iOverheid, burger in beeld

Datum:	20 December 2012
Auteurs:	Anne Fleur van Veenstra, Colette Cuijpers, Tom Bakker, Arnold Roosendaal, Sandra Olislaegers.
Opdracht:	Deze opdracht is uitgevoerd door het Privacy & Identity Lab in opdracht van het Ministerie van Binnenlandse Zaken.
Penvoerder:	Partners van het Privacy & Identity Lab zijn: SIDN, TiU, RU, TNO. Penvoerder voor deze opdracht namens het Privacy & Identity Lab: TNO.
Rapportnummer:	TNO 2012 R11216
Opdracht voorwaarden:	Deze opdracht is uitgevoerd onder de in de offerte genoemde voorwaarden. Aanbiedingsbrief: TNO-060-DTM-2012-02030; Offertenummer: 161907

Dit rapport is tot stand gekomen vanuit het Privacy & Identity Lab. De Radboud Universiteit, TNO, Universiteit van Tilburg (TILT) en SIDN, het bedrijf achter.nl, werken gezamenlijk aan betere oplossingen voor het beheren van online privacy en elektronische identiteiten. Daartoe hebben ze het Privacy & Identity Lab opgericht, een expertisecentrum waarin ze bestaand onderzoek bundelen en nieuw onderzoek opzetten. Het samenwerkingsverband is uniek, omdat het de technische, juridische en socio-economische aspecten van privacy en identiteit integraal onderzoekt.

De verschillende partijen die samenwerken via het Privacy & Identity Lab hebben zitting genomen in de klankbordgroep van dit project. De leden van de klankbordgroep zijn:

Drs. Gabriela Bodea, TNO
Prof. dr. Bart Jacobs, Radboud Universiteit
Prof. dr. Ronald Leenes, TILT

Inhoudsopgave

1 Inleiding

De Wetenschappelijke Raad voor het Regeringsbeleid constateert in haar *iOverheid* rapport dat het niet langer mogelijk is om alleen te spreken van een eOverheid, waarbij individuele organisaties en toepassingen gebruik maken van ICT. Veel meer is er sprake van een iOverheid, die wordt vorm gegeven door vele informatiestromen. Deze informatiestromen banen zich een weg langs vele overheidsinstanties, maar ook over de grenzen van de publieke sector heen. Deze iOverheid is onder de politieke radar ontstaan en zal, volgens de WRR, zo ook onbekommerd doorgroeien.

Informatisering is tot in de haarvaten van de overheid doorgedrongen en ICT wordt in toenemende mate ingezet voor de oplossing van complexe maatschappelijke problemen. Het gebruik van grote hoeveelheden informatie in deze iOverheid biedt grote kansen voor het inrichten van handhaving en beleid. Het gebruik van ICT gaat hand in hand met doelstellingen als het verhogen van de efficiëntie en het verbeteren van de dienstverlening aan burgers. Maar tegelijkertijd levert de iOverheid ook risico's op. Verhoging van efficiëntie en verbetering van dienstverlening gaan soms ten koste van publieke waarden als transparantie, accountability en privacy.

1.1 Recht op privacy

In deze studie richten wij ons op het fundamentele recht op privacy. Hoewel definiëring van dit recht niet eenvoudig is, kan in het algemeen gesteld worden dat het bij privacy gaat om bescherming van persoonlijke vrijheid. Het recht op privacy kan onderverdeeld worden in verschillende dimensies, zoals het huisrecht, lichamelijke integriteit en relationele privacy, ofwel de vrijheid om te kiezen met wie relaties aan te gaan. Voor dit rapport is de informationele dimensie van privacy, ook bekend als het recht op gegevensbescherming, van groot belang. Deze dimensie van privacy is in het Nederlandse recht nader uitgewerkt in de Wet bescherming persoonsgegevens.

Zonder een diepgaande analyse van dit recht te geven, is het wel van belang om erop te wijzen dat er twee verschillende rechten geschonden kunnen worden. In veel gevallen wordt een schending van het recht op gegevensbescherming niet direct ervaren als een inbreuk op privacy. Echter, het gebruik dat gemaakt wordt van persoonsgegevens, en acties die op deze gegevens gebaseerd worden, kunnen wel als zodanig ervaren worden. Een voorbeeld kan dit verduidelijken. Wanneer de medische gegevens van een burger niet goed beschermd blijken in het ziekenhuis, *ervaart* hij dit niet direct als privacy inbreuk. Als hij echter vervolgens een telefoontje krijgt van de verzekeraar dat de premie voor de zorgverzekering flink wordt verhoogd, dan voelt hij zich waarschijnlijk zowel in zijn privacy, als in zijn portemonnee, aangetast. Daarnaast kunnen mensen in hun privacy aangetast worden doordat derden misbruik maken van gegevens die door de overheid openbaar gemaakt zijn. Het is dus noodzakelijk om bij de omgang met persoonsgegevens ervan doordrongen te zijn dat de verwerking van persoonsgegevens een scala aan risico's met zich mee brengt.

Een implicatie van de iOverheid is dat het risico op privacy schending door de overheid groter wordt. Veel politici en beleidsmakers nemen ten onrechte aan dat het primaire proces niet verandert door de inzet van ICT. Echter, de inzet van technologie kan bijeffecten hebben. Een voorbeeld hiervan is *function creep*, waarbij een bepaalde applicatie is opgezet voor de ene functie, maar in de loop van de tijd ook voor andere functies ingeburgerd raakt. Hierdoor worden gegevens die zijn verzameld met een specifieke bedoeling ook gebruikt voor andere doeleinden. Dit kan mogelijk de privacy aantasten, wanneer gegevens vervolgens oneigenlijk worden hergebruikt. Daarnaast kan de privacy van burgers in het gedrang komen doordat het ook voor de overheid zelf niet langer duidelijk is hoe persoonsgegevens verwerkt worden en onder verantwoordelijkheid van wie.

Zo kan het gebeuren dat toepassingen en informatie die met de beste bedoelingen zijn ingericht om invulling te geven aan beleid, in de praktijk een risico vormen voor de privacy van individuele burgers. De informatiestromen binnen de overheid gaan hun eigen leven leiden, in plaats van dat er door de overheid een afweging wordt gemaakt tussen verschillende publieke waarden als efficiëntie, dienstverlening en privacy.

1.2 Privacy schending als gevolg van overheidsbeleid

Het doel van het *iOverheid, burger in beeld* project is om de spanningen in kaart te brengen tussen beleidsdoelstellingen (bijvoorbeeld om de (elektronische) dienstverlening aan de burger te verbeteren) en de mogelijk negatieve gevolgen van dit beleid ten aanzien van de privacy van burgers. Door deze spanningen in kaart te brengen, kunnen overheden bij de inrichting en uitvoering van beleid een betere afweging maken tussen de verschillende belangen. Het expliciet maken van deze spanningen draagt bij aan de *verinnerlijking* van het begrip van de mogelijke gevolgen van de schending van privacy van burgers onder ambtenaren.

Dit onderzoek geeft inzicht in de spanning tussen beleidsdoelstellingen enerzijds en privacy anderzijds door negen cases te beschrijven. In de cases wordt zowel het perspectief van de burger als van het overheidsbeleid uitgediept. Uit deze casebeschrijvingen worden lessen getrokken voor de overheid zodat risico's voor de privacy in de toekomst kunnen worden vermeden, bijvoorbeeld door beleid anders in te richten of uit te voeren. Er zijn veel verschillende manieren waarop de privacy van burgers geschonden kan worden. In deze studie wordt expliciet aandacht besteed aan de negatieve effecten voor de privacy van burgers als gevolg van beleidsdoelstellingen en -uitvoering. Dit onderzoek gaat over keuzes en afwegingen die voortkomen uit:

1. Onzorgvuldigheden rondom de beveiliging van persoonsgegevens
2. Schending van de Wet bescherming persoonsgegevens (Wbp)
3. Koppelen van gegevensbestanden

Per type oorzaak van de spanning wordt een drietal cases beschreven. Per categorie wordt een korte inleiding gegeven op de drie te bespreken cases. Hierbij wordt ingegaan op het type oorzaak van de mogelijke privacy schending dat in deze categorie centraal staat en op (het risico op) de schade die burgers ondervinden als gevolg van het beleidsdoel. Nadat alle cases zijn behandeld, worden mogelijke

oplossingen voor de spanning tussen het beleidsdoel en de negatieve effecten voor de privacy van burgers beschreven.

1.3 Methodologie en opzet van de case studies

De negen cases (drie per type privacy schending) zijn gekozen op basis van twee criteria. De eerste is dat de mogelijke negatieve gevolgen ten aanzien van de privacy van burgers een gevolg zijn van beleid, of de uitvoering hiervan. De tweede is dat het perspectief van de (potentieel) benadeelde duidelijk beschreven kan worden. Een ander aspect dat een rol heeft gespeeld bij het maken van een keuze voor de cases is de relevantie voor het werkgebied van het Ministerie van BZK.

De case studies moeten inzicht geven in de spanning tussen beleidsdoelstellingen enerzijds en schending van de privacy van burgers anderzijds. Hiertoe doen we desk research. In sommige cases, waar het lastig was om het perspectief van de burger terug te vinden in documenten, hebben we aanvullende interviews gehouden om de twee perspectieven nader uit te werken. Aan de hand van citaten worden in kaders zowel het burgerperspectief als het beleidsperspectief geïllustreerd.

Om beide perspectieven – dat van de overheid en van de burger – inzichtelijk te maken, zijn de cases beschreven aan de hand van een paar stappen. Omdat de privacybeleving van burgers centraal staat, worden de cases ingeleid door het burgerperspectief te benoemen. Vervolgens worden de aanleiding en de probleemstelling van de cases uitgewerkt, gevolgd door de beleidsdoelstellingen en de beleidsuitvoering. De cases beschrijven voorts de mogelijke negatieve gevolgen voor de privacy van burgers. Vervolgens zijn per case de waarborgen behandeld die zijn getroffen aan overheidszijde om negatieve gevolgen voor de burger te voorkomen of te beperken. Ten slotte worden per case (mogelijke) oplossingen beschreven om tegemoet te komen aan de spanning tussen beleidsdoelstellingen en de negatieve effecten op de privacy van burgers.

De volgende drie hoofdstukken behandelen de drie typen oorzaak van de privacy schending van burgers; per type oorzaak worden drie case studies uitgewerkt. In de laatste twee hoofdstukken worden de (mogelijke) oplossingen in samenhang geanalyseerd en wordt vanuit het perspectief van het gehele onderzoek meer uitvoerig ingegaan op oplossingen om de overheid enerzijds voldoende ruimte te bieden bij het implementeren van legitieme beleidsdoelstellingen, terwijl de overheid anderzijds voldoende oog heeft voor, en waarborgen inbouwt tegen, de negatieve effecten die de implementatie van dit beleid kan hebben voor de privacy van de burger. Op basis van het in kaart brengen en analyseren van de mogelijke oplossingen wordt het rapport afgesloten door een conclusie met daarin een aantal concrete aanbevelingen.

2 Onzorgvuldigheden rondom de beveiliging van persoonsgegevens

De eerste categorie privacy schendingen komt voor als gevolg van onzorgvuldigheden rondom de beveiliging van persoonsgegevens. De Wet bescherming persoonsgegevens beschrijft dat organisaties die persoonsgegevens verwerken, verplicht zijn deze goed te beveiligen. Bij de cases die hier beschreven zijn, zijn de negatieve effecten voor de privacy van burgers nadrukkelijk het gevolg van een beleidsdoelstelling en niet slechts van een fout in de beveiliging. De drie cases, het beleidsdoel en de schade die burgers hebben ondervonden als gevolg hiervan zijn weergegeven in tabel 2.1.

Tabel 2.1: Cases, het beleidsdoel en de schade die burgers hebben ondervonden.

Casus	Beleidsdoel	Schade voor burgers
Fraude met toeslagen	Aanvraagprocedure toeslagen vereenvoudigen	Fraude, waardoor toeslagen niet zijn ontvangen of werden teruggevorderd. Gebrek aan hulp bij het oplossen van het probleem.
Online publicatie bouwvergunningen	Efficiënte en transparante vergunningprocedure	Blootstelling aan risico voor misbruik gegevens door derden, via identiteitsfraude of inbraak.
CV's van werkzoekenden openbaar	Efficiënt matchen werkgever en werkzoekende	Blootstelling aan risico voor misbruik gegevens door derden.

2.1 Fraude met toeslagen

Kader 2.1: Perspectief van de burger casus 'Fraude met toeslagen'.

Burger in beeld
Wel recht hebben op toeslagen van de Belastingdienst, maar deze niet ontvangen omdat je slachtoffer bent geworden van fraude. Wat dit voor sommige mensen betekent, werd duidelijk in een reportage van het tv-programma De Ombudsman. Eén slachtoffer vertelt: "Ik kom in de ellende zonder huur- en zorgtoeslag, want ik heb maar 773 euro en mijn huur is 530 euro. Ik houd niets over. Zo ging dat maanden door – vier maanden in totaal. (…) Ik betaalde rekeningen maar voor helft, om niet afgesloten te worden van Eneco of van mijn televisie. En ik eet gewoon al vier maanden bij m'n moeder. Ik heb zelf bijna niets in m'n koelkast staan. (...) Het was echt crisis, je bent gewoon een zwerver in je eigen huis."

2.1.1 Aanleiding en probleembeschrijving

Een groep mensen die recht had op zorg-, huur-, of kinderopvangtoeslag ontving deze in 2011 gedurende enige tijd niet. De reden hiervoor was dat er was gefraudeerd met de aanvragen. Fraudeurs waren in staat persoonsgegevens van

burgers aan te passen, doordat toeslagen aangevraagd konden worden door ondertekening met de DigiD van anderen. Door de opgegeven inkomsten naar beneden bij te stellen en bankrekeningnummers te veranderen, werden toeslagen geïnd op een rekeningnummer dat niet van diegene was die recht had op de toeslag.

In deze casus werd de inbreuk op de gegevensbescherming doordat onbevoegden ongecontroleerd persoonsgegevens konden wijzigen niet direct door alle betrokkenen als negatief ervaren. Maar de gevolgen ervan werden des te sterker gevoeld: het niet ontvangen van toeslagen door fraude. Een kwetsbare groep burgers ontving gedurende enige tijd geen toeslag waar men wel recht op had. Uiteindelijk zijn mensen die geen toeslagen hadden ontvangen – wat op kon lopen tot duizenden euro's per geval – gecompenseerd door de juiste toeslagen alsnog uit te betalen.

2.1.2 Beleidsdoelstelling en –uitvoering

Kader 2.2: Beleidsperspectief casus 'Fraude met toeslagen'.

Beleid in beeld
Staatssecretaris van Financiën Frans Weekers zei over de mogelijkheid om toeslagen aan te vragen via authenticatie met DigiD van iemand anders, in antwoord op Kamervragen (23 september 2011) naar aanleiding van de fraude: "Zonder deze mogelijkheid was het, vanaf het begin van toeslagen, niet mogelijk geweest om hulpbehoevenden door derden te laten helpen bij het aanvragen of wijzigen van toeslagen". Dat het beleidsdoel het verbeteren van de dienstverlening was, blijkt uit de reactie van de Belastingdienst, die aan het woord komt in nrc.next van 19 september 2011: "Een kwestie van snelle dienstverlening en van vertrouwen".

Om toeslagen bij zoveel mogelijk rechthebbenden terecht te laten komen, besloot de Belastingdienst de aanvraagprocedure te vereenvoudigen. Door toe te staan dat bij de aanvraag willekeurige DigiD-authenticatie gebruikt kan worden, konden ook hulpverleners, vrienden of familie toeslagen aanvragen voor 'hulpbehoevenden'. Deze procedure werd echter op grote schaal misbruikt. In 2010 werden er 200 fraudegevallen bekend en in 2011 nog eens 2500.

2.1.3 Gevolgen voor de privacy van burgers

Het doel de dienstverlening te verbeteren is in deze zaak op gespannen voet komen te staan met de veiligheid en vertrouwelijkheid van persoonsgegevens. De voornaamste spanning wat betreft privacy is de mogelijkheid die derden werd geboden om ongecontroleerd aanvragen en wijzigingen aan te brengen in persoonlijke gegevens. In deze casus betekende dit namelijk dat de aanvrager met behulp van een beperkt aantal gegevens (naam, BSN en geboortedatum) wijzigingen kon aanbrengen op het gebied van inkomen.

Dat er door derden wijzigingen waren aangebracht in persoonsgegevens, werd duidelijk toen burgers door de Belastingdienst op de vingers werden getikt met de mededeling dat ze onterecht te veel toeslagen zouden hebben ontvangen. Door het opgegeven inkomen naar beneden bij te stellen, werden de voorschotten op zorg-, huur- en kinderopvangtoeslagen flink hoger dan ze hadden moeten zijn. Anderen werden geconfronteerd met de fraude toen ze zelf toeslagen wilden aanvragen: dit

bleek niet meer mogelijk te zijn, omdat anderen dit al hadden gedaan. Of het rekeningnummer bleek gewijzigd te zijn en het geld was op een andere rekening gestort.

2.1.4 Waarborgen van overheidszijde

Er waren geen waarborgen die de privacy schending of de fraude konden voorkomen. Pas toen de fraude werd opgemerkt, zijn deze ingebouwd. Daarnaast was er ook geen duidelijk aanspreekpunt ingericht waar burgers die slachtoffer waren geworden van de fraude terecht konden. Hoewel er verschillende instanties betrokken waren (de Belastingdienst, politie, helpdesk DigiD en het Centraal Meldpunt Identiteitsfraude en –fouten), blijkt uit de berichtgeving van nrc.next (19 september 2011) dat verschillende instanties naar elkaar verwezen.

2.1.5 (Mogelijke) oplossingen

De problemen van burgers die slachtoffer zijn geworden van fraude zijn opgelost door de onterecht niet ontvangen toeslagen alsnog uit te betalen. Daarnaast is een aantal maatregelen genomen om de fraude in de toekomst te voorkomen. Zo is het niet langer mogelijk om aanvragen te doen met willekeurige DigiD-authenticatie; deze moet nu altijd horen bij de aanvrager. Ook de controle bij eerste aanvragen is verscherpt. Er wordt een bevestigingsbrief gestuurd zodra een aanvraag tot wijziging van rekeningnummers wordt gedaan. En er wordt pas tot uitbetaling overgegaan zodra de bevestiging binnen is. Op korte termijn wordt het waarschijnlijk alleen nog mogelijk toeslagen uit te betalen op een rekening die ook daadwerkelijk op naam van de aanvrager staat.

Daarnaast is binnen de Belastingdienst een ‘antifraudebox’ opgericht, gericht op het voorkomen en bestrijden van fraude. Zo brengt de box verdachte BSN’s en rekeningnummers in beeld. Ook wordt er gewerkt aan een nieuw en (hoger) zekerheidsniveau van elektronische identificatie via het eNIK-systeem. Dit zou één van de technische oplossingen moeten zijn voor de toekomst. Maar volgens Rejo Zenger, privacy-voorvechter, had zo’n elektronische identiteitskaart de problemen niet voorkomen: “Het probleem was de loskoppeling tussen toeslagaanvrager en eigenaar van de DigiD. De oorzaak van de meeste problemen is vaak niet de techniek, maar eerder een verkeerde beleidsinrichting en het ontbreken van relatief eenvoudige beveiligingsmaatregelen.”

Ten slotte is de hulp aan slachtoffers verbeterd. Zo is het nu ook mogelijk om aangifte te doen van fraude bij de balie van de Belastingdienst, in plaats van gelijk naar de politie te moeten stappen. Ook worden burgers bij fraude per brief geïnformeerd en krijgen zij te horen wat de vervolgstappen zijn en welk telefoonnummer zij kunnen bellen voor meer informatie. Daarnaast zou gedacht kunnen worden aan een ander type oplossing voor het beleidsdoel om meer mensen die daar recht op hebben toeslagen aan te laten vragen: betere voorlichting. Zo zouden burgers die mogelijk recht hebben op toeslagen, actief aangeschreven kunnen worden over hun mogelijkheden; de Belastingdienst beschikt immers over inkomensgegevens. Ook betere voorlichting via wijkkranten of televisiespotjes en nog duidelijkere aanvraagprocedures, kan het aantal mensen dat aanspraak maakt op toeslagen, verhogen.

2.2 Online publicatie bouwvergunningen

Kader 2.3: Perspectief van de burger casus ‘Online publicatie bouwvergunningen’.

Burger in beeld
Het via internet beschikbaar stellen van een bouwvergunning met daarin de naam, het bankrekeningnummer en de handtekening van een aanvrager kan verstrekkende gevolgen hebben. In een interview voor RTVOOG zegt bestuursrechtspecialiste Aline Klingenberg hierover: “Iemand die kwaad wil, die fraude wil plegen, die jouw bankrekeningnummer wil gebruiken met jouw handtekening om aankopen te doen, die moet dat niet op internet kunnen vinden. En zeker niet als jij bij de gemeente een bouwvergunning hebt aangevraagd, want je hebt geen keuze wat dat betreft. Je moet naar die gemeente om een bouwvergunning aan te vragen, dus dan moet de gemeente daar zorgvuldig mee omgaan.”

De negatieve gevolgen van het online bekendmaken van een bouwvergunning, worden duidelijk uit de volgende passage: “Wij zijn eruit. We hebben besloten te verhuizen, want mijn vrouw en kinderen voelen zich hier niet meer veilig. Sinds de bouwvergunning van de zakelijke aanbouw aan onze villa online heeft gestaan, is er drie keer ingebroken. Hoewel we de opslag van de goederen van de zaak inmiddels allang verplaatst hebben naar een loods, blijken we nog steeds niet veilig in ons eigen huis." (Gebaseerd op www.higherlevel.nl)

2.2.1 Aanleiding en probleembeschrijving

De afgelopen jaren hebben verschillende gemeenten aanvragen voor bouwvergunningen online beschikbaar gesteld. In het kader van haar publiekrechtelijke taak is het aan de gemeente om belanghebbenden in staat te stellen bezwaar te maken tegen verlening van aangevraagde vergunningen. Om deze inzage voor burgers eenvoudig te maken, werd in een aantal gevallen gekozen voor publicatie op internet. Het beleidsdoel kan aldus omschreven worden als de ambitie van de overheid om klantvriendelijk, efficiënt en transparant te zijn.

Vergroting van transparantie kan leiden tot snellere besluitvorming, hetgeen de kwaliteit van besluitvorming en/of dienstverlening ten goede kan komen. Ook kan digitalisering een bijdrage leveren aan de inspanning om de administratieve lasten te verlichten. Voor een deel is openbaarmaking van persoonsgegevens ook terug te voeren op de wet. In de Wet Openbaarheid van Bestuur, Algemene Wet Bestuursrecht en de Woningwet zijn bepalingen opgenomen, die gemeentes verplichten om informatie over aanvragen van en beschikkingen op vergunningen openbaar te maken. Hierbij geldt echter wel de Wet bescherming persoonsgegevens die aan deze openbaarmaking beperkingen stelt.

2.2.2 Beleidsdoelstelling en –uitvoering

Kader 2.4: Beleidsperspectief casus ‘Online publicatie bouwvergunningen’.

Beleid in beeld
In 2005 plaatste de gemeente Nijmegen het Digitaal Bouwarchief online. De gemeente Nijmegen wil met het Digitaal Bouwarchief de gebouwde stad weergeven. Daarnaast betreft het een online publicatie van (aanvragen voor) bouwvergunningen bij dezelfde gemeente. De gemeente Nijmegen baseert het

Digitaal Bouwarchief onder andere op de Woningwet waarin een plicht is opgenomen om een openbaar register bij te houden met aantekening van alle aangevraagde en verleende bouwvergunningen. Het Digitaal Bouwarchief biedt de mogelijkheid om gratis, 7 dagen per week, 24 uur per dag, niet gehinderd door belemmerende openingstijden dossiers, in te zien. Op basis van vergelijkbare overwegingen besluit de gemeente Groningen in 2010 bouwdossiers integraal via internet openbaar te maken.

In Nijmegen werden door de gemeente via 'Procedures Online' formulieren en beschikkingen op internet met betrekking tot bouw- en milieuvergunningen gepubliceerd. Hierdoor waren gegevens als naam, adres, telefoon- en faxnummer, e-mailadres en handtekening van de aanvrager via internet beschikbaar. Tijdens de aanvraagprocedure waren deze gegevens te vinden in 'Procedures Online'. Nadat een bouwproject gereed was gemeld, werden de gegevens uit 'Procedures Online' verwijderd, maar vervolgens wel voor onbeperkte tijd integraal opgenomen in het via internet beschikbare 'Digitaal Bouwarchief'.

Na de eerste klachten in 2005 is door de gemeente Nijmegen op verschillende manieren tegemoet gekomen aan privacybezwaren. Zo zijn de aanvraag en vergunning opgenomen op een wijze waarbij bewerken en doorzoeken van de aanvragen niet mogelijk is. Ook is de database aangepast zodat deze niet langer bereikbaar is voor zoekmachines. De enige overgebleven zoekmogelijkheid is op adres, en dan ook nog slechts op één adres tegelijk. Na deze aanpassingen bleven 'Procedure Online' en het 'Digitaal Bouwarchief' met goedvinden van het CBP online, maar in 2008 werd er door het CBP wel een ambtshalve onderzoek ingesteld, waarna Nijmegen haar procedure verder heeft aangepast.

In Groningen was het mogelijk om via de databank van de gemeente te zoeken op straatnaam, of met een kaart te navigeren door de stad en zo lopende bouwdossiers te vinden. Er was geen bescherming tegen indexeren door zoekmachinerobots (spiders). Nadat onderzoeksjournalist Eric Henneman hieraan ruchtbaarheid heeft gegeven omdat hij vond dat deze handelswijze in strijd is met de uitspraak die het CBP in 2008 gedaan heeft in relatie tot het 'Digitaal Bouwarchief' in Nijmegen, besluit de gemeente Groningen de indexpagina van het web te verwijderen. Hierdoor kan niet meer gezocht worden naar bouwdossiers, maar de gemeente laat de bouwdossiers als zodanig wel staan. Weliswaar in een minder bekend formaat, maar met een speciale plug-in zijn alle individuele dossiers nog te vinden op hun oude webadres. Bovendien kunnen door het simpelweg veranderen van het getal in het webadres van een bekend bouwdossier ook andere dossiers bekeken worden.

Kader 2.5: Beleidsperspectief casus 'Online publicatie bouwvergunningen'.

Beleid in beeld

Michel de Man, beleidsadviseur ICT bij de gemeente Capelle aan den IJssel, is als projectleider verantwoordelijk voor de uitvoering van het 'Project Internetpublicatie Vergunningen'. "Het enige echte knelpunt in het traject is het werken met privacygevoelige gegevens. Hierdoor is het bijvoorbeeld niet mogelijk om het volledige aanvraagformulier te publiceren. We hebben bewust gekozen om datgene, dat gepubliceerd mag worden, te tonen. Het gaat tenslotte om de informatieverstrekking aan onze burgers en bedrijven. Om onze dienstverlening

verder te verbeteren hebben we in navolging van het landelijke project ‘Minder regels, meer service’ een lokaal (digitaal) meldpunt ingevoerd. Via dit meldpunt kunnen Capellenaren aangeven welke regels zij in praktijk als lastig of zelfs overbodig ervaren. We gebruiken de meldingen om onze dienstverlening zo veel mogelijk te verbeteren.” (www.e-overheid.nl)

2.2.3 Gevolgen voor de privacy van burgers

Hoewel het openbaar maken van vergunningen via internet is ingegeven door een gerechtvaardigd belang - het verbeteren van de dienstverlening aan de burger en het realiseren van transparantie, kan het openbaar maken van (gevoelige) gegevens via internet de privacy van de vergunningaanvrager schenden. Het grootste risico is dat kwaadwillende derden persoonsgegevens gebruiken in het kader van ongewenst contact (bijvoorbeeld spam). Maar ook dat gegevens, zoals handtekeningen en bankrekeningnummers, gebruikt worden voor identiteitsfraude.

In een reactie op de zaak in Groningen wijst ook Hennekam op de privacyrisico’s. Een ander punt van zorg is de informatie die bouwtekeningen vrijgeven. Voor criminelen kan het bijvoorbeeld interessant zijn om te weten waar de kluis is in winkelpanden. Bovendien wijst Hennekam op het risico dat de toch al uitgebreide informatie die via de vergunningaanvragen beschikbaar is, nog verder kan worden uitgebreid. Bijvoorbeeld met gegevens uit andere openbare bronnen en registers, zoals bijvoorbeeld http://www.123people.nl en de openbare registers van de Kamer van Koophandel.

2.2.4 Oplossingen

Het CBP heeft inmiddels in verschillende adviezen de nodige richtsnoeren gegeven over hoe om te gaan met publicatie van vergunningaanvragen op internet. In december 2007 heeft het CBP de ‘Richtsnoeren publicatie van persoonsgegevens op Internet’ uitgevaardigd. Deze zijn door het ICTU verwerkt tot een landelijke standaard voor het online publiceren van vergunningen ‘Informatie Publicatie Model 4.0’.

Als hoofdregel geldt dat informatie die niet noodzakelijkerwijs online beschikbaar hoeft te zijn, alleen online gepubliceerd mag worden wanneer de privacygevoelige informatie onleesbaar is gemaakt. Bovendien is het niet alleen zaak zo min mogelijk persoonsgegevens te verzamelen, maar ook om persoonsgegevens alleen te verstrekken aan anderen indien, voor zover en zolang de noodzaak daartoe bestaat. Daarnaast wordt in de richtsnoeren aandacht besteed aan de invulling van informatie- en beveiligingsplichten en, indien van toepassing, aan de manier waarop een burger zijn rechten kan inroepen, zoals het recht van verzet.

Naar aanleiding van het onderzoek in 2008 heeft de gemeente Nijmegen het online aanvraagformulier voor bouwvergunningen aangepast. Bij het nieuwe formulier moet de aanvrager kiezen of hij toestemming geeft voor publicatie van een deel van zijn persoonsgegevens op internet, zoals zijn naam, zijn contactgegevens en de hoogte van de bouwsom. Een deel van de gegevens wordt nooit openbaar gemaakt. Dit betreft gevoelige gegevens zoals het BSN en de handtekening van de aanvrager. Een klein deel van de persoonsgegevens op het aanvraagformulier, zoals het adres inclusief het huisnummer, wordt door de gemeente altijd openbaar gemaakt, samen met overige gegevens uit het aanvraagformulier zoals de bouwtekening, de gebruikte materiaalsoorten en kleuren.

2.3 CV's werkzoekenden openbaar

Kader 2.6: Perspectief van de burger casus 'CV's werkzoekenden openbaar'.

Burger in beeld
"Het probleem zit hem vooral in de suggestie van het UWV dat alleen werkgevers inzage hebben in de CV's, terwijl het in werkelijkheid zo is dat iedereen die gegevens kan inzien. Vervolgens is het onmogelijk om te achterhalen wie deze gegevens bekijkt en gebruikt. Het liefst zou ik zien dat een werkgever die interesse heeft in mijn CV, mijn verdere gegevens pas krijgt nadat hiervoor via het UWV om toestemming was gevraagd. Mijn contact met het UWV berust nu eenmaal niet op een vrije keuze en het openbaar maken van mijn gegevens krijgt hierdoor een dwingend karakter. Dit kwam mede door het beleid dat UWV voerde, zo kreeg ik meermaals bericht dat gecontroleerd zou worden of mijn CV op www.werk.nl was geplaatst en werd steeds aanbevolen het CV op 'openbaar' te zetten. Als het CV op anoniem bleef staan zou de werkgever eerst contact moeten opnemen met het UWV om een e-mailbericht naar de werkzoekende te kunnen sturen. Dat zou het verschil kunnen betekenen tussen een baan of werkzoekend blijven." (Gebaseerd op De Nationale Ombudsman, Rapport 2011/191, 28-06-2011).

2.3.1 Aanleiding en probleembeschrijving

Werkzoekenden die zich inschrijven bij het UWV zijn verplicht zich in te schrijven op de website werk.nl. Op deze site van het UWV is het voor werkzoekenden ook mogelijk hun CV achter te laten voor potentiële werkgevers. Hoewel het plaatsen van een CV geen uitkeringsvoorwaarde is, was het proces in eerste instantie zodanig ingericht dat het niet mogelijk was af te zien van het plaatsen van een CV. Werkzoekenden konden ervoor kiezen om het CV anoniem of openbaar te plaatsen. De optie anoniem suggereerde dat de beschikbare gegevens op het CV (zonder de personalia) niet te herleiden zijn tot één persoon, maar dat bleek wel te kunnen. Daarnaast bleek de toegang niet voorbehouden aan werkgevers: via de knop 'werkgever' kon elke bezoeker van de website de CV's inzien. Hiervoor was geen authenticatie nodig.

Tenminste één werkzoekende heeft hierover een klacht ingediend bij het UWV. Toen de organisatie geen verandering bracht in dit systeem, is dezelfde klacht ingediend bij de Nationale Ombudsman. Daarop heeft het UWV haar werkwijze aangepast. Uit het Rapport van de Nationale Ombudsman over deze zaak blijkt dat de klacht volgens de juiste klachtprocedure werd afgehandeld, maar dat de inhoudelijke reactie onbevredigend was. Het UWV veronderstelde ten onrechte dat personalia in 'openbare CV's' alleen zichtbaar zouden zijn nadat de werkgever was ingelogd. Daarnaast werd ten onrechte verondersteld dat door bij de optie 'anoniem' alleen de personalia te anonimiseren, het CV niet te herleiden was tot één persoon.

2.3.2 Beleidsdoelstelling en -uitvoering

De doelstellingen van het UWV zijn het bevorderen van de arbeidsparticipatie door het verzorgen van arbeidsbemiddeling en re-integratie. Uit het UWV Jaarplan 2012 blijkt dat het UWV dat vooral digitaal wil faciliteren omdat dit kosten bespaart. Daarnaast wordt de verdere ontwikkeling van digitale dienstverlening gezien als onderdeel van de bredere doelstelling voor klantgerichtheid en service. Benodigde gegevens kunnen immers snel worden geleverd, vaker worden gebruikt, en klanten

(burgers en bedrijven) hoeven hun gegevens maar één keer in te vullen. Wat betreft de digitale dienstverlening, staat in het UVW Jaarplan 2012 dat ICT-veiligheid en functionaliteit voorop staat. Privacy en gegevensbescherming worden niet expliciet genoemd.

De bovengenoemde doelstellingen worden onder meer verwezenlijkt via de website werk.nl. Daar komen werkgevers en werkzoekenden samen. De gegevens die werkgevers en werkzoekenden er plaatsen, kunnen door meerdere werkgevers en werknemers worden gebruikt. De beveiliging van de website liet in 2011 te wensen over omdat, zoals blijkt uit het rapport van de Nationale Ombudsman over deze zaak, de optie 'anoniem' geen anonimiteit garandeerde, en inloggen niet vereist was voor inzage in de geplaatste CV's.

Kader 2.7: Beleidsperspectief casus 'CV's werkzoekenden openbaar'.

Beleid in beeld
"Voor een goede vervulling van de publiekrechtelijke taak van het UWV is het noodzakelijk dat werkzoekenden en werkgevers elkaar kunnen vinden op een laagdrempelige manier. Dat betekent, naar de mening van het UWV, dat werkgevers zonder veel moeite te hoeven doen moeten kunnen zoeken in CV's van werkzoekenden en dat het UWV werkgevers hiervoor geen kosten in rekening brengt. Om de privacy van de werkzoekende te waarborgen kan deze kiezen tussen twee opties. Een commerciële site als Monsterboard.nl werkt op vergelijkbare wijze met vertrouwelijke en openbare CV's. Wel moet de werkgever betalen voor de diensten van dergelijke vacaturesites. Dat wil het UWV, als publieke organisatie, nu juist niet". (Nationale Ombudsman, 2011/191).

2.3.3 Gevolgen voor de privacy van burgers

Met de optie 'anoniem' wekte het UVW de schijn dat de gegevens ook daadwerkelijk geanonimiseerd waren. Dit was echter niet zonder meer het geval, omdat ook met het ontbreken van de personalia er voldoende gegevens in een CV kunnen staan om daarmee een enkele persoon te kunnen identificeren. Omdat met de optie 'anoniem' de schijn van privacybescherming werd gewekt, zullen veel gebruikers zich niet bewust zijn geweest van de openbaarheid van hun gegevens en de daarmee samenhangende risico's. Het UWV heeft dus in de oorspronkelijke opzet van het systeem niet de juiste, of op z'n minst onvolledige, informatie verstrekt waardoor werkzoekenden ongewild persoonlijke gegevens openbaar hebben gemaakt.

Aangezien het UWV het plaatsen van een CV op werk.nl niet beschouwt als ingangsvoorwaarde voor het verkrijgen van een WW-uitkering, worden de gegevens verwerkt op basis van toestemming. Probleem is dat deze toestemming volgens het UWV verkregen moet worden via de werkcoach, maar hier is in de praktijk niet altijd sprake van. Bovendien is toestemming op grond van de Wbp alleen geldig als deze op juiste informatie berust. Ook hiervan is geen sprake als een werkzoekende ervan uitgaat dat zijn gegevens bij de optie 'anoniem' ook echt anoniem zijn.

Daarnaast moet toestemming een uiting van vrije wil zijn. In het geval van werkzoekenden is het twijfelachtig of dit zo is. Hoewel het UWV het plaatsen van een CV niet beschouwt als ingangsvoorwaarde, is hiervan in de praktijk wel sprake

doordat inschrijving bij het UWV WERKbedrijf verplicht is. Na het invullen van het CV binnen de Werkmap (onderdeel van het UWV WERKbedrijf) wordt een CV automatisch gekopieerd naar werk.nl

Zowel de hoeveelheid gegevens die openbaar gemaakt wordt, als de kring van personen waaraan deze gegevens geopenbaard worden, staan niet in verhouding tot het doel arbeidsbemiddeling. Alternatieve opties, zoals beperkte inzage, zijn eenvoudig te verwezenlijken en moeten aangewend worden om misbruik van (gevoelige) persoonsgegevens door derden te voorkomen.

2.3.4 Waarborgen van overheidszijde

Na de klachten tegen het oorspronkelijke systeem, waarbij de waarborgen van overheidszijde onvoldoende bleken, is het systeem aangepast. Tegenwoordig is voor een beperkte inzage van de CV's inloggen met DigiD verplicht. Verder is, wanneer wordt gekozen voor de optie 'anoniem', de anonimiteit beter gegarandeerd. Werkgevers kunnen pas meer gegevens inzien wanneer zij een concrete vacature open hebben staan. Tevens is de informatievoorziening aan de zijde van het UWV verbeterd: inschrijvers worden nu beter op de hoogte gebracht van de privacyaspecten omtrent de verwerking van hun gegevens die ze achterlaten op de website.

Het UWV is, als verwerker van persoonsgegevens, verplicht zorg te dragen voor een goede beveiliging van persoonsgegevens. In dat kader heeft het UWV, onder meer naar aanleiding van de hierboven geschetste casus, het initiatief genomen een expertisecentrum op het gebied van informatiebeveiliging en privacybescherming op te richten. Naast het UWV, zijn de Belastingdienst, de Sociale Verzekeringsbank en de Dienst Uitvoering Onderwijs daarbij aangesloten. Dit expertisecentrum, het Centrum Informatiebeveiliging en Privacybescherming (CIP), zal de aangesloten ZBO's ondersteunen bij ICT-beleid en vraagstukken. Het CIP gaat zich bezighouden met alle beveiligingsincidenten die zich bij de aangesloten organisaties voordoen en zal noodscenario's en herstelplannen uitwerken voor dergelijke incidenten. Ook zal het CIP een aantal beveiligingshulpmiddelen regelen en trainingen verzorgen.

2.3.5 Mogelijke oplossingen

Het online plaatsen van vergunningen kan met meer waarborgen omkleed worden door bepaalde gegevens niet online inzichtelijk te maken. Ook kan de groep van personen die toegang heeft tot deze gegevens beperkt worden. Het eerste punt kan geadresseerd worden door te werken met gestandaardiseerde CV's waarbij werkzoekenden er op gewezen worden welke persoonsgegevens zij wel, en welke gegevens zij niet op moeten nemen in het CV dat openbaar gemaakt wordt.

Het punt van toegang kan door middel van authenticatie (bijvoorbeeld DigiD) en autorisatie gereguleerd worden. Zo kan het systeem dusdanig worden ingericht dat een werkgever uit de telecomsector geen CV's kan inzien van mensen die een functie zoeken in de zorg. De *ingangsvoorwaarden* voor toegang tot gegevens kunnen aldus verschillen per groep personen. Een ingangsvoorwaarde kan bijvoorbeeld zijn dat alleen die werkgevers die een openstaande vacature hebben toegang krijgen tot de CV's van werkzoekenden, en dan alleen die CV's die aansluiten op de openstaande vacature. Geredeneerd vanuit het principe van *privacy by default* zou alleen toegang tot CV's verkregen mogen worden als

vaststaat dat iemand hiertoe een gerechtvaardigd belang heeft. Vanuit dit perspectief moeten CV's ook standaard op 'anoniem' staan, waarbij duidelijk wordt gecommuniceerd aan de gebruiker dat pas openbaar gemaakt wordt als de gebruiker hiertoe zelf een handeling verricht. Ingebouwde controlemechanismen, zoals het loggen van iedereen die bestanden inziet, kunnen bijdragen aan de daadwerkelijke naleving van toegang beperkende maatregelen.

De beschreven casus maakt ook duidelijk dat het privacybeleid niet alleen voor werkzoekenden en werkgevers duidelijk moet zijn, maar ook voor de betrokken medewerkers, zoals de werkcoach. Aangezien toestemming verkregen moet worden via de werkcoach, moet juist deze zich bewust zijn van het belang van het vragen van toestemming en van de noodzaak om in dit verband correcte en volledige informatie te verschaffen. Het CIP kan hierbij een belangrijke rol spelen, zowel op het niveau van het opstellen van een centraal beleid, maar ook door bij te dragen aan de daadwerkelijke praktisch implementatie van dit beleid.

Tot slot geeft deze casus een mooi voorbeeld van hoe de praktische invulling van het proces in conflict kan komen met het privacybeleid. Door de koppeling met de Werkmap werd het plaatsen van een CV een onbedoelde ingangsvoorwaarde voor het kunnen verkrijgen van een uitkering.

3 Schending van de Wet bescherming persoonsgegevens (Wbp)

De tweede categorie privacy schendingen omvat gevallen waarin de Wet bescherming persoonsgegevens wordt geschonden om een beleidsdoel te realiseren. Hoewel ook in de andere categorieën privacy schending sprake kan zijn van schending van de Wbp, gaat het in dit geval doorgaans om gevallen waarin gegevens zijn verzameld in strijd met het beginsel van *doelbinding*. Doelbinding wil zeggen dat alleen die gegevens verwerkt mogen worden die nodig zijn voor het oorspronkelijke doel van de verwerking. Deze cases beogen dus meer inzicht te geven in hoe het niet naleven van het beginsel van doelbinding negatieve gevolgen met zich brengt voor de privacy van de burger. Daarnaast is er in de cases niet alleen sprake van de verwerking van 'gewone' persoonsgegevens, zoals NAW-gegevens, maar ook van de verwerking van gevoelige persoonsgegevens zoals etniciteit en medische gegevens. Voor gevoelige persoonsgegevens gelden strengere regels conform de Wet bescherming persoonsgegevens. De drie cases die worden beschreven, zijn, samen met het beleidsdoel en de schade voor burgers, weergegeven in tabel 3.1.

Tabel 3.1: Cases, het beleidsdoel en de schade die burgers hebben ondervonden.

Case study	Beleidsdoel	Schade voor burgers
Automatische nummerplaatherkenning leaserijders	Controle en handhaving vrijstelling inkomsten-belasting leaseauto	Gevoel van verdachtmaking door de overheid.
Registratie etniciteit van probleemjongeren	Hulpverlening aan probleemjongeren	Blootstelling aan het risico op discriminatie of stigmatisering
Declaratie psychiatrische behandelingen	Vereenvoudigen facturatie	Blootstelling aan het risico op discriminatie of stigmatisering

3.1 Automatische nummerplaatherkenning leaserijders

Kader 3.1: Perspectief van de burger casus 'Automatische nummerplaatherkenning leaserijders'.

Burger in beeld
Philip Ruijs (hoofdredacteur 'Belastingzaken'): "Mijn vrouw werd gebeld door een medewerker van de Belastingdienst. Zij wilde een afspraak maken voor een telefonisch overleg over het privégebruik van haar leaseauto. Specifiek haalde ze enkele ritten aan, zoals een zondag om 9.00 uur in de buurt van de Efteling, met het verzoek of mijn vrouw bij het vervolggesprek aan zou kunnen geven waarom zij op dat moment met haar auto daar was. In het vervolggesprek werd zij gewezen op de limiet van 500 km voor privégebruik van de leaseauto. De confrontatie met exacte gegevens over waar zij was op welk tijdstip vonden wij erg intimiderend. Mijn vrouw blijft netjes onder de 500 km-grens, houdt een keurige administratie bij

en maakt gebruik van een vrijstelling waar zij wettelijk gezien recht op heeft. Waarom wordt zij dan zo strikt in de gaten gehouden? Ze is toch geen verdachte?"

3.1.1 Aanleiding en probleembeschrijving

Automatische nummerplaatherkenning (Automatic Number Plate Recognition, ANPR) is de technologie waarmee voertuigen door camera's automatisch herkend kunnen worden op basis van hun kenteken. Automatische nummerplaatherkenning is oorspronkelijk ontwikkeld voor het handhaven van wet- en regelgeving. Voorbeelden hiervan zijn het controleren of auto's verzekerd zijn en of er voor voertuigen motorrijtuigenbelasting is voldaan. Er wordt echter ook geëxperimenteerd met nieuwe toepassingen waarbij de focus op dienstverlening (informatievoorziening) ligt om uiteindelijk handhavingsachterstanden weg te werken. Eén van die toepassingen is het gebruik van ANPR-gegevens door de Belastingdienst om te controleren of leaserijders, die zeggen dat ze privé geen gebruik van de leaseauto maken, dat ook werkelijk niet doen. De specifieke werkwijze, waarbij burgers individueel telefonisch benaderd worden met uitleg omtrent rechten en plichten, lijkt gepresenteerd te zijn als dienstverlening. Feitelijk draait het echter om controle en handhaving.

3.1.2 Beleidsdoelstelling en -uitvoering

Jan de Groot, senior beleidsmedewerker bij het Ministerie van Financiën zegt dat de Belastingdienst van mening is dat je een overtreding beter kunt voorkomen dan bestraffen. In dat opzicht is het van belang om burgers te doen beseffen dat ze het belastingvoordeel van vaak duizenden euro's per jaar verliezen als ze een onjuiste rittenregistratie hanteren. Wanneer er door de Belastingdienst, op basis van ANPR, wordt vermoed dat een leaseauto voor privédoeleinden wordt gebruikt, kunnen bestuurders tijdig gewezen worden op de wettelijke limiet voor privégebruik (500 km per jaar) en het juist invullen van hun belastingaangifte. Wanneer meer dan 500 km in een jaar wordt gereden voor privédoeleinden vindt namelijk een bijtelling op het inkomen plaats. Deze bijtelling is een percentage van de waarde van de auto dat wordt behandeld als extra inkomen. Hierover moet dus belasting worden betaald. Het aantal auto's waarvoor een bijtelling wordt toegepast is de laatste jaren toegenomen, wat vele miljoenen extra belastingopbrengst heeft opgeleverd. Het gebruik van ANPR heeft daaraan bijgedragen.

Kader 3.2: Beleidsperspectief casus 'Automatische nummerplaatherkenning leaserijders'.

Beleid in beeld

Jan de Groot, senior beleidsmedewerker bij het Directoraat-Generaal Belastingdienst van het Ministerie van Financiën: "We hebben te maken met een grote handhavingsachterstand op het gebied van controle op bijtellingen voor leaseauto's. Om dit probleem op te lossen kunnen we ons zo dienstverlenend mogelijk opstellen richting burgers en hen tijdig wijzen op hun rechten en plichten, met name voor het bijhouden van een goede rittenregistratie. Voorkomen is immers beter dan bestraffen. Een telefoongesprek is daarvoor volgens ons een goede manier, omdat het persoonlijk is en gelegenheid geeft tot het verschaffen van extra informatie wanneer burgers daar behoefte aan hebben. Om in het gesprek concreet te controleren of iemand de administratie op orde heeft, kunnen we specifieke ritten aanhalen die waarschijnlijk op privégebruik wijzen. Die ritten kunnen we identificeren op grond van ANPR-gegevens."

Door de Belastingdienst wordt gezegd dat de gehanteerde werkwijze is bedoeld om het besef te laten doordringen dat een juiste rittenregistratie noodzakelijk is en dat anders het fiscale voordeel kan vervallen. Burgers die een verklaring hadden ondertekend binnen de 500 kilometer te blijven en kort daarna op een ongebruikelijke tijd (weekend) of plek werden aangetroffen via ANPR, werden gebeld met de vraag of die rit zakelijk was. De Groot: “Als een voertuig van een vertegenwoordiger die in Groningen woont op zondag wordt gezien bij de Efteling is dat min of meer ‘verdacht’. De Belastingdienst heeft door deze actie laten zien dat belastingontduiking eenvoudig kan worden ontdekt en laat dat ook merken. Gevolg is dat deze belastingplichtige het waarschijnlijk zal laten om teveel privékilometers te gaan maken. Hij komt er – bij wijze van spreken – met een waarschuwing van af. Ik denk dat hij blij is, want een naheffing had ook gekund.”

3.1.3 Gevolgen voor de privacy van burgers

Bestuurders van auto’s zijn, mogelijk onterecht, individueel benaderd en hun persoonsgegevens zijn verwerkt in strijd met de principes van proportionaliteit en subsidiariteit. Burgers krijgen de indruk dat wordt gehandeld op basis van een vermoeden van schuld, zonder dat daar voldoende grond voor is. Ruijs en zijn vrouw ervoeren de werkwijze als ‘intimiderend’. Het gevoel ontstond dat wanneer je gebruik maakt van een regeling waar je wettelijk recht op hebt, je automatisch een verdachte bent. Leaserijders houden een kilometerregistratie bij die ze moeten overleggen aan de Belastingdienst. Op het moment dat deze registratie wordt ingeleverd en de Belastingdienst heeft een vermoeden dat er mogelijk gefraudeerd is, dan kunnen alsnog de ANPR-gegevens vergeleken worden met de ingeleverde kilometerregistratie. Het vooraf confronteren is dus niet *noodzakelijk* voor het beleidsdoel. Wel is het mogelijk dat deze confrontatie leidt tot minder misbruik en dus een betere uitvoering van het beleidsdoel als resultaat heeft dan controle achteraf. Burgers krijgen echter vanwege de individuele benadering het gevoel onderwerp van een opsporingsonderzoek te zijn.

De Belastingdienst meent dat wanneer de burger in kwestie een juiste verklaring kan geven voor het feit dat die auto daar op dat moment stond, dat natuurlijk ook goed is. Een juiste verklaring is in dit geval dat de auto zakelijk werd gebruikt of dat de gebruiker met deze rit onder de 500 km per jaar bleef. De Groot betoogt dat mensen die profiteren van een ruime faciliteit het over het algemeen niet vreemd vinden dat de overheid daar ook toezicht op uitoefent: “Een telefoontje is in eerste instantie misschien wel wat confronterend, maar dat is een blauwe brief waarin om tekst en uitleg wordt gevraagd ook, vooral als die wordt gevolgd door een naheffing met boete die al gauw tot wel 5.000 euro kan oplopen. Afhankelijk van de waarde van de auto kan het bedrag nog aanzienlijk hoger worden. Het doel is dat burgers zich aan de regels blijven of gaan houden, daar is het toezicht op gericht.”

Het intimiderende karakter van nauwkeurig in de gaten worden gehouden wordt dus als erg vervelend ervaren. Daarnaast is de vervaging van de grens tussen controle en opsporing een aandachtspunt. Hoewel de Belastingdienst het telefoontje een vorm van dienstverlening noemt, is het eigenlijk een vorm van handhaving.

3.1.4 Waarborgen van overheidszijde

Ten aanzien van de fiscaliteit staan voor burgers alle waarborgen (bezwaar en beroep) open om zich te verzetten tegen naheffingsaanslagen. Dit kan echter niet aangemerkt worden als een waarborg op het gebied van privacy. Het verschaft wel

de mogelijkheid tot correctie van onjuiste gegevens zoals die door de Belastingdienst zijn verwerkt, maar is geen waarborg tegen een ongerechtvaardigde verwerking van de gegevens.

3.1.5 Mogelijke oplossingen

Een mogelijkheid om de procedure te verbeteren, is om de koppeling van ANPR-gegevens aan direct identificerende gegevens alleen te laten plaatsvinden bij burgers die na afloop van het fiscale jaar nog steeds zeggen binnen de vrijstelling te zijn gebleven. Indien dan op basis van de ANPR-gegevens een vermoeden ontstaat dat dit onjuist is, kan actie ondernomen worden. De ANPR-gegevens worden dan wel gedurende het jaar verzameld, maar worden niet aan elke leaserijder gekoppeld – alleen aan diegenen die zeggen binnen de vrijstelling te zijn gebleven. Hierdoor wordt het gevoel van intimidatie en controle vooral, hetgeen ervaren werd als een aantasting van privacy, voorkomen. Voor controle achteraf geldt sterker dat de burger dit mag verwachten. De vraag is echter of misbruik in dit geval even goed wordt opgespoord als bij de confrontatie gedurende het jaar. Hierbij geldt overigens wel dat de burger over dergelijke controles (vooraf en achteraf) deugdelijk geïnformeerd moet worden. Met betrekking tot het doel van informatievoorziening en mensen wijzen op hun rechten en plichten kan echter ook volstaan worden met algemene voorlichting, bijvoorbeeld via TV-spotjes of advertenties in kranten.

3.2 Registratie etniciteit probleemjongeren

Kader 3.3: Perspectief van de burger casus ‘Registratie etniciteit probleemjongeren’.

Burger in beeld

Het College Bescherming Persoonsgegevens (CBP) oordeelde in 2011 dat de Rotterdamse deelgemeente Charlois de Wet bescherming persoonsgegevens (Wbp) overtrad door de etniciteit van probleemjongeren te registreren. De deelgemeente registreerde deze etniciteit om probleemjongeren, die vaak een andere culturele achtergrond dan de Nederlandse hebben, beter hulp te kunnen bieden. Door politici werd dit echter gezien als onacceptabel en zij kregen gelijk van het CBP. Hulpverleners in Charlois registreren nu niet langer de etniciteit van probleemjongeren en Charlois moet de geregistreerde gegevens vernietigen. Volgens Yvo Rodermans, fractiemedewerker van GroenLinks in Rotterdam, schiet dit systeem zijn doel voorbij. Betrokken hulpverleners kennen de jongere en zijn of haar problematiek, dus het is volgens Rodermans onnodig om de etniciteit ook nog eens te registreren, met mogelijk stigmatiserende gevolgen.

3.2.1 Aanleiding en probleembeschrijving

Rond de eeuwwisseling werd er in Charlois (net als in een aantal andere Rotterdamse deelgemeenten) geconstateerd dat er veel jongeren op straat rondzwierven. Hoewel zij hulp nodig hadden, werden zij vaak niet bereikt. Om te zorgen dat elke jongere die daar recht op heeft passende hulp krijgt en te voorkomen dat er op deze manier jongeren ‘tussen wal en schip’ belanden, heeft de deelgemeente Charlois de Deelgemeentelijke Organisatie Sluitende Aanpak (DOSA) ingericht. DOSA richt zich op de samenwerking tussen verschillende instanties bij de aanpak van probleemjongeren. Wanneer een jongere alleen in aanraking is met bijvoorbeeld jeugdzorg of de politie komen zij niet in DOSA

terecht. Pas wanneer een jongere bij tenminste drie verschillende hulpverleners bekend is, komt hij of zij in het systeem.

3.2.2 Beleidsdoelstellingen en -uitvoering

In het DOSA-systeem komen de verschillende hulpverleners (zoals jeugdzorg, politie, leerplichtambtenaren) bij elkaar en bespreken ze de jongeren één voor één om zo tot een passend hulpaanbod te komen. Zo kan het voorkomen dat iemand die vaak spijbelt ook een aantal keer in aanraking is gekomen met de politie vanwege winkeldiefstal. Afhankelijk van de aard van de informatie en de verwachte effectiviteit van het ingrijpen, kan worden besloten wie er werk maakt van de hulpverlening: de politie of de school. Op deze manier zijn de afgelopen jaren zo'n 600 jongeren per jaar besproken en hun gegevens zijn vastgelegd in de DOSA-registratie. Volgens de deelgemeente Charlois wordt aan deze jongeren per brief mede gedeeld welke gegevens er van hen werden geregistreerd.

Behalve de feiten over de problemen van de jongere, was een van de zaken die hierbij werd geregistreerd de etniciteit van de jongere. Het doel hiervan is om beter hulp te kunnen bieden en een gerichtere aanpak te kiezen die aansluit bij de culturele achtergrond van de jongere. Hierbij werd op basis van gegevens in de Gemeentelijke Basisregistratie (GBA) een inschatting gemaakt van de etniciteit op basis van de geboorteplaats van de ouders. De GBA bevat geen informatie over de etniciteit, maar houdt wel bij waar iemand geboren is en waar zijn of haar ouders geboren zijn. Omdat er persoonsgegevens worden verwerkt, is deze werkwijze vanwege de verwerking van persoonsgegevens in 2006 aangemeld bij het CBP. Volgens de deelgemeente heeft er geen enkele jongere bezwaar gemaakt naar aanleiding van de etnische registratie.

Kader 3.4: Beleidsperspectief casus 'Registratie etniciteit probleemjongeren'.

Beleid in beeld

De jongeren die in DOSA terecht komen, hebben een meervoudige hulpvraag en zijn daardoor vaak kwetsbaar. Om deze jongeren zo goed mogelijk te kunnen helpen, is het van belang dat er zo veel mogelijk informatie over hen bekend is, vertelt Herman Gerrits, locosecretaris van de deelgemeente Charlois. Op deze manier kunnen de verschillende betrokken hulpverleners het beste inschatten hoe zij deze jongeren kunnen helpen. Voor iemand die zowel bij Bureau Jeugdzorg bekend is omdat hij of zij verwaarloosd wordt, vaak spijbelt en dus bekend is bij een leerplichtambtenaar en ook onlangs in aanraking is gekomen met de politie vanwege een winkeldiefstal, kan bijvoorbeeld worden bepaald dat de school eerst in actie zal komen om te zorgen dat de jongere de school niet vroegtijdig verlaat. In een ander geval kan besloten worden dat Bureau Jeugdzorg ingrijpt. Om deze inschatting zo goed mogelijk te maken, is het volgens Gerrits ook van belang dat de culturele achtergrond van iemand bekend is. Er spelen in Antilliaanse gezinnen vaak andere problemen dan in Turkse gezinnen. Toch legt Charlois zich neer bij de uitspraak van het CBP. In NRC van 4 februari 2011 zegt een woordvoerder van de deelgemeente: "We deden het met de beste bedoelingen om jongeren met een achterstand te helpen, maar we willen niet iets doen wat tegen de wet is".

3.2.3 Gevolgen voor de privacy van burgers

In 2010 heeft het College Bescherming Persoonsgegevens (CBP) bepaald dat etnische registratie in strijd is met de Wbp. Hierin is vastgelegd dat de verwerking

van bijzondere persoonsgegevens, waaronder gegevens betreffende ras/etniciteit, verboden is. De deelgemeente Charlois is hiertegen in beroep gegaan omdat zij in het succes van de werkwijze geloofde en deze graag wilde voortzetten. Uiteindelijk heeft het CBP in 2011 definitief besloten dat het niet is toegestaan de etniciteit van de probleemjongeren te registreren. Op last van een dwangsom is Charlois toen gestopt met de registratie. In mei 2012 heeft ook de rechter het beroep dat Charlois had aangespannen tegen het CBP ongegrond verklaard. Dit heeft er toe geleid dat het niet langer mogelijk is voor DOSA-medewerkers om in de GBA te zien wat de geboorteplaats van de ouders is. Ook moeten geregistreerde gegevens vernietigd worden.

Daarnaast oordeelt het CBP dat voor de doelgroep en de werkwijze van DOSA ras/etniciteit geen onderscheidend criterium is. Dit is ook waar politici op wezen die in de Rotterdamse gemeenteraad bezwaar hebben gemaakt tegen de aanpak in Charlois. Volgens hen moet worden geconstateerd dat het bij de problemen van jongeren zelden gaat om een probleem dat voortkomt uit het ras of de etniciteit van de jongere. In de praktijk gaat het om problemen als schooluitval, verslaving of verwaarlozing. Het is lastig deze te herleiden tot een bepaalde etniciteit. Het vastleggen van de etniciteit kan echter mogelijk later tot stigmatisering leiden wanneer deze geregistreerd blijft. Bovendien deed de deelgemeente een interpretatieslag op de etniciteit, die mogelijk onjuist is. De etniciteit werd bepaald door naar de geboorteplaats van de ouders te kijken, wat vaak, maar niet altijd, leidt tot een correcte interpretatie.

3.2.4 Waarborgen van overheidszijde

De privacy werd gewaarborgd door gegevensbescherming door de deelgemeente en de geheimhoudplicht en professionaliteit van de hulpverleners. Naast technische beveiligingsmaatregelen d.m.v. wachtwoord en pincode is er organisatorische controle ingericht. Dit betekent dat de gegevens alleen toegankelijk zijn voor de DOSA-regisseur en dat de gegevens van de jongere alleen worden gedeeld tijdens het DOSA-overleg met de jeugdcoördinator van politie, de voorpostfunctionaris van Bureau Jeugdzorg, de leerplichtambtenaar, de coördinator Centrum voor Jeugd en Gezin en een medewerker van het jongerenloket.

De betrokken hulpverleners hadden een geheimhoudplicht. Zij mochten dus niet aan derden kenbaar maken hoe de situatie van hun cliënten (inclusief etniciteit) eruit ziet. Hulpverleners worden opgeleid om jongeren professioneel bij te staan. Zij zullen doorgaans dus nooit alleen naar etniciteit kijken, en zij zijn opgeleid om juist alle signalen mee te nemen in hun oordeel. Daarnaast wordt bij de aanmelding in DOSA de betreffende jongere (en bij een jongere die jonger is dan 16 jaar ook de wettelijke vertegenwoordiger) per brief geïnformeerd over de aanmelding bij DOSA. Hierin staat dat indien er vragen zijn over de registratie, er contact op genomen kan worden met de DOSA-regisseur.

3.2.5 Mogelijke oplossingen

In dit geval werd aan de voorwaarden van dataverwerking, zoals doelbinding en dataminimalisatie voldaan. Er was echter sprake van de onnodige verwerking van bijzondere persoonsgegevens, in dit geval t.a.v. de etniciteit. De oplossingsrichting die gekozen kan worden, is een andere uitvoering van het beleid om probleemjongeren te helpen. De problemen die jongeren ondervinden komen doorgaans niet voort uit hun etniciteit, maar zijn bijvoorbeeld het gevolg van

verwaarlozing of spijbelen. Er zijn echter wel problemen die vaker bij een bepaalde etniciteit voorkomen (zoals gedwongen huwelijken). Net als bij de vorige casus, kan daarom de vraag gesteld worden of het registreren van etniciteit in sommige gevallen wel betere hulpverlening kan bieden aan de jongeren. De beleidsuitvoering is bij het afschaffen van de registratie mogelijk minder effectief dan ervoor. Vanwege het zwaarder wegende belang van privacy is er in dit geval echter voor gekozen dat de registratie werd afgeschaft.

3.3 Declaratie psychiatrische behandelingen

Kader 3.5: Perspectief van de burger casus 'Declaratie psychiatrische behandelingen'.

Burger in beeld
"Zodra hij lucht kreeg van het systeem, lichtte Mengelberg zijn patiënten in. De meeste schrokken toen ze hoorden welke persoonlijke informatie bij zorgverzekeraar en staat terechtkomt. Wie het kon, opperde zijn behandeling uit eigen zak te gaan betalen. Maar Mengelberg kwam voor een tweede verrassing te staan: ook patiënten die uit eigen middelen betalen moet hij registreren". Mengelberg: "De meeste mensen weten dat niet (…) en als ze dat horen, schrikken ze. Ik weet uit betrouwbare bron dat topambtenaren die zelf in therapie gaan uit het DBC-systeem proberen te blijven. Een collega van mij heeft een directeur van een zorgverzekeraar in behandeling die na elke sessie geld op tafel legt om aan de declaraties te ontkomen. Nergens kun je nog hoogst privacygevoelige informatie delen met de zekerheid dat het binnenskamers blijft. Nederland begint totalitaire trekken te vertonen." (Lo Galbo, 2009)

3.3.1 Aanleiding en probleembeschrijving

Per 1 januari 2008 is een nieuw declaratiesysteem voor de geestelijke gezondheidszorg ingevoerd. Dit systeem vereist dat zorgaanbieders informatie over diagnose-behandelcombinaties (DBC's) over hun patiënten op de facturen aan zorgverzekeraars zetten, om zo het declareren te vereenvoudigen. DBC-informatie bestaat uit codes, die elk voor een bepaalde diagnose c.q. behandeling staan. Hierdoor kunnen declaraties digitaal verwerkt worden. Daarnaast gaat DBC-informatie gepseudonimiseerd naar het DBC-informatiesysteem (DIS), een centrale databank waar die informatie gebruikt kan worden voor wetenschappelijk onderzoek. Dit aspect wordt in dit rapport vanwege het minder ingrijpende karakter voor de privacy buiten beschouwing gelaten.

3.3.2 Beleidsdoelstellingen en -uitvoering

De voornaamste aanleiding voor de invoering van een nieuw declaratiesysteem was het probleem van 'overdekking' bij zorgverzekeraars. Uit onderzoek uitgevoerd in opdracht van Zorgverzekeraars Nederland bleek dat er 566 miljoen te veel aan DBC's gedeclareerd werd in 2005. De oorzaak leek gelegen in verschillende interpretatiemogelijkheden van de toenmalige DBC-bepalingen; er werd op verschillende wijzen gedeclareerd, doch steeds volgens regels. Het nieuwe systeem moest voor uniformiteit zorgen, waardoor ook controle mogelijk werd en overdekking zou worden voorkomen.

Daarnaast was er nog een aantal andere redenen voor invoering van het nieuwe systeem. Zo zou het gemakkelijker worden om de prijzen van zorgaanbieders te vergelijken, wat moest zorgen voor een transparantere zorgmarkt. Ook zou dit

concurrentie bevorderen en leiden tot een betere keuzepositie van de consument. Ook kunnen zorgverzekeraars door het nieuwe systeem de zorginkoop beter regelen.

Kader 3.6: Beleidsperspectief casus 'Declaratie psychiatrische behandelingen'.

Beleid in beeld
"Het vermelden van een vorm van diagnose-informatie op de declaratie is belangrijk voor patiënten en consumenten, vindt de Nederlandse Zorgautoriteit (NZa), omdat alleen zo inzichtelijk is waarvoor een zorgaanbieder declareert. Zo weten consumenten en verzekeraars welke zorg zij voor welke prijs geleverd krijgen en kunnen zij dit controleren. De NZa vindt de privacy van consumenten een zwaarwegend belang en vindt die privacy hier door tal van maatregelen voldoende beschermd. Artsen in de GGZ vermelden namelijk slechts de hoofddiagnosegroep op de declaratie, bijvoorbeeld 'angststoornis'. Individuele details van de behandeling kennen alleen de arts en patiënt. Bovendien hebben zorgverzekeraars de privacybelangen van verzekerden in een nieuwe 'Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars' gewaarborgd. Overigens komt het zelden voor dat medewerkers van de verzekeraar de informatie uit de declaratie zien: 95% wordt elektronisch verwerkt, de overige 5% komt onder ogen van medewerkers met een strikte geheimhoudingsplicht" (NZa 2011).

In het in 2008 ingevoerde declaratiesysteem zetten zorgaanbieders DBC-informatie over hun patiënten door middel van codes op hun facturen aan zorgverzekeraars. Er zijn codes die de diagnose aanduiden, bijvoorbeeld aandachtstekort- en gedragsstoornissen; pervasieve ontwikkelingsstoornissen; dementie, enz. Feitelijk vertegenwoordigen deze codes, in combinatie met de overige persoonsgegevens die naar de zorgverzekeraar worden gestuurd, zeer gevoelige gegevens over specifieke personen. Behandelaren moeten DBC-informatie ook verstrekken ten aanzien van al hun patiënten, ook diegenen die de kosten voor de behandeling zelf betalen. De reden hiervoor is dat NZa er vanuit gaat dat vanwege het bestaan van een verplichte zorgverzekering, iedereen een vergoeding voor zorgkosten kan en wil ontvangen van de zorgverzekeraar.

3.3.3 Gevolgen voor de privacy van burgers

Kader 3.7: Perspectief van de psychiater casus 'Declaratie psychiatrische behandelingen'.

Psychiater in beeld
"Privacy is niet alleen een ethisch principe, maar ook een instrument. Effectieve psychotherapie kan niet bedreven worden als er een breuk is in de vertrouwensrelatie. Het gaat er om samen gevoelens, emoties en motieven te onderzoeken die mensen niet met anderen durven te delen. De privacy van een patiënt is fundamenteel." (Psychiater M. Chayes, Vrij Nederland 2009)

Het probleem van het DBC-declaratiesysteem was dat zeer gevoelige gegevens terechtkomen bij (invloedrijke) derde partijen, waaronder het Ministerie van VWS en zorgverzekeraars. Deze gevoelige informatie kan bij de zorgverzekeraars worden ingezien door werknemers die niet onder het medisch beroepsgeheim vallen, terwijl dit bij het oude systeem niet het geval was. Vaak lopen mensen niet te koop met medische problemen, zeker wanneer deze van psychische aard zijn. Het openbaar worden van een dergelijke aandoening kan mensen het gevoel van stigmatisering

of achterstelling geven. Een situatie waarin dit bijvoorbeeld als problematisch ervaren kan worden is in de werksfeer, dan wel ten opzichte van de huidige werkgever, of in geval van solliciteren.

Ook binnen de relatie arts-patiënt kan het DBC-declaratiesysteem leiden tot vermindering van vertrouwen aan de zijde van de patiënt die het vertrouwen om vrijuit te kunnen praten kan verliezen. Hierdoor verkrijgt een arts mogelijk niet de juiste informatie om een diagnose te stellen, of besluit een patiënt wellicht zijn behandeling te stoppen.

3.3.4 Waarborgen van overheidszijde

Om tegemoet te komen aan privacybezwaren vermelden artsen in de geestelijke gezondheidszorg alleen de hoofddiagnosegroep op een declaratie, bijvoorbeeld ‘angststoornis’. Zo zijn details over een behandeling enkel bekend bij de arts en de patiënt. Ook is door zorgverzekeraars een 'Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars' opgesteld. Hierin staat met betrekking tot DBC-informatie dat deze alleen mag worden gebruikt door de zorgverzekeraars om de doelmatigheid en rechtmatigheid vast te stellen. Daarnaast stelt de NZa dat het systeem zo is ingericht dat het zelden voorkomt dat medewerkers van de verzekeraar de informatie uit de declaratie inzien.

Toch lijkt het College van Beroep voor het bedrijfsleven (CBb) in 2012, na een aantal eerdere vonnissen waarin de uitspraak verschilde, de discussie over DBC-informatie in het voordeel van privacy beslecht te hebben. Het CBb heeft namelijk bepaald dat patiënten de registratie van dergelijke informatie mogen weigeren. Daarbij heeft de rechter aangevoerd dat het belang van het medisch beroepsgeheim en privacy zwaarder weegt dan het economisch belang van het tegengaan van overdekking. Hierbij is mede van belang dat er alternatieven voor declaratie bestaan die minder inbreuk maken op de privacy.

3.3.5 Mogelijke oplossingen

Zoals uit de uitspraak van het CBb blijkt, moet bij de ontwikkeling van een systeem waarbij (gevoelige) persoonsgegevens worden verwerkt een goede afweging worden gemaakt tussen de beleidsdoelen enerzijds, en de privacybelangen anderzijds. Bij die afweging moet gekeken worden naar alternatieve mogelijkheden die minder inbreuk maken en of die inbreuk noodzakelijk is voor het verwezenlijken van het doel. Economische belangen wegen niet zondermeer zwaarder dan privacybelangen.

Een oplossing voor wat betreft de facturering is reeds aangedragen door het CBb: patiënten moet de optie gegeven worden om doorgifte van DBC-informatie aan de zorgverzekeraar te weigeren. Eigenlijk zou een omgekeerde variant, waarbij DBC-informatie alleen wordt doorgegeven na toestemming van de patiënt, de privacy nog beter waarborgen en beter aansluiten bij het beginsel van *privacy by default*.

4 Koppelen van gegevensbestanden

Het derde type privacy schendingen en –risico's dat wordt beschreven, gaat over de gevolgen van het koppelen van gegevensbestanden. Deze categorie gaat dus over de problematiek die is beschreven in het iOverheid rapport: gegevens die in de ene context zijn verzameld, hebben soms onvermoede gevolgen voor de privacy van burgers wanneer ze in een andere context worden hergebruikt. De drie cases die behandeld worden zijn, samen met het beleidsdoel en de schade voor de burger, weergegeven in tabel 4.1.

Tabel 4.1: Cases, het beleidsdoel en de schade die burgers hebben ondervonden.

Case study	Beleidsdoel	Schade voor burgers
Opsporing illegale bewoning en uitkeringsfraude	Opsporing en handhaving illegale bewoning en uitkeringsfraude	Gevoel van onbehagen door het binnendringen van de woning Intimidatie door onvoldoende informatie
Gegevenskoppeling voor gemeentelijke hulpverlening	Efficiënte en effectieve dienstverlening aan burgers	Nog geen schade, maar wel privacyrisico's, zoals het risico op misbruik door derden
Waarborgen in geval van identiteitsfraude	Efficiënte en effectieve uitvoering van beleid	Reisproblemen, strafrechtelijke antecedenten, inval in huis. Gebrek aan hulp bij het oplossen van de problemen

4.1 Opsporing illegale bewoning en uitkeringsfraude

Kader 4.1: Perspectief van de burger casus 'Opsporing illegale bewoning en uitkeringsfraude'.

Burger in beeld

"Enkele maanden geleden meldden zich twee heren van Stadstoezicht aan de deur die met klem toegang tot onze woning eisten. (…) Hun uitleg: ze hadden een melding binnen gekregen dat er zich illegale Polen zouden bevinden op ons adres. We weigerden (uiteraard) en vroegen ons af waar deze melding vandaan kwam. Hier werd geen antwoord op gegeven. De heren bleken in het bezit van onze namen en onze inschrijfgegevens via de gemeente. Toen wij bleven weigeren en mijn partner de stem ietwat verhief, werd ons medegedeeld; 'U vertoont agressief gedrag!' Belachelijk natuurlijk want dat was geenszins het geval. Eén van de heren liet ons weten dat de volgende keer andere mensen terug zouden komen om alsnog te zorgen dat er toegang tot de woning verleend zou worden. Want: er zou ook weleens sprake kunnen zijn van een illegale wietplantage als mensen de deur niet wilden openen" (Anarchiel, 2009).

4.1.1 Aanleiding en probleembeschrijving

Sinds 2005 worden huizen in risicowijken in Den Haag systematisch op illegaliteiten doorzocht, eerst onder de noemer van het 'Project Inhaalslag Handhaving', nu bekend als de 'Haagse Pandbrigade'. In Rotterdam is er een equivalent actief: het 'Rotterdams Interventieteam'. Hierbij wordt eerst digitaal onderzoek gedaan, op basis waarvan vervolgens overgegaan kan worden tot huisbezoeken. Deze twee projecten verschillen volgens de Haagse wethouder Marnix Norder in dit voortraject: "De kracht van onze aanpak is dat we álle panden controleren. We gaan met een stofkam door de wijk heen. De Rotterdamse interventieteams zijn vooral afhankelijk van meldingen" (Van der Bol, 2010).

Het beleid heeft echter zeer nadelige gevolgen gehad voor enkele getroffenen. Het is dan ook sterk bekritiseerd door privacyjuristen en belanghebbenden omdat het de kern van het privacyrecht raakt: onschendbaarheid van de woning. De uitvoering van het beleid is ook omstreden; vaak worden bewoners onder druk gezet om een pand te kunnen betreden. Daarbij wordt dan niet gezegd dat de bewoner niet verplicht is de brigade binnen te laten. Verder gaat het binnentreden vaak gepaard met groot machtsvertoon. Deze manier van fraudebestrijding was in 2010 dan ook een Big Brother award waard, omdat het beleid disproportioneel zou zijn in relatie tot de beleidsdoelen.

4.1.2 Beleidsdoelstellingen en -uitvoering

Volgens de website van de gemeente Den Haag werkt het project Haagse Pandbrigade, dat in 2009 is gestart, aan het verbeteren van de leefbaarheid en veiligheid in de kwetsbare wijken van Den Haag. Er wordt een vijftal taken onderscheiden:

- de opsporing en aanpak van onrechtmatige bewoning;
- controleren of de persoonsgegevens van de bewoners hetzelfde zijn als in de gemeentelijke basisadministratie;
- de aanpak van ernstige onderhoudsgebreken aan panden;
- controleren van cafés/restaurants en milieubedrijven op de geldende wet- en regelgeving;
- onderzoeken of mensen verkeerd gebruik maken van sociale voorzieningen zoals uitkeringen.

Het beleid om door middel van huisbezoeken uitkeringsfraude tegen te gaan, bestaat al langer. Wat nieuw is aan deze aanpak is dat de Haagse Pandbrigade tevens wordt ingezet voor de andere bovengenoemde doeleinden. De Rotterdamse Interventieteams handelen op basis van vergelijkbare beleidsdoelen.

Kader 4.2: Beleidsperspectief casus 'Opsporing illegale bewoning en uitkeringsfraude'

Beleid in beeld

De gemeente Den Haag beschrijft, op haar website, de werkwijze van de Haagse Pandbrigade als volgt: "Alle woningen in de wijken waar de Haagse Pandbrigade actief is, worden eerst digitaal gecontroleerd. Dit houdt in dat de gegevens die over een adres bekend zijn bij verschillende gemeentelijke diensten met elkaar worden vergeleken. Uit dit onderzoek kunnen zaken naar voren komen die niet kloppen. Bijvoorbeeld: wanneer er zes alleenstaanden staan ingeschreven in een woning kan er sprake zijn van illegale kamerverhuur. Als het nodig is, gaat de Haagse Pandbrigade naar de woning toe. De inspecteurs bellen aan, stellen zich voor en

leggen uit waarvoor ze komen. Vaak volgt dan een korte rondgang door het huis. Is alles in orde dan blijft het daar bij. Wanneer er onregelmatigheden worden aangetroffen kan er een juridische maatregel worden genomen. Dit houdt in dat de eigenaar/bewoner verplicht is de foute of gevaarlijke activiteit te stoppen. Gebeurt dit niet, dan kan de eigenaar/bewoner een dwangsom opgelegd krijgen Bij gevaarlijke situaties kunnen de medewerkers van de Pandbrigade de woning ook sluiten en verzegelen. Niemand mag de woning dan meer betreden."
Leonard Kok, Algemeen Directeur Stedelijke Ontwikkeling bij Gemeente Den Haag: "De aanleiding van de controle van uw woning is dat de gemeente Den Haag haar bewoners een veilige en leefbare woonomgeving wil bieden. In het bijzonder in 'kwetsbare' wijken, waar veel panden op illegale wijze worden gebruikt" (Tokmetzis, 2010).

4.1.3 Gevolgen voor de privacy van burgers

Voor de burger is zijn woning de plek bij uitstek waar hij zich veilig moet voelen. Hoewel veiligheid en handhaving legitieme gronden kunnen zijn om inbreuk te maken op de onschendbaarheid van de woning, moet een dergelijke inbreuk wel met de nodige waarborgen omkleed worden. Hierbij kan gewezen worden op een deugdelijke informatievoorziening, zowel vooraf als achteraf bij gerezen vragen, en de wijze waarop toegang verzocht wordt, zonder machtsvertoon en intimidatie. Indien hiervan geen sprake is kan een burger zich niet langer vrij en ongestoord voelen in zijn eigen huis. Schrijnend is het incident in 2010 waarbij een bewoner zijn eigen huis niet meer binnen kon na een bezoek van de Haagse Pandbrigade. De woning was opengebroken en voorzien van een nieuw slot terwijl de verdenkingen ten aanzien van het pand onjuist bleken te zijn. Toen de betrokkene om uitleg vroeg bij de gemeente en politie werd hij niet geholpen en moest hij zelf zijn woning openbreken.

4.1.4 Waarborgen van overheidszijde

Er zijn verschillende wettelijke vereisten gekoppeld aan respectievelijk het binnentreden van een woning, een huiszoeking en een huisbezoek. In het kader van strafrechtelijk onderzoek mag binnentreden zonder toestemming alleen op basis van een machtiging, die verstrekt wordt door een advocaat-generaal of een (hulp)officier van justitie. Een burgemeester mag een machtiging voor het binnentreden uitgeven voor niet-strafrechtelijke doeleinden.

Bij het binnentreden mag een pand niet worden doorzocht, maar mag men zoekend rondkijken. Kasten en laatjes mogen bijvoorbeeld niet worden opengemaakt. Dat mag wel wanneer er een huiszoekingsbevel is, maar die worden alleen verstrekt in het kader van opsporing van zware strafrechtelijke delicten. In dat geval mag de huiszoeking niet enkel zijn gebaseerd op een anonieme tip, maar moet er een gegronde verdenking zijn. Een huiszoeking mag ook plaatsvinden bij dringende noodzakelijkheid.

Een huisbezoek mag alleen volgen op vrijwillige toelating door de bewoner. Hier zullen overheden zich aan moeten houden. Zoals blijkt uit het rapport van de gemeentelijke ombudsman over de Rotterdamse Interventieteams worden mensen vaak niet gewezen op de vrijwillige aard van de huisbezoeken. In sommige gevallen oefenen interventieteams zelfs een dusdanige druk uit dat mensen niet durven te weigeren.

De gemeente Rotterdam hanteert een protocol bij huisbezoeken door het Rotterdamse Interventieteam, waarin onder meer staat dat niet meer dan drie personen het huisbezoek zullen afleggen, dat expliciet toestemming moet worden gevraagd voor het binnentreden, dat bij weigering of twijfel niet mag worden binnengetreden en dat bij een bezoek altijd duidelijk uitgelegd wordt waar het bezoek over gaat. De Gemeente Den Haag heeft geen protocol voor het afleggen van huisbezoeken, maar een werkinstructie. Daarin staat onder meer dat elk huisbezoek schriftelijk of mondeling vooraf wordt aangekondigd, dat de reden van het bezoek kenbaar wordt gemaakt, dat een bezoek doorgaans met twee personen wordt afgelegd, dat vooraf toestemming wordt gevraagd voor het binnentreden en dat gemeld moet worden dat weigering mogelijk is.

4.1.5 Mogelijke oplossingen

Het beleid omtrent interventieteams is reeds uitvoerig onderzocht, zoals door de gemeentelijke ombudsman Rotterdam in haar rapport ‘Kijken en bekeken worden’ (2011). Ook zijn een aantal incidenten met interventieteams behandeld door de Nationale Ombudsman. Hieruit blijkt dat met name op twee punten waarborgen ingebouwd, en daadwerkelijk nageleefd, moeten worden bij huiselijke interventies. In de eerste plaats gaat het om informatievoorziening. Betrokkenen moeten vooraf goed geïnformeerd worden. Bovendien moet een burger na een interventie niet alleen goed geïnformeerd worden, maar ook goed opgevangen worden door de betrokken instanties om de inbreuk te beperken. Zaken waarover de burger geïnformeerd moet worden, zijn o.a. de reden van het bezoek, de juridische gronden voor het bezoek en de hulp bij het herstel van eventueel toegebrachte schade.

In de tweede plaats moet de manier waarop de interventie wordt uitgevoerd dusdanig worden ingericht dat een burger zich niet geïntimideerd voelt. Dit komt bijvoorbeeld tot uiting in het aantal ambtenaren dat de huiszoeking komt doen, de toon waarop toegang wordt verzocht tot de woning en of er wordt gewezen op het vrijwillige karakter van het huisbezoek. Een meer genuanceerde aanpak van interventies zal leiden tot een betere privacybescherming en mogelijk ook tot meer acceptatie van interventieteams bij burgers.

Een ander belangrijk aspect is de veelvoud van onnodige bezoeken. Om deze te voorkomen, zou een nog betere digitale analyse voorafgaand aan een huisbezoek kunnen worden uitgevoerd. Wanneer de kans op valse positieven, d.w.z. controles waarbij geen overtreding ontdekt worden, verkleind wordt, zal dit de acceptatie van de burger mogelijke vergroten.

Wat betreft de inhoudelijke informatievoorziening is de brief van de Dienst Stedelijke Ontwikkeling, Gemeente Den Haag, in antwoord op een bezwaarschrift dat is ingediend tegen een bezoek van de Haagse Pandbrigade, een voorbeeld van hoe het wel zou moeten. In deze brief wordt uitgelegd wat de bevoegdheden en werkwijzen van de Haagse Pandbrigade zijn, welke wettelijke regelingen ten grondslag liggen aan hun handelen en waar de concrete verdenking uit bestaat. Het is noodzakelijk dat, waar de situatie dit toelaat, dit soort informatie in een veel eerder stadium wordt verstrekt aan de burger die een bezoek te wachten staat, of daar tijdens een bezoek naar vraagt. In dit geval moest de burger veel moeite doen om deze informatie te verkrijgen. Door middel van standaardbrieven, folders of

wellicht zelfs via een specifiek loket zouden burgers beter geïnformeerd en geholpen moeten worden.

4.2 Gegevenskoppeling voor gemeentelijke hulpverlening

4.2.1 Aanleiding

Mens Centraal is een informatiesysteem dat verschillende losstaande informatiesystemen en databases van dienstverlenende overheidsorganisaties verbindt. Hierdoor hoeven burgers die een meervoudige hulpvraag hebben niet elke keer hetzelfde verhaal te vertellen. Mens Centraal is ontwikkeld door het Kwaliteitsinstituut Nederlandse Gemeenten (KING) voor de gemeentelijke dienstverlening. Overheidsorganisaties die relevante informatie beheren voor gemeentelijke dienstverlening (zoals UWV WERKbedrijf, DUO, Jeugdzorg, Sociale Dienst etc.) zijn aangesloten. Bovendien is het systeem aangesloten op de Gemeentelijke Basisadministratie (GBA).

Voor burgers betekent het dat de hulp of dienstverlening die ze krijgen bij verschillende instanties beter op elkaar kan worden afgestemd. Ook kan het systeem ‘signalen’ afgeven aan instanties die daarop in actie kunnen komen. Hoewel met Mens Centraal de dienstverlening van samenwerkende instanties beter op elkaar kan worden afgestemd, bestaan er ook privacyrisico’s. Bij gemeenten waar met Mens Centraal wordt gewerkt, is immers een systeem actief waar op grote schaal privacygevoelige informatie wordt ontsloten. Hoe veilig zijn gegevens als ze, in theorie, door zoveel instanties ingezien kunnen worden? En hoe ver werken foutief ingevoerde gegevens door?

4.2.2 Beleidsdoelstelling- en uitvoering

Kader 4.3: Beleidsperspectief casus ‘Gegevenskoppeling voor gemeentelijke hulpverlening’

Beleid in Beeld
Het Mens Centraal-systeem koppelt de systemen en databases van dienstverleners waardoor burgers beter geholpen kunnen worden. De website van Mens Centraal geeft het volgende voorbeeld: “Natasja is 19 jaar en volgt een opleiding bij een ROC. Zij stopt met haar opleiding en doet even niets. Het systeem Mens Centraal maakt bekend dat ze geen startkwalificatie noch betaald werk heeft. Mens Centraal waarschuwt automatisch het RMC (het Regionale Meld- en Coördinatiepunt begeleidt jongeren tussen 18 en 23 jaar zonder startkwalificatie naar een opleiding of baan – *red.*) De trajectbegeleider van het RMC nodigt Natasja uit voor een gesprek. Zij wil over een half jaar beginnen met een andere opleiding. In de tussentijd wil ze werken. Met behulp van Mens Centraal wordt het CWI (Centrum Werk en Inkomen, tegenwoordig het UWV WERKbedrijf – *red.*) ingelicht. Het CWI kent de situatie van Natasja en vindt snel een passende baan voor haar.”

De beleidsdoelstelling van Mens Centraal is het efficiënter en beter organiseren van de hulpverlening van gemeenten. Mens Centraal koppelt verschillende systemen van dienstverleners van de overheid, waardoor zorgverleners gebruik maken van dezelfde gegevens. Er wordt op basis van gegevens uit verschillende databases (van UWV Werkbedrijf, GBA, Sociale dienst etc.) één digitaal klantdossier getoond. Ook kunnen de verschillende ketenpartners gebeurtenissen als ontslag, toeslagaanvragen en schooluitval registreren. Deze signalen worden vervolgens

beschikbaar gesteld aan aangesloten partners, zodat zij hun dienstverlening kunnen opstarten of aanpassen. Door het BSN van de klant plus eventueel een beperkt aantal andere persoonsgegevens in te voeren, legt Mens Centraal de link met de systemen van relevante ketenpartners om in te zien wat er (nog meer) bekend is over de klant. Op deze manier kan al in een vroeg stadium worden bepaald welke dienstverlening opgestart moet worden, of de klant bij de juiste instantie heeft aangeklopt en of de vraag om hulp of zorg terecht is.

4.2.3 Risico's voor de privacy van burgers

Vooralsnog zijn er geen privacy schendingen als gevolg van Mens Centraal bekend. Aan het invoeren van het informatiesysteem, waarbij op grote schaal met zeer gevoelige gegevens wordt gewerkt, kleven wel verschillende privacy*risico's*.

Eén mogelijk risico is het verstrekkende gevolg dat één foute registratie kan hebben in een systeem. Wanneer bijvoorbeeld een fout wordt gemaakt bij het invoeren van gegevens, werkt deze registratie mogelijk door in het hele systeem. Een kleine fout zou er dan toe kunnen leiden dat hulpverlening wordt stopgezet, zoals hulp bij schuldsanering of begeleiding van Jeugdzorg.

Een tweede risico is dat hulpverleners onterecht gegevens van personen opvragen. Hoewel er met 'autorisatierollen' wordt gewerkt binnen Mens Centraal, kan het voorkomen dat dienstverleners ongevraagd of onterecht gegevens opvragen. Peter de Punder, projectmanager Dienstverlening bij de gemeente Tilburg en betrokken bij de invoering van Mens Centraal, geeft aan dat in een ideale situatie burgers een overzicht zouden moeten krijgen om inzicht te krijgen in wie er toegang heeft tot hun persoonsgegevens, maar zegt ook: "Wie gaat dat betalen? Het bouwen van dit soort mogelijkheden kost erg veel geld en dat is er op dit moment niet." Het feit dat eerdere onderzoeken naar het gebruik van informatie uit Suwinet door gemeenten zeer kritisch waren over de veiligheid, stemt tot zorgen. In deze onderzoeken werd melding gemaakt van regelmatig misbruik of oneigenlijk gebruik en inkijk van persoonsgegevens.

Een derde risico van het systeem is dat in het geval van hacking zeer veel gevoelige persoonsgegevens openbaar kunnen worden gemaakt. In plaats van dat er slechts één systeem wordt gehackt waarin een beperkte hoeveelheid persoonsgegevens zijn vastgelegd, zijn dan ineens veel meer persoonsgegevens in handen van onbevoegde personen. Deze gegevens kunnen bijvoorbeeld online gepubliceerd worden, met het risico van bijvoorbeeld fraude.

4.2.4 Waarborgen vanuit overheidszijde

Kader 4.4: Waarborgen casus 'Gegevenskoppeling voor gemeentelijke hulpverlening'

Waarborg vanuit overheidszijde
"In Mens Centraal wordt nauwelijks informatie geregistreerd, alleen de ingevoerde signalen en opgestarte taken worden opgeslagen. Ook worden de antwoorden op de vragen om de juiste dienstverlening te bepalen opgeslagen. De toegang tot deze informatie kan worden afgeschermd." (Website Mens Centraal)

In Mens Centraal zijn verschillende waarborgen ingebouwd voor het beschermen van de privacy van burgers. Ten eerste is er geen centrale opslag van alle gegevens. Dossiers worden op aanvraag en direct samengesteld door gegevens op te vragen uit verschillende relevante databases. Ook wordt informatie niet langer dan wettelijk toegestaan opgeslagen, en bovendien is het mogelijk foutieve of achterhaalde gegevens te verwijderen. Ook wordt informatie niet uitgewisseld op groepsniveau en worden ingevoerde 'signalen' alleen aan relevante ketenpartners doorgegeven. Mens Centraal geeft op de website een voorbeeld: "Zo worden er geen signalen over de wens om een andere baan doorgegeven aan inkomenspartijen, omdat dit signaal voor deze partijen gezien hun wettelijke taak niet relevant is."

Verder is monitoring van toegang ingericht in Mens Centraal. Alle acties en bewerkingen binnen Mens Centraal worden gelogd en kunnen later worden gereproduceerd, bijvoorbeeld voor onderzoek naar rechtmatig gebruik van informatie. Deze mogelijkheid tot monitoring van toegang is bijvoorbeeld niet of minder goed geregeld bij Suwinet-Inkijk, een informatiesysteem van het UWV (Inspectie Werk en Inkomen, 2011). Uit dit onderzoek: "Het gebruik van Suwinet-Inkijk wordt in de regel niet gemonitord en ongeautoriseerde toegangspogingen worden niet gedetecteerd, waardoor oneigenlijk gebruik of misbruik waarschijnlijk niet wordt opgemerkt."

Tot slot zijn er autorisatiemogelijkheden ingericht in Mens Centraal, waardoor niet elke dienstverlener willekeurige informatie kan opvragen van ketenpartners. Niet elke dienstverlener heeft de mogelijkheid om *alle* persoonlijke gegevens van een klant op te vragen. Alleen de informatie die relevant en nodig is voor het uitvoeren van een taak, wordt getoond. Mens Centraal legt op de website uit: "De toegang tot deze zaken is gebaseerd op het maatschappelijke doel dat zij nastreven; medewerkers die verantwoordelijk zijn voor Passend werk krijgen de klantinformatiepagina Werk, de signaalpagina Werk en de werkvoorraad van die organisatie(-s) die zich richten op het realiseren van werk." Ook kunnen burgers in de meeste gevallen meekijken op het scherm van de dienstverlener, waardoor ze zien welke informatie wordt getoond aan de medewerker die hen helpt.

4.2.5 Mogelijke oplossingen

Hoewel Mens Centraal verschillende maatregelen heeft genomen om de privacy van burgers te beschermen, is verbetering mogelijk.

Zo zou transparantie en informatievoorziening aan burgers ingericht kunnen worden. Gezien de complexiteit van het systeem, de mogelijke risico's en de gevoeligheid van gegevens, zou het relevant kunnen zijn burgers inzicht te geven in hoe en waar hun gegevens staan opgeslagen, met wie ze gekoppeld kunnen worden en hoe er met hun gegevens wordt omgesprongen (veranderingen, aanvullingen, inzien van persoonlijke gegevens). Op die manier kan de overheid, explicieter dan slechts de belofte, burgers duidelijk maken dat zorgvuldig met privacygevoelige informatie wordt omgesprongen. Ook zou meer inzicht voor burgers het oneigenlijk gebruik en inzien van gegevens kunnen verminderen, omdat bekend is dat klanten inzicht hebben in deze acties. Echter, dergelijke transparantie kan helpen mogelijke gevolgen van privacyschending te signaleren, maar kan de privacyschending zelf niet oplossen. Die kan alleen opgelost worden door alleen de juiste informatie met de bevoegde partijen te delen.

Een andere oplossing is om burgers te laten kiezen of hun gegevens gedeeld mogen worden via mens Centraal. Deze keuzemogelijkheid is er nu niet. Een variant hierop is om burgers expliciet toestemming te vragen wie welke identificerende gegevens in mag zien en wie niet.

4.3 Waarborgen in geval van identiteitsfraude

Kader 4.5: Perspectief van de burger casus 'Waarborgen in geval van identiteitsfraude'.

Burger in beeld
"Ik ben meer dan veertig keer onder groot machtsvertoon van de weg geplukt. Dat ben je op een gegeven moment spuugzat. Daarom blijf ik nu liever thuis.'' Zakenman Ron Kowsoleea (49) ziet er moe uit. "Ik slaap heel slecht,'' bekent hij, "Ik loop bij een psychiater. Als iemand me ooit had gezegd dat ik dat zou doen, had ik gezegd: je bent gek." (…) "Ik ging er in het begin nonchalant mee om als mensen vertelden dat ik veroordelingen op mijn naam had staan,'' vertelt Kowsoleea. Hij kijkt weg. Dan zegt hij: "Ze hebben mijn bedrijf kapotgemaakt. De marechaussee heeft zakenpartners verboden zaken met mij te doen. De politie zegt: Kowsoleea is een grote, zware jongen. Ik kan niet constant zeggen: er is niets aan de hand. Mensen denken: hij zal wel iets hebben uitgevreten.'' (AD 2009) "Wanneer je te maken krijgt met identiteitsfraude, heb je geen leven meer. Je wordt geconfronteerd met een situatie waarvan je eerst denkt dat het een grap is. Later zie je pas de ernst van de zaak in. Van het ene op het andere moment vergaat je wereld" (RNW 2011).

4.3.1 Aanleiding en probleembeschrijving

Uit het onderzoek 'Burgers aan bod' uit 2004 blijkt dat een van de ergernissen van de burger ten opzichte van de overheid het steeds opnieuw moeten aanleveren van dezelfde gegevens betreft. Vanuit dit perspectief is ingezet op de zogenaamde één-loket-gedachte. Hoewel hiermee aan de voorkant een portaal gecreëerd wordt voor de burger, ontstaat er in de back office een verknoping van informatiesystemen waar overzicht en controle problematisch blijken, zoals uitgebreid beschreven in het WRR-rapport.

Wanneer iemand verkeerd in één systeem geregistreerd staat, heeft dit vervolgens mogelijk zeer grote implicaties voor andere databronnen. Hierdoor kunnen de negatieve gevolgen voor burgers die verstrikt raken in deze informatiekluwen erg groot zijn. Een voorbeeld hiervan is identiteitsfraude. Identiteitsfraude is mogelijk doordat anderen toegang hebben tot persoonsgegevens en deze misbruiken. Recent onderzoek laat zien dat het probleem van identiteitsfraude groeit, en momenteel een van de grootste risico's vormt van privacyschending (Van der Meulen, 2011).

4.3.2 Beleidsdoelstellingen en -uitvoering

Zoals eerder beschreven in het iOverheid rapport en geïllustreerd in de voorgaande casus over gemeentelijke dienst- en hulpverlening, is (keten-)digitalisering binnen de overheid ingezet om de efficiëntie en effectiviteit te vergroten en voor (administratieve) lastenverlichting en klantvriendelijkheid richting te burger. Deze specifieke beleidsdoelstellingen staan niet per se op gespannen voet met privacy. Maar de privacyschending – en mogelijke andere negatieve gevolgen – kan wel het

gevolg zijn van deze verknoping van informatiesystemen. Daarnaast blijkt, dat wanneer deze verknoping eenmaal is ontstaan, het soms erg lastig is om deze nog terug te draaien en eventuele fouten op te sporen. Zo is het soms niet langer duidelijk wie eigenaar is van bepaalde gegevens. Daarbij is er behoefte behoefte aan beleid over de wijze waarop de overheid verantwoordelijkheid neemt om ontstane problemen (mee) op te lossen.

Kader 4.6: Beleidsperspectief casus 'Waarborgen in geval van identiteitsfraude'.

Beleid in beeld
Minister Ernst Hirsch Ballin: "In de eerste plaats zijn alle onjuiste gegevens betreffende de heer K. op mijn verzoek verwijderd uit de justitiële documentatie en uit de systemen van de politiekorpsen. Ten tweede heeft de Immigratie- en Naturalisatiedienst op mijn verzoek de alias in de signalering verwijderd en zijn er afspraken - om hinder bij grenspassage te voorkomen - gemaakt met de Koninklijke marechaussee. In de derde plaats heeft mijn departement met de Meldpunt Identiteitsfraude afspraken gemaakt voor een vast aanspreekpunt voor de heer K. voor het geval dat de heer K. in de toekomst toch nog hinder zou ondervinden van identiteitsfraude. (…) Aanvankelijk is door mijn ministerie een bedrag uitgekeerd voor de hinder die de heer K. heeft ondervonden als gevolg van onjuiste registraties. (…) Vervolgens is door mijn ministerie op verzoek van de advocate een voorschot vooruitlopend op de uitkomst van de bemiddeling uitbetaald." (Tweede Kamer, aanhangselnummer 2503)

4.3.3 Gevolgen voor de privacy van burgers

Twee voorbeelden van burgers die zeer negatieve gevolgen ondervonden van de koppeling van persoonsgegevens in de back office zijn Ron Kowsoleea en Steven Romet. Bij de zaak Kowsoleea gaf een crimineel zich uit voor Ron Kowsoleea waardoor deze ten onrechte als crimineel geregistreerd werd in verschillende overheidsbestanden, waaronder die van regionale politiekorpsen. De identiteitsfraude werd reeds in 1994, tijdens de eerste rechtszaak, vastgesteld maar Kowsoleea's strafdossier werd niet opgeschoond, waardoor hij steeds opnieuw werd verdacht van criminele activiteiten. Het bleek vrijwel onmogelijk voor Kowsoleea om deze registraties te schonen, vanwege gebrek aan inzichtelijkheid in deze systemen, de onderlinge relaties tussen de systemen en de verantwoordelijkheidsverdeling met betrekking tot deze systemen.

Ook in de voor het Europees Hof voor de Rechten van de Mens gebrachte zaak Romet (no. 7094/06) was sprake van identiteitsfraude. Hoewel Steven Romet aangifte had gedaan van een verloren rijbewijs, werd dit door de Nederlandse politie niet correct verwerkt. Hierdoor was het mogelijk dat in de periode tussen het verlies en de aanvraag van een nieuw rijbewijs, zo'n anderhalf jaar, 1737 motorvoertuigen op zijn naam geregistreerd werden, zonder Romet's toestemming. Als gevolg hiervan werd Romet vervolgd voor allerlei ongevallen, overtredingen en belastingvorderingen. Tevens verloor hij hierdoor zijn uitkering.

De zaak Kowsoleea illustreert hoe identiteitsfraude in combinatie met een verkeerde inrichting van datasystemen binnen de overheid, grote gevolgen kan hebben voor iemands persoonlijke leven. Kowsoleea moest meerdere malen onterecht een huiszoeking van opsporingsdiensten ondergaan, is vele malen gehinderd en/of staande gehouden wanneer hij naar het buitenland wilde reizen, en

mede hierdoor heeft hij zijn reputatie verloren en is zijn zaak uiteindelijk failliet gegaan. Omdat het Kowsoleea niet lukte databestanden berustend bij de overheid te schonen, bleven er allerlei inbreuken op zijn persoonlijke levenssfeer plaatsvinden. De zaak Romet illustreert hoe een kleine vergissing aan de zijde van de overheid, zeer vergaande gevolgen kan hebben voor de burger. Van lastig gevallen worden met boetes, tot het verliezen van een uitkering aan toe.

4.3.4 Waarborgen van overheidszijde

Behalve dat de zaken Kowsoleea en Romet een voorbeeld zijn identiteitsfraude, laten beide gevallen ook een beeld zien waarbij de burger geen gehoor kreeg bij de overheid, waardoor via de Nationale Ombudsman en de rechter een oplossing gevonden moest worden. Het belang van goede waarborgen om op te treden in geval van identiteitsfraude is dus van belang.

Hier kan evenwel gewezen worden op twee zaken waarbij de overheid wel heeft ingezet op het bieden van waarborgen; zij het in beide situaties achteraf, nadat de burger reeds geconfronteerd was met een probleem. In de eerste plaats een zaak waarbij een groep ZZP'ers mogelijk ten onrechte werd verdacht van fraude. De overheid heeft in deze zaak een speciale commissie ingesteld onder leiding van Irene Asscher-Vonk. Deze commissie heeft 551 van deze gevallen opnieuw onderzocht. Op basis van deze beoordeling is in vele zaken geadviseerd om terugvorderingen van uitkeringsgeld en boetes ongedaan te maken – en het strafblad van de getroffen ZZP'ers te wissen.

Een ander voorbeeld van hoe de overheid op een positieve wijze het hoofd biedt aan de problematiek die samenhangt met 'datakluwen', is het 'Murphy netwerk' van het UWV. Het 'Murphy netwerk' (de naam is afgeleid van de Wet van Murphy die stelt dat als een ding fout gaat, meteen alles fout gaat) heeft als doel schrijnende gevallen te detecteren waarin de burger bij het zoeken naar een oplossing voor een probleem met de overheid van het kastje naar de muur gestuurd wordt. De vervolgstap is het helpen van de burger bij het daadwerkelijk oplossen van het probleem.

Het gaat bij deze aanpak vaak om burgers die vanwege een specifieke situatie opeens met verschillende overheidsinstanties te maken krijgen. Deze instanties werken in beginsel los van elkaar. De beslissingen van iedere afzonderlijke instantie kunnen echter directe gevolgen hebben voor de beslissingen van een andere instantie. Bij het UWV neemt een apart team direct de regie in handen om zo samen met de verschillende betrokkenen een oplossing te zoeken voor de benadeelde burger. De medewerkers hebben piketdienst waardoor er altijd iemand beschikbaar is voor de burger.

4.3.5 Mogelijke oplossingen

De zaken Kowsoleea en Romet maken duidelijk dat het nodig is dat de overheid het overzicht moet houden over de datakluwens die ontstaan zijn binnen de iOverheid. Hierdoor kunnen dergelijke gevallen van verstrikking in de systemen worden voorkomen. Niet alleen moeten de inrichting van en de verantwoordelijkheid van partijen over afzonderlijke systemen duidelijk zijn, maar ook is meer transparantie en accountability nodig in relatie tot het geheel aan databestanden en informatiestromen binnen de overheid. Hierbij is het van groot belang te weten

welke datasystemen gekoppeld zijn en of hiërarchische verhoudingen tussen bepaalde systemen bestaan.

Het Murphy netwerk maakt duidelijk dat behalve transparantie en inzicht in de koppelingen tussen databestanden, waarborgen voor burgers ook van essentieel belang zijn om te voorkomen dat burgers jarenlang last hebben van verstrikking in de datakluwen van de iOverheid. Voor de burger is het van groot belang dat hij weet waar hij met problemen terecht kan, en dan ook daadwerkelijk geholpen wordt om gegevens te corrigeren of te schonen. Met het oog hierop is door de overheid reeds het Centraal Meld- en informatiepunt Identiteitsfraude en –fouten (CMI) opgericht.

5 Analyse van de spanning tussen beleid en privacy

In deze studie zijn negen voorbeeldcases behandeld om een beeld te geven van de spanning tussen overheidsbeleid en privacy van de burger. In dit hoofdstuk wordt eerst een aantal algemene observaties beschreven naar aanleiding van de beschreven cases. Vervolgens worden de spanningen tussen beleid en privacy die zijn geobserveerd in de case studies geanalyseerd in twee stappen: eerst worden beleidsdoel, -inrichting en -uitvoering beschreven en vervolgens worden de neveneffecten voor de privacy van burgers geanalyseerd. Hierbij worden waar mogelijk oplossingsrichtingen genoemd. Opgemerkt moet worden dat deze zijn afgeleid uit de cases, en niet aan nader onderzoek zijn onderworpen.

5.1 Algemene observaties

De spanningen die optreden zijn van verschillende aard en niet in alle gevallen zijn deze spanningen voorzien. Dat is met name het geval wanneer de overheid zich dienstverlenend wil opstellen richting de burger. De intentie van de overheid is dan immers om de burger behulpzaam te zijn. Bij handhaving door politie en justitie is de spanning tussen beleid en privacy vaak wel van meet af aan in beeld, maar gaat het met name om de vraag of een juiste afweging is gemaakt tussen het doel dat de overheid nastreeft en de (mogelijke) privacyschending die dit bij de burger veroorzaakt. De beginselen van proportionaliteit (verhouding beleidsdoel en inbreuk) en subsidiariteit (is er een minder ingrijpend middel) vormen in beide situaties een belangrijk toetsingskader. De uitdaging is dus steeds om de meest geschikte maatregel te vinden die tegelijkertijd de minste inbreuk op privacy maakt.

Ook bij het type waarborgen kan een onderscheid gemaakt worden: waarborgen die proberen privacyinbreuken te voorkomen (zoals technische beveiligingsmaatregelen) enerzijds, en waarborgen die, nadat privacyinbreuken hebben plaatsgevonden, de burger mogelijkheden bieden om hier tegen op te treden, anderzijds. Hierbij kan gedacht worden aan bezwaar en beroep en mogelijkheden om persoonsgegevens te corrigeren of te verwijderen, of aan (financiële) genoegdoening aan de burger indien een inbreuk op de privacy de grenzen van het toelaatbare overschreden heeft. Probleem bij dit tweede type waarborgen is dat vaak alleen de negatieve gevolgen die de privacyschending met zich brengt worden opgelost, maar dat de schending van de privacy van de burger als zodanig een feit blijft. Hoewel het probleem binnen de relatie overheid-burger dan is opgelost, kan de burger door kwaadwillende derden nog steeds geconfronteerd worden met negatieve gevolgen die voortkomen uit de initiële privacyschending door de overheid.

Als een derde misbruik maakt van gegevens waardoor een burger in zijn privésfeer geraakt wordt (en/of in zijn portemonnee), ervaart hij vaak alleen deze tweede schending. Hierbij wordt over het hoofd gezien dat deze tweede schending enkel mogelijk was door een eerdere privacyschending, namelijk het ten onrechte registreren of openbaren van persoonsgegevens. Dit wordt geïllustreerd aan de hand van de eerste categorie privacy schendingen (‘onzorgvuldigheden rondom de beveiliging van persoonsgegevens’). De drie cases die dienen als voorbeelden van deze categorie, zijn alle drie gevallen waarin de gevolgen van de privacyschending sterker werden gevoeld dan de privacyschending zelf.

Het risico van misbruik van persoonsgegevens, zoals identiteitsfraude, dat gelegen is in het registreren en openbaar maken van, met name risicovolle combinaties van gegevens (zoals bankrekeningnummer en handtekening zoals het geval was bij de bouwvergunningaanvragen), staat op het moment van registreren vaak niet op het netvlies van de burger. Het feit dat een CV of een bouwvergunning openbaar is zal lang niet door elke burger ervaren worden als een inbreuk op zijn privacy – sterker nog, vele burgers zetten zelf hun CV online. Pas wanneer de burger wordt geconfronteerd met de negatieve gevolgen van identiteitsfraude, komt vaak het besef dat deze identiteitsfraude samenhangt met een eerdere openbaarmaking van persoonsgegevens.

Ook vanuit het overheidsperspectief, of meer specifiek het perspectief van de ambtenaar die met gegevens om moet gaan, is het besef dat het één kan leiden tot het ander van groot belang. Als ambtenaren zich niet realiseren wat de risico's zijn van het openbaar maken van gegevens, zullen zij wellicht minder zorgvuldig zijn. Immers, zij zijn vooral bezig met burgers te helpen bij het vinden van werk, of de vergunningprocedure te vereenvoudigen. Ambtenaren moeten zich van meet af aan afvragen of door verwerking en/of openbaarmaking van persoonsgegevens anderen gefaciliteerd worden deze gegevens te misbruiken. Dat moet er toe leiden dat ze voorzichtiger met gegevens omgaan, minder gegevens openbaren, en de toegang tot deze gegevens beperken tot bevoegden.

Hier raken we een belangrijk punt, namelijk dat binnen de overheid het besef moet groeien dat derden mogelijk minder goede intenties hebben met persoonsgegevens dan de overheid zelf. De redenering van een ambtenaar kan zijn dat inzage in persoonsgegevens niet zo problematisch is omdat de overheid de gegevens alleen gebruikt om de burger beter van dienst te zijn. Echter, diezelfde gegevens worden zowel door de overheid zelf, maar ook door derden, mogelijk voor heel andere doeleinden gebruikt. Dat dit zeer vergaande gevolgen kan hebben, maken de zaken Kowsoleea en Romet pijnlijk duidelijk.

Daarnaast speelt de diversiteit in (beleving van) inbreuk en schade nog een rol. De daadwerkelijke inbreuk op privacy brengt vaak niet meer dan een gevoel van onbehagen teweeg, terwijl de vervolgactie wel financiële of fysieke schade geeft, zoals het niet ontvangen van toeslag of een huiszoeking. Het is echter niet eenvoudig om hier gradaties van ernst aan te verbinden. In de eerst plaats geldt het gevoel van onbehagen, wanneer men weet dat de overheid mogelijk op huisbezoek kan komen, voor een zeer grote groep burgers. Het zal echter een veel kleinere groep van burgers zijn die geconfronteerd wordt met het daadwerkelijke huisbezoek en de negatieve consequenties die daarmee samen (kunnen) hangen, zoals het openbreken van een deur. Daarnaast zal er per burger verschillend gedacht worden over welke inbreuk zij groter achten. De afweging welk belang groter is, zal dan ook per geval gemaakt moeten worden.

5.2 Analyse van de spanning tussen beleid en privacy

Als we de cases in samenhang analyseren, dan valt op dat het beleidsdoel als zodanig over het algemeen en onder omstandigheden verenigbaar kan zijn met privacy, waaronder gegevensbescherming. De spanning tussen beleid en privacy is in deze cases dan ook niet onvermijdelijk, maar het gevolg van de inrichting of de

uitvoering van beleid. Slechts in enkele gevallen, zou de effectiviteit van het beleid mogelijk groter zijn wanneer er wel (meer) inbreuk wordt gemaakt op de privacy. Privacy is geen absoluut recht, maar moet worden afgewogen tegen andere belangen. Vanuit dit perspectief zijn ook handhaving en opsporing door politie en justitie, waarbij het belang van en de mogelijke spanning met privacy direct zichtbaar zijn, beleidsdoelen die niet per se conflicteren met privacy. Of hiervan sprake is, hangt af van de wijze waarop de beleidsdoelen geïmplementeerd worden, en hoe hier in de praktijk uitvoering aan gegeven wordt.

Om de cases te analyseren, worden de cases beknopt weergegeven aan de hand van vier kenmerken: beleidsdoel, -implementatie, -uitvoering en het probleem dat leidde tot het optreden van het ongewenste neveneffect: de privacyschending.

Tabel 5.1: Schematische samenvatting van de cases.

Casus	**Doel**	**Inrichting**	**Uitvoering**	**Probleem**
Fraude met toeslagen (via DigiD)	Aanvraag-procedure toeslagen vereen-voudigen	Aanvraag kan met willekeurige DigiD	Persoons-gegevens kunnen worden veranderd door derden	Gebrek aan controle
Online publicatie Bouwver-gunningen	Efficiënte en transparante vergunning-procedure	Bouw-vergunning online beschikbaar	Niet geanonimiseerde gegevens zijn openbaar	Teveel (gevoelige) gegevens inzichtelijk
CV's van werkzoe-kenden zichtbaar (bij UWV)	Efficiënt matchen werkgever en werk-zoekende	CV's online beschikbaar stellen	Niet geanonimiseerde gegevens zijn openbaar Onvolledige en onjuiste informatie verstrekt Werkcoach moet om toestemming vragen Koppeling tussen CV en Werkmap	Teveel gegevens inzichtelijk voor teveel partijen Door onvolledige en onjuiste informatie niet kenbaar voor burger Lastig om publicatie te weigeren: openbaarmaking CV is 'default'
ANPR leaserijders (Belasting-dienst)	Controle en handhaving	Gebruik ANPR voor proactieve individuele controle	Telefoontje naar mensen naar aanleiding van daadwerkelijk afgelegde autoritten	Telefoontjes (verwerking van gegevens op persoons-niveau)

Casus	Doel	Inrichting	Uitvoering	Probleem
Registratie etniciteit probleem-jongeren (Charlois)	Hulpverlening aan probleem-jongeren	Registratie etniciteit	Registratie etniciteit	Registratie etniciteit
Declaratie psychiatrische behandelingen (NZa)	Vereen-voudigen facturatie	Vermelden DBC-informatie op factuur	Verplichting deze informatie op factuur te plaatsen	Zeer gevoelige informatie komt terecht bij derden
Opsporing illegale bewoning en uitkeringsfraude (Pandbrigades)	Opsporing en handhaving	Digitale en fysieke controle woningen	Huisbezoeken, interventies	Gebrek aan informatie-voorziening Machts-vertoon en/of intimidatie Veelheid aan huisbezoeken Gebrek aan hulp achteraf
Gegevens-koppeling voor gemeentelijke hulpverlening (Mens Centraal)	Efficiënte en effectieve dienst-verlening aan burgers	Toegan-kelijk maken gegevens-bestanden voor meerdere partijen	Vele partijen hebben toegang tot de gegevens	Toegang tot meer gegevens voor meer partijen leidt tot meer risico bij lekken of doorwerken van fouten; ook voor externe hacks
Waarborgen in geval van identiteitsfraude (Romet; Kowsoleea)	Efficiënte en effectieve uitvoering van beleid	Ontstaan van data kluwen	Ontstaan van datakluwen	Burger raakt verstrikt in datakluwen en gebrek aan hulp bij verstrikking

Uit tabel 5.1 wordt duidelijk dat het bij de meeste cases gaat om gevallen die een proportionaliteits- en subsidiariteitstoets niet kunnen doorstaan. Met de nodige aanpassingen in de vorm van juridische, technische en organisatorische waarborgen zou het beleidsdoel bereikt kunnen worden zonder de privacy van burgers onevenredig aan te tasten.

Nu beleid en probleem per casus duidelijk zijn, volgt de tweede stap: het inzichtelijk maken van de negatieve effecten voor de burger die dit mogelijk met zich brengt. Hierbij wordt een onderscheid gemaakt tussen negatieve aspecten die een direct gevolg zijn van overheidshandelen en effecten die het gevolg zijn van handelingen van kwaadwillende derde partijen, die mogelijk gemaakt zijn door het overheidshandelen.

Tabel 5.2: Analyse van de effecten voor privacy van burgers.

Casus	**Overheid**	**Derden**
Fraude met toeslagen (via DigiD)	Vervuiling gegevens Geen toeslag ontvangen of toeslagen teruggevorderd Gebrek aan hulp om ontstane problemen op te lossen	Ongeautoriseerde toegang door derden die persoonsgegevens wijzigen Fraude
Online publicatie Bouwvergunningen	Inzicht in persoonlijke levenssfeer	Risico op misbruik door derden, zoals identiteitsfraude
CV's van werkzoekenden zichtbaar (bij UWV)	Ingangsvoorwaarde uitkering	Risico op misbruik door derden, zoals identiteitsfraude
Automatische nummerplaat-herkenning leaserijders (Belastingdienst)	Vermoeden van schuld Gevoel van intimidatie	
Registratie etniciteit van probleem-jongeren (Charlois)	Risico op stigmatisering, discriminatie	
Declaratie psychiatrische behandelingen (NZa)	Risico op discriminatie of stigmatisering	Risico op discriminatie of stigmatisering
Opsporing illegale bewoning en uitkeringsfraude (Pandbrigades)	Intimidatie, machtsvertoon Onbehagen dat men geconfronteerd kan worden met huisbezoek Gebrek aan hulp na interventie	Risico op discriminatie of stigmatisering

Casus	Overheid	Derden
Gegevenskoppeling voor gemeentelijke hulpverlening (Mens Centraal)	Risico op misbruik gegevens Risico op doorwerking van fout binnen de keten	Risico op misbruik door derden, zoals identiteitsfraude
Waarborgen in geval van identiteitsfraude (Kowsoleea, Romet)	Reisproblemen, strafrechtelijke antecedenten, inval in huis Gebrek aan hulp om ontstane problemen op te lossen	Identiteitsfraude

De schendingen en risico's zoals hierboven weergegeven, dienen als leidraad voor de hieronder te bespreken waarborgen die noodzakelijk zijn om (mogelijke) negatieve gevolgen voor de privacy van burgers te voorkomen. Hierbij wordt onderscheid gemaakt tussen de waarborgen die een rol spelen bij de inrichting van beleid en bij de uitvoering van beleid.

De belangrijkste fase is die van de inrichting van beleid. In deze fase moet een afweging gemaakt worden tussen het beleidsdoel en de mogelijke schending die dit met zich brengt voor de privacy van de burger. Uit tabel 5.2 blijkt duidelijk dat de overheid hierbij niet alleen haar eigen perspectief in ogenschouw moet nemen, maar ook de mogelijke risico's die samenhangen met derde partijen in haar afwegingen moet betrekken. In feite gaat het dan om het uitvoeren van een zogenaamde Privacy Impact Assessment (PIA), waarin de vraag centraal staat welke gevolgen het beleid heeft, of kan hebben, voor de privacy van de burger en hoe waarborgen ingebouwd kunnen worden om deze gevolgen teniet te doen of te minimaliseren. Hierbij geldt, mede op basis van de uitgangspunten neergelegd in de voorgestelde Europese Privacyverordening, dat gekozen moet worden voor een zo privacyvriendelijk mogelijke inkleding van het beleid. Zoals eerder opgemerkt vormen proportionaliteit en subsidiariteit hierbij belangrijke afwegingsmechanismen. *Is een bepaalde maatregel noodzakelijk om het beleidsdoel te bereiken? Zijn er minder ingrijpende alternatieven beschikbaar?*

Bij veel cases gaat het reeds in deze eerste fase mis. Bij de bouwvergunningen-casus en de UWV-casus hadden minder gegevens openbaar gemaakt kunnen worden, of had de toegang tot gegevens beperkt kunnen worden tot belanghebbenden. De DigiD-casus laat zien dat van meet af aan gekozen had moeten worden voor een systeem waarbij gecontroleerd wordt of degene die met zijn DigiD heeft ingelogd, degene is die de toeslag heeft aangevraagd, danwel is bevoegd/gemachtigd deze aan te vragen. In de Charlois-casus had het probleem, in plaats van de etniciteit, geregistreerd kunnen worden teneinde het beleidsdoel te bereiken. In de ANPR-casus had in plaats van telefonisch individueel contact gekozen kunnen worden voor informatie, en eventueel waarschuwingen, via de media.

De vraag is bij deze laatste twee cases of het beleidsdoel wellicht beter bereikt had kunnen worden wanneer toch voor een inrichting was gekozen waarin de privacy (meer) werd geschonden. Ook bij de casus NZa rijst de vraag of het beleidsdoel, vereenvoudigde facturatie, bereikt kan worden op een andere, minder ingrijpende

manier. Hier speelt echter het probleem dat bij een afweging tussen beleidsdoel en privacy, het belang van privacy zwaarder weegt (mede vanwege het feit dat het in deze casus om de verwerking van gevoelige persoonsgegevens gaat). In deze casus lijkt een optioneel systeem, waarbij het gebruiken van de DBC-code op een factuur alleen met toestemming van de burger is toegestaan, de enige mogelijkheid om binnen de grenzen van de Wbp te blijven.

De tweede fase is de uitvoering van beleid. Zelfs wanneer beleid als zodanig met voldoende waarborgen omkleed is om de privacytoets te doorstaan, kunnen er toch nog privacyrisico's bestaan wanneer dit beleid in de praktijk niet goed ten uitvoer wordt gebracht. Hierbij hoeft zeker niet gedacht te worden aan kwade intenties. Meer waarschijnlijk ontstaan privacy schendingen door een gebrek aan bewustwording en/of scholing in de uitvoeringspraktijk. Ambtenaren zouden als het ware de nodige 'achterdocht' moeten cultiveren voor het verzamelen of verwerken van persoonsgegevens, waarbij ze zich steeds afvragen of dit nodig is, of dat er hierdoor mogelijk ruimte worden gegeven aan kwaadwillende derden. Hierbij kan het vragen van toestemming door de werkcoach in de UWV-casus als voorbeeld genoemd worden, alsmede de wijze waarop de pandbrigade de burger bij een huisbezoek bejegent. In deze casus werd de privacyschending erger doordat druk werd uitgeoefend om panden te betreden, zonder hierbij duidelijk te maken dat burgers niet verplicht waren om toegang tot de woning verschaffen. In sommige cases, zoals de UWV- en de Pandbrigade-casus, zijn de gevolgen voor de privacy dus het gevolg van zowel de inrichting als de uitvoering van het beleid.

6 Oplossingen voor de spanning tussen beleid en privacy

Dit hoofdstuk beschrijft de oplossingsrichtingen voor de spanningen tussen beleid en privacy die zijn gevonden in de cases.

6.1 Categorieën privacyrisico's

Bij het beschrijven van de oplossingen voor de gevonden spanningen tussen beleid en privacy wordt tabel 5.2, die de gevonden effecten voor de privacy van burgers beschrijft aan de hand van hun veroorzaker (de overheid of derden), als uitgangspunt genomen. Hierbij kunnen we vier hoofdcategorieën van risico's voor de burger in relatie tot privacy identificeren:

1. Misbruik van gegevens/fraude (hieronder ook begrepen stigmatisering en discriminatie);
2. Gevoel van onbehagen in de privésfeer (intimidatie, machtsvertoon, controle);
3. Vervuiling gegevens of doorwerking van een fout in de keten; en
4. Gebrek aan hulp na privacyschending.

In onderstaande tabel (tabel 6.1) wordt per risicocategorie geïnventariseerd welke oplossingsrichtingen er zijn. In het algemeen gaat het bij de oplossingsrichtingen om het inbouwen van waarborgen om zo privacy schendingen te voorkomen, of te beperken. Zoals eerder gesteld zijn beleidsdoelen als zodanig niet problematisch in de meeste onderzochte gevallen, maar moet de implementatie en de uitvoering van beleid met meer, of andere, waarborgen omkleed worden. Op basis van de analyse van de negen cases kunnen waarborgen onderverdeeld worden in drie categorieën: juridische, organisatorische en technische.

Hierbij moet met betrekking tot juridische waarborgen worden opgemerkt dat deze veelal bestaan. In verschillende wetten zijn bijvoorbeeld informatieplichten en geheimhoudplichten opgenomen. Tevens bestaan er wettelijke regels omtrent bepaalde bevoegdheden (zoals om al dan niet binnen te mogen treden in een woning). Probleem is vaak het bewerkstelligen van de naleving van dergelijke juridische waarborgen in de praktijk. Om dit te realiseren kan gedacht worden aan betere voorlichting, strengere controle en zwaardere straffen op overtreding. Hierbij kan een rol zijn weggelegd voor het College Bescherming Persoonsgegevens (CBP) naast die van een privacyfunctionaris.

In de tweede plaats moet opgemerkt worden dat sommige oplossingsrichtingen door meerdere waarborgen ingekleed kunnen worden. Zo kan de toegang tot persoonsgegevens bij wet beperkt worden tot een bepaalde groep personen (de wet bepaald bijvoorbeeld wie voor welke gegevens het BSN mag gebruiken), kan hier organisatorisch een waarborg voor ingebracht worden (alleen toegang tot persoonsgegevens vanaf pc's die staan opgesteld op de afdeling), en kan dit ook technisch bewerkstelligd worden (elke medewerker heeft vanaf de eigen pc toegang tot persoonsgegevens, maar alleen na deugdelijke authenticatie, terwijl toegang wordt gelogd). Het loggen van toegang tot gegevens kan een preventieve werking hebben. Wat als privacyinbreuk kan gelden voor burgers, kan een controle-instrument zijn voor functionarissen.

Tabel 6.1: Oplossingsrichtingen voor de spanningen tussen beleid en de privacy van burgers.

Risico-categorie	**Oplossingsrichtingen**		
	Juridisch	**Organisatorisch**	**Technisch**
Misbruik gegevens	Privacy by design/default principes Aanstellen privacy-functionaris Toestemming burger	Minder gegevens verzamelen en minder gegevens delen met andere partijen Bewustwording, opleiding en werkinstructies voor ambtenaren (Betere) informatie-voorziening aan burgers Transparantie van gegevensverwerking	Gegevens-beveiliging via: - Autorisatie/ authenticatie - Anonimisering - Versleuteling - Logging Controle over toegang tot persoonsgegevens
Onbehagen privésfeer	Privacy by design/default principes Aanstellen privacy-functionaris Toestemming burger voor toegang tot persoons-gegevens	Bewustwording, opleiding en werkinstructies voor ambtenaren (Betere) informatie-voorziening aan burgers Bezwaar- en klachtenprocedures	Andere vormen van controle (bijvoorbeeld digitaal)
Vervuiling/ Doorwerking	Juridisch beleggen verantwoor-delijkheid	(Betere) informatie-voorziening aan burgers Transparantie van de gegevensverwerking Bezwaar- en klachtenprocecures Inzage- en herstelmogelijkheden	Overzichtelijkheid systeemstructuur Signalering en geautomatiseerde consistentiechecks Gegevens-beveiliging en controle via: - Autorisatie/ authenticatie - Logging

In de volgende paragrafen worden de verschillende categorieën waarborgen nader uitgewerkt.

6.2 Juridische waarborgen

In principe liggen de juridische waarborgen met betrekking tot privacy en gegevensbescherming reeds verankerd in de huidige wetgeving. Daarom worden in deze categorie oplossingsrichtingen vier zaken behandeld die strikt genomen eerder organisatorische oplossingen dan juridische waarborgen zijn: inrichten van processen via privacy by design en/of privacy by default, aanstellen van privacy officers of privacyfunctionarissen, mogelijk maken dat burgers expliciet toestemming geven voor de verwerking van hun persoonsgegevens en juridisch beleggen van verantwoordelijkheden. Er zijn twee redenen om deze vier oplossingsrichtingen toch onder deze categorie te scharen. De eerste is dat deze waarborgen alle als doel hebben dat de juridische waarborgen die al in wetgeving verankerd zij) beter worden gehanteerd of nageleefd. De tweede is dat dergelijke waarborgen waarschijnlijk worden opgenomen in de nieuwe Europese Privacyverordening. Hierin zullen zaken als het inrichten van processen volgens privacy by design principes een grotere rol gaan spelen.

6.2.1 Privacy by design en privacy by default principes

In de voorgestelde Privacyverordening van de Europese Commissie is bepaald dat bij de implementatie van beleid of nieuwe technologie, waarbij risico's voor de privacy bestaan, de beginselen van *privacy by design* en *privacy by default* gehanteerd moeten worden. Hierdoor is het niet voldoende om beleid te toetsen op proportionaliteit en subsidiariteit, maar moet proactief gezocht worden naar een inrichting van het beleid die het best de privacy van de burger waarborgt, en kunnen aanvullende zaken alleen nog plaatsvinden met toestemming van de burger.

Een voorbeeld is de UWV-casus waarbij een CV standaard niet online wordt geplaatst. Dit is alleen toegestaan met toestemming van de burger, waarbij de burger erop gewezen moet worden dat het verstandig is om niet alle personalia online beschikbaar te stellen. Er zou bijvoorbeeld ook een standaard formaat ontwikkeld kunnen worden waarbij zo veel mogelijk persoonsgegevens uit het CV weggelaten worden. In de NZa-casus kan gedacht worden aan een systeem waarin standaard niet op basis van DBC-codes gefactureerd wordt. Verwerking is mogelijk op basis van toestemming, maar dan moet de patiënt die geen toestemming verleent, niet benadeeld worden ten opzichte van die patiënt die dit wel doet.

De naleving van beginselen als privacy by design en privacy by default zal samenhangen met toezicht en controle, en eventuele sancties op niet naleving. Hoewel privacy by default een juridisch begrip is, zal het organisatorisch en technisch mogelijk gemaakt moeten worden, zoals bovenstaande voorbeeld uit de UWV-casus duidelijk maakt. Naast de rol van het CBP en een FG, kan hier tevens gewezen worden op sectorale initiatieven zoals de oprichting van het CIP, het Centrum Informatiebeveiliging en Privacybescherming. Dit expertisecentrum zal de aangesloten ZBO's (zoals UWV, Belastingdienst, SVB en DUO) ondersteunen bij ICT-beleid en -vraagstukken. Het CIP gaat zich bezighouden met alle beveiligingsincidenten die zich bij de aangesloten organisaties voordoen en zal noodscenario's en herstelplannen uitwerken voor dergelijke incidenten. Ook zal het CIP een aantal beveiligingshulpmiddelen regelen en trainingen verzorgen.

6.2.2 *Privacy officers of functionarissen gegevensbescherming (FG's)*

Hoewel de juridische waarborgen in wet- en regelgeving zijn vastgelegd, biedt dit geen garantie dat deze in de praktijk ook daadwerkelijk worden nageleefd. Voor niet naleving kunnen verschillende redenen bestaan. Personen kunnen zich niet bewust zijn van deze waarborgen of kunnen deze verkeerd interpreteren of uitvoeren. Hiervan was sprake bij de werkcoach in de UWV-casus die vergat om toestemming te vragen.

Echter, er kan ook sprake zijn van het bewust negeren van deze waarborgen omdat de kans dat niet naleving consequenties heeft erg klein is, terwijl het niet naleven van de waarborgen voordeel oplevert. Hier kan gewezen worden op de Pandbrigade-casus, die door het niet verschaffen van deugdelijke informatie en machtsvertoon proberen om ook zonder wettelijke grondslag een woning te betreden. Ook in de Charlois-casus was hier sprake van. Hoewel in de Wbp is vastgelegd dat ras/etniciteit niet mag worden geregistreerd, meende deelgemeente dat het nuttig was voor de hulpverlening aan probleemjongeren.

De naleving van juridische waarborgen zal dus samenhangen met vergroting van bewustwording (zie organisatorische waarborgen) en het vergroten van controle op de naleving, eventueel gepaard met zwaardere straffen op niet naleving. Hier is een rol weggelegd voor het CBP. Ook kan het aanstellen van privacy officers of FG's hieraan bijdragen. Zowel het beleid als zodanig, als de uitvoering ervan, moet actief getoetst en gecontroleerd worden op verenigbaarheid met privacy en gegevensbescherming. Met name een FG kan bijdragen aan de kenbaarheid van het juridisch raamwerk betreffende privacy en gegevensbescherming binnen een organisatie. Bovendien kan hij of zij de risico's en nadelige gevolgen die privacy schendingen kunnen hebben voor de burger onder de aandacht brengen van die personen die in de praktijk werken met (gevoelige) persoonsgegevens.

6.2.3 *Toestemming van de burger*

Op grond van de Wbp is de verwerking van persoonsgegevens alleen toegestaan op basis van een legitieme verwerkingsgrond. Een van de mogelijkheden is wanneer het belang van de verantwoordelijke, degene die de gegevens verwerkt, zwaarder weegt dan het belang van de burger wiens gegevens verwerkt worden. In de casus NZa was hier echter geen sprake van, het doel van vereenvoudigde facturatie kon niet aangemerkt worden als belangrijker dan privacy. En ook in de Charlois-casus kon niet worden aangetoond dat etnische registratie zodanig belangrijk was voor de hulpverlening, dat dit zwaarder woog dan het privacyrisico dat ermee gemoeid is. In een dergelijk geval kan de verwerking van persoonsgegevens enkel gebaseerd worden op toestemming. Toestemming in de zin van de Wbp vereist een vrije, specifieke en op informatie berustende wilsuiting van de burger. Hier ligt dus een relatie met het belang van een correcte en volledige informatievoorziening. Hier lag bijvoorbeeld een probleem in de UWV-casus met de openbaarheid van CV's. Hier lag ook een probleem in relatie tot het vereiste van vrij verkregen, aangezien door de inkleding van het systeem het verlenen van toestemming verworden was tot ingangsvoorwaarde voor een uitkering, waardoor voor de burger geen keuze bestond zonder vergaande negatieve gevolgen toestemming te weigeren.

6.2.4 Juridisch beleggen verantwoordelijkheden

Wanneer door het ontstaan van datakluwen binnen de overheid de burger in de problemen raakt door fouten in deze datakluwen, moet het duidelijk zijn wie hiervoor verantwoordelijk is. Een burger die in de datakluwen verstrikt raakt zal hier veelal buiten zijn schuld om in verzeild raken, waardoor het onrechtvaardig zou zijn de verantwoordelijkheid bij de burger zelf te beleggen. Bij de veelheid aan informatiestromen en -bestanden binnen de overheid zijn vele verschillende partijen betrokken. Hierbij gaat het niet alleen om verschillende overheidspartijen, maar bijvoorbeeld ook om private partijen die hardware en software leveren en beheren. Hierdoor ontstaat bij fouten het risico dat alle partijen naar elkaar verwijzen om verantwoordelijkheid te nemen, waar de burger dan de dupe van wordt. Het is daarom van belang dat er binnen de overheid nagedacht wordt hoe dit voorkomen kan worden. Een van de oplossingen is het wettelijk nader inkaderen van de verplichtingen en verantwoordelijkheden die met betrekking tot overheidsinformatie gelden. Gezien de complexiteit van dit vraagstuk is het aan te bevelen nader onderzoek te verrichten naar de wijze waarop, en binnen welke wetgeving, de belegging van verantwoordelijkheid voor informatiestromen en –bestanden binnen de overheid het beste vormgegeven kan worden.

6.3 Organisatorische waarborgen

Uit tabel 6.1 blijkt dat veel mogelijke oplossingsrichtingen liggen in de sfeer van organisatorische waarborgen voor privacy. Ook hier geldt dat een aantal waarborgen die als organisatorisch bestempeld zijn, rechtstreeks voortvloeien uit wettelijke plichten, zoals bijvoorbeeld een deugdelijke informatievoorziening, het inrichten van bezwaar- en klachtenprocedures en zo min mogelijk gegevens delen met zo min mogelijk partijen (beginsel van dataminimalisatie en doelbinding). De zes categorieën die worden besproken, zijn: dataminimalisatie en minder data vrijgeven aan minder partijen, bewustwording, opleiding en werkinstructies voor ambtenaren, (betere) informatievoorziening aan burgers, transparantie van gegevensverwerking, inzage- en herstelmogelijkheden, bezwaar- en klachtenprocedures en betere afstemming binnen de overheid.

6.3.1 Minder informatie verzamelen en minder data vrijgeven aan andere partijen

De principes van dataminimalisatie en doelbinding wijzen erop dat er zo min mogelijk gegevens verzameld moeten worden om een beleidsdoel te kunnen bereiken (dataminimalisatie) en dat de verzamelde gegevens alleen voor dat specifieke doel gebruikt mogen worden (doelbinding). Daarnaast is het van belang dat deze gegevens alleen gedeeld worden met partijen waarvoor het, gezien het doel, noodzakelijk is dat zij toegang hebben tot deze gegevens. De UWV- en bouwvergunningen-cases zijn voorbeelden van het verzamelen en openbaar maken van te veel gegevens, zonder dat dit noodzakelijk was voor het realiseren van het beleidsdoel. Bij de inrichting van Mens Centraal is wel gepoogd hier rekening mee te houden en te zorgen dat privacygevoelige informatie alleen gedeeld wordt met die partijen die deze ook echt nodig hebben voor het uitvoeren van hun taak. Gegevens die hier niet aan voldoen, maar wel in het systeem zijn opgeslagen, zijn niet zichtbaar. Hetzelfde is gebeurd bij de Charlois-casus, waar na het oordeel van het CBP dat etniciteit niet langer geregistreerd mocht worden, het niet langer mogelijk was voor de hulpverleners om informatie over de geboorteplaats van de ouders uit de GBA in te zien.

6.3.2 Bewustwording, opleiding en werkinstructies voor ambtenaren

Uit de UWV-casus blijkt het belang van een goede organisatorische inbedding van privacybewustzijn. In deze casus werd duidelijk dat het bewustzijn en belang niet binnen alle lagen van de organisatie (in dit geval de werkcoach) voldoende aanwezig was. Betere en specifiekere scholing van werknemers zou één van de maatregelen kunnen zijn. Daarnaast kan gedacht worden aan het opstellen van werkinstructies (inclusief controle op naleving) voor ambtenaren. Een voorbeeld uit de Charlois-casus is de geheimhoudplicht voor de hulpverleners die met de gevoelige informatie in het DOSA-systeem werken. De twee aspecten (opleiding en werkinstructies) staan los van elkaar, maar kunnen elkaar versterken. Opleiding is niet bindend en kan ongeoorloofd gedrag niet bestraffen, terwijl werkinstructies die niet begrepen worden, mogelijk niet uitgevoerd worden.

6.3.3 (Betere) informatievoorziening aan burgers

Naast de organisatorische, juridisch en technische maatregelen die de spanning tussen beleid en privacy kunnen wegnemen of verminderen, is betere informatievoorziening voor burgers een belangrijk middel bij de omgang met persoonsgegevens. In een aantal gevallen (ANPR, Pandbrigades) kwam duidelijk naar voren dat burgers verrast waren en niet op de hoogte waren over het gebruik van hun persoonsgegevens en andere persoonlijke informatie door de overheid. In het geval van ANPR werden burgers gebeld en verteld waar en wanneer hun auto was geregistreerd, zonder dat er een concrete of bewijsbare ‘verdenking’ was. Betere informatievoorziening kan de spanning wegnemen, zoals in het geval van de Pandbrigades. Niet alleen betere maar vooral ook vroegtijdige informatievoorziening aan burgers had veel spanning kunnen wegnemen op het moment dat ambtenaren aanbelden. Door burgers vooraf op heldere wijze uit te leggen op grond waarvan er toegang tot de woning wordt gevraagd, leidt dit naar alle waarschijnlijkheid tot minder verzet en gevoel van privacyinbreuk. In de zaak van het UWV wordt ook gesuggereerd om burgers te wijzen op de mogelijke privacyrisico’s die kleven aan het openbaar maken van bepaalde gevoelige of persoonlijke informatie in CV’s.

6.3.4 Transparantie van de gegevensverwerking

Door de digitalisering en koppeling van veel systemen en gegevens, kan burgers het gevoel bekruipen dat de overheid alles van ze weet en dat instanties onrechtmatig en ongevraagd toegang opvragen tot gegevens. Dit kan het vertrouwen in digitale dienstverlening door de overheid schaden. Om het gevoel van gegevensmisbruik te verminderen, is het noodzakelijk om burgers inzicht te geven in welke overheidsinstanties, welke persoonsgegevens, voor welke doeleinden gebruiken. Hiertoe bestaat in de Wbp ook een expliciet recht voor de burger, namelijk het recht op inzage. In het geval van Mens Centraal of UWV zou bijvoorbeeld gekozen kunnen worden om burgers een overzicht te geven (pagina, mailtje, sms’je) van de tijdstippen en personen die toegang hebben gevraagd tot gegevens en wat ze hebben gedaan (opvragen, mutaties, toevoegingen). Ook andere controlemechanismen, zoals een brief ter verificatie van de wijziging van de toeslaginformatie in de DigiD-casus, hadden meer inzicht kunnen geven in de verwerking van persoonsgegevens.

6.3.5 Bezwaar- en klachtenprocedures

Uit verschillende cases (DigiD, Pandbrigade, Kowsoleea) blijkt de noodzaak dat het voor burgers duidelijk is waar en bij wie zij aan kunnen kloppen indien er problemen

geconstateerd zijn. Doordat dit niet duidelijk is, frustreert dit de burger die al slachtoffer is van een privacyschending omdat hij nu ook nog van het kastje naar de muur gestuurd wordt. Bovendien kan het hierdoor (te) lang duren voordat fouten en privacy schendingen hersteld of beperkt worden. In de cases DigiD en UWV was het voor 'slachtoffers' onduidelijk hoe en bij wie ze bezwaar moesten maken. In het geval van DigiD werden slachtoffers niet snel en adequaat geholpen en was het onduidelijk hoe de verantwoordelijkheden tussen de Belastingdienst, politie, DigiD en Centraal Meldpunt Identiteitsfraude en -fouten was geregeld.

6.3.6 Inzage- en herstelmogelijkheden

Behalve dat burgers inzicht hebben in wie er toegang heeft tot hun persoonsgegevens (d.m.v. logging) en dat ze de kans krijgen bezwaar te maken indien er problemen zijn ontstaan, is er nog een mechanisme dat kan helpen om mogelijk fouten in de gegevenskoppeling te voorkomen: inzage- en herstelmogelijkheden. Wanneer burgers inzage krijgen in welke gegevens partijen van hebben en hoe ze geregistreerd staan in systemen, zullen zo mogelijk ook zelf in actie komen om deze op te lossen. Dit komt de gegevenskwaliteit ten goede. Dit zou zowel organisatorisch als technisch ingericht kunnen worden. Een voorbeeld is het Mens Centraal systeem, waarbij fouten mogelijk door kunnen werken door het koppelen van gegevens. Er zou technisch mogelijk gemaakt kunnen worden dat wanneer burgers een dergelijke fout opmerken, zij dit zelf kunnen terugkoppelen aan het systeem, dat weer een signaal geeft aan de partij die de gegevens beheert. Uiteraard zal er wel controle moeten plaatsvinden op of de gegevens juist zijn.

6.3.7 Betere afstemming binnen de overheid

Om te voorkomen dat fouten doorwerken in de keten, is betere afstemming binnen de overheid nodig, tussen de verschillende partijen die gegevens verwerken en koppelen. Voorbeelden hiervan zijn de cases over identiteitsfraude (Kowsoleea en Romet). Deze laten duidelijk zien wat er gebeurt wanneer deze afstemming niet plaatsvindt: fouten blijven dan steeds opnieuw doorwerken in de keten. Zo kan het voorkomen dat iemand meerdere keren van de weg wordt gehaald, terwijl bij een andere instantie al bekend is dat deze persoon slachtoffer is geworden van identiteitsfraude. Het Murphy netwerk van het UWV biedt een oplossing voor het inrichten van deze afstemming door benadeelde burgers (gevallen die van het kastje naar de muur worden gestuurd) te bespreken met verschillende partijen binnen de organisatie en zo een passend oplossing te formuleren.

6.4 Technische waarborgen

De technische waarborgen kunnen worden ondergebracht in vier categorieën: toepassen van privacy by design en privacy by default principes, gegevensbeveiliging, controle over persoonsgegevens, signaleringsmechanismen en overzichtelijke systeemarchitectuur.

6.4.1 Toepassen van privacy by design en privacy by default principes

Hoewel de beginselen van privacy by design en privacy by default niet expliciet zijn vastgelegd in de voorgestelde Europese Privacyverordening, moeten deze wel technisch en organisatorisch worden ingevuld. Voor privacy by default geldt dat de standaardinstelling zo privacyvriendelijk mogelijk moet zijn. Alleen na actief ingrijpen door de burger kan de instelling wijzigen. Een burger kan dit doen omdat hij de verwerker toestemming verleent voor een verwerking die niet strikt

noodzakelijk is met het oog op het beleidsdoel, maar die ook voor de burger voordelen met zich kan brengen.

Als voorbeeld kan gewezen worden op DigiD-, UWV- en NZa-cases. In beide systemen was de standaardinstelling niet privacyvriendelijk. In de DigiD-casus werd het technisch mogelijk gemaakt dat willekeurige personen (mits ze een aantal basisgegevens bezaten) toeslagaanvragen konden doen, zonder dat hierop controle plaatsvond. In de UWV-casus werden gegevens ongevraagd openbaar gemaakt zonder dat dat nodig was (niet subsidiair en niet proportioneel) en was inloggen niet noodzakelijk voor inzage door derden. In de NZA-casus kan gedacht worden aan een systeem waarin standaard niet op basis van DBC-codes gefactureerd wordt, tenzij de patiënt hiertoe toestemming verleent.

6.4.2 Gegevensbeveiliging

Uit de Wbp vloeit direct de plicht voort dat beveiligingsmaatregelen genomen moeten worden. Hier gaat het om een juridische waarborg, waaraan op organisatorische en technische wijze invulling gegeven moet worden. Er zijn verschillende technische mogelijkheden om gegevens te beschermen tegen corruptie, maar ook tegen ongeautoriseerde toegang, zoals autorisatie- en authenticatiemechanismen, anonimiseren, versleuteling en logging. Om een deugdelijke invulling te kunnen geven aan de beveiligingseisen, is input vanuit een Privacy Impact Assessment onontbeerlijk. Op basis hiervan moet immers in kaart gebracht worden voor wie toegang tot bepaalde gegevens onder welke voorwaarden noodzakelijk is.

In de UWV-casus had toegang bijvoorbeeld beperkt kunnen worden tot die werkgevers die daadwerkelijk een vacature open hadden staan. Beter nog, als een werkzoekende op zoek was naar werk in de zorg, zou zijn CV alleen inzichtelijk moeten zijn voor werkgevers die een vacature open hebben staan in de zorg. Hier komt het onderscheid in beeld tussen ‘right to know’ versus ‘need to know’. Bij right to know gaat het om een personenkring die op grond van functieniveau of doel in beginsel toegang moet hebben tot bepaalde gegevens, zoals de UWV-medewerkers. Bij need to know gaat het er om dat ze alleen toegang moeten hebben tot informatie die ze werkelijk nodig hebben voor hun functioneren. Right to know is technisch af te dwingen met autorisatierollen. Bij need to know ligt dat vaak lastiger. In het geval van de IT-werkgevers is dat eenvoudiger dan in het geval van UWV-medewerkers, die je eigenlijk alleen toegang zou willen geven tot ‘hun’ dossiers. In het geval toegang wordt gelogd kunnen betrokkenen worden aangesproken op ongepast gedrag.

In sommige gevallen lijkt het mogelijk om het gewenste beleid te realiseren met geanonimiseerde gegevens. Ook hier geldt, vanuit het oogpunt van privacy by default, dat hiervoor gekozen *moet* worden als het beleidsdoel bereikt kan worden. Hiervan is bijvoorbeeld sprake bij de casus over bouwvergunning en de openbaarmaking van CV’s. Om bezwaar te maken tegen een vergunning, zijn enkel zaken als adres, afmetingen en materiaalsoorten van belang om te vermelden, alle andere persoonsgegevens kunnen verwijderd of onleesbaar gemaakt worden. Bij een CV is het vrijgeven van personalia eigenlijk pas nodig op het moment dat een werkgever interesse toont in een werkzoekende. Hierbij zou het proces ook omgekeerd kunnen worden. Op basis van bijvoorbeeld een nummeringsysteem voor de CV’s kan de werkgever kenbaar maken in welk nummer CV hij interesse

heeft, vervolgens kan het UWV de werkzoekende de personalia van de werkgever verstrekken zodat hij contact kan leggen. In het algemeen is het wenselijk om gegevens zo veel mogelijk te anonimiseren wanneer het niet noodzakelijk is een koppeling met een natuurlijke persoon te leggen, dan wel de gegevens te versleutelen wanneer die koppeling, onder voorwaarden, wel gelegd moet kunnen worden. De sleutels voor ontsleuteling moeten dan in handen liggen van een partij die toezicht kan houden op het gebruik.

6.4.3 Controle over persoonsgegevens

Niet alleen vooraf, maar ook door controlemechanismen achteraf, kan toegang tot persoonsgegevens beperkt worden. Indien door middel van logbestanden bijgehouden wordt wie er op welk tijdstip toegang hebben gehad tot welke gegevens, zal dit een drempel vormen om zich toegang tot gegevens te verschaffen wanneer hiervoor geen goede reden bestaat. Zeker indien het binnen de organisatie bekend is dat ongeautoriseerde toegang consequenties kan hebben. Hoewel hiervan in de bouwvergunning casus in Nijmegen en Groningen geen sprake was, had de gemeente Tilburg wel een dergelijk systeem geïmplementeerd. Door het verplicht te maken met DigiD in te loggen kunnen kwaadwillende derden worden afgeschrikt, terwijl voor goedwillende burgers het gemak van online raadpleging gewaarborgd blijft. Een ander duidelijk voorbeeld waar uitgebreide logs worden bijgehouden met als doel de veiligheid te waarborgen en in de gaten te houden, is Mens Centraal.

6.4.4 Signaleringsmechanismen of geautomatiseerde consistentiechecks

In het verlengde van bovenstaande kan gewezen worden op technische signaleringsmogelijkheden. Bij ongewone of afwijkende activiteit in een systeem, zou de burger automatisch een waarschuwing kunnen krijgen. In de DigiD-casus werd 260 maal met dezelfde DigiD een aanvraag gedaan zonder dat de techniek ervoor zorgde dat de alarmbellen afgingen en systemen werden geblokkeerd. Hetzelfde geldt met betrekking tot de zaak Romet, waar het mogelijk bleek 1737 motorrijtuigen op een naam te registreren. In het verlengde daarvan kunnen ook geautomatiseerde consistentiechecks genoemd worden. Dit zijn controlemechanismen die bijvoorbeeld laten zien dat er wel heel erg vaak met dezelfde DigiD toeslagen worden aangevraagd, of dat er wel erg veel auto's op dezelfde naam staan.

6.4.5 Overzichtelijkheid systeemstructuur

Beveiliging en controle zijn niet alleen op systeemniveau van belang, maar ook op een meer overkoepelend niveau. Doordat systemen en bestanden gekoppeld worden, rijzen er nieuwe en andere beveiligingsvragen. Als door de verknoping van systemen het overzicht over het geheel verloren gaat, blijkt uit de cases Mens Centraal, Kowsoleea en Romet dat hieruit grote bedreigingen voor de privacy kunnen voortvloeien. In de Europese Privacyverordening staat dat er voor elke koppeling van bestanden steeds opnieuw een Privacy Impact Assessment uitgevoerd zou moeten worden. Want het feit dat de privacy per systeem voldoende gewaarborgd is, geeft geen garantie dat deze ook gewaarborgd is na koppeling van systemen. De zaak Kowsoleea laat overigens ook zien hoe een gebrek aan koppelingen en verificatiemechanismen tussen systemen problematisch kan zijn. Hierdoor was het mogelijk dat in zeer veel verschillende bestanden foutieve informatie stond, hetgeen het voor de burger bemoeilijkte deze informatie te

schonen. Bovendien ligt de verantwoordelijkheid om fouten in systemen te schonen bij de overheid, al dan niet op verzoek van de burger.

6.5 Conclusie

De cases maken duidelijk dat er ondanks goede bedoelingen van de overheid, tal van privacy inbreuken plaatsvinden als gevolg van overheidsbeleid en -uitvoering. De gevolgen zijn gedeeltelijk te voorzien, te voorkomen en te repareren. Het feit dat het niet erg moeilijk was om een verzameling van negen cases te vinden, laat echter ook zien dat verbetering mogelijk en nodig is. Een opvallende observatie is dat veel van de problemen die geconstateerd worden, veroorzaakt worden door de *eOverheid* in plaats van de *iOverheid*. Ondanks dat de iOverheid zorgt voor een toename in de gegevenskoppeling tussen verschillende registraties en databases, spelen veel van de privacyvraagstukken rondom de inrichting van dienstverlening richting burgers – de eOverheid. Er is dan ook geconstateerd dat de meeste privacy schendingen die zijn onderzocht niet per se het resultaat zijn van het beleidsdoel, maar van de inrichting van het beleid.

Verwacht wordt dan ook dat wanneer de iOverheid zich zal blijven ontwikkelen, zoals in het WRR-rapport wordt geschetst, de risico's met betrekking tot privacy alleen maar groter worden. Daar komt bij dat de aandacht voor privacy groeiend is. Dit komt bijvoorbeeld tot uiting in het groeiend aantal burgerrechtorganisaties dat zich inzet voor de privacy. De overheid en maatschappij worden, op sommige punten, dus gevoeliger voor privacy en de zorgvuldige omgang met persoonsgegevens. De analyse, het voorkomen van problemen en de aanpak van gerezen problemen, vergt kennis en kunde op de gebieden van privacy by design en privacy by default. Ook zal er in toenemende mate toezicht nodig zijn op de naleving van privacywetgeving, bijvoorbeeld door het CBP of door het aanstellen van privacy officers of FG's. We moeten constateren dat deze velden in ontwikkeling zijn. De auteurs hopen dat deze rapportage een bijdrage levert om deze onderwerpen hoger op de agenda te krijgen.

Referenties

Wetenschappelijke Raad voor het Regeringsbeleid (WRR), *iOverheid*, WRR-rapport nr. 86, 15-03-2011.

DigiD-casus

NRC Next, 19 september 2011, Makkelijker konden ze het niet maken
http://www.ad.nl/ad/nl/1012/Binnenland/article/detail/2840928/2011/08/08/Ombudsman-bekritiseert-overheid-om-DigiD.dhtml
Brief van Staatssecretaris van Financiën, beantwoording Kamervragen
Interview Rejo Zenger, privacyvoorvechter, 7 november 2012.
Toeslagfraude, 23 september 2011,
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/09/23/beantwoording-kamervragen-toeslagfraude/beantwoording-kamervragen-toeslagfraude.pdf
Tv-programma De Ombudsman, http://ombudsman.vara.nl/Fragment-detail.8315.0.html?&tx_ttnews[tt_news]=57251&cHash=a0966b42e76478213fb0bd16d7ae1c79
Sargasso, Massafraude met belastingtoeslagen via DigiD,
http://sargasso.nl/wvdd/massafraude-met-belastingtoeslagen-via-digid/

Bouwvergunningen-casus

Arnoud Engelfriet, http://blog.iusmentis.com/2010/04/13/gemeente-groningen-publiceert-volledige-vergunningen-online/, met commentaar van Eric Hennekam
http://www.higherlevel.nl/forum/index.php?board=50;action=display;threadid=41315
Brief van het CBP van 1 december 2005 met als kenmerk z2005-00212,
Beschikbaar via: www.cbpweb.nl
CBP, *Advies Wabo/BOR,* 15 mei 2007 z2007-00304.
CBP, *Aanvragen bouwvergunning niet meer integraal op internet. Gemeente Nijmegen en ministerie van VROM passen werkwijze aan*, 10 maart 2008 z2007-00238.
Informatie Publicatie Model (IPM) Vergunningen 4.0.,
http://www.overheidheeftantwoord.nl/producten,vergunningen
https://www.ictu.nl/archief/www.e-overheidvoorburgers.nl/faq,Vergunningen-Organisatie.html
RTVOOG 13 juli 2010, www.youtube.com/watch?v=wCSrVFkT3d

UWV-casus

De Nationale Ombudsman, Rapport 2011/191, 28-06-2011, http://ombudsman-acc.triquanta.nl/rapporten/2011/191?aresult=25#.
Jaarverslag UWV 2011, http://jaarverslag.uwv.nl/
Besluit SUWI aan de Minister van Sociale Zaken en Werkgelegenheid,
http://www.cbpweb.nl/downloads_adv/z2010-00496.pdf.
Uitvoeringsprogramma "Compacte Rijksdienst",
http://www.rijksoverheid.nl/documenten-en-publicaties/jaarplannen/2011/02/14/uitvoeringsprogramma-compacte-rijksdienst.html.

CBP (2010) *Wetgevingsadvies wijziging UWV Jaarplan 2012*, http://www.rijksoverheid.nl/documenten-en-publicaties/jaarplannen/2011/12/20/uwv-jaarplan-2012.html
UWV Werkbedrijf, http://www.uwv.nl/OverUWV/wat_is_uwv/wat_doet_uwv/uwv-werkbedrijf.aspx.

ANPR-casus

Alfen, S. van 'Fiscus bespioneert leaserijders', *De Telegraaf*, 11 februari 2011.
Fleetlogic Nieuws, 'Controlethema Belastingdienst: Privégebruik van de leaseauto', 22 maart 2011.
Interview Jan de Groot, senior beleidsmedewerker bij Directoraat-Generaal Belastingdienst van het Ministerie van Financiën, 26 september 2012.
Interview Peter Ruijs, hoofdredacteur 'Belastingzaken', 18 september 2012.
Pekarek, M., Roosendaal, A. & Sluijs, J. 'Surveillance as a Service', *Conference proceedings CPDP 2012* (in druk).
Ruijs, P. 'Big Brother', Redactioneel in *Belastingzaken*, 2012 (7), p. 3.

Charlois-casus

http://versbeton.nl/2012/04/einde-etnisch-voorkeursbeleid-charlois-ophanden/.
http://www.rijnmond.nl/nieuws/24-01-2012/charlois-wil-etnische-registratie-doorzetten.
College Bescherming Persoonsgegevens, *Onderzoek naar de verwerking van persoonsgegevens betreffende ras/etniciteit in het kader van DOSA door het dagelijks bestuur van de Deelgemeente Charlois, Rotterdam. Z2009-00449. Rapport van definitieve bevindingen*, april 2012.
College Bescherming Persoonsgegevens, *Beslissing op bezwaarschrift van deelgemeente Charlois*, 19 juli 2011.
College Bescherming Persoonsgegevens, *Last onder dwangsom*, 27 januari 2011.
College Bescherming Persoonsgegevens, *Rechtbank verklaart beroep Charlois tegen besluit CBP ongegrond Deelgemeente mag geen gegevens over etniciteit risicojongeren registreren*, 23 mei 2012,
http://www.cbpweb.nl/Pages/med_20120523_beroep-charlois-tegen-besluit-cbp-ongegrond.aspx
Interview Herman Gerrits, locosecretaris van de deelgemeente Charlois, 19 oktober 2012.
Interview Yvo Rodermans, beleidsmedewerker GroenLinks-fractie Rotterdam, 19 oktober 2012.
NRC, *Charlois stopt etnische registratie onder dreiging van dwangsom CBP*, 2 februari 2011.
Trouw, *Charlois: registratie van etniciteit werkt*, 5 februari 2011.
09GR1534 Van B en W de beantwoording van de schriftelijke vragen van mevrouw Verwijs over registratie van etniciteit,
http://www.bds.rotterdam.nl/Bestuurlijke_Informatie:7/Raadsinformatie/Gemeenteraad_2006_2010/2009/Kwartaal_2/Raadsvergadering_van_11_juni_2009/Mededeling_van_ingekomen_stukken_2009_week_18_t_m_22/Beantwoording_van_schriftelijke_vragen/09GR1534_Van_B_en_W_de_beantwoording_van_de_schriftelijke_vragen_van_mevrouw_Verwijs_over_registratie_van_etniciteit.

NZa-casus

Lo Galbo, C. *De psychiater en uw privacy*, (Vrij Nederland, 14 april 2009). http://www.vn.nl/Archief/Samenleving/Artikel-Samenleving/De-psychiater-en-uw-privacy.htm.
CBb 8 maart 2012, LJN: BV8297.
CBb 2 augustus 2010, LJN: BN3056 en CBb 2 augustus 2010, LJN: BN3059.
http://www.enrgin.nl/xdata/devrijepsych/Downloads/BoB%20NZa%20050411.pdf.
De Rechtspraak (2010) *Vermelding diagnose op declaraties voorlopig van de baan.* http://www.rechtspraak.nl/Organisatie/CBb/Nieuws/Pages/Vermelding-diagnose-op-declaraties-voorlopig-van-de-baan.aspx.
Taskforce DBC Declaraties (2006) *Eindrapport Taskforce DBC Declaraties*. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2006/10/09/eindrapport-taskforce-dbc-declaraties.html
DeVrijePsych (2011) *Archief nieuwsberichten 2011,* http://www.devrijepsych.nl/?pagina=Archief%20%2711&id=276.
Schoemaker, R. (Webwereld) (2011) *Artsen naar rechter vanwege 'risicovolle' database,* http://webwereld.nl/nieuws/106732/artsen-naar-rechter-vanwege--risicovolle--database.html.
NZa (2011) *Privacy voldoende gewaarborgd bij GGZ-declaraties,* http://www.nza.nl/publicaties/nieuws/282504/

Haagse pandbrigades/Rotterdams interventieteam-casus

Nationale ombudsman, rapporten 2009/030, 2009/095 en 2009/210 van de Nationale ombudsman en de gemeentelijke ombudsman Zeist, www.nationaleombudsman.nl.
Gemeentelijke Ombudsman Rotterdam (2011) *Interventieteams: kijken en bekeken worden. Een onderzoek naar de dagelijkse praktijk van de Rotterdamse interventieteams,* http://www.ombudsman.rotterdam.nl/publicaties/Rapport%20Interventieteams.pdf.
Bits of Freedom (2010) *Juryrapport Big Brother Awards 2010,* https://www.bigbrotherawards.nl/wp-content/uploads/2011/02/bba2010-juryrapport-WEB-FINAL.pdf.
DenHaag.nl (2012) *De Haagse Pandbrigade. Verbeteren van de leefbaarheid en veiligheid in Den Haag,* http://www.denhaag.nl/home/bewoners/to/De-Haagse-Pandbrigade.htm.
Rotterdam.nl (Gemeente Rotterdam) *Interventieteams op huisbezoek*, http://www.rotterdam.nl/interventie.
Dumpert (2009) *GemeenteGestapo Rotterdam* (video) http://www.dumpert.nl/mediabase/707001/9b6372a9/gemeentegestapo_rotterdam.html.
Protocol Huisbezoeken stedelijke & deelgemeentelijke interventieteams en Bureau Frontlijn in Rotterdam (juni 2010), http://www.rotterdam.nl/Directie%20Veilig/PDF/Overige%20publicaties/protocol%20huisbezoeken%20interventieteams%202010.pdf.
Anarchiel (2009) *Hallo, doet u even open? Wij komen uw woning controleren,* http://www.anarchiel.com/display/hallo_doet_u_even_open_wij_komen_uw_woning_controleren en http://www.anarchiel.com/library/read/telefoongesprekpandbrigade_in_tekst.

DenHaag.nl (2010) *Controle Haagse Pandbrigade - RIS 173946,* http://www.denhaag.nl/home/bewoners/de-gemeente-Den-Haag/Ris/document/Controle-Haagse-Pandbrigade.htm.
Gemeente Den Haag (2010) *Beantwoording schriftelijke vragen van het raadslid de heer G.H.M. Wijsmuller. Sv 2010.186; RIS 173946; Regnr. DSO/2010.1753,* http://www.denhaag.nl/web/wcbservlet/com.gxwebmanager.gxpublic.risbis.fileservlet?fileid=67709744-b4c5-47d8-a17a-23afcc189954.
DenHaag.nl (2012) *Protocol huisbezoeken - RIS 247261*, http://www.denhaag.nl/home/bewoners/de-gemeente-Den-Haag/Ris/document/Protocol-huisbezoeken.htm.
Van der Bol, B. (voor Binnenlands Bestuur, 2010) *Pandbrigade kuist Haagse wijken*, http://www.binnenlandsbestuur.nl/ruimte-en-milieu/achtergrond/achtergrond/pandbrigade-kuist-haagse-wijken.158102.lynkx.
Tokmetzis, D. (voor Sargasso, 2010) *Haagse Pandbrigade: Verzet en vragen,* http://sargasso.nl/haagse-pandbrigade-verzet-en-vragen/
Gemeentelijke ombudsman Rotterdam (2007) *"Tja, wij komen eigenlijk voor alles…" Rapport van een ambtshalve onderzoek naar de praktijk van huisbezoeken,* http://www.ombudsman.rotterdam.nl/publicaties/Eindrapport%20Baas%20in%20eigen%20Huis.pdf.
Brief Dienst Stedelijke Ontwikkeling, Gemeente Den Haag:
http://img18.imageshack.us/img18/8489/briefgemeentedeel1.jpg
http://img35.imageshack.us/img35/2174/briefgemeentedeel2.jpg

Mens Centraal-casus

http://www.operatiemenscentraal.nl
http://www.menscentraal.com
Kennisdocument Achtergrondinformatie Mens Centraal, april 2009. http://www.kinggemeenten.nl/media/11966/kennnisdocument_mens_centraal_270409_definitief%20(1).pdf
Inspectie Werk en Inkomen. Beveiliging en privacy in de SUWI-keten en Vervolgonderzoek Beveiliging en privacy in de SUWI-keten.
Interview Peter de Punder, projectmanager Dienstverlening bij de gemeente Tilburg, 5 november 2012.
http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2009/06/04/iwi-onderzoek-beveiliging-en-privacy-in-de-suwi-keten/129-2009-3-13109.pdf
Inspectie Werk en Inkomen. Vervolgonderzoek Beveiliging en privacy in de SUWI-keten. http://www.inspectieszw.nl/images/nvb%20info%2011-10%20d%20vervolgonderzoek%20beveliging%20en%20privacy%20in%20de%20suwi-keten_tcm335-327743.pdf

Identiteitsfraude-casus

http://www.ioverheid.nu/rapport.html
Europees Hof voor de Rechten van de Mens, 14 Februari 2011, *Romet v. The Netherlands*, Application no. 7094/06, http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109080
Eerherstel gloort voor 'frauderende' zzp'er, nu.nl 3 juni 2011, http://www.nuzakelijk.nl/algemeen/2531549/eerherstel-gloort-frauderende-zzper.html

Alsnog gelijk voor WW-starters na extra check, De Telegraaf 12 december 2011, http://www.telegraaf.nl/mijnbedrijf/financiele_zaken/11108769/__Alsnog_gelijk_voor_WW-starters_na_extra_check__.html
Onschuldig maar bekend als zware crimineel, Algemeen Dagblad 15-03-2009, http://www.ad.nl/ad/nl/1012/Nederland/article/detail/2000648/2009/03/15/Onschuldig-maar-bekend-als-zware-crimineel.dhtml
Als je identiteit gestolen wordt, verwoest dat je hele leven, Radio Nederland Wereldomroep 13-01-2011, http://www.rnw.nl/suriname/article/als-je-identiteit-gestolen-wordt-verwoest-dat-je-hele-leven
Tweede Kamer, vergaderjaar 2009-2010, 8 juni 2010, aanhangselnummer 2503, *Vragen van de leden Gerkens (SP) en Teeven (VVD) aan de minister van Justitie over de verantwoordelijkheid voor de afwikkeling van schade door identiteitsfraude (ingezonden 16 april 2010), Antwoord van minister Hirsch Ballin (Justitie) (ontvangen 19 mei 2010).*
Van der Meulen, N.S. (2011). *Financial Identity Theft: Context, Challenges and Countermeasures.* T.M.C. Asser Press.
Frank Bongers et al., *Burgers aan bod. Elektronische overheidsdienstverlening in het perspectief van de vraagzijde. In opdracht van het Ministerie van Binnenlandsze Zaken en Koninkrijksrelaties Directie Innovatie- en Informatiebeleid Openbare sector.* Dialogic, Utrecht, 2004, www.rinc.nl/KASS/download.php?object=531859
Kafka brigade*, http://www.kafkabrigade.nl/index.php?page=2010-2&hl=nl_NL*