. Koppeling van persoonsgegevens vindt plaats op basis van het Burger Service Nummer (BSN). Het is belangrijk dat burgers een ‘veilige’ PC gebruiken om te voorkomen dat kwaadwillende personen toegang kunnen krijgen tot de gegevens uit het DKD[84].

Een uitgebreid autorisatiesysteem wordt gebruikt voor het verlenen van toegang tot klantdossiers aan medewerkers. Deze toegang wordt gerealiseerd met Suwinet-Inkijk. De geautoriseerde medewerkers hebben niet allemaal toegang tot het volledige klantdossier, maar alleen tot de voor hun werk relevante gegevens. Autorisatie van medewerkers vindt plaats in twee stappen. BKWI autoriseert één of enkele personen van een aangesloten organisatie door hem of haar ‘administrator’ rechten te verlenen. Deze personen autoriseren vervolgens de medewerkers van de aangesloten instellingen waarbij ze,

[83] http://www.digid.nl/
[84] http://www.digid.nl/veiligheid/

afhankelijk van hun rol, al dan niet rechten op inzage en/of wijzigingen van bepaalde gegevens krijgen. Vanuit de ketenafspraken mag de rol voor het volledige klantdossier slechts aan een beperkte groep personen beschikbaar gesteld worden.

Medewerkers zijn bij gegevensontsluiting gehouden aan wetgeving zoals de Wet Bescherming Persoonsgegevens. Tevens zijn aangesloten organisaties, naast gezamenlijke richtlijnen omtrent privacy en beveiliging, gehouden aan de Regeling Suwi en het Suwinet-Normenkader. Naleving wordt jaarlijks beoordeeld door een externe auditor. Naleving wordt jaarlijks beoordeeld door security officers en auditor van de betrokken organisaties, en door externe auditors. Gemeenten zijn niet gehouden aan deze wijze van verantwoorden. De keten krijgt geen informatie van gemeenten of en in hoeverre zij voldoen aan de gestelde eisen en de gemaakte afspraken.

3.3.1.7 Veranderingen ingevolge (het gebruik van) ICT

Uitbreidingen van DKD staan op stapel. Nieuwe koppelingen, onder andere met SVB, staan zijn gepland. Ook koppelingen met Kadaster en IBG zijn in de toekomst niet uit te sluiten.

3.3.1.8 Relevante kwesties die rijzen/zijn gerezen in de betreffende case

De Regeling Suwi beschijft een aantal eisen waar aangesloten organisaties zich aan moeten houden. Het ketenbreed handhaven en naleven blijkt in de praktijk lastig te realiseren. Niet alle aangesloten gemeenten hebben een beveiligingsplan (zie appendix D, de staatssecretaris van Sociale Zaken vraagt de gemeenten hier wel om). Tevens is het begrip ‘beveiligingsplan’ niet uitgewerkt voor wat betreft de hieraan te stellen eisen. Hierdoor loopt de volwassenheid van de beveiligingsplannen sterk uiteen. De Regeling Suwi richt zich voornamelijk op Gemeentelijke Sociale Diensten (GSD’en), terwijl men van gemeentes zou mogen verwachten dat zij gemeentebreed een beveiligingbeleid en beveiligingsplan zouden hebben vastgesteld.

3.3.1.9 Dilemma’s waar men in de case tegenaan is gelopen

Er ontbreekt een *ketenbreed* effectief toezicht op de wijze waarmee met (persoons)gegevens wordt omgegaan en een mandaat om op te kunnen treden indien overtredingen worden geconstateerd. Dit belemmert het aanspreken van individuele organisaties en personen op hun verantwoordelijkheden binnen de keten en het treffen van passende maatregelen.

Het basisvoorzieningenstelsel legt een basis voor het distribueren van verantwoordelijkheden omtrent het bijhouden van actuele brongegevens. Zo is de Gemeentelijke Basisadministratie verantwoordelijk voor het bijhouden van persoonsgegevens. Het is echter niet altijd duidelijk wie historische gegevens bewaart, met als gevolg dat verschillende organisaties dit zelf (kunnen) gaan bijhouden.

Bij de keten werk en inkomen is iemands arbeidsverleden zeer relevante persoonsinformatie. Opvallend is het feit dat steeds meer mensen juist deze informatie over henzelf op internet publiceren (bijvoorbeeld via Hyves of LinkedIn). Dit wil echter niet zeggen dat hun persoonsgegevens daarmee vogelvrij worden. Het is dus niet zo dat de Wbp door het internet wordt achterhaald. Organisaties (ook die binnen DKD) die persoonsgegevens van cliënten via internet verzamelen zijn gehouden aan Wbp zodra zij

enige feitelijke macht over de gegevens kan uitoefenen, bijvoorbeeld door die gegevens op te slaan in een eigen systeem. Die organisaties zullen vervolgens ook in staat zijn om doel en middelen van deze verwerking van persoonsgegevens vast te stellen. Daardoor worden zij verantwoordelijke in de zin van de Wbp en rust op hen o.a. een informatieplicht jegens degenen van/over wie zij de gegevens hebben verzameld.

3.3.1.10 Analyse door projectteam

Hieronder worden kansen en bedreigingen geïdentificeerd. Deze kansen en bedreigingen zijn niet noodzakelijk specifiek voor DKD, maar kunnen soms ook van toepassing zijn op andere elektronische (keten)dossiers.

Kans: DKD is een voorbeeld van een ketendossier dat daadwerkelijk en op grote schaal gebuikt wordt. Volgens Digitaal Bestuur (juli 2008) en Automatiseringsgids (september 2008) zijn 442 van de 443 gemeenten aangesloten[85,86]. Alle gemeentelijke sociale diensten (GSD's) zijn echter wel aangesloten op Suwinet. Sommige GSD'en hebben zelf geen aansluiting met Suwinet maar hebben de werkzaamheden uitbesteed (al dan niet in een samenwerkingsverband) aan andere gemeenten.
Eenmalige uitvraag en een consistent klantbeeld binnen de hele keten zijn kansen voor de burger. Voor de overheid liggen er kansen op het verbeteren van de efficiency en de kwaliteit van dienstverlening.

Kans: In het bijzonder worden ook enkele problemen met papieren dossiers, zoals het geen beeld hebben van waar een dossier is (kwijtraken), of het willen weten wie een dossier heeft ingezien opgelost (zie ook Azouz e.a. (2007)).

Kans: Door koppeling van gegevens binnen een keten wordt het mogelijk een ketenbreed klantbeeld te creëren. Dit stelt medewerkers in staat om de persoonlijke situatie van een klant beter in te schatten, en de dienstverlening af te stemmen op de persoonlijke situatie van de klant. Bovendien krijgen de medewerkers in de keten een consistent klantbeeld van de klant omdat ze allemaal van hetzelfde dossier uitgaan. Dit reduceert het risico van tegenstrijdige adviezen door verschillende medewerkers uit de keten op basis van de inconsistente klantdossiers. Deze kans is overigens niet DKD-specifiek, maar geldt voor alle (keten)dossiers.

Bedreiging: Gegevens in dossiers zijn in veel gevallen het resultaat van interpretatie van 'ruwe' data en betreffen niet slechts objectieve feiten. Een ketenbreed klantbeeld is daarmee niet noodzakelijk een juist beeld. Aan het begrip 'loon' wordt bijvoorbeeld door verschillende ketenpartners een andere invulling gegeven (bruto, netto, loongrondslagen, etc.).

Kans: Door klantdossiers te doorzoeken op correlaties en te vergelijken zouden groepen van klanten onderkend kunnen worden. Een voorbeeld van zo'n groep zou kunnen zijn de hoogopgeleide professional die werkzoekende is geworden, of de vroegtijdige schoolverlater. Voor dergelijke groepen kunnen groepsgerichte aanpakken worden

[85] Zie Digitaal Bestuur (juli 2008): http://digitaalbestuur.nl/nieuws/dkd-online-te-raadplegen
[86] Digitaal Klantdossier een geruisloos succes, zie http://www.automatiseringgids.nl/artikelen/2008/39/digitaal%20klantdossier%20een%20geruisloos%20succes.aspx

gedefinieerd, bijvoorbeeld door twee typen intakeformulieren te ontwikkelen (doelgroepen diversificatie).

Bedreiging: Doordat een ketendossier als basis voor alle diensten binnen een keten wordt gebruikt hebben incorrecte dossiers grote gevolgen voor de dienstverlening naar de klant. Veel diensten baseren zich immers op de incorrecte gegevens in een ketendossier. Een terugmeldfaciliteit kan dit enigszins ondervangen. Met een terugmeldfaciliteit kunnen klanten zelf melden wanneer ze vinden dat het dossier incorrect is.

Bedreiging: De gebrekkige kwaliteit van gegevens door de aanleverende organisaties/voorzieningen kan een bedreiging zijn voor de kwaliteit van het dossier als geheel. Op zijn beurt is de kwaliteit van het dossier weer bepalend voor de kwaliteit van diensten die worden geleverd op basis van dit dossier. Indien de gegevens van aanleverende organisaties/voorzieningen van onvoldoende kwaliteit is kan dit dus de kwaliteit van het dossier negatief beïnvloeden. Inzicht in, en mogelijk sturing van, de kwaliteit van de gegevens afkomstig van aanleverende voorzieningen is momenteel niet altijd aanwezig.

Bedreiging: Een keten is zo sterk als de zwakste schakel. Ketenpartners zullen vertrouwen in elkaar moeten hebben om een veilige uitwisseling te realiseren. Ketenbrede afspraken en manieren om deze afspraken te handhaven kunnen dit vertrouwen borgen.

Bedreiging: In de Suwi-Regeling worden de voorwaarden beschreven waaronder aansluiting plaats mag vinden. Audits en veiligheidsplannen worden gebruikt als middel om het vertrouwen in ketenorganisaties vast te stellen. Inzicht in de mate of en in hoeverre partijen voldoen aan de aan hen gestelde eisen, en mogelijk sturing dat alle aangesloten partijen zich op vergelijkbare manier verantwoorden, biedt basis voor onderling vertrouwen. Gemeenten zijn echter niet gehouden aan deze wijze van verantwoorden. De keten krijgt geen informatie van gemeenten of en in hoeverre zij voldoen aan de gestelde eisen en de gemaakte afspraken. Er ontbreekt dus een *ketenbreed* effectief toezicht op de wijze waarmee met (persoons)gegevens wordt omgegaan en een mandaat om op te kunnen treden indien overtredingen worden geconstateerd.

Kans en bedreiging: Het DKD is een voorbeeld van een ketendossier. In het stuk 'Digitaal klantdossier een geruisloos succes'[87] wordt het DKD gepresenteerd als een succesvol ketendossier. In hetzelfde stuk geeft staatssecretaris Aboutaleb aan dat uitbreiding dan ook in de lijn der verwachting ligt. In het bijzonder wordt er gezinspeeld op 'een breder gebruik als in het domein werk en inkomen'. VNG/Divosa en UWV zijn al om plannen gevraagd. Gemeenten denken aan uitbreiding met WMO en onderwijs. Naast de kansen die aansluiting bij DKD biedt zit er ook een bedreiging in. De bedreiging is dat uitbreiding buiten de keten Werk en Inkomen het gevaar voor misbruik van privacygevoelige informatie kan inhouden. Het gevaar van *function creep* ligt hier op de loer.

Bedreiging: Het DKD is voor burgers toegankelijk via een DigiD en BSN. Dit levert een beveiligingsprobleem op. Het BSN van burgers is niet erg lastig te achterhalen, zeker niet op termijn en DigiD's kunnen worden verkregen zonder dat een deugdelijke authenticatie

[87] Zie 'Digitaal klantdossier een geruisloos succes'. Verschenen in Automatiserings Gids 26 september 2008.

van de aanvrager plaatsvindt aan de hand van visuele inspectie van een deugdelijk identiteitsdocument (in sectie 0 gaan we hier nader op in).

3.3.2 Omgevingsvergunning (casus in ontwikkeling)

3.3.2.1 Algemene beschrijving van de casus

Het verkrijgen van de benodigde vergunningen voor infrastructurele projecten is niet eenvoudig. Hier zijn meerdere oorzaken voor aan te wijzen, waaronder:

- Er zijn vaak meerdere vergunningen of toestemmingen nodig
- Er zijn vaak verschillende bevoegde gezagsdragers betrokken bij het verlenen van de toestemmingen
- Tevens zijn er vaak verschillende organisaties bij betrokken (zelfs binnen een gemeente)
- De organisaties en gezagsdragers hanteren vaak verschillende procedures en tijdslijnen
- De onderlinge coördinatie tussen de organisaties en gezagsdragers is vaak niet optimaal

Het gevolg is dat een het rond krijgen van de vereiste vergunningen en toestemmingen vaak een complexe zaak is en meestal een lange adem vergt.

Om dit probleem te ondervangen is de omgevingsvergunning[88] ingevoerd. Met de omgevingsvergunning kunnen alle vereiste toestemmingen middels één vergunning en één procedure worden aangevraagd en verkregen. De omgevingsvergunning vervangt circa 25 toestemmingsstelsel voor de fysieke leefomgeving, waaronder sloop, bouw, aanleg, oprichting en gebruik van een fysiek object.

De omgevingsvergunning wordt mogelijk gemaakt door het Wetsvoorstel algemene bepalingen omgevingsrecht (Wabo). Dit wetsvoorstel leidt niet tot nieuwe toetsingscriteria, maar maakt het mogelijke vele vergunningen te integreren tot de één enkele omgevingsvergunning. De omgevingsvergunning kan elektronisch worden ingediend bij de Landelijke Voorziening Omgevingsloket.

3.3.2.2 Beleidsontwikkeling

Uitgangspunten voor de ontwikkeling van de Wabo zijn[89]:

- Streven naar modernisering van regelgeving en betere dienstverlening.
- Door de verbeterde samenhang tussen de besluiten wordt bescherming van de fysieke leefomgeving niet aangetast of zelfs verbeterd.
- De omgevingsvergunning zal leiden tot minder vergunning en dus tot een administratieve lastenverlichting.
- De omgevingsvergunning leidt tot een verbeterende dienstverlening en noodzaakt samenwerking tussen overheden.

[88] Zie http://omgevingsvergunning.vrom.nl/
[89] Zie http://omgevingsvergunning.vrom.nl/html/vromomgevingsvergunning/document_download.cfm?doc=D8ACB584-1438-5103-7127EBCB3A104C51.PDF&doc_name=Samenvatting%20Wabo%20juni%202008

3.3.2.3 Juridische setting

De wettelijke basis voor de omgevingsvergunning wordt verschaft door het Wetsvoorstel algemene bepalingen omgevingsrecht (Wabo). Dit wetsvoorstel omvat alle vergunningen op VROM-gebied, zoals wonen, bouwen, ruimte en milieu. Daarnaast omvat de Wabo vergunningen van andere departementen zoals vergunningen voor monumenten, water, natuurbescherming, flora, fauna en water.

- *Wetsvoorstel algemene bepalingen omgevingsrecht (Wabo)*

In het wetsvoorstel inzake de Wet algemene bepalingen omgevingsrecht (Wabo)[90] staat de dienstverlening door de overheid aan burgers en het bedrijfsleven centraal. De wet voegt daartoe de toestemmingen samen die nodig zijn als een burger of een bedrijf op een bepaalde plek iets wil gaan slopen, (ver)bouwen, oprichten of gaan gebruiken. De Wabo integreert een groot aantal (circa 25) vergunningen, ontheffingen en meldingen ('toestemmingen') tot één 'omgevingsvergunning'. De dienstverlening aan burger en bedrijf zou moeten verbeteren als gevolg van de introductie van de omgevingsvergunning voor de betreffende toestemmingsstelsels. Eén omgevingsvergunning moet vervolgens leiden tot de invoering van één loket, één (digitaal) aanvraagformulier, één bevoegd gezag (één aanspreekpunt), één uniforme en in het algemeen ook kortere procedure, één procedure voor bezwaar en beroep en één handhavend bestuursorgaan. De samenvoeging van deze toestemmingen moet leiden tot een omvangrijke vermindering van het aantal toestemmingen en een daarmee overeenkomende vermindering van administratieve lasten. De omgevingsvergunning moet ook impulsen bieden om te komen tot een organisatieverbetering en samenwerking binnen en tussen overheden. De omgevingsvergunning maakt een goede organisatie van het omgevingsloket (frontoffice) en een goede organisatie en samenwerking tussen overheden achter dat loket (backoffice) noodzakelijk. De Wabo beoogt het huidige juridische stelstel voor bouwen, ruimte, natuur, monumenten en milieu, dat is opgezet vanuit de organisatie van de overheid en de behartiging van publieke belangen, zodanig te veranderen dat het project dat de burger of het bedrijf wil realiseren centraal komt te staan. Naar wordt verwacht zal de wet op 1 januari 2010 in werking treden.[91]

De invoering van het wettelijk stelsel van omgevingsvergunningen heeft consequenties voor de volgende wettelijke regelingen die onder de reikwijdte van de omgevingsvergunning vallen:[92]

- Wet milieubeheer (Wm)
- Wet ruimtelijke ordening (WRO)
- Woningwet (Ww)
- Tracéwet
- Monumentenwet 1988
- Natuurbeschermingswet 1998 en Flora- en faunawet
- Wetsvoorstel Waterwet[93]

[90] Regels inzake een vergunningstelsel met betrekking tot activiteiten die van invloed zijn op de fysieke leefomgeving en inzake handhaving van regelingen op het gebied van de fysieke leefomgeving (Wet algemene bepalingen omgevingsrecht). *Kamerstukken II*, 2006/07, 30 844.
[91] *Kamerstukken I*, 2007/08, 30 844, nr. G (Nadere memorie van antwoord Eerste Kamer, 4 september 2008), p. 2.
[92] Zie *Kamerstukken II*, 2006/07, 30 844, nr. 3, p. 78-91.
[93] Regels met betrekking tot het beheer en gebruik van watersystemen (Waterwet). *Kamerstukken II*, 2006/07, 30 818.

- Mijnbouwwet
- Wet openbaarheid van bestuur

❑ *Ondersteuning door ICT*

De invoering van de Wabo gaat, zoals gezegd, gepaard met de ontwikkeling van één loket: de Landelijke Voorziening Omgevingsloket (LVO).[94] Dit loket zal bestaan uit een aanvraagdeel en een dossierdeel. Via dit loket is het voor burgers en bedrijven eenvoudiger om een aanvraag te doen en om te beschikken over de daarvoor benodigde gegevens. Ten behoeve van de vergunningaanvraag worden tevens andere bouwstenen van de elektronische overheid gebruikt, zoals DigiD, Basisregistraties, het Bedrijvenloket en MijnOverheid. Daardoor hoeven de bij de overheid reeds bekende gegevens niet telkens opnieuw te worden opgegeven.[95]

Tevens zou de procedure voor de terinzageleggingen, bijvoorbeeld van ontwerpbeschikkingen, door ICT kunnen worden ondersteund. Zoals in paragraaf 3.3.2.3 is uiteengezet, zal daarbij wel rekening moeten worden gehouden met de juridische voorwaarden op het terrein van de gegevensbescherming en het auteursrecht.

In het wetgevingsadvies van het CBP over de Wabo en het bijbehorende Besluit Omgevingsrecht (BOR) wijst het CBP er op dat het wetsontwerp Wabo bepalingen bevat over de digitale verwerking en publicatie op internet van persoonsgegevens, waarop de Wbp van toepassing is.[96] Volgens het CBP is bij het opstellen van het wetsontwerp onvoldoende rekening gehouden met een aantal elementaire uitgangspunten voor de bescherming van persoonsgegevens. Het CBP is van mening dat de publicatie op internet van ingescande documenten niet vanzelfsprekend voortvloeit uit het doel waarvoor die informatie is verzameld, te weten: een uniforme aanvraagprocedure. Het CBP wijst op het gevaar dat persoonsgegevens die op internet worden gepubliceerd door een onbekend aantal internetgebruikers wereldwijd voor eigen doeleinden kunnen worden verzameld en verwerkt. Dat zou tot nadelig gevolg hebben dat persoonsgegevens vogelvrij zijn op internet. Met name van de overheid mag worden verwacht dat het de persoonlijke levenssfeer van de burger respecteert. Dat blijkt niet uit het wetsontwerp Wabo. Het CBP pleit in dat verband voor 'dataminimalisatie' en verwijst naar de nieuwe Handelsregisterwet 2007 als goed voorbeeld van 'privacy-by-design'. Daarin wordt namelijk onderscheid gemaakt tussen de verplichte opname van sommige persoonsgegevens in het Handelsregister en de publicatie ervan op internet. Na aanvaarding van een amendement luidt het tweede lid van art. 21 Handelsregisterwet 2007 dat een ('natte') handtekening niet in elektronische vorm kan worden ingezien.[97]

---

[94] Zie: "De ICT achter de omgevingsvergunning". ICT – VROM Kennisplein Omgevingsvergunning. Op internet: <http://omgevingsvergunning.vrom.nl/index.cfm/t/ICT/vid/9D735EFE-3FFA-497D-97F0368F3482FE29> (geraadpleegd op 30 september 2008).
[95] Zie: 'Samenvatting wetsvoorstel', versie 1.2 juni 2008. Beschikbaar op internet: <http://omgevingsvergunning.vrom.nl/> (geraadpleegd op 30 september 2008).
[96] College bescherming persoonsgegevens, Vergunningaanvraag niet integraal publiceren op internet. Wetgevingsadvies, 15 mei 2007, z2007-00304. Op internet: <http://www.cbpweb.nl/documenten/adv_z2007-00304.shtml?refer=true&theme=purple> (geraadpleegd op 30 september 2008).
[97] *Kamerstukken II*, 2006/07, 30656, nr. 23a (Amendement van de leden J.J. van Dijk en Smeets ter vervanging van dat gedrukt onder nr. 17).

In 2008 heeft het CBP een tweede onderzoek afgerond naar het online bouwarchief van de gemeente Nijmegen.[98] In dat onderzoek concludeert het CBP onder meer dat de gemeente Nijmegen weliswaar wettelijk verplicht is om een bouwarchief in te stellen, maar dat die verplichting niet inhoudt dat het een digitaal bouwarchief moet zijn. Het online aanbieden van het bouwarchief, inclusief persoonsgegevens, vloeit daarom niet voort uit een wettelijke verplichting. Dat heeft tot gevolg dat deze vorm van verwerking van persoonsgegevens in strijd is met de Wet bescherming persoonsgegevens (Wbp). De online publicatie vloeit ook niet voort uit art. 8 van de Wet openbaarheid van bestuur (Wob), die een instructienorm is en niet voorziet in het op grote schaal openbaar maken van persoonsgegevens. Het CBP wees voorts op het specifieke risico van identiteitsdiefstal door de publicatie van de 'natte handtekening' op internet. De gemeente Nijmegen heeft intussen de procedure aangepast en besloten de documenten op internet te zuiveren van in ieder geval BSN en handtekening en alleen dan online te publiceren met toestemming (opt-in) van de betrokkene.

Met betrekking tot online publicatie van bouwtekeningen kan voorts het bestaan van een auteursrecht, bijvoorbeeld van de architect, als een juridische belemmering worden gezien.

3.3.2.4 Institutionele setting

De ministers van VROM en OCW zijn indiener van Wabo. Het voorstel heeft betrekking op veel gemeentelijk en provinciale instellingen. Er wordt samengewerkt met het ministerie van Verkeer en Waterstaat, bijvoorbeeld voor het aanvragen van watervergunningen.

3.3.2.5 Elektronische dienstverlening aan de burger

Veel gemeenten ondersteunen de omgevingsvergunning door middel van een virtueel loket. Met dit virtuele loket kunnen burgers omgevingsvergunningen aanvragen en inzien. Naast een virtueel loket wordt ook vaak een fysiek loket ingericht.

Belangrijkste dienst richting burger is dat er één vergunning ingediend kan worden toestemmingsstelsel, dat er één procedure wordt gebruikt en dat er één bevoegd gezag dat het stelsel toestemmingen al dan niet verleent. Dit is de omgevingsvergunning. Burgers kunnen omgevingsvergunningen

- Indienen
- Inzien
- Volgen

Door samenwerking met andere bouwstenen van de e-overheid (zoals Basisregistraties, Bedrijvenloket en Persoonlijke Internet Pagina) wordt voorinvulling mogelijk gemaakt.

3.3.2.6 Identity management

DigiD wordt gebruikt door burgers als authenticatiemiddel voor burgers voor eenvoudige vergunningsaanvragen zoals eenvoudige bouwvergunningen. Complexe vergunningen

[98] College bescherming persoonsgegevens, *Aanvragen bouwvergunning niet meer integraal op internet. Gemeente Nijmegen en ministerie van VROM passen werkwijze aan*. Mededeling, 29 mei 2008.

moeten op dit moment bij de gemeente Enschede nog steeds bij het loket worden aangevraagd. Waarnodig vindt identificatie plaats op basis van officiële identiteitspapieren (paspoort, rijbewijs, identiteitskaart).

3.3.2.7 Veranderingen ingevolge (het gebruik van) ICT

Het aanvragen, inzien en volgen van de status van een omgevingsvergunning wordt elektronisch ondersteund. Voor het indienen van de aanvraag wordt een centrale voorziening, de Landelijke voorziening Omgevingsloket gerealiseerd.

3.3.2.8 Relevante kwesties die rijzen/zijn gerezen in de betreffende case

In de gemeente Enschede is het in principe mogelijk om een vergunning aan te vragen, bijvoorbeeld een sloopvergunning, voor een pand wat niet in het bezit is van de aanvrager. Een dergelijke vergunning kan, op basis van de regels, worden verleend. Dit wil echter niet zeggen dat het pand gesloopt mag worden. Immers, het pand is geen eigendom van de aanvrager en mag dus op basis van eigendomsrecht niet worden gesloopt (ondanks dat de vergunning is verstrekt). Het verkrijgen van een vergunning is dus geen voldoende voorwaarde voor het mogen effectueren van de vergunning. Het is ons niet bekend of deze situatie in meer gemeenten voorkomt.

3.3.2.9 Dilemma's waar men in de case tegenaan is gelopen

Er is een spanningsveld tussen de privacy van vergunningsaanvrager versus de wettelijke plicht tot publicatie. Meestal worden in de wettelijke publicatie persoonsgegevens dan ook weggelaten. Wel worden er objectgegevens en adresgegevens gepubliceerd. Door adresgegevens te combineren met andere bronnen (zoals online telefoonboek) kunnen persoonsgegevens worden herleid. Soms hoeven persoonsgegevens niet te worden herleid om toch inbreuk te maken. Als er een vergunning voor het uitbreiden van de woonkamer wordt aangevraagd op een bepaald adres dan kan dat voor een verkoper van gordijnen of vloerbedekking aanleiding zijn om ongevraagde reclame te sturen. Hier speelt de balans tussen het openbaar maken van overheidsinformatie, privacyaspecten, en economische meerwaarde voor derden.

Bij digitale aanvragen is identificatie erg belangrijk. Daar waar vroeger face-to-face contact was tussen burger en ambtenaar, is dat bij digitale aanvragen vaak niet het geval. Het gebrek aan face-2-face contact kan het vertrouwen tussen burger en ambtenaar aantasten. Op dit moment is het op basis van DigiD (niveau basis) nog relatief makkelijk om de digitale identiteit van een ander te ge- of misbruiken. Het zou moeten worden onderzocht of een betrouwbaarder niveau dan DigiD basis bij ambtenaren dezelfde perceptie van veiligheid (d.w.z. geen misbruik) geeft als face-2-face contact.

3.3.2.10 Analyse door projectteam

Bij de omgevingsvergunning zien wij de volgende kansen en bedreigingen.

Kans: Het verkorten van de doorlooptijd van een vergunningsaanvraag wordt door burgers op prijs gesteld. Elektronische aanvraag biedt kansen om de verwerking van de vergunning te versnellen waardoor aanvragen daadwerkelijk sneller kunnen worden afgehandeld.

Kans: Bij het aanvragen van een vergunning is het (theoretisch) mogelijk te controleren of de aanvrager gerechtigd is de aanvraag te doen (bijvoorbeeld door te verifiëren of hij eigenaar is van het betreffende pand). Momenteel vinden dergelijke verificaties niet expliciet en structureel plaats. Een dergelijke verificatie kan de burger behoeden voor fouten.

Kans: Door aanvragen elektronisch te verwerken kunnen onvolkomenheden in de aanvraag eerder gedetecteerd worden. Gemeenten kunnen dit sneller identificeren en de burger informeren over onvolkomenheden in de vergunningsprocedure. Gemeente Enschede heeft goede ervaringen met deze vorm van dienstverlening aan de burger.

Bedreiging: Het publiceren van vergunningsaanvragen op Internet verhoogt de kans op identiteitsdiefstal of privacyinbreuk. Dit gebeurt dan ook alleen met toestemming van de betrokkene.

N.B.: Sommige gemeenten, waaronder gemeente Enschede, bieden als dienstverlening aan de burger een service aan waarmee zich burgers kunnen abonneren op een elektronisch nieuwsoverzicht waarin recente vergunningsaanvragen in een bepaald (postcode)gebied worden gepubliceerd. Om gebruik te maken van deze dienst dient de burger zich te authenticeren met behulp van DigiD. In dit geval worden vergunningen wel elektronisch gepubliceerd, maar is de verzameling abonnees door de overheid traceerbaar. Identiteitsdiefstal of privacyinbreuk is dan ook minder waarschijnlijk dan bij onvoorwaardelijke publicatie op Internet.

Bedreiging: Als bij digitale aanvragen vooral op efficiëntie wordt gelet, en minder op bijvoorbeeld betrouwbare authenticatie, kan dit het vertrouwen van burgers schaden. Denk hier bijvoorbeeld aan het aanvragen van een sloopvergunning van een pand dat van een ander is. Dit risico zou met name kunnen ontstaan als digitale aanvragen vooral worden toegepast bij ‘eenvoudige’ vergunningen.

Bedreiging: Vergunningsaanvragen worden in zijn geheel gepubliceerd tenzij de aanvrager aangeeft dat er redenen zijn om bepaalde informatie in de aanvraag niet te publiceren (bijvoorbeeld een productieproces als onderdeel van een milieuvergunning). Het gevaar is dat de aanvrager zelf actie moet ondernemen om de gevoelige informatie buiten de publicatie te houden. Als de aanvrager dit vergeet wordt de gevoelige informatie alsnog ontsloten. Merk hierbij op dat de genoemde gevoelige informatie niet altijd betrekking heeft op persoonsgegevens. Merk tevens op dat bij publicatie op internet – wat in toenemende mate plaatsvindt – de gemeente Nijmegen de burgers eerst om toestemming vraagt met betrekking tot de persoonsgegevens (naar aanleiding van een uitspraak van het CBP, zie casus in paragraaf 3.3.2.3).

4 Ontwikkelingen in het persoonsinformatiebeleids-domein in het licht van het juridisch kader

In de derde onderzoeksvraag staat de vraag centraal hoe de geschetste ontwikkelingen en bevindingen in het persoonsinformatiebeleidsveld zich verhouden tot het juridische kader dat door de Wbp en andere relevante wet- en regelgeving ter bescherming van persoonsgegevens wordt geboden (zie Appendix E voor een toelichting op de Wbp). In hoofdstuk 3 is in het kader van de daarin beschreven cases per case study het relevante juridische kader uiteengezet. Appendix E bevat een algemene uiteenzetting van de Wbp. Wanneer we vanuit het perspectief van deze juridische kaders kijken naar de trends die in Hoofdstuk 2 zijn gesignaleerd, leidt dat tot een aantal knelpunten. Deze knelpunten hebben betrekking op de noties van privacy, op transparantie en vertrouwen en op de technologie. In hoeverre noodzaken deze knelpunten tot aanpassing van de wetgeving?

4.1 Noties van privacy

In paragraaf 2.1.1 is gesignaleerd dat de notie van privacy verandert doordat steeds meer burgers persoonlijke informatie over zichzelf op het internet publiceren. Voorbeelden als Hyves en MySpace werden daar genoemd. Tegelijkertijd riep dat de vraag op of van de overheid dan nog wel moet worden verwacht dat die zorgvuldig moet omgaan met persoonsgegevens die de betrokkene zelf reeds aan een ieder beschikbaar heeft gesteld. Deze verandering in de notie van privacy knelt in zoverre niet met het juridisch kader dat de verwerking van persoonsgegevens regelt, omdat het niet afdoet aan de toepasselijkheid van de ‘fair-play’ regels voor zorgvuldig gegevensbeheer. De notie van privacy staat in die zin los van de regels voor gegevensbescherming. Het feit dat burgers informatie over henzelf willen delen met een door hen zelf af te bakenen deel van de wereld, neemt niet weg dat de overheid als “verantwoordelijke” de regels van de Wbp en eventuele bijzondere regels ter bescherming van persoonsgegevens zal moeten blijven respecteren.

In dezelfde paragraaf is ook gesignaleerd dat de technologische ontwikkelingen de schaal heeft veranderd waarop het mogelijk is om persoonsgegevens van burgers met elkaar te koppelen. Koppeling moet worden gezien als een vorm van gebruik van persoonsgegevens. Volgens de Wbp – en meer in het algemeen volgens de algemene privacybeginselen – is het gebruik van persoonsgegevens slechts toegestaan als het doel waarvoor die gegevens worden gebruikt niet onverenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verkregen. Wordt een bepaalde vorm van koppeling noodzakelijk geacht, dan kan men dat wettelijk regelen.

Het gebruik van profielen, waarop in paragraaf 2.1.2 is ingegaan, hoeft op zichzelf niet in strijd te komen met de Wbp, maar creëert wel een risico voor schending van groepsprivacy. In het bijzonder kan de koppeling van onschuldige gegevens grote gevolgen hebben voor de beslissingen die over een individu worden genomen. Die gevolgen zijn veelal niet te overzien voor de burger, tot het moment dat er iets mis gaat, bijvoorbeeld wanneer mensen op grond van etno-selectie niet in een bepaalde wijk worden toegelaten (Cuijpers, 2007).

Eveneens in paragraaf 2.1.2 wordt gewezen op de privacyaspecten die spelen bij *ambient intelligence*. Knelpunten die vanuit de Wbp c.s. kunnen ontstaan betreffen dan

bijvoorbeeld de vraag wie de “verantwoordelijke” is voor de desbetreffende toepassing en – omdat *ambient intelligence* nauwelijks merkbaar is voor de burger – op wie de informatieplicht rust en jegens wie (de burger of diens vertegenwoordiger) die informatieplicht al dan niet moet worden nagekomen.

De vraag of de regels ter bescherming van persoonsgegevens wel van toepassing zijn kan als een knelpunt worden gezien wanneer convergerende technologieën worden toegepast, bijvoorbeeld in de vorm van sensoren of actuatoren die inzicht geven in de fysieke gesteldheid van een persoon. Omdat met dergelijke toepassingen persoonsgegevens worden verzameld en verder verwerkt zijn de regels voor gegevensbescherming er onverkort op van toepassing.

Deze regels (zoals de Wbp) zijn tevens van toepassing wanneer de overheid de over haar burgers beschikbare persoonsgegevens wil gaan gebruiken voor persoonlijke (pro-actieve) dienstverlening (CBP, 2002).

4.2 Transparantie en vertrouwen

In paragraaf 2.2 is een aantal trends gesignaleerd die tot juridische knelpunten kunnen leiden. Deze trends zijn: (1) de toenemende tendens tot verbreding van de gegevensuitwisseling binnen een keten; (2) verbreding van gegevensuitwisseling door de toenemende publiekprivate samenwerking; (3) (toekomstige) mogelijkheden van identiteitsmachtiging; (4) *multi-channeling*; en (5) gegevensontsluiting via *portal-sites*.

Deze trends leveren bijvoorbeeld een knelpunt op met het vereiste van ‘verenigbaar gebruik’ in de Wbp: het gebruik van persoonsgegevens moet verenigbaar zijn met het doel waarvoor ze oorspronkelijk zijn verzameld. Ook zal een grondslag voor de gegevensverwerking, als bedoeld in artikel 8 Wbp, moeten kunnen worden benoemd. *Multi-channeling* en het gebruik van *portal-sites* kunnen leiden tot knelpunten met betrekking tot de authenticatie of gegevensbeveiliging in het algemeen. Voor *portal-sites* geldt voorts dat onduidelijkheid kan bestaan over de vraag wie “verantwoordelijke” daarvoor is in de zin van de Wbp: is dat de gebruiker van MijnOverheid.nl, de overheid die deze faciliteit aanbiedt, de makers van de programmatuur of “iedereen een beetje” (Schreuders en Gardeniers, 2005)? Deze onduidelijkheid over de verantwoordelijke bestaat overigens ook wanneer meerdere organisaties samenwerken in ketens of andere samenwerkingsverbanden.

Wanneer de uitwisseling van persoonsgegevens is geregeld in bijzondere wetgeving, zoals in het Suwi-domein, dan is het mogelijk om het verstrekkingenregime bij wet te wijzigen.

De gesignaleerde trends en als gevolg daarvan eventuele wetswijzigingen kunnen leiden tot afname van transparantie en vertrouwen bij de burger.

4.3 Technologie

Met betrekking tot identiteit en identiteitsfraude kan worden gesteld dat op de overheid een verplichting rust om de digitale identiteit van de burger in relatie tot die overheid voldoende te beveiligen ter voorkoming van identiteitsdiefstal en -fraude. Daarvoor zijn “passende technische en organisatorische maatregelen vereist”, aldus artikel 13 Wbp. De derde volzin van artikel 13 Wbp schrijft bovendien voor dat dergelijke maatregelen er mede op gericht moeten zijn om onnodige verzameling en verdere verwerking van (tot

personen herleidbare) persoonsgegevens te voorkomen. Daarmee wordt gedoeld op de inzet van *Privacy Enhancing Technologies* (PET). De Tweede Kamer heeft tijdens de parlementaire behandeling van de Wbp kamerbreed een motie aangenomen waarin het de regering verzocht de ontwikkeling en gebruik van PET krachtig ter hand te nemen en de bevorderen dat de overheid het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens. De noodzaak voor de overheid om PET in te zetten lijkt toegenomen doordat gegevensbescherming niet slechts de (informationele) privacy moet beschermen, maar tevens identiteitsdiefstal moet kunnen voorkomen.

Er zijn voorts drie overige aan technologie gerelateerde trends gesignaleerd in paragraaf 2.3.4: *macromyopia*, *function creep* en *co-evolutie*. *Macromyopia* en *co-evolutie* kunnen leiden tot juridische knelpunten omdat beide trends indiceren dat de technologische mogelijkheden onvoorzienbaar kunnen zijn als het gaat om de vraag in hoeverre persoonsgegevens (zullen) worden verwerkt. *Function creep* is een trend waarbij de technologie voor andere doelen wordt gebruikt dan waarvoor die oorspronkelijk is ontwikkeld of ingevoerd. Dat kan derhalve ook leiden tot het verwerken van persoonsgegevens voor andere doeleinden dan waarvoor die oorspronkelijk zijn verzameld, hetgeen in strijd is met de Wbp en met het meer algemeen erkende privacybeginsel dat bekend staat als ‘doelbinding’.

Tenslotte zijn enkele trends gesignaleerd in paragraaf 2.3.5 op het gebied van de overheidsdienstverlening. Trends die knelpunten kunnen opleveren zijn vooral:

- In paragraaf 2.3.5 signaleerden wij een toenemende druk van de overheid op burgers om persoonsinformatie over zichzelf prijs te geven. Ter illustratie wezen wij op de opvatting van de minister van Justitie dat het afstaan van DNA-materiaal als een burgerplicht zou moeten worden beschouwd. Het knelpunt hierbij is dat er een dringende maatschappelijke noodzaak (*pressing social need*) moet bestaan voor de overheid om persoonsgegevens bij burgers te mogen verzamelen. Dat het “wel handig” is die persoonsgegevens te verkrijgen, is juridisch onhoudbaar.[99]

- Tegelijkertijd kunnen we aannemen dat de overheid over steeds meer persoonsinformatie van burgers beschikt. Die informatie zou in sommige gevallen interessant kunnen zijn om voor andere doeleinden te gebruiken dan waarvoor die oorspronkelijk zijn verzameld. Ook daarvoor is dan een dringende maatschappelijke noodzaak vereist. In sommige gevallen zal een wetswijziging nodig zijn om een dergelijk gebruik mogelijk te maken.

- In paragraaf 2.3.5 signaleerden wij vervolgens een trend richting centralisatie van basisgegevens. Daarmee doelen wij op de basisregistraties. Hoewel basisregistraties gebruik maken van data bij de bron (dus in feite: gedecentraliseerde gegevens) bestaat een mogelijk knelpunt –waar wij in paragraaf 2.3.5 ook al op hebben gewezen– uit de grotere kwetsbaarheid door het aantal overheidsinstanties dat van deze basisgegevens gebruik maakt. Anderzijds moet ook worden vermeld dat die instanties anders zelf allerlei persoonsgegevens verzamelen en opslaan. De kring van toegangsgerechtigde instanties (bijvoorbeeld afnemers) zal in overeenstemming dienen te zijn met de Wbp (bijvoorbeeld de

[99] Ahmet Olgun, ‘Wel handig die data, vindt de overheid.’ Interview met prof. Corien Prins. *NRC Handelsblad*, 19 januari 2008.

voorwaarde van ‘verenigbaar gebruik’) en de eventueel van toepassing zijnde bijzondere wet- en regelgeving voor gegevensuitwisseling. De overheid kan dat garanderen door (wets)wijzigingen eerst te toetsen aan de juridische toelaatbaarheid.

– Elektronische dossiervorming: deze trend heeft diverse knelpunten tot gevolg. Ten eerste ligt het gevaar van misbruik op de loer. Elektronische dossiers zijn immers sneller te vermenigvuldigen en te verspreiden dan papieren dossiers en eenvoudiger te koppelen met andere gegevensverzamelingen. Ten tweede leiden elektronische dossiers tot juridische onduidelijkheden met betrekking tot vragen als: wie is de “verantwoordelijke” in de zin van de Wbp? In gevallen waarin sprake is van samenwerking tussen verschillende overheidsorganisaties op bepaalde beleidsterreinen of bij bepaalde activiteiten (geïntegreerd of integraal beleid), is er mogelijk sprake van één gemeenschappelijke verantwoordelijke. Veelal zal dit de minister zijn van het betreffende departement (Buitelaar en Borking, 2005).

– In paragraaf 2.3.5 wezen wij op de trend om persoonsgegevens langer te bewaren. In beginsel mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze oorspronkelijk zijn verzameld (art. 10 Wbp). Langer bewaren is – onder bepaalde voorwaarden – toegestaan voor historische, statistische of wetenschappelijke doeleinden of als er een wettelijke bewaarplicht bestaat. Knelpunt is dat de algemene norm uit art. 10 Wbp onbepaald en daardoor voor toepassing in de praktijk niet duidelijk is. Bovendien is niet duidelijk, c.q. moet in de praktijk zelf invulling worden gegeven, aan het noodzakelijkheidsvereiste. Als er al wel een vaste bewaartermijn geldt, is bovendien niet duidelijk wie daar toezicht op houdt.

4.4 Tot slot

De materiële normen van de Wbp zijn met name te vinden in de artikelen 6-9 en 11. Persoonsgegevens mogen uitsluitend worden verzameld voor een legitiem doel. Dat verzameldoel is bepalend voor het gebruik dat er vervolgens van mag worden gemaakt. Voorts moet er voor iedere verwerking (raadpleging, verstrekking, etc.) een rechtmatige grondslag zijn. Bovendien moeten de persoonsgegevens juist en volledig zijn. Alleen verwerkingen van persoonsgegevens die aan de voorwaarden van de Wbp voldoen zijn toegestaan. Tenzij uiteraard niet de Wbp maar een bijzondere wet van toepassing is, zoals de Wet GBA (Schreuders en Gardeniers, 2005).

Toepassing van de Wbp in de praktijk is om meerdere redenen echter niet eenvoudig (Schreuders en Gardeniers, 2005). Ten eerste gelden de voorwaarden uit de Wbp voor elke afzonderlijke verwerking van persoonsgegevens. Ten tweede blijkt het lastig te zijn om de vele open normen in de Wbp (‘noodzaak’, ‘gerechtvaardigd’, ‘ behoorlijk’, ‘zorgvuldig’, ‘niet-onverenigbaar’) in de praktijk te concretiseren.

De door ons gesignaleerde trends zouden aanpassing van de Wbp wenselijk kunnen maken. Daarbij dient evenwel in acht te worden genomen dat aanpassing van de Wbp mede afhankelijk moet zijn van de evaluatie van de Wbp (de 2^{e} fase loopt momenteel). Maar ook dan zal het lastig zijn om de wet aan te passen omdat de hoofddoelstelling van de Wbp de implementatie is van de Europese Richtlijn 95/46/EG (Zwenne e.a., 2007). Als gevolg daarvan zijn fundamentele wijzigingen in de Wbp (en in de bijzondere gegevensbeschermingswetgeving voor zover die voortvloeit uit de Richtlijn) eerst

mogelijk na aanpassing van de Richtlijn. De eerste fase van de evaluatie van de Wbp heeft een aantal vragen opgeleverd voor de tweede fase. Deze vragen hebben betrekking op mogelijke verbeteringen van inhoud en toepassing van de Wbp “binnen het kader van de richtlijn” (Zwenne e.a., 2007; p. 177 e.v.). Die vragen betreffen – voor zover hier relevant – met name de werking en reductie van administratieve lasten, alsmede de ontwikkelingen in informatie- en communicatietechnologie zoals dienstverlening via internet.

5 Samenvatting en conclusies

In hoofdstuk 3 zijn een vijftal specifieke casussen beschreven. In dit hoofdstuk vatten we de kansen en bedreigingen vanuit de verschillende casussen samen (sectie 5.2), en trekken vervolgens enkele generieke conclusies over de verschillende casussen heen (secties 5.3 t/m 5.5). Hierbij grijpen we tevens terug op de literatuur (zie ook hoofdstuk 2) en onze juridische observaties (zie ook hoofdstuk 4. We maken in dit hoofdstuk gebruik van de in hoofdstuk 2 beschreven trends als kader om onze conclusies te ordenen. Deze trends vatten we eerst samen in sectie 5.1.

5.1 Terugblik op maatschappelijke en technologische trends

Onderliggend onderzoek is opgezet vanuit de vraag of het persoonsinformatiebeleid van de overheid moet worden herijkt in het licht van de kansen en bedreigingen van ICT voor overheid en burger. Daartoe is in hoofdstuk 2 een aantal (maatschappelijke en technologische) ontwikkelingen en trends in kaart gebracht. Dit bracht ons in hoofdstuk 2 tot drie afwegingen:

- Traditioneel focusseert het persoonsinformatiebeleid sterk rond gegevensbescherming en -verwerking. In sociale netwerken lijkt de burger echter vrij losjes met zijn persoonsgegevens om te gaan. Technologische ontwikkelingen maken ook nieuwe modellen mogelijk, zoals de traceerbaarheid van data-inzage. Dit leidt tot een spanningsveld en balans tussen informationele privacy enerzijds en nieuwe noties van privacy anderzijds.
- We merken een groeiende behoefte aan het uitwisselen van gegevens bij de (semi-) overheid. Technologisch gezien kan ook meer worden uitgewisseld dan wettelijk mag. De vraag speelt wat het zicht van de burger hierop is: wie doet wat met zijn data. Dit geeft een spanningsveld en balans tussen het vertrouwen van de burger in de overheid enerzijds versus de behoefte tot informatie-uitwisseling bij de overheid anderzijds.
- Technologie kan een bedreiging zijn voor privacy, denk bijvoorbeeld aan identiteitsdiefstal via Internet. Anderzijds kunnen *privacy enhancing technologies* mogelijk ook de oplossing zijn voor al onze problemen. Ook hier ligt een balans tussen technologie als bedreiging versus technologie als oplossing.

Deze drie afwegingen ‘(nieuwe) noties van privacy’, ‘transparantie en vertrouwen’ en ‘technologie’ zijn steeds meegenomen bij het onderzoeken van kansen en bedreigingen voor specifieke cases.

5.2 Casus specifieke conclusies

In ons onderzoek hebben we vijf specifieke cases geanalyseerd:

1. Identiteitsvaststelling in de strafrechtketen
2. Elektronisch patiëntendossier EPD
3. Elektronisch kinddossier Jeugdgezondheidszorg EKD-JGZ en de Verwijsindex Risicojongeren VIR
4. Digitaal klantdossier DKD
5. Omgevingsvergunning.

Voor al deze cases zijn kansen en bedreigingen voor het persoonsinformatiebeleid geïdentificeerd.

5.2.1 Kansen

Onderstaande tabel vat beknopt de kansen samen zoals genoemd in hoofdstuk 3.

KANSEN	Notie privacy	Transparantie / vertrouwen	Technologie
Identiteits-vaststelling	Het gebruik van context-informatie (bijvoorbeeld iemands locatie) verbetert identificatie	Vertrouwen in de overheid stijgt als de juiste personen hun straf uitzitten door betere kwaliteit informatie.	Betrouwbaardere identificatie is mogelijk door het gebruik van biometrie
EPD	Binnen medische sector in context behandelrelatie is er vrije uitwisseling van medische informatie, ook tijdens de waarneming.	Kans op medische fouten kleiner. Medicijn gegevens zijn bekend. Eenmalige uitvraag patiëntgegevens. Aanvullende patiëntinformatie mogelijk via privé dossiers (Google Health, Microsoft HealthVault).	Data-aggregatie voor (statistisch) onderzoek mogelijk. EPD kan leiden tot meer aandacht voor informatie-beveiliging. Eenvoud ontstaat door een kleiner aantal verschillende zorgsystemen. Mandateringsinfrastructuur kan veel praktische problemen oplossen.
EKD	Voor EKD-JGZ: binnen de JGZ keten vrije doorgave van dossier (EPD model), bij inschatting van sterk verhoogd risico voor individuele jongeren waarschuwing aan brede jeugdsector (VIR model). Voor VIR: bij inschatting van sterk verhoogd risico voor individuele jongeren, door individuele hulpverleners waarschuwing aan brede jeugdsector.	Vroegtijdig signaleren probleemgevallen. Geen kinderen uit het oog verliezen.	Epidemiologisch onderzoek in de jeugdzorg is eenvoudiger uit te voeren. EPD infrastructuur –waarin al veel is geregeld– is voor het EKD-JGZ te gebruiken.

KANSEN	Notie privacy	Transparantie / vertrouwen	Technologie
DKD	Beter en consistenter klantbeeld door het ketenbreed uitwisselen van gegevens.	Goed voorbeeld dat uitstraling kan hebben. Verhoogde kwaliteit (en efficiëntie) door koppeling (of inzage).	Groepsaanpak wordt mogelijk door evaluatie over grotere aantallen. De technologie maakt dat minder dossiers kwijtraken en inzage te traceren is.
Omgevings-vergunning	Één loket als aanspreekpunt (intrinsieke eigenschap van de omgevingsvergunning).	De burger stelt kortere doorlooptijden bij een vergunningaanvraag op prijs. Automatische detectie (en snelle terugkoppeling) van manco's in aanvraag.	Verdere kwaliteitsverhoging is mogelijk door het koppelen van gegevens-bestanden (bijv. verificatie eigenaarschap).

5.2.2 Bedreigingen

Onderstaande tabel vat kort de bedreigingen samen zoals genoemd in hoofdstuk 3).

BEDREI-GINGEN	Notie privacy	Transparantie / vertrouwen	Technologie
Identiteits-vaststelling	Koppeling van een fysieke persoon aan een 'identiteit in de keten' via de controle van identiteitsdocumenten is de zwakke schakel. Identiteitsdiefstal –als eenmaal gepleegd– is lastig te corrigeren	Weinig transparantie rond de registratie van bezoekers bij Penitentiaire Inrichtingen (valt enkel onder de Wbp).	Technologie is feilbaar: het is een risico blindelings te vertrouwen op technologie (in plaats van op het proces van identificatie) of zelfs afhankelijk te zijn van technologie.
EPD	Druk op het 'hek' rond de medische data omdat technisch gezien meer kan worden uitgewisseld dan wettelijk mag. Informatiebeveiliging valt of staat me het gedrag van medewerkers: 'werking' UZI-passen is afhankelijk van discipline gebruikers. Onvoldoende risico-bewustzijn bij patiënten of medewerkers.	Draagvlak beroepsgroep en angst voor claims door onduidelijkheid rond aansprakelijkheid. Opbouw van schaduwdossier met privé aantekeningen (= niet willen delen dossiers). Het gebruik van centrale medische dossiers bij commerciële partijen (zoals Google Health) is een inherent risico.	Schaalgrote geeft grotere risico's bij criminaliteit of fouten in gegevens. Grootschalig gebruik van een beperkt aantal systemen maakt kwetsbaarder voor inbreuk. Toegang tot gegevens voor (alle) patiënten geeft beveiligingsrisico, alleen al wegens het ontbreken van sterke authenticatiemecha-nismen voor patiënten.

BEDREI-GINGEN	Notie privacy	Transparantie / vertrouwen	Technologie
EKD	Procedures voor privacy bescherming in de medische zorg en "hek" om EKD-JGZ gegevens in de jeugdgezond-heidszorg (valt onder het beroepsgeheim) heeft voor risicojongeren een natuurlijk lek bij melding via de VIR aan de bredere jeugdsector.	Onduidelijkheid over de scope van het EKD en het onderscheid EKD-JGZ en VIR geeft onrust bij ouders.	Koppeling of integratie van het EKD-JGZ met VIR, leerlingvolgsysteem, en dossiers van politie en Justitie geeft een risico (*function creep by design*).
DKD	Door het succes is er een roep tot breder gebruik van het dossier / koppelen meer partijen (risico van zgn. *function creep*). Verschillende ketenpartners kunnen dezelfde klantgegevens verschillend interpreteren.	Kwaliteit van de gegevens van één partner beïnvloedt de kwaliteit van de hele keten. Een keten is zo sterk als de zwakste schakel en daarom is vertrouwen nodig voor het delen van gegevens. Gemeenten informeren de keten niet of en in hoeverre zij voldoen aan gestelde eisen en gemaakte afspraken (een ketenbreed effectief toezicht ontbreekt daarmee).	Fouten hebben een grotere doorwerking en impact door het ketenbreed gebruik. Toegang tot gegevens door betrokkenen kent een beveiligingsrisico wegens het ontbreken van een sterk authenticatiemechanisme
Omgevings-vergunning	Initiatief ligt bij burger om gevoelige informatie buiten de publicatie te houden.	Onbetrouwbare authenticatie kan bedreiging vormen voor het vertrouwen van de burger.	Het via Internet publiceren van vergunningsaanvragen geeft privacyrisico's.

5.3 Spanningsveld databescherming versus nieuwe noties privacy

Traditioneel richt het persoonsinformatiebeleid zich op de bescherming en verwerking van gegevens. Dit leidde tot uitgangspunten als enkelvoudige uitvraag, tijdelijke opslag, decentraal beheer bij gemeenten en multifunctioneel gebruik (zie sectie 1.1). Persoonsgegevens worden echter niet alleen uitgevraagd, maar ook 'automatisch' verzameld (bijvoorbeeld het gebruik van elektronische labels voor locatiebepaling rond open inrichtingen, zie sectie 3.1.1.8). Of persoonsgegevens 'ontstaan' naar aanleiding van de combinatie van gegevens uit meerdere bronnen (denk aan risicosignalering bij VIR, zie sectie 3.2.2.2). De digitalisering en uitwisseling van gegevens maakt ook dat foutieve gegevens op grote schaal een grotere (negatieve) impact kunnen hebben (zie onze analyse bij EPD en DKD). Mogelijk gebeurt dit zelfs opzettelijk (cybercrime, digitaal pesten, identiteitsfraude, zie sectie 2.3.2). In ieder geval speelt ook de interpretatie van (uitgevraagde) gegevens buiten de oorspronkelijke context (vooral bij het EPD, zie sectie 3.2.1.7). Dit vraagt om aanvullende uitgangspunten voor persoonsinformatiebeleid.

5.3.1 Risicobewustzijn

Alles begint eigenlijk met de vraag hoe identiteit, en daarmee ook de bescherming van persoonsgegevens of privacy, vanuit de burger wordt beleefd. Is het echt iets van de burger of is het iets dat hij heeft gekregen om zichzelf te kunnen of moeten verantwoorden. Is het echt iets van de burger zelf, dan zal deze er heel zuinig mee om moeten springen. In de praktijk is dat niet altijd zo. Hoe eenvoudig geven burgers bijvoorbeeld hun creditcard af in een restaurant waarmee de ober naar achter loopt, laat de burger zijn paspoort achter op de camping, blijven kassabonnen met bank- of PINpas gegevens liggen, etc. In sectie 3.2.1 zijn voorbeelden aangehaald hoe ook in de zorgsector medewerkers onzorgvuldig kunnen omgaan met de persoonsgegevens van patiënten.

Bescherming van persoonsgegevens en identiteit begint bij het gedrag van de burger zelf.

5.3.2 Persoonsgegevens en identiteit

Uit de casussen blijkt dat uitwisseling van gegevens vele kansen biedt voor de gebruikers, rond de toepassingen. Uitwisselen betekent echter ook dat gegevens over een persoon geïnterpreteerd gaan worden door derden zonder dat er direct contact is geweest met de betrokken persoon. Een begrip als loon, bijvoorbeeld, kan bij verschillende partners van het DKD een verschillende connotatie hebben, of bij de VIR is weer een zeer brede en daarmee diverse doelgroep betrokken. Hierbij wordt (indirect) een beeld gevormd van deze persoon. Het kan ook betekenen dat gegevens daar terechtkomen waar de betrokken persoon ze in eerste instantie mogelijk niet verwacht had. Hierbij speelt de vraag of de betrokken persoon zelf zich kan herkennen in het beeld dat indirect van hem of haar ontstaat. Het gaat dan niet meer om de persoonsgegevens zelf, maar de integratie van gegevens uit verschillende bronnen die buiten hun context worden gebruikt om een integraal (nieuw) beeld te schetsen van een burger. Een inzagerecht in de aldus gecreëerde samengestelde identiteit lijkt daarom op zijn plaats. Hiervoor is echter wel weer nodig dat de burger daadwerkelijk weet waar zijn gegevens ergens zijn of worden verwerkt. In het licht van de trends zoals beschreven in bijvoorbeeld sectie 2.1.1 (koppelen, delen informatie) en sectie 2.3.4 (function creep) is het de vraag of dit altijd het geval is.

Bij het uitwisselen en combineren van gegevens neemt de kans op onjuiste interpretaties toe. Om hier mee om te gaan zijn semantische afspraken (standaardisatie) nodig, of kan een maat van betrouwbaarheid aan gegevens worden gerelateerd (zoals bronvermelding, geldigheidsduur, etc.).

Als bestanden eenmaal zijn vervuild, bijvoorbeeld in het geval dat iemand als gevolg van identiteitsfraude ten onrechte een strafblad heeft gekregen, dan is correctie lastig[100]. Er

[100] De Nationale ombudsman heeft bijvoorbeeld een zaak behandeld van een persoon die door fraude met zijn identiteit – een drugsverslaafde bleek zich voor hem uit te geven – dertien jaar lang ten onrechte geregistreerd stond als harddrugscrimineel in informatiesystemen van de overheid. De overheid slaagde er niet in de registraties als harddrugscrimineel en het strafblad met 43 criminele vergrijpen van zijn naam te halen.

moet worden gewaakt voor Kafkaëske situaties waarin burgers niet weten bij wie ze aan moeten kloppen voor correctie van fouten, als al duidelijk is dat het gaat om verkeerde gegevens, en daarom van het kastje naar de muur worden gestuurd. Ook is correctie lastig bij het ongewenst op Internet publiceren van persoonsgegevens door derden. Hierbij valt te denken aan foutieve, imagoschadende gegevens of stigmatiserende persoonsgegevens (zedendelict). Persoonsgegevens zijn nauwelijks van het internet te verwijderen. Naast de bescherming van persoonsgegevens is ook de bescherming van de identiteit van belang. Hier liggen weer technologische uitdagingen (*privacy enhancing technology*). Inmiddels onderzoekt de minister een meldingsplicht voor de diefstal van persoonsgegevens[101]. Uit dit alles trekken we de volgende algemene conclusie:

De huidige nadruk in het persoonsinformatiebeleid ligt op het beschermen en verwerken van persoonsgegevens. In de toekomst dient meer de nadruk te komen op het beschermen van de identiteit van burgers.

Dit vergt een sterke identiteits- en authenticatie-infrastructuur voor de toegang tot de verschillende elektronische dossiers. Immers, het EPD weerspiegelt iemands 'medische identiteit', het DKD iemands 'sociale identiteit', etc. De samengestelde identiteiten vertegenwoordigen rijke en daarmee gevoelige beelden van de betrokkenen. Wanneer deze toegankelijk zijn met behulp van zwakke authenticatiemiddelen, creëert dit veiligheids- en privacyrisico's. Bij authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken zoals geregistreerd in een systeem. Authenticatie vindt typisch plaats op basis van wie je bent (biometrie), wat je hebt (bankpas, paspoort, etc.) en wat je weet (zoals een pincode of antwoord op een controlevraag), zie sectie 2.3.1. Hoe meer factoren worden meegenomen, hoe 'sterker' de authenticatie. Voor de (geautoriseerde) toegang tot verschillende diensten kan een sterkere of zwakkere authenticatie vereist zijn, afhankelijk van het risico. Zo is in de financiële sector voor het overmaken van geld in het algemeen een sterkere authenticatie nodig dan voor het opvragen van een saldo. In het laatste geval volstaat vaak een pincode (wat je weet), in het eerste geval is meestal ook een fysiek object nodig (wat je hebt, zoals een pasje of een mobiele telefoon), soms zelf een vingerafdruk (wie je bent, biometrie).

De combinatie van DigiD en BSN kan objectief worden geclassificeerd als een zwak authenticatiemiddel omdat bij het gebruik hiervan de toegang tot een dienst plaats vindt enkel op basis van wat iemand weet (geen biometrie, geen fysiek object). Daarnaast speelt dat een burgerservicenummer weinig geheim is, en een DigiD kan worden aangevraagd zonder visuele inspectie van de aanvrager of overlegging van een deugdelijk identiteitsbewijs. Behalve als authenticatiemiddel wordt DigiD ook nog eens gebruikt voor het signeren (digitale handtekening) waarbij de mogelijkheid tot delegatie (machtiging) nog niet is geregeld. Het uitlenen van DigiDs in de sociale context geeft aan dat er minder zorgvuldig met DigiDs wordt omgesprongen, of ze op dit moment niet als strikt persoonlijk worden opgevat door veel betrokkenen[102]. Het belang van bescherming van de digitale identiteit staat onvoldoende op het netvlies van zowel burgers als ambtenaren (zie ook sectie 5.3.1).

---

http://www.nationaleombudsman.nl/nieuws/persberichten/2008/Mandertienjaarlangslachtoffervan identiteitsfraude.asp

[101] http://www.nu.nl/news/1834397/52/Meldpunt_voor_diefstal_persoonsgegevens.html

[102] http://www.nrc.nl/binnenland/article1785120.ece/Overheid_erkent_fout_met_DigiD

De toegang tot elektronische dossiers vergt een sterke identiteits- en authenticatie-infrastructuur. De combinatie van DigiD en BSN zonder visuele controle is niet altijd voldoende om burgers toegang te geven tot elektronische dossiers. Het is in dit verband zeer wenselijk dat de eNIK op korte termijn wordt ingevoerd.

Merk op dat de authenticatie eenvoudig sterker kan worden gemaakt door het gebruik van middelen zoals die ook bij elektronisch bankieren worden toegepast. Zie hiervoor ook een recent rapport van Innopay over e-herkenning (Bottelberghs en Liezenberg, 2008).

5.4 Spanningsveld vertrouwen versus uitwisselen

Vertrouwen komt te voet en gaat te paard. Hierbij speelt ook perceptie een rol. Ambtenaren van de gemeente Enschede gaven in ons onderzoek bijvoorbeeld aan dat rond een vergunningaanvraag het persoonlijk contact anders cq. betrouwbaarder 'aanvoelt' dan een digitale aanvraag (zie sectie 3.3.2.9). Uit onze juridische analyse constateren we dat de specifieke wetgeving, zoals rond het EPD, zorgvuldig en doordacht is opgezet (zie ook sectie 3.2.1.10). Dit neemt niet weg dat er gevallen kunnen zijn die hier buiten vallen, waarvan wij er enkele zullen benoemen in deze paragraaf.

5.4.1 Risicoklassen van persoonsgegevens

Sommige informatie is gevoeliger dan de andere. Dit hangt ten eerste af van het proces waarin de persoonsgegevens worden verwerkt (salarisadministratie, patiëntendossier, etc.). Ten tweede hangt dit samen met de aard, omvang en het gebruik van de gegevens. Ten derde spelen de mogelijke vormen van onbevoegde of mogelijk onzorgvuldige bewerking van gegevens (kans op verlies etc.). En ten vierde is de mogelijke schade die veroorzaakt kan worden in het licht van de kans hierop (impact) een factor die speelt. Dit bepaalt de risicoklasse. Van Blarkom en Borking (2001) noemen vier risicoklassen: publiek niveau, basis niveau, verhoogd risico en hoog risico. Deze A&V-studie van het CBP over de beveiliging van persoonsgegevens wordt momenteel herzien.

Afhankelijk van het type informatie dat wordt ontsloten (risicoklassen: gevoelige medische gegevens, gegevens van mijnoverheid.nl, etc.) moet het beveiligingsniveau worden aangepast. Niet alleen classificatie van elektronische gegevens is gewenst, maar ook koppeling van de risicoklassen aan de hiervoor gewenste authenticatie- en autorisatieprocessen.

Ook dit punt wijst in de richting van een noodzaak voor een betrouwbare en deugdelijke identiteits- en authenticatie-infrastructuur. Zowel burgers als gebruikers van digitale bestanden zullen zich in voorkomende gevallen moeten kunnen authenticeren om deugdelijke autorisatie mogelijk te maken en eventueel misbruik te kunnen detecteren. Voor zorgverleners is er de UZI-pas. Ook burgers moeten dergelijke middelen krijgen om te voorkomen dat de ene kant van het datagebruik deugdelijk is geregeld, terwijl aan de andere kant (burger) een significant lek bestaat. Hier ligt ook een kans om een relatie te leggen tussen risicoklassen enerzijds en (nieuwe) niveaus van DigiD anderzijds.

5.4.2 Verantwoordelijkheid

Bij het uitwisselen van gegevens in grote systemen zoals het geval in onze casussen (EPD, EKD, DKD, etc.) spelen vragen op het gebied van aansprakelijkheid als er onjuistheden, omissies of onduidelijkheden in een dossier voorkomen. Naarmate gegevens met (onbekende) derden worden gedeeld en door hen worden geïnterpreteerd, neemt de kans toe dat er een keer iets niet goed gaat. Bij het EPD is benoemd dat het 20 minuten per patiënt kost om het dossier te uniformeren en op een niveau te brengen dat het überhaupt deelbaar is (sectie 3.2.1.10), bij de VIR speelt een grote diversiteit van de doelgroep (sectie 3.2.2.9), en ook bij het DKD is de interpretatie van data als bedreiging genoemd (sectie 3.3.1.10). Het lijkt er op dat in die gevallen de gebruiker (bijvoorbeeld een behandelend arts) aansprakelijk wordt gesteld, terwijl deze te goeder trouw handelt op basis van onjuiste gegevens (zie sectie 3.2.1.4). Overigens ontslaat de beschikking over gegevens in elektronische dossiers de arts in dit geval niet van de plicht om bij de betrokkene om nadere informatie te vragen.

Dit verschijnsel versterkt zich nog bij afgeleide informatie die ontstaat door het koppelen van meerdere bronnen (zie ook sectie 2.1.2). Het is dan onduidelijk van wie deze informatie nu eigenlijk is. Die onduidelijkheid kan bijvoorbeeld betrekking hebben op de vraag wie de “verantwoordelijke” is/zijn als bedoeld in de Wbp (zie appendix E.2), of wie de “producent” is/zijn van de databank als bedoeld in de Databankenwet. Controle van persoonsinformatie door de betreffende persoon waar het over gaat is al helemaal lastig als onbekend is dat informatie wordt uitgewisseld en gecombineerd.

Het eventueel delen van toegangscodes heeft hoe dan ook tot consequentie dat bijvoorbeeld onduidelijk is wie een bepaalde wijziging in een medisch dossier heeft aangebracht (zie sectie 3.2.1.6 over disciplinair gebruik van UZI-passen en sectie 3.2.1.9 over het negeren van beveiliging). Wanneer fouten optreden leidt dit tot ongewenste aansprakelijkheids- en verantwoordelijkheidskwesties (ook al is formeel duidelijk wie verantwoordelijk is voor het dossier).

Bij het uitwisselen en combineren van gegevens neemt de kans op onjuiste interpretaties toe. Er is aandacht nodig hoe hier mee om te gaan in relatie tot verantwoordelijkheden. Semantische afspraken kunnen (ook hier) onjuiste interpretaties voorkomen. Ook is aandacht nodig voor de toepasselijkheid van de Databankenwet.

In Nederland kennen we een stelsel van basisregistraties. Informatie moet aan bepaalde eisen voldoen voordat deze in een basisregistratie wordt opgenomen. Ook zijn er grote, landelijke dossiers –zoals EPD, EKD, DKD, HAVANK, etc.– die hier gebruik van kunnen maken. Daarnaast zijn er nog vele andere, vaak lokale registratiesystemen. Voorbeelden zijn bezoekersregistraties in inrichtingen (zie sectie 3.1.1.8), huisartsinformatie buiten het EPD (zie sectie 3.1.1.10), etc. De privacycontrole hierop lijkt veel minder strikt, terwijl dit even zo goed onder de Wbp en/of bijzondere wet- en regelgeving valt. In het kader van het koppelen en uitwisselen van gegevens dient er echter rekening mee te worden gehouden dat ook lokale systemen wel eens landelijke systemen kunnen worden (zie sectie 3.2.1.7). Denk bijvoorbeeld aan het EKD.

Dit speelt nog sterker bij toepassingen op het terrein van Justitie (zie heel sectie 3.1.1). Politie/justitie hebben in gevolge van strafvorderlijke bepalingen altijd de bevoegdheid gegevens te vorderen en zo nodig zich de toegang te verschaffen bij een vermoeden van strafbare feiten. Deze bevoegdheid geldt ook voor de inlichtingen- en

veiligheidsdiensten. Uitwisseling mag plaatsvinden, in het bijzonder ook in het internationale circuit tussen politie, justitie en veiligheidsdiensten. Ook biedt de Wet justitiële en strafvorderlijke gegevens mogelijkheden voor uitwisseling. Dit kan betekenen dat organisaties die samenwerken met politie/justitie ook de beschikking over de gegevens uit de registraties kunnen krijgen. Het Rathenau Instituut (2008) wijst erop dat de politiek weinig zicht heeft op de schaal waarop politie en justitie gebruikmaken van deze bevoegdheden, in wat voor soort situaties ze dat doen en hoe groot de risico's zijn van onterechte verdachtmaking. Hierbij geldt overigens wel de verplichting gegevens te wissen: niet langer bewaren dan noodzakelijk.

Er bestaat een tendens (o.a. geobserveerd in de case over het EKD en DKD) om het gebruik van (landelijke) dossiers verder te verbreden. In gevallen waarin politie of justitie gegevens opvragen bij beroepsbeoefenaren met een geheimhoudingsplicht, zoals artsen, moet rekening worden gehouden met het verschoningsrecht van deze geheimhouders.

5.4.3 Burgerservicenummer (BSN)[103]

Heemskerk e.a. (2007) gaan in op de rol van het burgerservicenummer in de verhouding tussen burger en overheid. Ze wijzen op het gevaar dat het BSN een instrumenteel nummer kan worden om de burger te controleren en de efficiency van de uitvoering van de overheid nog beter te maken, hetgeen de balans kan doen doorslaan ten nadele van de burger. Ze geven ook aan hoe juist het BSN goede dienstverlening en transparantie voor de burger –en daarmee vertrouwen– kan verhogen.

Cruciaal punt in dit alles is wel dat het BSN nummer uniek is. Het toewijzen van dit nummer is zeker uniek. Maar of daarmee het gebruik van dit nummer uniek is, is de vraag: iemand zou (via een alias) twee nummers kunnen hebben.

Een andere vraag is of het een burger is toegestaan zelf zijn eigen BSN op internet te publiceren. Een burger valt niet onder de categorie ‘overheidsorgaan’, waardoor niet de Wabb maar de Wbp van toepassing zou zijn.[104] Daarmee valt de burger onder de beperking van art. 24 Wbp dat het “slechts” toelaat om wettelijk voorgeschreven identificatienummers (zoals het BSN) te gebruiken ter uitvoering van de betreffende wet of voor doeleinden bij de wet bepaald. Het zelf publiceren van het eigen BSN op internet valt daar niet onder. Dat volgt ook uit de memorie van toelichting bij art. 24 Wbp, die vermeldt dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen.[105] Deze dreiging is toegenomen, aldus de memorie van toelichting, sinds het

[103] Bij verschillende cases komt het BSN ter sprake. Omdat het BSN niet relateert aan een specifieke casus is de analyse rond BSN samengenomen in dit hoofdstuk. Daarnaast speelt er onder experts een discussie over de voor- en nadelen van het gebruik van één BSN voor verschillende sectoren, dan wel of er niet geopteerd moet worden voor een apart zorgnummer (etcetera) zoals dat in veel andere EU lidstaten is gebeurd. Deze discussie wordt in dit document echter niet gevoerd, de huidige situatie met één BSN is als bestaand uitgangspunt gehanteerd.
[104] Zie bijv. *Handleiding voor de gebruiker van het burgerservicenummer. Aanbevelingen voor een goed gebruik van het burgerservicenummer*. November 2007. Op internet: <http://www.burgerservicenummer.nl/documents/upload/handleiding_bsn.pdf>.
[105] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 128.

sofi-nummer (thans BSN) mede door de inwerkingtreding van de Wet op de identificatieplicht, ook ter kennis van particulieren kan komen. Ook de Raad van State heeft gewezen op het gevaar dat het BSN op internet opduikt. Heemskerk e.a. (2007) verwachten daarentegen niet dat BSN's op internet zullen gaan circuleren.

BSN speelt een centrale rol. Als bepaalde aannames niet kloppen, zoals het uniek zijn van het BSN nummer, haalt dit het hele model onderuit. Het zelf publiceren door burgers van hun BSN op internet is juridisch en maatschappelijk niet verantwoord. De verwachtingen over het al dan niet circuleren van BSN's op internet lopen uiteen.

Een belangrijk probleem bij het gebruik van het BSN is dat het kan worden opgevat als onderdeel van de authenticatie van burgers. De wet en memorie van toelichting verbieden dit, maar de praktijk laat zien dat dienstverleners bij gebrek aan fatsoenlijke authenticatiemiddelen terugvallen op 'gedeelde geheimen'. Daartoe worden in de private sector geboortedata, namen van ouders en huisdieren en dergelijke gebruikt. Er kan een neiging bestaan om het BSN in de publieke sector op te vatten als een dergelijk geheim dat alleen de rechtmatige aanvrager geacht is te kennen. Dat levert serieuze beveiligingsproblemen op aangezien het BSN wijd verbreid is en dus zeker geen aanspraak kan maken op de status van geheim. Veel identiteitsfraude in de VS is het gevolg van precies dit probleem. Het Social Security Number wordt daar veelal gebruikt ter authenticatie van aanvragers. Ook al is sec bekeken het BSN in Nederland niet te vergelijken met het SSN in de VS, ook hier is er een risico dat het BSN *de facto* gebruikt gaat worden voor identificatiedoeleinden (al is dit *de jure* niet de bedoeling).

Ook hier geldt dat het ontwikkelen van een deugdelijke identiteits- en authenticatie-infrastructuur noodzakelijk is. Smart cards en vergelijkbare systemen uitgegeven in een gecontroleerd proces en voorzien van sterke digitale handtekeningen lijken hierbij onontbeerlijk.

5.5 Technologie als kans of bedreiging

De insteek van dit document is vooral een technologische, zoals blijkt uit onze opdrachtformulering (sectie 1.1). Technologische ontwikkelingen als bedreiging, maar ook weer als een oplossing zijn daarom inherent ter sprake gekomen bij onze eerdere kansen, bedreigingen en conclusies. Ook is eerder genoemd dat daar waar de technologie te omslachtig is, mensen er omheen gaan werken (zie sectie 3.2.1.9). In deze paragraaf willen we ten slotte nog dieper ingaan op twee casusoverschrijdende onderwerpen: identiteitsfraude en macromyopia.

5.5.1 Identiteitsfraude

Rond identiteitsfraude zien we procedures en technologie een grote rol spelen om het proces van identiteitsvaststelling betrouwbaarder te maken en de kwaliteit van geregistreerde gegevens te verhogen. In het teveel vertrouwen op technologie of procedures zit ook een risico. Als iemand identiteitsgegevens verstrekt (bijvoorbeeld via een identiteitsdocument), en deze gegevens kloppen (het document is echt, de gegevens stemmen overeen met die uit de GBA), dan kan de neiging ontstaan om verdere controle achterwege te laten. Een zelfde verschijnsel kan spelen rond technische middelen voor de echtheidsanalyse van identiteitsdocumenten of het toepassen van biometrie. Het

vertrouwen op systemen kan afleiden van het ontwikkelen van een juist *fingerspitzengefühl*. Of er sprake is van het meeliften op de identiteit van een ander vereist tevens *human intelligence*.

Een vergelijking met de Belastingdienst of de Douane kan dit wellicht verduidelijken. Dergelijke organisaties werken risicogericht. Dit wil zeggen dat in verband met het steeds groter wordende aanbod van informatie- of goederenstromen op basis van profielen selectief controles plaatsvinden. Het risicomanagement is in de loop der tijd meer en meer een geautomatiseerde taak geworden die wordt uitgevoerd op basis van (gestructureerde) informatiestromen. Kern van de fraudebestrijding blijft echter de mens: fraudemeldingen van informanten, afwegingen en onderzoek door rechercheurs, etc.

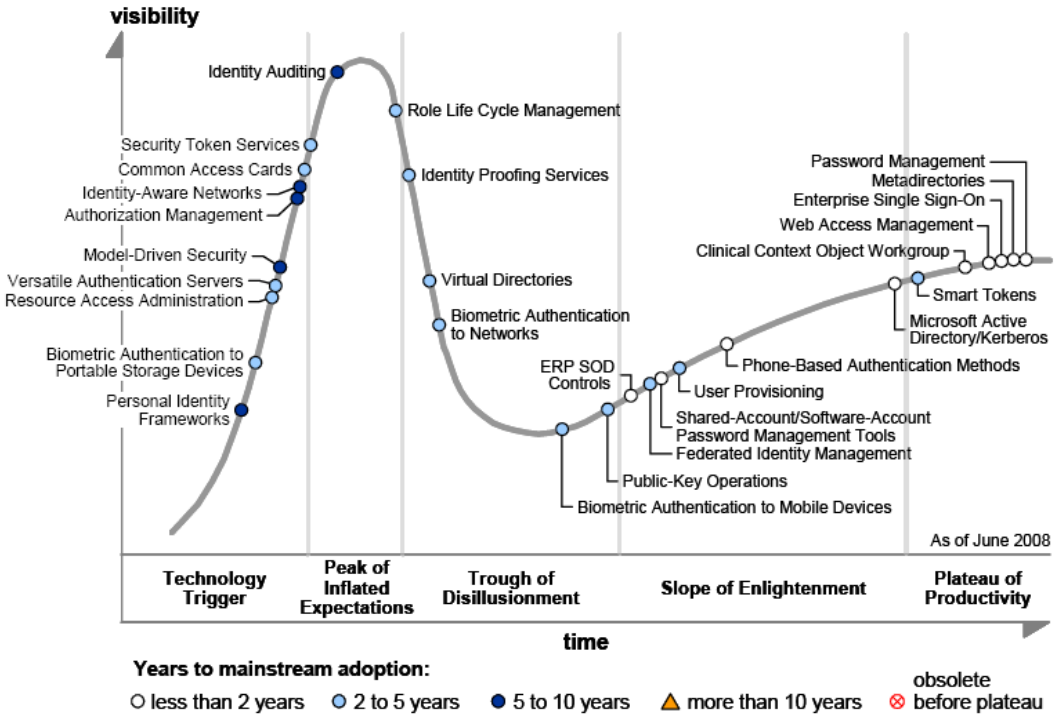
Waar technologie wordt ingezet voor identiteitsvaststelling, dient dat te gebeuren (a) in alle gevallen direct in de eerste lijn, aan het begin van de keten, en niet bijvoorbeeld alleen bij verdenkingen; en (b) altijd in combinatie met en ter ondersteuning van menselijke intelligentie, in plaats van ter vervanging hiervan. Technologie is een middel, geen doel.

Daarnaast speelt dat door technologische koppelingen de consequenties van fouten groter kunnen zijn. Dit geldt zeker bij identiteitsfraude, waar sporen leiden naar het slachtoffer in plaats van de dader. Daarom moet rond identiteitsfraude vooral worden ingezet op preventie. Een “Wet bestrijding identiteitsfraude” of het bevorderen van een effectiever gebruik van bestaande instrumenten (met name in de uitgiftecyclus) kunnen daartoe bijdragen. Dit leidt tot de volgende conclusies en aanbevelingen:

Alle (nieuwe) relevante wetten en regelingen op bestuurlijk terrein dienen, behoudens op de bescherming van persoonsgegevens (Wbp), tevens te worden getoetst op het feit in hoeverre de kwaliteit van gegevens gewaarborgd wordt en het meeliften op iemands identiteit wordt bemoeilijkt. Een Wet bestrijding identiteitsfraude of een effectiever gebruik van bestaande instrumenten is wenselijk, omdat identiteitsdiefstal vooral een zaak van preventie is.

5.5.2 Macromyopia

In sectie 2.3.4 is macromyopia genoemd als verschijnsel dat verwachtingen op korte termijn worden overschat en verwachtingen op lange termijn worden onderschat. Dit is gerelateerd aan de zogenaamde *hype cycle* van Gartner. Figuur 3 toont als voorbeeld de hype cycle voor *identity and access management*. Deze heeft betrekking op technologieën die de digitale identiteit van gebruikers representeren, technologieën die de relatie leggen tussen digitale en burgerlijke identiteit en technologieën rond de communicatie over en weer van digitale identiteiten met systemen. De figuur toont dat bij nieuwe technologieën vaak hoge verwachtingen zijn gebaseerd op eerste successen, vaak nog in laboratorium stadium of pilot fase. Bij verdere uitrol loopt men tegen de praktijk aan maar uiteindelijk ontstaat een stabiele marktsituatie.



Figuur 3: De Hype Cycle voor Identity and Access Management (uit Kreizman e.a. (2008)).

Hier is mogelijk een relatie te leggen met het DKD. Het succes hiervan resulteert in een roep om het breder te gebruiken (hoge verwachtingen). Algemener gesteld is het opvallend dat er technisch gezien vaak meer kan dat er juridisch gezien mag, bijvoorbeeld rond het koppelen van gegevens. Men ziet de mogelijkheden van technologie en wil dat direct toepassen (korte termijn). De praktijk kan hier worden onderschat, maar de potentie op lange termijn blijft.

Er zit een spanningsveld tussen wat wettelijk mag en technisch kan. Technisch kan er vaak meer dan wat mag. Dit geeft een inherent risico op function creep waar beter van te voren rekening mee kan worden gehouden.

Referenties

Azouz, A., Gardeniers, H., Jörg, P., Polman, F., Pluut, B., en Zuurmond, A. (2007). *De toekomst van persoonsinformatiebeleid: Een dynamische kijk op privacy.* Den Haag: Zenc / Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Barendrecht, J.M., van den Berg, M.F.M., Tjong Tjin Tai, T.F.E. en Zegveld, C.B.M.C. (reds.) (2008). *Aansprakelijkheden rond het EPD.* Rapport in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport. Tilburg: Universiteit van Tilburg. http://www.minvws.nl/kamerstukken/meva/2008/invoering-elektronisch-patientendossier.asp

Blarkom, G.W. van, en Borking, J.J. (2001). *Beveiliging van persoonsgegevens.* Achtergrondstudies en Verkenningen 23. Den Haag: Registratiekamer.

Bos, Tj. (2007) Privacy-Enhancing Technologies: Theorie en Praktijk bij de Overheid. *.ego* jrg. 6, nr. 2, 26-28. http://www.sbit.nl/ego/bestanden/EKSBIT1.pdf

Bottelberghs, L., en Liezenberg, Ch. (2008). *Verkenning e•Herkenning een andere opzet voor DigiD: Een verkennende studie naar de mogelijkheden van elektronische herkenning van bedrijven en burgers.* Den Haag: Innopay in opdracht van het Ministerie van Economische Zaken en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. http://www.ez.nl/dsresource?objectid=161246&type=PDF

Bremer, P.J.J., Kokkeler, B.J.M., Glas, M., Kerkdijk, H., Hulsebosch, B., en Ebeling, E. (2008) *Kernrapport Ketenbrede Informatie Uitwisseling binnen de Jeugdsector.* Den Haag: Programmaministerie Jeugd en Gezin.. http://www.jeugdengezin.nl/includes/dl/openbestand.asp?File=/images/djg-2880085b-_tcm21-173353.pdf

Buitelaar, J.C. en J. Borking, 'Invulling van de FG-functie bij een ministerie.' *Privacy & Informatie*, 2005, nr. 1, p. 8-14.

Bzk (2005). *Evaluatierapport biometrieproef 2b or not 2b.* Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. http://www.minbzk.nl/54771/evaluatierapport

CBP College bescherming persoonsgegevens (2002). *Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatieinfrastructuur van de overheid.* Den Haag: College bescherming persoonsgegevens.

COM (2007). *Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy enhancing technologies (PETs).* Brussels: Commission of the European Communities, COM (2007) 228. 2nd May 2007. http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf

Cuijpers, C. (2007). 'Privacy in context'. In: *J.M.A. Berkvens en J.E.J. Prins (red.), Privacyregulering in theorie en praktijk.* Deventer: Kluwer, vierde druk, p. 7-25.

Dekker, P. (2001). *Vertrouwen in de overhead: Een verkenning van actuele literatuur en enquêtegegevens.* Rapport 01.03. Tilburg: Universiteit van Tiburg. http://www.tilburguniversity.nl/globus/publications/publications01/publ01.03.html

EZ (2008). ICT-agenda 2008-2011: *De gebruiker centraal in de digitale dienstenmaatschappij*. Den Haag: Ministerie van Economische Zaken. http://www.ez.nl/dsresource?objectid=157980&type=PDF

Frissen, V., van Staden, M., Huijboom, N., Kotterink, B., Huveneers, S., Kuipers, M., en Bodea, G. (2008). *Naar een 'User Generated State'? De impact van nieuwe media voor overheid en openbaar bestuur*. TNO-rapport 34466. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. http://www.minbzk.nl/actueel/115718/brief-aan-de-tweede_6

Grijpink, J.H.A.M. (2006a). "Identiteitsfraude en overheid." *Justitiële Verkenningen*, jrg. 32, nr. 7, 37-57.

Grijpink, J.H.A.M. (2006b). *Keteninformatisering in kort bestek: Theorie en praktijk van grootschalige informatie-uitwisseling.* Den Haag: Lemma.

Grijpink, J.H.A.M. (2008). "Biometrie, veiligheid en privacy. Enkele opvallende, richtinggevende ontwikkelingen." *Privacy & Informatie*, 2008/3.

Grimmelmann, J. (2008). Accidental Privacy Spills. *Journal of Internet Law*, July 2008. NYLS Legal Studies Research Paper No. 07/08-35. http://ssrn.com/abstract=1147195

Hayat, A., Posch, R. and Rössler, T. (2005). Giving an interoperable solution for incorporating foreign e-ED's in Austrian E-government', in: *Proceedings of IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens, 17-18 February, Brussels, Belgium.* pp. 147-156. http://ec.europa.eu/idabc/en/document/3910/5803#proceedings

Heemskerk, P., Hooghiemstra, T., van Lunteren, J., Mettau, P. en Schravendeel, D. (2007). *Naar een goed gebruik van het burgerservicenummer (BSN).* Den Haag: Stichting Het Expertise Centrum

IGZ/CBP (2008). *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm*. Den Haag: Inspectie voor de Gezondheidszorg / College bescherming persoonsgegevens, november 2008. Zie http://www.cbpweb.nl/documenten/rap_2008_informatiebeveiliging_ziekenhuizen.shtml?refer=true

Jacobs, B., S. Nouwt, A. de Bruijn, O. Vermeulen, R. van der Knaap, C. de Bie (2008), *Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD)* PricewaterhouseCoopers, Universiteit van Tilburg, Radboud Universiteit Nijmegen, 2 december 2008. http://www.minvws.nl/kamerstukken/meva/2008/elektronisch-patientendossier.asp

Kreizman, G., Allan, A.,Enck, J., Litan, A., Wagner, R., Orans, L., MacDonald, N., Young, G., Ouellet, E., Runyon, B., en Perkins, E. (2008). *Hype Cycle for Identity and Access Management Technologies*. Stamford, CT: Gartner.

Kruissink, M., B. Post e.a. (2007). "De gevangenis van de toekomst?" *Justitiële verkenningen*, jrg. 33, nr. 4, pp. 44-59.

Leeuw, E. de (2007). "Biometrie en nationaal identiteitsmanagement." *Privacy & Informatie* 2007/59.

Meulenbroek, A.J. (2008). *De Essenties van forensisch DNA-onderzoek.* Versie 4. Den Haag: Nederlands Forensisch Instituut. http://www.forensischinstituut.nl/nfi/publicaties/#paragraph6

Rathenau Instituut (2008). *Opsporing behoeft 'checks and balances'*. Bericht aan het Parlement. Den Haag: Rathenau instituut. http://www.rathenau.nl/downloadfile.asp?ID=1466

Schreuders, E. en Gardeniers, H. (2005). 'Materiële normen: de kloof tussen de juridische normen en de praktijk'. *Privacy & Informatie* 2005, nr. 6, p. 260-263.

Schuurman, J.G., Moelaert El-Hadidy, F., Krom, A., en Walhout, B. (2007). *Ambient Intelligence: Toekomst van de zorg of zorg van de toekomst?* Den Haag: Rathenau instituut.

Spaink, Karin (2005). *Medische geheimen. Risico's van het elektronisch patiëntendossier*. Nijgh & Van Ditmar / XS4ALL.

Sulem, P.e.a. (2007). "Genetic determinants of hair, eye and skin pigmentation in Europeans", *Nature Genetics* vol. 39, december 2007, pp. 1443 – 1452.

Teeuw, W.B., en Vedder, A. (red.) (2008). *Security Applications for Converging Technologies. Impact on the constitutional state and the legal order.* Den Haag: Boom Juridische Uitgevers.

Vedder, A.H., Van der Wees, L., Koops, B.J., en De Hert, P.(2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag: Rathenau Instituut.

Zwenne, G.-J., Duthler, A.-W., Groothuis, M., Kielman, H., Koelewijn, W., en Mommers, L. (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens: Literatuuronderzoek en knelpuntanalyse*. Den Haag: WODC / Ministerie van Justitie. http://www.wodc.nl/onderzoeksdatabase/1382a-evaluatie-wet-bescherming-persoonsgegevens-wbp-1e-fase.aspx

Appendix A: Begeleidingscommissie

Roos van der Hilst	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Suzie Kenswil	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Nicole Maarse	UWV
Lotte Nijland	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Jan Timmermans	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Appendix B: Geïnterviewden

Identiteitsfraude gedetineerden

Dick Heerschop	Ministerie van Justitie, DG Rechtspleging & Rechtshandhaving, Hoofd Keteninformatievoorziening Directie Instrumentatie Rechtspleging en Rechtshandhaving (DIRR) / programmamanager PROGIS Programma Informatievoorziening Strafrechtsketen
Henk van de Stolpe	Ministerie van Justitie, senior beleidsadviseur Expertisecentrum Rechtspleging en Rechtshandhaving.
Roel Loermans	Ministerie van Justitie, beleidsmedewerker Platform Interceptie Decryptie & Signaalanalyse.
Ulco van der Pol	Amsterdamse Gemeentelijke Ombudsman, voorheen registratiekamer

Elektronisch patiëntendossier

Jessica Aarnink	Ministerie VWS, secretaris programmadirectie ICT & Innovatie ministerie van VWS. Verbonden aan directoraat MEVA (Macro Economische Vraagstukken en Arbeidsmarktvoorwaardenbeleid, stafdirectie van het ministerie). Zij is secretaris van de directeur, houdt het parlementaire proces in de gaten en is inhoudelijk vooral betrokken bij toegang van de patiënt tot het EPD.
Albert Vlug	Manager Ontwerp en Onderhoud NICTIZ

Elektronisch kinddossier

Gerda van ’t Bosch	Programmaministerie Jeugd en Gezin, Projectleider EKD in de Jeugdgezondheidszorg

Verwijsindex risicojongeren

Nicolette Damen	Programmaministerie Jeugd en Gezin, projectleider Verwijs Index Risicojongeren
Gregor Neggers	Programmaministerie Jeugd en Gezin, beleidsmedewerker

Digitaal klantdossier

Jan Breeman	BKWI, security officer, vz. domein Privacy en Beveiliging.
Nicole Maarse	UWV, Strategisch Beleidsadviseur Elektronische Overheid (tevens lid stuurgroep van dit project).
Freek Kamst	UWV, sr. adviseur en teamleider Beleid en Procesontwikkeling bij Directie UWV Gegevensdiensten.

Omgevingsvergunning

Tjapko Poppens	Gemeente Enschede, clusterleider bouwen en milieu.
Frank Herik	Gemeente Enschede, verantwoordelijk voor digitaliseringkant Wabo bij het cluster bouwen en milieu, tevens werkzaam binnen gemeentebrede werkgroepen.
Dhr. Kreeft	Gemeente Enschede, hoofd afdeling bedrijfsvoering binnen het cluster bouwen en milieu.

Algemeen

Naast de interviews hebben de heren Jan Grijpink en Wim Borst van het Ministerie van Justitie hun reactie gegeven op sectie 3.1, welke is verwerkt in de betreffende paragraaf.

Appendix C: Case study protocol

Onderstaande opzet / protocol is als uitgangspunt gehanteerd voor het houden van de interviews en het beschrijven van de cases:

Algemeen
- Wie zijn de geïnterviewden, en wat zijn hun rollen?
- Welke organisaties vertegenwoordigen ze?

Beleidsontwikkeling
- Welke beleidsuitgangspunten liggen er ten grondslag aan dossier X?
- Wat is de invloed van dit beleid op de uitwisseling van persoonsinformatie?
- Wat zijn de toekomstplannen betreffende dossier X? Met welke organisaties gaat u welke gegevens uitwisselen?
- Zijn er wijzingen in het beleid te verwachten, en zo ja welke (bijvoorbeeld uitbreiden van de dossierpartners met private partijen)?
- Welke controlemechanismen zijn er geïmplementeerd om te valideren of het beleid op de juiste wijze is geïmplementeerd?

Juridische setting
- Welke wet- en regelgeving ligt ten grondslag aan dossier X?
- Hoe wordt naleving afgedwongen?
- Welke (juridische) mogelijkheden zijn er om niet-naleving aan te pakken?
- Hoe is de uitwisseling van gegevens/samenwerking gedocumenteerd?
- Wie is de 'eigenaar' van de gegevens en wie is proceseigenaar?

Institutionele setting
- Welke organisaties zijn betrokken bij de uitwisseling?
- Op basis waarvan (wetgeving/beleid/eigen wensen) vindt de samenwerking/uitwisseling plaats?
- Wie heeft het initiatief tot de samenwerking/uitwisseling genomen?
- Is het te verwachten dat er in de toekomst meer organisaties betrokken worden bij de uitwisseling? Zo ja, welke organisaties en op welke termijn?
- Hoe wordt voorkomen dat ongeauthoriseerde personen/organisaties gebruik maken van de uitwisselingsgegevens?

Elektronische dienstverlening aan de burger
- Welke diensten worden geleverd aan burgers?
- Hebben burgers een plicht om aan de dienst(verlening) mee te werken of gegevens aan te leveren?
- Welke gegevens dienen burgers te overleggen om van deze diensten gebruik te maken?
- Wie hebben toegang tot die gegevens en wat wordt er met deze gegevens gedaan?
- Welke (persoons)gegevens worden uitgewisseld?
- Met welke partijen worden persoonsgegevens uitgewisseld?
- Wat is perceptie van gebruikers omtrent uw dienstverlening? Voelen ze zich veilig? Laten ze vol vertrouwen gegevens bij u achter?
- Weten burgers welke gegevens u bijhoudt/verzamelt?
- Weten burgers waarvoor hun gegevens gebruikt worden?
- Wat doet u met de gegevens van burgers?

- Hebben burgers inzage in wie hun gegevens kan bekijken / heeft bekeken? Zo ja, maken ze veel gebruik van het inzagerecht?
- Op welke manier zijn gegevens beveiligd?
- Welke technieken en instrumenten gebruikt u om de burger het vertrouwen te geven dat gegevens bij u veilig zijn?
- Hoe worden gebruikerservaringen verzameld/gemeten?
- Welke gebruikerservaringen heeft u opgedaan met betrekking tot uitwisseling van persoonsgegevens? (NB: gebruiker kan zowel klant als ambtenaar zijn).

Identity management
- Welke technieken worden gebruikt voor authenticatie en authorisatie?
- Welke technologische maatregelen zijn getroffen in het kader van privacy bescherming?
- Hoe detecteert u misbruik? Hoe vaak komt misbruik voor?
- Wat is uw 'privacy policy' ten aanzien van de privacy van de klant en medewerker?
- Welke rollen/partijen zijn bij de uitwisseling betrokken, en hoe worden de rollen geïdentificeerd?
- Wie hebben welke toegangsrechten tot welke gegevens, en hoe wordt dit afgedwongen?
- Welke toekomstige ontwikkelingen ziet u met betrekking tot uitwisseling van persoonsinformatie voor uw dossier?

Verandering ingevolg gebruik van ICT
- Welke technische, bestuurlijke en organisatorische ontwikkelingen beïnvloeden in uw opinie persoonsinformatiebeleid, en in welke richting (positief / negatief)
    - Bijvoorbeeld, hoe beïnvloeden de geïdentificeerde trends het persoonsinformatiebeleid in de visie van de geïnterviewden?
- Hoe wordt technologie gebruikt om privacy te beschermen?
- Welke maatregelen heeft u getroffen om misbruik te detecteren / voorkomen?

Relevante kwesties die rijzen
- Welke knelpunten bent u tegengekomen met betrekking tot uitwisseling van persoonsgegevens?
- Wat zijn naar uw mening de belangrijkste knelpunten ten aanzien van de samenwerking/uitwisseling van gegevens?
- Welke kansen en bedreigingen ziet u in de toekomst mbt uitwisseling persoonsinformatie?
- Ervaart u een verschuiving in het gemak waarmee persoonsgegevens worden uitgewisseld? Zo ja, waaruit blijkt dat?
- In hoeverre signaleert u zorgen bij de burger omtrent het koppelen van persoonsgegevens?
- Zou, in uw opinie, de uitgangspunten van persoonsinformatiebeleid aangepast moeten worden, en zo ja, hoe dan?

Dilemma's
- Welke dilemma's komt u tegen bij het beheren en bewaken van persoonsgegevens? Hoe gaat u daar mee om?
- Signaleert u een mismatch tussen het huidige juridische kader en de toekomstige mogelijkheden voor het uitwisselingen van persoonsinformatie?

Appendix D: Brief SZW over beveiligingsplannen Suwi-net gemeenten

Ministerie van Sociale Zaken en Werkgelegenheid

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 1 A
2513 AA S GRAVENHAGE

Postbus 90801
2509 LV Den Haag
Anna van Hannoverstraat 4
Telefoon (070) 333 44 44
Fax (070) 333 40 33
www.szw.nl

Ons kenmerk W&B/SFI/08/24336
Datum 3 september 2008

Onderwerp Beveiligingsplannen Suwi-net gemeenten

Zoals toegezegd bij mijn brief van 14 juni 2007 informeer ik u over de uitkomsten van de in het voorjaar van 2008 door IWI uitgevoerde quick-scan naar de mate waarin gemeenten voorzien in een informatiebeveiligingsplan, zoals dat verplicht is voorgeschreven in de Regeling SUWI.

Uit het bijgevoegde onderzoek komt naar voren dat 36% van de gemeenten in februari 2008 (nog) niet beschikt over een informatiebeveiligingsplan. Hoewel dit ten opzichte van voorgaande jaren een verbetering is (was 50% in 2005), ben ik van oordeel dat een te grote groep gemeenten onvoldoende actief is ten aanzien van informatiebeveiliging. Om meer inzicht te krijgen in de daadwerkelijke beveiligingspraktijk zal IWI onderzoek verrichten naar de beveiliging van de Suwi-keten in zijn algemeenheid en daarbij geconstateerde risico's in kaart brengen. Bij dit (vervolg)onderzoek zal IWI ook worden gevraagd aandacht te besteden aan de regels die ik onlangs heb gesteld aan de stelselinrichting van de keten werk en inkomen en de informatiebeveiliging daarbinnen. Deze regels bieden ondermeer faciliteiten voor het maken van onderlinge afspraken tussen de ketenpartijen en het doen van horizontale verantwoording.

IWI heeft voornoemde quick-scan uitgevoerd onder een steekproef van 175 gemeenten. Ik zal IWI verzoeken ook bij de overige 268 gemeenten te inventariseren of deze gemeenten over een informatiebeveiligingsplan beschikken én om alle gemeenten die nog niet beschikken over een informatiebeveiligingsplan te vragen of zij bereid zijn binnen een te stellen termijn alsnog in een plan te voorzien én mij ten slotte over het resultaat te informeren.

De Staatssecretaris van Sociale Zaken
en Werkgelegenheid,

(A. Aboutaleb)

Appendix E: Wet bescherming persoonsgegevens

E.1 Wanneer is de Wbp van toepassing?

De Wet bescherming persoonsgegevens (Wbp) is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op handmatig beschikbare gegevens, voor zover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen (art. 2, lid 1).

Met het oog op het persoonsinformatiebeleid van de overheid is het van belang er op te wijzen dat er belangrijke uitzonderingen bestaan op de toepasselijkheid van de Wbp. Zo is de Wbp niet van toepassing op verwerking van persoonsgegevens:

a) ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden;
b) door of ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002;
c) ten behoeve van de uitvoering van de politietaak, bedoeld in de artikelen 2 en 6, eerste lid, van de Politiewet 1993;
d) die is geregeld bij of krachtens de Wet gemeentelijke basisadministratie persoonsgegevens;
e) ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens en
f) ten behoeve van de uitvoering van de Kieswet.

Op verwerkingen van persoonsgegevens die vallen onder de reikwijdte van de Wet op de inlichtingen- en veiligheidsdiensten 2002, de Wet politiegegevens, de Wet gemeentelijke basisadministratie persoonsgegevens, de Wet justitiële en strafvorderlijke gegevens en de Kieswet, is de Wbp dus niet van toepassing.
De Wbp is in die gevallen niet van toepassing omdat daarop exclusief andere wetgeving van toepassing is. Is er ook andere, maar geen exclusieve wetgeving van toepassing, dan speelt de Wbp een aanvullende rol. Gedacht kan bijvoorbeeld worden aan wetgeving die van toepassing is op openbare registers, zoals het voogdijregister, huwelijksgoederenregister, kadastrale registratie, of aan andere wetgeving die van toepassing is op specifieke vormen van verwerking van persoonsgegevens, zoals de Wet openbaarheid van bestuur en de Archiefwet 1995 (zie ook 4.2).

De Wbp is voorts niet van toepassing op de verwerking van persoonsgegevens door de krijgsmacht in geval van operationeel optreden door Nederlandse militairen in het buitenland, bijvoorbeeld bij internationale crisisbeheersingsoperaties.

Zoals ook in het rapport “Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse” volgt, kan als uitgangspunt worden aangenomen dat de Wbp van toepassing is, tenzij er in een sectorale wet anders is bepaald.[106]

[106] Gerrit-Jan Zwenne, Anne-Wil Duthler, Marga Groothuis, Hugo Kielman, Wouter Koelewijn en Laurens Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*. Den Haag: WODC / Ministerie van Justitie 2007, p. 43.

In de sectorale wetten wordt grotendeels aangehaakt bij de begrippen en definities uit de Wbp. Ook het toezicht van het College bescherming persoonsgegevens strekt zich uit over de sectorale wetgeving ter bescherming van persoonsgegevens (Wet GBA, Wet politiegegevens, Wet justitiële en strafvorderlijke gegevens). Op grond daarvan kan worden gesteld dat de Wbp 'leading' is voor die andere wetten.

Teneinde vast te stellen of de Wbp van toepassing is, moet men zich afvragen of de gegevens waarover men beschikt 'persoonsgegevens' zijn en vervolgens of er sprake is van een 'verwerking' van persoonsgegevens of van een 'bestand'.

E.2 Relevante begrippen uit de Wbp

- *Persoonsgegeven*

Onder het begrip 'persoonsgegeven' vallen alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon. Er bestaat dus een onderscheid tussen gegevens en informatie.

Gegevens kunnen een beslissing weergeven die over een bepaalde persoon is genomen. Gegevens kunnen ook betrekking hebben op een product of een proces en daarbij tevens informatie verschaffen over een persoon. Zo kan de arbeidsproductiviteit van een werknemer bijvoorbeeld in kaart worden gebracht. Het gegeven dat een bepaalde persoon aangifte heeft gedaan van diefstal van een auto is ook een persoonsgegeven omdat het informatie verschaft over die persoon als slachtoffer van een misdrijf.

In deze context wordt met een persoonsgegeven gedoeld op een gegeven over een persoon dat vervolgens informatie kan verschaffen over die persoon.

De toelichting op het begrip 'persoonsgegeven' in de WBP legt uit dat deze definitie van persoonsgegeven twee elementen bevat:

1. Om een persoonsgegeven te zijn moet een gegeven informatie opleveren 'betreffende' een natuurlijke persoon. Gegevens verschaffen informatie over een persoon, als die gegevens mede bepalend zijn voor de wijze waarop een persoon wordt beoordeeld of behandeld door degene die over die gegevens beschikt. In dat geval zijn die gegevens 'persoonsgegevens'. Sommige gegevens bevatten duidelijk feitelijke informatie over een persoon. Dat zijn bijvoorbeeld iemands naam, geboortedatum of geslacht. Maar ook telefoonnummers, kentekens van auto's en postcodes met huisnummers zijn persoonsgegevens.

2. De identificeerbaarheid van de persoon is het tweede element dat bepaalt of al dan niet sprake is van een 'persoonsgegeven'. Een persoon is identificeerbaar indien redelijkerwijs, zonder onevenredige inspanning, zijn identiteit vastgesteld kan worden. Bepalend daarvoor zijn de aard van de gegevens en de mogelijkheden waarover de verantwoordelijke beschikt om de identificatie tot stand te brengen.

In verband met de aard van de gegevens bestaat onderscheid tussen direct en indirect herleidbare gegevens:

- Direct herleidbare gegevens horen bij personen waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen. Dat zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar gemakkelijk een persoon kunnen identificeren.

- Indirect herleidbare gegevens zijn gegevens die zijn ontdaan van naam, maar door combinatie met andere gegevens tot een persoon herleidbaar zijn. Daarnaast zijn sommige gegevens zo uniek, dat zij ook herleidbaar zijn. Voorbeelden hiervan zijn het Burger Service Nummer en unieke biometrische gegevens, zoals stem, vingerafdruk of DNA-profiel.

Ook de mogelijkheden waarover de verantwoordelijke beschikt om een persoon te kunnen identificeren zijn mede bepalend voor de vraag of sprake is van 'persoonsgegevens'. Het gaat hierbij om alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke zijn in te zetten om een persoon te identificeren. Daarbij wordt uitgegaan van een redelijk toegeruste verantwoordelijke.

❑ *Identificatienummers*

Persoonsnummers of identificatienummers vergemakkelijken het koppelen van bestanden met persoonsgegevens. Daardoor vormen identificatienummers een potentiële bedreiging voor de persoonlijke levenssfeer, maar tegelijkertijd een kans omdat de koppeling kan leiden tot een betere kwaliteit van persoonsgegevens. Een voorbeeld van een idenfiticatienummer is het burgerservicenummer (BSN). Het gebruik van het BSN is geregeld in de Wabb en het gebruik ervan in de gezondheidszorg in de Wbsn-z. Daarnaast kennen we bijvoorbeeld het A-nummer in de bevolkingsadministratie. Het gebruik van het A-nummer is geregeld in de Wet GBA. Ook in het kader van de kentekenregistratie wordt een persoonsidentificerend nummer aan iedere geregistreerde toegekend.

De Wbp schrijft voor dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, zoals het BSN, bij de verwerking van persoonsgegevens uitsluitend mag worden gebruikt ter uitvoering van de betreffende wet of voor doeleinden die bij wet zijn vastgesteld. Bij AMvB kunnen andere gevallen worden aangewezen waarin een identificatienummer mag worden gebruikt. In het algemeen mogen persoonsgegevens (dus ook identificatienummers) niet voor andere doelen worden gebruikt als dat gebruik onverenigbaar is met de doelen waarvoor ze zijn verkregen (zie hierna: 4.1.3). Voor identificatienummers geldt dus de extra voorwaarde dat het gebruik daarvan voor andere doelen uitsluitend is toegestaan als daarin bij wet is voorzien. Het is daarom de formele wetgever die eventuele andere gebruiksdoelen vaststelt.

❑ *Verwerken van persoonsgegevens*

Als is vastgesteld dat de gegevens persoonsgegevens zijn, moet men zich afvragen of men die persoonsgegevens ook 'verwerkt' in de zin van de WBP. De 'verwerking van persoonsgegevens' is "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens." Dit wil in feite zeggen dat alles wat men met persoonsgegevens kan doen, vanaf het verzamelen tot en met het vernietigen van persoonsgegevens (inclusief het raadplegen, verstrekken, e.d.), onder het begrip 'verwerken van persoonsgegevens' valt. Bepalend daarvoor is of men enige feitelijke macht of invloed over de gegevens kan

uitoefenen, al dan niet via een computersysteem. Men moet dus een handeling met de gegevens kunnen verrichten. Als men geen macht of invloed kan uitoefenen op de persoonsgegevens, hoeft men niet aan de eisen van de WBP te voldoen.

- *Verantwoordelijke voor de verwerking van persoonsgegevens*

De 'verantwoordelijke' is bijvoorbeeld de natuurlijke persoon, rechtspersoon of bestuursorgaan dat formeel-juridisch de zeggenschap over de verwerking heeft. Het gaat om degene die bevoegd is doel en middelen vast te stellen. Dat laat onverlet dat het feitelijk beheer over de gegevensverwerking aan een ander kan worden gemandateerd.

In de publieke sector geldt het krachtens het geldende staats- en bestuursrecht bevoegde bestuursorgaan als de verantwoordelijke. Deze bevoegdheid is te vinden in de Grondwet en in de bestuursrechtelijke wetgeving. Daarbij komt in de eerste plaats de Algemene wet bestuursrecht (Awb) in beeld. Binnen de overheid zullen als verantwoordelijke te kwalificeren zijn: de afzonderlijke ministers op rijksniveau, het college van gedeputeerde staten en de commissaris van de Koningin op provinciaal niveau en het college van burgemeesters en wethouders en de burgemeester op gemeentelijk niveau. Bij zelfstandige bestuursorganen op rijksniveau en functionele commissies op provinciaal en gemeentelijk niveau zal het orgaan, belast met de taken en uitoefening van bevoegdheden waarvoor de gegevens worden verwerkt, als verantwoordelijke zijn aan te merken. Problemen kunnen zich met name voordoen als de juridische zeggenschap over de verwerking onvoldoende duidelijk is, dan wel geen regeling voorhanden is op grond waarvan een bepaalde persoon of instantie daadwerkelijk door de betrokkene kan worden aangesproken. In zodanige situaties dient aan de hand van in het maatschappelijk verkeer geldende maatstaven te worden bezien aan welke natuurlijke persoon, rechtspersoon of bestuursorgaan de betreffende verwerking moet worden toegerekend.[107]

E.3 Relevante bepalingen uit de Wbp

- *Materiële normen in de WBP*

Een klassieke tweedeling in het recht is die in materieel recht en formeel recht. Materieelrechtelijke regels verlenen, verruimen, beperken of ontzeggen aanspraken, verplichtingen of bevoegdheden. Formeel recht regelt procedures en bevat vormvoorschriften en organisatorische bepalingen.

De materiële normen van de WBP zijn in drie groepen te verdelen:
1. de voorwaarden die de WBP stelt aan het verwerken van persoonsgegevens in het algemeen;
2. de voorwaarden die de WBP stelt aan het verwerken van bijzondere gegevens; en
3. de voorwaarden die de WBP stelt aan de doorgifte van persoonsgegevens naar landen buiten de Europese Unie.

We beperken ons tot de eerste twee groepen van materiële normen in de Wbp.

[107] T. Hooghiemstra, S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*. Den Haag: Sdu Uitgevers, 2007, derde herziene druk, p. 38.

- Voorwaarden voor rechtmatige gegevensverwerking

De eerste groep is van toepassing op elke verwerking van elke soort persoonsgegevens. Voor elke handeling met persoonsgegevens geldt dat deze moet voldoen aan de voorwaarden uit de eerste groep. Deze voorwaarden houden in dat de handeling altijd in overeenstemming met de wet, behoorlijk en zorgvuldig moet zijn (art. 6 WBP). Het verzamelen van persoonsgegevens is alleen toegestaan als dat gebeurt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7 WBP). Deze gerechtvaardigde doeleinden zullen in de praktijk meestal overeenkomen met een of meer van de grondslagen waarop elke verwerking van en handeling met persoonsgegevens moet berusten (art. 8 WBP):

(a) de ondubbelzinnige toestemming van de betrokkene;
(b) de noodzakelijkheid voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het treffen van voorbereidende maatregelen daartoe;
(c) de noodzakelijkheid om een wettelijke verplichting van de verantwoordelijke na te kunnen komen;
(d) de noodzakelijkheid ter vrijwaring van een vitaal belang van de betrokkene;
(e) de noodzakelijkheid ter vervulling van een publiekrechtelijke taak door een bestuursorgaan;
(f) de noodzakelijkheid voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het (privacy) belang van de betrokkene voorrang verdient.

Deze gronden zijn alternatieve gronden, dat wil zeggen dat het voldoende is als men een gegevensverwerking kan baseren op één van deze gronden (meer dan één kan en mag ook).

Wanneer men eenmaal op rechtmatige wijze verzamelde persoonsgegevens wil gebruiken (verder verwerken), dan is dat uitsluitend toegestaan als:

- het doel van dat gebruik niet in strijd is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (art. 9 WBP);
- de persoonsgegevens niet langer in tot personen herleidbare vorm worden bewaard dan noodzakelijk is voor de verwerkelijking van de doelen waarvoor ze oorspronkelijk zijn verzameld (art. 10 WBP). Langer bewaren is wel toegestaan mits de gegevens uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden gebruikt;
- de persoonsgegevens die worden verwerkt juist, volledig en actueel te zijn (art. 11 WBP);
- deze onder geheimhouding worden verwerkt (art. 12 WBP). Dit artikel neemt niet weg dat bijvoorbeeld reeds op grond van het medisch beroepsgeheim of ambtsgeheim een plicht tot vertrouwelijkheid kan bestaan;
- de verantwoordelijke voor de gegevensverwerking passende technische en organisatorische maatregelen treft om de persoonsgegevens voldoende te beveiligen (art. 13 WBP);
- in het geval een verantwoordelijke de feitelijke verwerking van de persoonsgegevens heeft uitbesteed aan een ‘bewerker’, daaraan een overeenkomst of andere rechtshandeling ten grondslag ligt (art. 14 WBP);
- de verantwoordelijke er voor zorgt dat de artikelen 6 tot en met 14 uit de eerste groep worden nageleefd (art. 15 WBP).

- Voorwaarden voor bijzondere persoonsgegevens

Naast bovengenoemde voorwaarden zijn op bijzondere gegevens nog enkele aanvullende voorwaarden van toepassing: d.i. de tweede groep materiële normen. Bijzondere persoonsgegevens zijn, aldus de Wbp, gegevens waaruit raciale of etnische afkomst blijkt (ras), politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijkt en gegevens over iemands gezondheid of seksuele leven. Ook strafrechtelijke een aanverwante gegevens (veroordeling, verdenking, straatverbod), zijn bijzondere gegevens volgens de Wbp. Het verwerken van bijzondere gegevens is verboden, tenzij een dergelijke verwerking bij wet (Wbp art. 17-22 of andere wet) is geregeld. Voorts is de verwerking daarvan toegestaan als aan bepaalde voorwaarden is voldaan. Die voorwaarden zijn dat de verwerking noodzakelijk moet zijn met het oog op een waarwegend algemeen belang, passende waarborgen ter bescherming van de persoonlijke levenssfeer worden geboden en dat bij wet is bepaald of het CBP daarmee bij beschikking heeft ingestemd.[108]

- *Procedurele voorschriften in de Wbp*

Naast de materiële normen die hierboven in grote lijnen zijn uiteengezet bevat de Wbp een aantal formeelrechtelijke normen, bestaande uit procedurele of administratieve voorschriften waaraan moet worden voldaan bij het verwerken van persoonsgegevens.

- Meldingsplicht

Voor alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens geldt op grond van de Wbp een meldingsplicht (art. 27). De meldingsplicht houdt in dat in principe alle verwerkingen, behalve handmatige verwerkingen, moeten worden aangemeld bij het College bescherming persoonsgegevens of bij een Functionaris voor de Gegevensbescherming (FG), als die binnen de branche of organisatie is benoemd. Naast handmatige verwerkingen hoeven ook verwerkingen die vallen onder het Vrijstellingsbesluit Wbp niet te worden aangemeld, mits deze voldoen aan de voorwaarden die in dat Vrijstellingsbesluit zijn aangegeven. In het algemeen geldt die vrijstelling voor de meer eenvoudige verwerkingen.

- Informatieplicht

De Wbp bevat voorts een plicht voor de verantwoordelijke om de betrokkenen, van wie persoonsgegevens worden verwerkt, daarover te informeren (art. 33 en 34). De informatieplicht schrijft voor dat de betrokkene voordat diens gegevens worden verwerkt geïnformeerd moet worden over de identiteit van de verantwoordelijke en de doeleinden van de gegevensverwerking. Daarnaast moet informatie worden verstrekt voorzover dat nodig is om van een rechtmatige verwerking van persoonsgegevens te kunnen spreken. De informatieplicht bestaat niet wanneer de betrokkene al op de hoogte is van deze informatie.

[108] T. Hooghiemstra, S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*. Den Haag: Sdu Uitgevers, 2007, derde herziene druk, p. 22-23.

- Rechten van betrokkenen

De Wbp kent de betrokkenen van wie persoonsgegevens worden verwerkt voorts diverse rechten toe. Deze rechten bestaan met name uit het inzagerecht (art. 35), het correctierecht, het recht op aanvulling, verwijdering en afscherming (art. 36) en het recht op verzet (art. 41 en 42).

In sommige gevallen zal het uit technisch oogpunt niet mogelijk zijn om aan deze rechten van betrokkenen tegemoet te komen. Dat geldt bijvoorbeeld voor de verplichting om verbeteringen of aanvullingen aan te brengen. Sommige gegevensdragers, zoals microfiches of cd-roms, laten technisch geen wijzigingen toe. In dergelijke gevallen zal de verantwoordelijke aanvullende maatregelen moeten treffen om bij het gebruik van de opgeslagen gegevens de gebruiker toch te kunnen voorzien van de juiste gegevens. Bij raadpleging van een duurzame gegevensdrager zal de gebruiker er dan moeten worden gewezen op de noodzaak om een aanvullend bestand te raadplegen waarin eventuele verbeteringen zijn opgenomen. Een dergelijke oplossing kan ook worden toegepast op back-up tapes.

- Toezicht en handhaving

Het toezicht op en de handhaving van de Wbp is primair in handen van het College bescherming persoonsgegevens. Sinds de inwerkingtreding van de Wbp beschikt het CBP over een aantal effectieve bevoegdheden: bestuurlijke boete, bestuursdwang en last onder dwangsom, hetgeen inhoudt dat het CBP een last (bevel) kan opleggen (om iets te doen of na te laten) onder een dwang- som wanneer die last niet wordt uitgevoerd (bijvoorbeeld € 600 per overtreding met een maximum van € 120.000).

Naast handhaving door de toezichthouder voorziet de Wbp ook in handhaving door de rechter: de bestuursrechter, burgerlijke rechter en de strafrechter die in bepaalde gevallen een verplichting tot schadevergoeding of een strafrechtelijke boete kunnen opleggen.

De Wbp kent de mogelijkheid voor bedrijven, organisaties of brancheorganisaties om een Functionaris voor de Gegevensbescherming (FG) aan te stellen. Wanneer een FG is aangesteld hoeven de verwerkingen niet bij het CBP te worden gemeld,maar mag dat ook bij de eigen FG. Het CBP stelt zich op het punt van toezicht en handhaving terughoudend op ten opzichte van organisaties met een FG.

- Beveiligingsplicht

Op een ‘verantwoordelijke’ rust een beveiligingsplicht. Ter voorkoming van onrechtmatige verwerkingen, zoals onbevoegde toegang tot of verlies van patiëntengegevens, moet een verantwoordelijke ‘passende technische en organisatorische maatregelen’ treffen. Een organisatorische maatregel is bijvoorbeeld het treffen van een regeling voor de toegang tot de gegevens. In een overzicht kan worden aangegeven welke functionaris tot welke gegevens toegang heeft. Een technische maatregel is bijvoorbeeld het gebruik van een wachtwoord om toegang tot de gegevens te kunnen krijgen.

- Bewerkersovereenkomst

Een verantwoordelijke kan ervoor kiezen om zelf de geautomatiseerde verwerking van persoonsgegevens te beheren of kan ervoor kiezen om deze uit te besteden aan een andere organisatie. In het laatste geval vindt de verwerking van persoonsgegevens plaats door een derde die voor de verantwoordelijke persoonsgegevens verwerkt, zonder dat hij diens hiërarchisch ondergeschikte is. In termen van de Wbp is die derde dan “bewerker” van de persoonsgegevens. Vindt de verwerking intern plaats, bijvoorbeeld door een eigen afdeling Automatisering van de verantwoordelijke, dan is die interne afdeling geen bewerker, want er is immers sprake van hiërarchische ondergeschiktheid (arbeidsovereenkomst) aan de directie of Raad van Bestuur. In plaats van bewerker kan (het hoofd van) de afdeling Automatisering als “beheerder” worden aangemerkt.

Een bewerker mag persoonsgegevens uitsluitend in opdracht van een verantwoordelijke verwerken overeenkomstig diens instructies. Een bewerker verwerkt de gegevens dus onder de uitdrukkelijke verantwoordelijkheid van de verantwoordelijke. Dat houdt in dat een bewerker geen beslissingen mag nemen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de bewaartermijn van de gegevens, etc. Dergelijke beslissingen mogen uitsluitend door de verantwoordelijke worden genomen, die daartoe vervolgens de bewerker opdracht kan geven.

Een verantwoordelijke die de persoonsgegevens buiten zijn rechtstreeks gezag wil laten verwerken door een bewerker is verplicht een overeenkomst te sluiten met die bewerker.