TNO
Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO-rapport 35598

Trusted Technology
Een onderzoek naar de toepassings-voorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid

Datum	05 december 2011
Auteur(s)	L. Kool, B. van Schoonhoven en M. van Lieshout (TNO) A. Vedder en F.M. Fleurke (UvT)
Aantal pagina's	89 (incl. bijlagen)
Aantal bijlagen	2
Opdrachtgever	Alliantie Vitaal Bestuur

Inhoudsopgave

Management Samenvatting

1. Aanleiding en probleemstelling onderzoek

De inzet van informatie- en communicatietechnologie (ICT) biedt kansen voor een effectieve overheidsdienstverlening. Bovendien maakt ICT het leveren van maatwerk eenvoudiger, brengt het gemak en draagt het bij aan de emancipatie van de burger. Toekomstige technologische ontwikkelingen, zoals intelligente sensoren of geavanceerde dataminingtechnieken, zullen nog meer mogelijkheden voor effectieve en gepersonaliseerde overheidsdienstverlening creëren (Frissen et al, 2007). Inherent aan deze ontwikkeling is de toenemende verzameling, opslag, verwerking en verspreiding van persoonlijke gegevens van burgers door de overheid. Ook nu al zorgt dit voor maatschappelijke discussie. Het behoeft geen uitleg dat de privacy van burgers bij de inzet van deze en toekomstige ICT innovaties onder druk kan komen te staan als er niet zorgvuldig met deze gegevens wordt omgegaan.

Door de snelle technologische ontwikkeling wordt de uitvoering en handhaving van bestaande wetgeving om privacy te beschermen steeds moeilijker. Daarom is er in toenemende mate belangstelling voor aanvullende mogelijkheden om privacy beter te beschermen. Een van die mogelijkheden is *Privacy by Design* (PbD). Onder *Privacy by Design* (PbD) wordt verstaan dat al bij het ontwerpen en de toepassing van technologie in (elektronische) dienstverlening rekening wordt gehouden met de noodzaak van privacybescherming. Het concept wordt van belang geacht voor de herziening van de Europese dataprotectierichtlijn 95/46/EG)[1]. De algemene veronderstelling is dat PbD het vertrouwen in en de legitimiteit van ICT-overheidshandelen kan vergroten. Dit vertrouwen is essentieel, gezien de geweldige opkomst van online (overheids-)dienstverlening en de ontwikkeling van de informatiemaatschappij als geheel. De precieze relatie tussen het toepassen van *Privacy by Design* en het vergroten van vertrouwen, legitimiteit en acceptatie is echter nog niet systematisch onderzocht. Het is dus allerminst zeker dat het toepassen van PbD ook daadwerkelijk het vertrouwen van burgers in overheid én technologie vergroot. Dat is het onderwerp van voorliggend onderzoek.

De centrale probleemstelling van het onderzoek luidt:
In hoeverre, en onder welke voorwaarden, vergroot de inzet van PbD de legitimiteit en verantwoordelijkheid[2] *van de overheid – ofwel de acceptatie en het vertrouwen van de burger in elektronische overheidsdienstverlening – zonder de effectiviteit en doelmatigheid van dat handelen onaanvaardbaar te verkleinen*?

---

[1] Reding, V. (2010) Doing the single market justice, Speech for Conference of the Lisbon Council, Speech/10/441, 16 September 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/441&format=HTML&aged=0&language=EN&guiLanguage=en; Article 29 Data Protection Working Party and Working Party on Policy and Justice (2009) The future of privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/ENWP 168, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[2] Wij gebruiken deze term als het Nederlandse equivalent van de term 'accountability' in het politiek theoretische en ethische debat. Het gaat hierbij om verantwoordelijkheid in de zin van zich goed kunnen ventwoorden.

De focus van dit onderzoek ligt op eOverheidsdiensten, zoals het aanvragen van vergunningen, identiteitsdocumenten, belastingaangiftes, sociale verzekeringen e.d. ICT-toepassingen in het opsporings- en veiligheidsdomein vallen daarmee buiten het bereik van dit onderzoek.

2. Doelstelling
De doelstelling van het onderzoek is een afwegingskader te formuleren met behulp waarvan de overheid kan beslissen onder welke voorwaarden PbD kan worden ingezet zodanig dat de verantwoordelijkheid en de legitimiteit van de overheid en het vertrouwen in en de acceptatie van de overheidsdienstverlening zichtbaar wordt gemaakt of vergroot zonder teveel afbreuk te doen aan de effectiviteit[3] en doelmatigheid van de dienstverlening.

3. Trendverkenning
In Hoofdstuk 3 wordt beknopt in kaart gebracht welk technologische trends (gerelateerd aan ICT) de komende jaren belangrijk zullen worden met een impact op de persoonlijke levenssfeer. Aan de orde komen: breedbandige en convergerende infrastructuren, utility computing, het intelligente web, informatieverwerking en convergerende technologieën. De trends laten nieuwe mogelijkheden over overheidsdienstverlening zien met mogelijkheden voor personalisatie en *empowerment* van de burger, maar tonen tegelijkertijd ook mogelijke risico's voor het waarborgen van privacy. De beschreven trends brengen daarnaast nieuwe beveiligings- een aansprakelijkheidskwesties met zich mee en de verantwoordelijkheidsverdeling tussen overheidsinstanties wordt complexer en diffuser.

4. Overheidsdienstverlening en privacybescherming
In Hoofdstuk 4 beschrijven we de belangrijkste begrippen in dit onderzoek: privacy, elektronische dienstverlening door de overheid, Privacy by Design en de elementen die onder dit begrip vallen. Onder *bescherming van privacy* verstaan we in dit rapport activiteiten die erop zijn gericht om de toegang tot het individu in ruimtelijke, relationele en informationele zin te reguleren. Privacybescherming gaat daarmee uitdrukkelijk verder dan de bescherming van persoonsgegevens (dataprotectie). Bescherming van privacy is er uiteindelijk op gericht om de persoonlijke autonomie van mensen te beschermen of te vergroten en hun kwetsbaarheid (bijvoorbeeld voor materiële schade, discriminatie, stigmatisering) te verminderen of in elk geval niet verder te vergroten.

In dit rapport hanteren wij de volgende stipulatieve definitie voor *Privacy by Design*: *Privacy by Design houdt in dat vanaf het (her)ontwerp en gedurende de gehele levenscyclus van een informatiesysteem (tot aan afbouw dan wel vervanging) met behulp van zowel technische als organisatorische maatregelen inbreuken op de persoonlijke levenssfeer worden vermeden.*

[3] Met effectiviteit wordt hier primair bedoeld: het verwezenlijken van het oorspronkelijk beoogde doel van de dienstverleningstoepassing. Uiteraard kan de verwezenlijking van dat doel op verschillende manieren in gevaar worden gebracht, bijv. doordat de toepassing van PET/PbD de vereiste handelingen van de burger te omslachtig maken, maar ook doordat PbD bijvoorbeeld transparantie kan vereisen die direct in strijd is met een indirect beoogd opsporingsdoel (wanneer bijvoorbeeld een kentekenregistratiesysteem-met-smart camera's wordt gebruikt om bankovervallers te vinden).

Bij de uitwerking van de definitie van PbD hanteren wij de volgende parameters[4]:

1. Privacy Impact Assessments (PIA): De eerste stap bij het toepassen van PbD is een goed beeld te krijgen van de mogelijke privacykwesties die de introductie of aanpassing van een IT-systeem of dienst teweeg brengt. Een PIA *maakt* vooraf een inschatting van de privacyrisico's van het te ontwerpen informatiesysteem (risicoanalyse). Tevens wordt in kaart gebracht hoe deze risico's vermeden of verkleind kunnen worden.
2. *Privacy in de organisatie*: Om de legitimiteit van het informatiesysteem te verzekeren zal nagedacht moeten worden over de inbedding van het systeem binnen de organisatie die er gebruik van maakt. Voor de organisatie is het in de eerste plaats van belang welke wettelijke eisen worden gesteld aan de bescherming van de privacy. Welke verplichtingen heeft de beheerder van het informatiesysteem en hoe is deze aanspreekbaar? Uit het Europese recht vloeit een aantal concrete verplichtingen voort, zoals doelbinding, dataminimalisatie, transparantie van gegevensverwerking, meldingsplicht e.d. In Nederland zijn de Europeesrechtelijke verplichtingen geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Samengevat vereist de Wbp explicitering van de verantwoordelijkheden voor de verwerking van persoonsgegevens en een deugdelijk beveiligingsregime voor de opslag en verwerking van de betrokken gegevens. Daarnaast zijn er andere elementen die de legitimiteit en verantwoordelijkheid van organisaties kunnen vergroten, zoals het aanstellen van een Privacy Officer en het bewust maken en het trainen van personeel in het beleid dat de organisatie heeft opgesteld ten aanzien van de omgang met persoonsgegevens.
3. *Privacy Enhancing Technologies*: In aanvulling op de organisatorische maatregelen wordt steeds meer ingezet op technische middelen om privacy te garanderen. Privacy Enhancing Technologies (PET's) zijn technische instrumenten om privacyrisico´s te verkleinen of in zijn geheel te vermijden. Toepassingsmogelijkheden zijn er in overvloed. Ze kunnen zich bijvoorbeeld richten op het minimaliseren van de hoeveelheid gegevens die over een persoon verzameld en opgeslagen worden, of op het voorkomen van strijdigheid met privacyprincipes, of op het inzetten van controle-instrumenten die gebruikers kunnen hanteren om na te gaan welke informatie over hen verzameld en gebruikt wordt. Hier vallen ook (transparantie)tools en instrumenten onder om datasubjecten meer inzicht te geven in en controle te geven over de processen rond de verzameling en verwerking van hun persoonsgegevens.

5. Legitimiteit, verantwoordelijkheid, vertrouwen en acceptatie

In Hoofdstuk 5 is onderzocht hoe volgens de literatuur vertrouwen en acceptatie bij de burger en de verantwoordelijkheid en legitimiteit van de betrokken overheden elkaar beïnvloeden. Aan de hand van stipulatieve definities van de noties verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie is de onderlinge samenhang van deze begrippen weergegeven en is dit toegepast op elektronische dienstverlening door de overheid. Daarbij dient te worden vermeld dat specifiek onderzoek naar de legitimiteit van elektronische dienstverlening door de overheid

4 Hierbij moet worden opgemerkt dat ook andere parameters kunnen worden onderscheiden, zoals privacy in de fysieke ruimte (zie bijvoorbeeld Cavoukian, 2009) of de representatie van de gebruiker (zie bijvoorbeeld van Lieshout et al., 2011). Wij hebben gekozen voor deze parameters, omdat zij het beste bij het onderzoeksobject (overheidsdiensten) van dit rapport passen.

tot dusver ontbreekt, voor zover dit niet direct of indirect wordt geïmpliceerd door het debat over vertrouwen en acceptatie. Tenslotte gaan we in op de rol die privacyoverwegingen spelen bij verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie m.b.t. elektronische dienstverlening door de overheid. Ook hier geldt hetzelfde voorbehoud ten aanzien van bestaand onderzoek en literatuur.
[deze nog nalopen op belangrijkste conclusies H5]

6. Empirisch onderzoek
In hoofdstuk zes is de perceptie van burgers ten aanzien van de inzet van PbD met het oog op de aanvaardbaarheid van de toepassing en het vertrouwen in overheidshandelen onderzocht. Het onderzoek naar de perceptie van burgers vond plaats aan de hand van drie focusgroepen. In interviews worden overheidsfunctionarissen en experts op het gebied van privacy, legitimiteit en techniek gevraagd om te reflecteren op de gevonden resultaten en de relatie tussen legitimiteit, functionaliteit en PbD te verkennen en de condities voor het afwegingskader te bespreken. De uitkomsten van de focusgroepen en de expertinterviews vormen input voor het uiteindelijke afwegingskader. Privacy by Design biedt de overheid de mogelijkheid om op een systematische manier privacybescherming in te bouwen in (nieuwe) overheidsdiensten. Het empirisch onderzoek wijst echter uit dat Privacy by Design – in de ogen van de burger – niet perse leidt tot meer vertrouwen en acceptatie van e-overheidsdienstverlening. Uit het onderzoek blijkt dat de perceptie van burgers verschilt voor de verschillende parameters van PbD. Vooral die elementen van Privacy by Design die de transparantie van gegevensverwerking door de overheid vergroten, lijken een positief effect te hebben op vertrouwen. Samenvattend:

- PET's zijn moeilijk te doorgronden en lijken door deelnemers niet altijd even effectief te worden geacht, waardoor toepassing van PET niet zonder meer leidt tot meer vertrouwen en hogere acceptatie. Mogelijk kan het toepassen van PET wel indirect leiden tot meer vertrouwen en acceptatie doordat de kans op privacy-incidenten afneemt. Aangezien de deelnemers aangeven dat berichtgeving over privacy-incidenten een negatieve invloed heeft op hun vertrouwen in dienstverlening, kan het voorkomen van incidenten – en de berichtgeving daarover – tot minder vertrouwensverlies leiden.
- PIA's lijken een positief effect te hebben op het vertrouwen en acceptatie. Uit de focusgroepen komen geen situaties naar voren waar PIA's een negatief effect zouden kunnen hebben op vertrouwen en acceptatie. Wel geven burgers aan zich zorgen te maken over de openbaarmaking van PIA's omdat kwaadwilligen mogelijk misbruik kunnen maken van de geconstateerde kwetsbaarheden. Tegelijkertijd vinden deelnemers het wel belangrijk dat een dergelijke analyse wordt uitgevoerd.
- Wetgeving en organisatorische elementen die zichtbaar zijn voor de burger lijken een positief effect te hebben op vertrouwen, als deze maatregelen zichtbaar zijn of worden gemaakt aan burgers (zoals een herkenbaar aanspreekpunt, de *data breach notification*, daaraan gekoppelde sancties, openheid over gegevensverwerking, toegeven van mogelijke fouten). Het positieve effect van maatregelen die de transparantie over gegevensverwerking verhogen, kan worden aangetast op het moment dat het betekent dat er veel incidenten zichtbaar worden voor burgers (bij wijze van spreken: 1 keer een fout toegeven is sympathiek, bij 10x ben je een kluns);

- Keuze, controle en zeggenschap van burgers in de dienst: meer zeggenschap bij burgers zelf lijkt positief effect te hebben op vertrouwen en adoptie.

De ene eOverheidsdiensten is echter de andere niet. Uitvoeringsprojecten bij de overheid kunnen sterk verschillen in de mate van complexiteit, omvang en maatvoering. Daarom dient, alvorens het hierna volgende beoordelingsinstrument te hanteren, het desbetreffende project eerst te worden geïdentificeerd. Dat kan met behulp van de volgende vragen:

- Wat is de doelstelling, reikwijdte en rationale van het project?
- Worden er in het project of het te ontwikkelen systeem nieuwe informatietechnologieën toegepast die een substantiële impact op de persoonlijke levenssfeer van burgers kunnen hebben (zoals biometrie, gezichtsherkenning, locatiebepaling, profilering e.d.)?
- Worden er in het te ontwikkelen/implementeren systeem persoonsgegevens verwerkt en op welke schaal?
- Zijn er meerdere overheidsinstanties bij de ontwikkeling, implementatie of uitvoering van het informatiesysteem betrokken of worden er gegevens gebruikt, verzameld of verwerkt van of bij andere uitvoeringsinstanties of private organisaties?

7. Afwegingskader PbD

Een afwegingskader (zie Hoofdstuk 7) is een instrument in handen van een overheidsorganisatie die (delen van) haar dienstverlening met behulp van ICT wil institutionaliseren, en daarbij Privacy by Design (PbD) toepast. De vraag daarbij is aan welke eisen of condities PbD, in welke vorm dan ook en gelet op de resultaten van het empirisch onderzoek, moet voldoen. Deze eisen of condities zijn afgeleid uit het in hoofdstuk vier en vijf ontwikkelde theoretische kader en de empirische resultaten uit hoofdstuk zes en hebben betrekking op de volgende elementen of aspecten:

I Condities voor verantwoordelijkheid (‘accountability’, d.w.z. zich goed kunnen verantwoorden);
II Condities voor vertrouwen in en acceptatie van overheidsdienstverlening;

Beiden zijn voorwaarden voor vertrouwen en acceptatie van overheidsdienstverlening (door middel van ICT) en hangen nauw met elkaar samen, waarbij de condities voor verantwoordelijkheid generieke voorwaarden zijn en de condities voor vertrouwen en acceptatie specifieke voorwaarden zijn.

I *Condities voor verantwoordelijkheid*

a. Het standaard vooraf uitvoeren van een Privacy Impact Assessment en het herhalen van een PIA bij substantiële wijziging van informatiesystemen en –processen of wetgeving.[5] De PIA karakteriseert het IT-systeem (datatypen, datastromen, opslag en verwerking van gegevens), identificeert privacyrisico’s en bijbehorende beheersmechanismen[6].

[5] De PIA kan het Integrale Afwegingskader (IAK) van het Rijk en de daarbij behorende uitvoeringstoetsen (zie Rijksoverheid, 2010) verrijken
[6] Hierbij kan gebruik worden gemaakt van bestaande PIA-raamwerken en zogenaamde ‘templates’.

b. Het aanstellen van een (part-time) Privacy Officer/Gegevens Functionaris in de betreffende overheidsorganisatie, die tot taak heeft toezicht uit te oefenen op het functioneren van de dataverwerkers c.q. contactambtenaren en tot wie burgers toegang hebben indien zij naar hun mening niet adequaat worden geholpen door de dataverwerkers c.q. contactambtenaren[7].
c. Actieve voorlichting van de overheidsorganisatie over alle aspecten van het ICT-instrument aan de doelgroep.
d. Het helder positioneren van de betreffende ICT-dienstverlening en de uitvoerende overheidsinstantie ten opzichte van andere publieke en private dienstverleners en de sociale media: Welke overheidsorganisatie is aanbieder van dienst en waarvoor wordt de dienst gebruikt?
e. Burgers standaard inzage geven van alle gegevens die op hem/haar betrekking hebben en hoe deze worden verwerkt.[8]
f. Duidelijke afspraken, afbakening en communicatie naar de burgers over: i) van welke gegevens wordt gebruik gemaakt (nieuwe verzameling of wordt er gebruik gemaakt van bestaande databases van andere overheidsorganisaties), ii) welke andere (overheids-) organisaties maken gebruik van de verzamelde gegevens, iii) waar worden de gegevens bewaard en iv) welke organisatie is voor welke dataverzamelingen verantwoordelijk?

II *Condities voor vertrouwen in en acceptatie van overheidsdienstverlening*

a. Het standaard realiseren van dataminimalisatie en datavernietiging als het doel waarvoor de gegevens zijn verzameld is bereikt.
b. Accuraatheid, up-to-date zijn en compleetheid van de opgeslagen data.
c. Heldere, specifieke en eenduidige formulering van het doel van de dataverzameling.
d. Het afdwingen van doelbinding[9] en overige privacyprincipes in de volledige levenscyclus van het systeem en de uitvoering van constante controles daarop.
e. Adequate beveiliging van de data, inclusief de technische uitwerking daarvan.
f. Het inbouwen van technische privacywaarborgen waar dit van toepassing is, zoals anonimiteit, pseudonimiteit, onverbondenheid, onwaarneembaarheid.
g. Het beschikbaar stellen van voldoende expertise in beveiliging.
h. Het beschikbaar stellen van instrumenten aan 'data-subjecten' om datasporen te kunnen volgen binnen de organisatie.
i. Openheid over geconstateerde privacy-incidenten en communicatie over de genomen maatregelen naar burgers.[10]
j. De aanwezigheid van een sterke onafhankelijke toezichthouder die controleert in hoeverre regelgeving omtrent privacy en dataprotectie wordt nageleefd

[7] Een Privacy Officer heeft een ander aandachtsgebied van de Information Officer die belast is met de besturing en beheersing van grootschalige ICT-projecten binnen de overheid en de positionering en kwaliteit van informatiemanagement en in 2009 binnen de ministeries zijn aangesteld.
[8] Een voorbeeld hiervan is mijnoverheid.nl. Ook bij de OV-chipkaart is het sinds kort mogelijk voor reizigers om hun gegevens in te zien.
[9] Hierbij moet worden opgemerkt dat het doel van het systeem kan veranderen als de wettelijke basis is veranderd (door wijziging van wet of het aannemen van een nieuwe wet).
[10] In de volgende wetswijziging van de Wet bescherming persoonsgegevens zal hiervoor een meldpunt worden ingericht.

Indien aan deze 16 condities is voldaan, kan de conclusie worden getrokken dat de betreffende overheidsorganisatie (i.c. haar bestuurders/beleidsmakers) beschikt over een ICT-overheidsdienstverlening die de kwalificatie 'trusted technology' verdient. Dat is een technologie waarin op overtuigende wijze privacy, vertrouwen, verantwoordelijkheid en acceptatie zijn gerepresenteerd.

Tot slot dient nog te worden nagegaan of en hoe deze 'trusted technology' kan worden ingevoerd of kan functioneren, zonder dat afbreuk wordt gedaan aan de effectiviteit en doelmatigheid van de overheidsdienstverlening. De criteria hiervoor zijn geformuleerd aan de hand van de volgende vragen, waarop de beleidsmakers een expliciet antwoord moeten geven:

a. Botst de concrete toepassing van de technologie met condities die de legitimiteit van het systeem (condities onder I) zichtbaar maken of vergroten? Zo ja, om welke condities gaat het?
b. Botst het zichtbaar maken of vergroten van de legitimiteit op zijn beurt met de oorspronkelijk nagestreefde belangen van de dienstverlening?
c. Zijn de uitgewerkte condities voor verantwoordelijkheid (condities onder II) aanvaardbaar uit een oogpunt van kostenefficiëntie?

1 Inleiding

De inzet van informatie- en communicatie technologie (ICT) biedt kansen voor een effectieve overheidsdienstverlening. Bovendien maakt ICT het leveren van maatwerk eenvoudiger, brengt het gemak en draagt het bij aan de emancipatie van de burger. Denk bijvoorbeeld aan nieuwe manieren van burgerparticipatie (zoals petities.nl of de vele burgerpanels van gemeenten)[11], het online aanvragen van allerhande overheidszaken zoals bouwvergunningen of de vooringevulde belastingaangifte. Toekomstige technologische ontwikkelingen, zoals intelligente sensoren of geavanceerde dataminingtechnieken, zullen nog meer mogelijkheden voor effectieve en gepersonaliseerde overheidsdienstverlening creëren (Frissen et al, 2007).

Inherent aan deze ontwikkeling van dienstverlenend maatwerk, gemak en personalisatie is de toenemende verzameling, opslag, verwerking en verspreiding van persoonlijke gegevens van burgers door de overheid. Ook nu al zorgt dit voor maatschappelijke discussie. De vooringevulde belastingaangifte is makkelijk, maar betekent ook dat gegevens van burgers uit de databanken van verscheidene organisaties worden verzameld en gecombineerd. Het opzetten van een Digitaal Dossier Jeugdgezondheidszorg voor alle kinderen van nul tot negentien jaar die met de jeugdgezondheidszorg in aanraking komen, kan hulp eerder op gang brengen, maar gaat ook gepaard met de verzameling en opslag van persoonlijke gegevens. Het behoeft geen uitleg dat de privacy van burgers bij de inzet van deze en toekomstige ICT innovaties onder druk kan komen te staan als er niet zorgvuldig met deze gegevens wordt omgegaan. Het vertrouwen in de overheid en de legitimiteit van het overheidshandelen kunnen hierbij – zeker in de toekomst – ter discussie komen te staan. Dit kan op zijn beurt gevolgen hebben voor de mate waarin de toepassing van de technologie wordt geaccepteerd door burgers.

Door de snelle technologische ontwikkeling wordt de uitvoering en handhaving van bestaande wetgeving om privacy te beschermen steeds moeilijker. Daarom is er in toenemende mate belangstelling voor aanvullende mogelijkheden om privacy beter te beschermen. Een van die mogelijkheden is *Privacy by Design* (PbD). PbD veronderstelt een privacyvriendelijke benadering van het ontwerpen van (informatieverwerkende) systemen die direct of indirect (bijvoorbeeld voor de uitvoering van een ander doel) gericht zijn op de verzameling, verwerking en benutting van persoonlijke gegevens. Het concept richt zich op de totale levenscyclus van deze systemen en is bedoeld de mogelijke privacy impact daarvan op individuen te minimaliseren (ICO, 2008). Door bij het ontwerp van deze systemen al rekening te houden met privacybescherming kan gedurende de gehele levenscyclus van het systeem gemakkelijker worden voldaan aan voorwaarden die gesteld worden aan de omgang met tot een persoon herleidbare gegevens. Op dit moment wordt Privacy by Design in de praktijk nog weinig toegepast.

[11] Voor een overzicht van verschillende eParticipatie initatieven, zie: http://www.eparticipatiemonitor.tno.nl/overzicht/

In veel Europese, maar ook steeds meer nationale beleidsdocumenten, wordt het belang van Privacy by Design benadrukt (zie bijvoorbeeld de Digitale Agenda voor Europa, de Europese Toezichthouder voor Dataprotectie en de Artikel 29 Werkgroep). In een brief van de Ministers van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties van april 2011 geeft het kabinet aan dat ze de toepassing van Privacy by Design zoveel mogelijk zal stimuleren (TK 2010-2011).

In veel beleidsdocumenten is de veronderstelling dat *Privacy by Design* – door een beter privacybescherming – het vertrouwen in en de legitimiteit van overheidshandelen met betrekking tot ICT kan vergroten. De precieze relatie tussen het toepassen van *Privacy by Design* en het vergroten van vertrouwen, legitimiteit en acceptatie is echter niet systematisch onderzocht. Het is dus allerminst zeker dat het toepassen van PbD ook daadwerkelijk het vertrouwen van burgers in overheid én technologie vergroot, of zelfs maar op hetzelfde niveau wordt gehandhaafd. In de eerste plaats is niet duidelijk welke rol privacybescherming speelt bij het vertrouwen van en de acceptatie door de burger. In de tweede plaats worden bepaalde toepassingen van *Privacy by Design* puur technisch geregeld. Deze toepassingen zijn complex en vaak onzichtbaar: geloven en vertrouwen burgers de overheid wanneer die toezegt *Privacy by Design* toe te passen? Of treedt een omgekeerd effect op: worden burgers juist wantrouwig als de overheid expliciet meldt dat ze Privacy by Design toepast? Ten derde kunnen maatregelen om vertrouwen en acceptatie te vergroten (bijvoorbeeld optimale transparantie over het gebruik) de effectiviteit van de inzet van technologieën voor de dienstverlening nadelig beïnvloeden. Hoe moet in dat geval de winst in vertrouwen worden afgewogen tegen de effectiviteit voor de dienstverlening? Deze vragen zijn het onderwerp van dit rapport.

Het onderzoek hanteert daarbij één algemene veronderstelling en één algemene hypothese. De veronderstelling is dat burgers zich ongerust maken over het verzamelen van gegevens over hen en het delen van die gegevens door verschillende overheden. Deze veronderstelling wordt in dit onderzoek niet nader onderzocht. De algemene hypothese is dat er een causaal verband bestaat tussen de bescherming van de burger *via Privacy by* Design (hierna: PbD) enerzijds en het vertrouwen in en de acceptatie van die burger van de overheid anderzijds. Het onderzoek tracht inzicht te verschaffen in welke mate dit het geval is.

De focus van dit onderzoek ligt op eOverheidsdiensten, zoals het aanvragen van vergunningen, identiteitsdocumenten, belastingaangiftes, sociale verzekeringen e.d. ICT-toepassingen in het opsporings- en veiligheidsdomein vallen daarmee buiten het bereik van dit onderzoek.

2 Probleemstelling en onderzoeksmethode

De centrale probleemstelling van het onderzoek is:

In hoeverre, en onder welke voorwaarden, vergroot de inzet van PbD de legitimiteit en verantwoordelijkheid[12] *van de overheid – ofwel de acceptatie en het vertrouwen van de burger in de overheidsdienstverlening – zonder de effectiviteit en doelmatigheid van dat handelen onaanvaardbaar te verkleinen*?

De doelstelling van het onderzoek is het formuleren van een afwegingskader, op basis waarvan de overheid kan beslissen onder welke voorwaarden PbD kan worden ingezet zodanig dat de verantwoordelijkheid en de legitimiteit van de overheid en het vertrouwen in en de acceptatie van de overheidsdienstverlening zichtbaar wordt gemaakt of vergroot zonder teveel afbreuk te doen aan de effectiviteit[13] en doelmatigheid van de dienstverlening. Zoals aangegeven in Hoofdstuk 1 ligt de focus in dit hoofdstuk op eOverheidsdienstverlening.

Het onderzoek kent de volgende deelvragen:

1. Welke ICT-trends met impact op de persoonlijke levenssfeer die relevant zijn voor overheidsdienstverlening kunnen worden onderscheiden?
2. Wat wordt onder PbD verstaan en welke factoren en elementen maken deel uit van het conceptuele kader die vertrouwen en acceptatie, legitimiteit, verantwoordelijkheid, privacy, doelmatigheid en effectiviteit beïnvloeden?
3. Wanneer botst de toepassing van PbD met voorwaarden die de legitimiteit zichtbaar maken of vergroten? Wanneer botst het zichtbaar maken of vergroten van de legitimiteit op haar beurt met de oorspronkelijk nagestreefde belangen?
4. Hoe percipiëren burgers en de overheid de relaties tussen privacybescherming, doelmatigheid, effectiviteit, en vertrouwen en acceptatie?
   b. Hoe zien zij de inzet van PbD met het oog op de acceptatie van de toepassing en het vertrouwen in overheidshandelen?
5. Hoe kan de beantwoording van bovenstaande vragen worden vertaald naar een afwegingskader voor beleidsmakers?

Het onderzoek bestaat uit twee delen: een theoretisch en empirisch deel.

[12] Wij gebruiken deze term als het Nederlandse equivalent van de term ‘accountability’ in het politiek theoretische en ethische debat. Het gaat hierbij om verantwoordelijkheid in de zin van zich (als overheid) goed kunnen verantwoorden.

[13] Met effectiviteit wordt hier primair bedoeld: het verwezenlijken van het oorspronkelijk beoogde doel van de dienstverleningstoepassing. Uiteraard kan de verwezenlijking van dat doel op verschillende manieren in gevaar worden gebracht, bijv. doordat de toepassing van PET/PbD de vereiste handelingen van de burger te omslachtig maken, maar ook doordat PbD bijvoorbeeld transparantie kan vereisen die direct in strijd is met een indirect beoogd opsporingsdoel (wanneer bijvoorbeeld een kentekenregistratiesysteem met “intelligente” camera’s wordt gebruikt om bankovervallers te vinden).

1. Theorie
Dit deel bevat de resultaten van verkennend literatuuronderzoek en conceptuele analyses van de verschillende relevante begrippen. Het begrip Privacy by Design is relatief nieuw en nog niet vastomlijnd. In kaart zal moeten worden gebracht welke elementen van PbD (bijvoorbeeld transparantie, organisatorische elementen, een Privacy Impact Assessment[14] etc.) operationeel zijn en deel uitmaken van het begrip. Aan de hand van de geïdentificeerde elementen van PbD zal een definitie worden geformuleerd (hoofdstuk vier). Uitgangspunt daarbij is dat het empirische deel van het onderzoek zich zal richten op de perceptie van burgers en overheidsfunctionarissen van PbD.

Vervolgens wordt onderzocht hoe volgens de literatuur vertrouwen en acceptatie bij de burger en de verantwoordelijkheid en legitimiteit van de betrokken overheden elkaar beïnvloeden (hoofdstuk vijf). Daarna volgt een nadere begripsbepaling. Aan de hand van stipulatieve definities van de noties verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie wordt de onderlinge samenhang van deze begrippen weergegeven en tegelijkertijd een compact overzicht gegeven van recente relevante literatuur. Vervolgens richten we ons specifiek op verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie rond elektronische dienstverlening door de overheid. Hier kan alvast worden opgemerkt dat onderzoek en literatuur over elektronische dienstverlening door de overheid in het licht van legitimiteit van die overheid tot nu toe ontbreekt, voor zover zij niet direct of indirect wordt geïmpliceerd door het debat over vertrouwen en acceptatie. Tenslotte gaan we in op de rol die privacy-overwegingen spelen bij verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie rond elektronische dienstverlening door de overheid. Ook hier geldt hetzelfde *caveat* ten aanzien van bestaand onderzoek en literatuur.

2. Empirie
In dit deel wordt de perceptie van burgers en overheidsfunctionarissen respectievelijk politiek verantwoordelijken ten aanzien van de inzet van PbD met het oog op de aanvaardbaarheid van de toepassing en het vertrouwen in overheidshandelen onderzocht (hoofdstuk zes). Het onderzoek naar de perceptie van burgers vindt plaats aan de hand van focusgroepen. Hiervoor wordt een protocol opgesteld. Het onderzoek naar de perceptie van overheidsfunctionarissen wordt aangevuld met interviews met enkele experts op het gebied van privacy, legitimiteit en techniek. De uitkomsten van de focusgroepen en de interviews vormen input voor het uiteindelijke afwegingskader.

Verhouding tot eerder AVB-onderzoek
Eerder uitgevoerd en lopend AVB-onderzoek richt zich op de rol van vertrouwen bij publieke dienstverlening. Dit is onder meer het geval in het project ‘Vertrouwen in Hybride Ketens’ en het onderzoek ‘Vertrouwen in identiteitsinfrastructuren’. Ook eerder verricht onderzoek zoals ‘The use of privacy enhancing aspects of biometrics’ wordt meegenomen. Voorliggend onderzoek bouwt voort op de bevindingen van deze studies, met name op de geboden inzichten rond vertrouwen en de inzet van PbD die uit deze eerder uitgevoerde studies zijn af te leiden. Het voorliggende onderzoek onderscheidt zich van de al uitgevoerde studies doordat het zich toespitst op drie aanvullende thema’s:
- verbreding van ‘vertrouwen’ naar het bredere thema ‘legitimiteit’

[14] Deze term wordt in Hoofdstuk vier nader toegelicht.

- verbinding met verantwoordelijkheid van de overheid (rekenschap afleggen)
- formulering van een afwegingskader.

Leeswijzer
In het volgende hoofdstuk (drie) beschrijven we de resultaten van de trendanalyse. In hoofdstuk vier worden de belangrijkste begrippen gedefinieerd en maken we duidelijk welke elementen onder Privacy by Design vallen. Hoofdstuk vijf brengt in kaart welke factoren vertrouwen en acceptatie bij de burger, en verantwoordelijkheid en legitimiteit van overheden beïnvloeden. In hoofdstuk zes volgt het empirisch gedeelte; de percepties van burgers ten aanzien van deze factoren. Tot slot volgen de conclusies in hoofdstuk zeven, waarin we het afwegingskader presenteren.

3 Trendverkenning 2011-2015

3.1 Inleiding

Technologie dringt steeds verder door in ons leven: het is overal om ons heen, gepersonaliseerd en aangepast aan de omgeving. De verdere ontwikkeling van infrastructuren en opkomende of convergerende technologieën zoals nanotechnologie, biotechnologie, informatietechnologie en de cognitieve wetenschappen (vaak afgekort tot NBIC), en combinaties daarvan, maken steeds nieuwe toepassingen mogelijk, ook op het terrein van overheidsdienstverlening. Het leveren van maatwerk en personalisatie zijn belangrijke trends in zowel het private als het publieke domein.

Hierdoor groeit de hoeveelheid persoonlijke informatie die over burgers kan worden verzameld en daarmee wordt ook de mogelijkheid groter dat inbreuken op de persoonlijke levenssfeer van individuen plaatsvinden. De vraag die hieruit naar voren komt – en een steeds centralere rol zal spelen in de toekomst – is hoe publieke waarden zoals privacy, vertrouwen, autonomie, persoonlijke integriteit, verantwoording en legitimiteit, kunnen worden gewaarborgd in toekomstige overheidsdienstverlening.

In dit hoofdstuk brengen we beknopt in kaart welke technologische trends – gerelateerd aan ICT – naar verwachting de komende vier jaar belangrijk zullen worden voor de overheid. We richten ons daarbij op trends die een impact op de persoonlijke levenssfeer kunnen hebben. Gekozen is voor een tijdshorizon van vier jaar, om aan te sluiten bij de strategische agenda en tijdshorizon van de Alliantie Vitaal Bestuur[15]. De trends laten nieuwe mogelijkheden voor overheidsdienstverlening zien, maar tegelijkertijd ook mogelijke risico's voor het waarborgen van de privacy. De implementatie van deze technologieën kan de uitvoering en handhaving van privacy- en dataprotectiewetgeving aanmerkelijk bemoeilijken.

De signalering van trends is gebaseerd op een *quick-scan* van relevante toekomststudies. Deze studies zijn ondergebracht in het door TNO beheerde Dynamosysteem[16]. Daarnaast is aanvullend literatuuronderzoek uitgevoerd. Onderstaande *tagcloud* toont de meest relevante technologische ontwikkelingen. We lichten daar een aantal elementen uit. Zoals de *tagcloud* illustreert, zijn opkomende technologieën en concepten nauw met elkaar verweven en speelt convergentie een centrale rol.

[15] Dit betekent dat we ontwikkelingen waarvan een wezenlijke impact wordt verwacht maar die verder in de toekomst liggen (zoals quantum computing) niet mee nemen in dit rapport. Quantum computing is een nieuwe vorm van computerarchitectuur die gebruik maakt van quantummechanica waardoor computers enorme hoeveelheden data kunnen verwerken. Zie bijvoorbeeld http://en.wikipedia.org/wiki/Quantum_computer

[16] Deze database geeft een overzicht van ontwikkelingen op verschillende gebieden van technologische innovaties en maatschappelijke vraagstukken. De Dynamo database voorziet in uitgewerkte technologische trends, maatschappelijke issues en toekomstige ontwikkelingen op gebieden van innovaties die in de toekomst (10-15 jaar) zijn te verwachten.

Figuur 1: Overzicht van de meest relevante technologische ontwikkelingen en toepassingen (TNO, juli 2010)

Bij het schetsen van toekomstige technologische ontwikkelingen dient te worden opgemerkt dat het verloop van deze ontwikkelingen per definitie onzeker is. Technologische ontwikkelingen en hun toepassing worden beïnvloed door een breed scala aan economische- en maatschappelijke factoren. Hoewel we in dit hoofdstuk de ontwikkelingen vanuit een hoofdzakelijk technologisch perspectief beschrijven – en daarmee een zekere '*technology push*'-lens hanteren – gaan we ervan uit dat technologische en maatschappelijke ontwikkelingen elkaar wederzijds beïnvloeden (de zogenaamde '*mutual shaping*' benadering).

3.2 Ordening van trends in vijf clusters

Voor deze trendverkenning onderscheiden we vijf trendclusters (zie Figuur 2). De *longlist* (met trends, innovaties, toepassingen, concepten) hebben we binnen deze clusters geordend. Het onderscheid tussen de eerste drie clusters is in grote lijnen: de infrastructuur (de basis om informatie uit te wisselen), nieuwe diensten en andere wijze van gebruik van de infrastructuur, respectievelijk nieuwe toepassingen, en tools die hiervoor beschikbaar komen. Het vierde cluster is van een iets andere orde; hier gaat het om de bewerking en verwerking van data. Het vijfde cluster – de opkomende convergerende technologieën (van informatietechnologie met andere terreinen) – kan worden beschouwd als overkoepelend. De verwachting is dat de innovaties op dit gebied pas op wat langere termijn een rol gaan spelen.

In paragraaf 3.3 tot en met 3.7 worden de afzonderlijke trends beschreven.
In paragraaf 3.8 worden de effecten voor de overheid en overheidsdienstverlening beschreven.

Figuur 2: Overzicht trendclusters en innovaties

5 trendclusters & innovaties < 2015		innovaties > 2015
1. Breedbandige convergerende infrastructuur	• Verglazing van netwerken • Mobiele breedbandige netwerken • Krachtiger (draadloze) apparaten • Interoperabiliteit tussen netwerken en apparaten	**5. Convergerende technologieën** • Biotechnologie en ICT • Nanotechnologie en ICT • Cognitiewetenschappen en ICT
2. **Utility computing** (diensten)	• Grid computing • Cloud computing • Software als service (SAAS) / everything as a service • Verbeterde computer-architecturen (o.a. virtualisatie)	
3. **Het intelligente web** (applicaties) *Ook: Semantisch web, Web 3.0, Internet-of-things*	• Convergentie van applicaties • Meer, gemakkelijkere en betere creatie- & sharing tools • Web 3.0 tools • Lokalisatie van applicaties	
4. **Informatieverwerking**	• Datamining: vinden en analyseren van informatie • Interfaces en representatie (agenttechnologie) • Modellering en simulatie	

Ter toelichting en aanvulling op deze indeling twee opmerkingen:

- Vervagend onderscheid informatie- en communicatietechnologie: Vier van de vijf clusters kunnen ook worden ingedeeld in het binnen de ICT gemaakte onderscheid tussen informatietechnologie (cluster 4) en communicatietechnologie (cluster 1-3). Onder informatietechnologie wordt verstaan het verkrijgen, converteren, opslaan en verwerken van informatie met behulp van hardware, software en diensten. Onder communicatietechnologie worden communicatieapparatuur, -netwerken en –diensten gerekend. Anders gezegd, bij communicatietechnologie gaat het er vooral om dat alles met elkaar wordt verbonden, terwijl bij informatietechnologie de nadruk ligt op wat er met de infrastructuren wordt gedaan. Omdat ook bij dit onderscheid al langere tijd sprake is van convergentie waardoor scheidslijnen vervagen en het minder betekenis heeft, is dit niet expliciet in de ordening opgenomen.
- Alternatieve indelingen uit andere bronnen: Vanuit de literatuurscan naar ICT trends is ook een aantal indelingen uit andere studies gevonden. Twee hiervan hebben we gebruikt, zowel bij het maken van onze indeling, als bij de uitwerking per cluster en de analyse in het resterende deel van dit hoofdstuk. Ten eerste is

de studie van RAND voor de Europese Commissie, naar Trends in connectivity technologies (Cave et al, 2009) een belangrijke referentie, waarvan we de indeling in trendclusters op hoofdlijnen volgen. Dit onderzoek focust op de vraag met welke toekomstige uitdagingen de ubiquitous internet society te maken zal krijgen. Het tweede rapport waarnaar we regelmatig zullen verwijzen is 'Dilemmas for Privacy' van de Royal Academy of Engineering, dat tevens een 'technology roadmap' bevat (RAENG, 2007).

De hierna volgende uitwerking van deze vijf trendclusters bevat eerst een kernachtige beschrijving van het trendcluster en vervolgens wordt specifieker ingegaan op een aantal innovaties dat al bestaat of waarvan mag worden verwacht dat ze in de komende vijf jaar een rol gaan spelen.

3.3 Cluster 1: Breedbandige convergerende infrastructuur

Dit cluster gaat over de beschikbaarheid van steeds krachtiger *breedbandige netwerken*, met nieuwe mogelijkheden voor plaatsonafhankelijke connectiviteit: de realisatie van de (al lang verwachte) belofte van '*anywhere, anytime'*. Inmiddels voegen we hier ook (de wens van) '*any device'* aan toe (het maakt niet meer uit met welk apparaat verbinding wordt gemaakt).

Daarnaast gaat het ook om de *convergentie van verschillende ICT-infrastructuren* die – met de meest geschikte en beschikbare technologie – (idealiter) samensmelten tot één naadloos op elkaar aansluitende infrastructuur. Het netwerk kiest de beste technologie voor elk doel of activiteit van de gebruiker. De onderliggende verschillen in technologie zijn grotendeels onzichtbaar of doen er niet meer toe voor de gebruiker (Cave et. al, 2009). Vele innovaties, bijvoorbeeld diensten als *cloud computing*, zijn mede gebaseerd op en tegelijkertijd afhankelijk van een snelle, betrouwbare en gemakkelijke toegang tot breedbandige infrastructuur.

De nieuwe generatie breedbandnetwerken maakt snelheden van meer dan 1000 gigabit per seconde mogelijk. Verwacht wordt dat de vraag naar breedbandcapaciteit snel toeneemt, met in 2020 een verwachte gemiddelde downloadsnelheid in Nederland van 75-100 megabit per seconde (TNO en Dialogic, 2010)[17]. Opslag, ruimte, snelheid en betrouwbaarheid zijn in de toekomst nauwelijks nog een probleem (Teeuw en Vedder, 2008). Nieuwe generaties van efficiëntere, kleinere en goedkopere chips liggen hieraan ten grondslag (OSI, 2006).

Een andere belangrijke ontwikkeling is de invoering van het *Internet Protocol Version 6 (IPv6)*. IPv6 is onder andere ontwikkeld om het tekort aan IP-adressen op te lossen en tegelijk zijn andere beperkingen van IPv4 aangepakt. Zo biedt IPv6 de mogelijkheid van gegevensbeveiliging tijdens het transport, waardoor *closed user groups* kunnen worden gecreëerd van computers die op willekeurige plekken op het internet aangekoppeld worden. Dit biedt de mogelijkheid voor het opbouwen van volkomen virtuele netwerken.

[17] De onvoorspelbaarheid van het succes van toekomstige diensten en apparaten die veel bandbreedte gaan gebruiken – zoals Net TV, HD-streaming, cloud computing of HD-teleconferencing – ondergraven voorspellingen voor 2020 in grote mate (TNO en Dialogic, 2010).

Verglazing van netwerken & opkomst full fiber netwerken
Verschillende (vaste) netwerken concurreren met elkaar: de kabelnetten (waarschijnlijk niet voor 2015 met High Fibre Coax), het fiber-koper netwerk (gedigitaliseerd en steeds verder opgewaardeerd, bijvoorbeeld met vdsl2), respectievelijk Full Fiber (in combinatie met FttH) (TNO en Dialogic, 2010). De grootste en meest omvangrijke vervanging in Nederland betreft de *last (*of *first) mile* ofwel *fibre to the home* (FttH), de aansluiting van woningen. Verwachting is dat voor de landelijke uitrol hiervan nog circa 15 jaren nodig is[18].

Mobiele breedbandige netwerken / Broadband Wireless Access (BWA)
De breedbandcapaciteit van de derde (3G) en vierde (4G) generatie mobiele netwerken neemt verder toe, o.a. door de invoering van (nieuwe) mobiele radiotechnologieën als HSPA+ WiMax of LTE. Het snel groeiend gebruik van apparaten met mobiel internet - zoals laptops en notepads, netbooks, smartphones, eReaders etc. - zorgt voor een explosieve groei van het mobiele dataverkeer. De noodzakelijke aansluiting van basisstations van 3G/4G netwerken is tegelijkertijd mede verantwoordelijk voor de toenemende capaciteitsvraag op het vaste aansluitnetwerk (TNO en Dialogic, 2010).

Krachtiger (draadloze) apparaten
Ook de capaciteit van ICT-apparaten, zoals mobiele telefoons, neemt toe. Nieuwe generaties mobiele apparatuur hebben extra processorkracht, kleinere chips en maken gebruik van GPS (Global Positioning System) of NFC (Near Field Communication), wat veel mogelijkheden voor plaatsbepaling (*location based services*) en andere diensten biedt. Nieuwe technologie voor batterijen en energieopslag, zoals lithium-ion, zorgt er voor dat deze apparaten minder energie verbruiken en langer meekunnen. Verwacht wordt dat mobiele toepassingen een centrale rol gaan spelen in de komende jaren.

Interoperabiliteit tussen netwerken en apparaten
Interoperabiliteit is een belangrijke voorwaarde om te komen tot een convergerende infrastructuur. Hiervoor zullen aanbieders van technologie, randapparatuur en diensten met elkaar moeten samenwerken, bijvoorbeeld door gedeelde protocollen te gaan gebruiken (Cave et. al, 2009). Op geïntegreerde platformen kunnen dan verschillende diensten en apparaten worden aangesloten. Het onderscheid tussen de verschillende functies van apparaten verdwijnt steeds meer: televisie kijken kan bijvoorbeeld op de tv maar ook via de computer of diverse mobiele apparaten en navigeren kan met een navigatiesysteem maar ook op de mobiele telefoon, et cetera.

[18] Zie o.a. ook het in augustus 2009 opgerichte FttH Platform Nederland, http://www.ftthplatform.nl

3.4 Cluster 2: Utility Computing[19]

Dit concept bestaat al langer en is gebaseerd op de beschikbaarheid van opslag, computerkracht en allerhande diensten als een algemene nutsvoorziening. De achterliggende gedachte hierbij is dat computerkracht en digitale opslagruimte in de toekomst nauwelijks nog een probleem zijn voor gebruikers en organisaties: er is zoveel beschikbaar als er nodig is (Cave et. al, 2009). Om gebruik te maken van opslagdiensten hebben eindgebruikers, waaronder overheidsdienstverleners, geen kennis of controle nodig over de technologie waarmee dit gebeurt. Utility computing levert een infrastructuur op afroep, op basis van betalen naar rato van gebruik (*pay for use*) en met de mogelijkheid dit op te schalen of anders te configureren waar nodig (*pay as you grow*). Een nauw hiermee verbonden trend is *open source software* (en ook in bredere zin: open standaarden, open technologieën etc.).

Een belangrijk verschil tussen het *utility computing concept* en een traditionele nutsvoorziening, is dat de verdienmodellen sterk afwijken. Gebruikers 'huren' en betalen alleen voor wat ze op dat moment nodig hebben, maar ze zijn niet de eigenaar van deze infrastructuur. Er ontstaat daarmee een nieuw toeleverings- en afnamemodel voor ICT-diensten met dynamisch schaalbare en virtuele resources.

Grid computing
Grid computing maakt gebruik van de mogelijkheid om apparatuur en informatie te delen en te bundelen. Computers die in een netwerk met elkaar verbonden zijn en samenwerken zijn een vorm van *distributed computing* (de techniek om een enkele – complexe, omvangrijke – computerbewerking te verdelen over meerdere computers). *Grid computing* kan – na de ontwikkeling van *stand alone* computers tot computers verbonden via het internet – worden beschouwd als een volgende stap in de evolutie van het computergebruik. Onder andere semantische grids (semantisch web) of sensor grids zijn specifieke typen grids.

Cloud computing
Cloud computing is een relatief nieuw fenomeen[20], waarbij gebruikers toegang hebben tot applicaties en hardware via internet, in plaats van die te gebruiken vanuit het eigen netwerk of de eigen computer. Online wordt informatie tijdelijk op het apparaat van de gebruiker geplaatst. In de praktijk worden vaak verschillende definities van *cloud computing* gehanteerd en er worden verschillende type diensten toe gerekend, zoals opslag, backup/hersteldiensten of het gebruik van bepaalde softwarepakketten. Voorbeelden zijn alle varianten die 'als een dienst' ('as a service') worden aangeduid (RAENG, 2009; Computable 18 aug. 2010; Cave, et al, 2009).

[19] Met de term utility computing wordt een groot aantal begrippen en concepten met elkaar in verband gebracht, waarbij de eenduidigheid in definities soms ver te zoeken is. Zo wordt bijvoorbeeld cloud computing ook wel utility computing genoemd of Infrastructure as a Service (IaaS).
[20] Cloud computing wordt (anno 2011) wel gezien als de toekomst van de IT, met een verandering van paradigma. Er zijn ook tegengeluiden van degenen die veronderstellen dat het een hype of slechts een marketingterm betreft.

Software als een dienst of: alles als een dienst
Software as a Service (SaaS) valt ook binnen het *cloud computing* model, waarbij het gaat om applicaties die via internet aan gebruikers beschikbaar worden gesteld. Denk bijvoorbeeld aan accounting of factuurpakketten. In bredere zin ('alles als een dienst') kan dit over van allerlei soorten diensten gaan, met als kenmerk dat het gaat om online flexibele, schaalbare diensten.

Verbeterde computerarchitecturen zoals IT-virtualisatie en System on Chip
Een andere gerelateerde technologische ontwikkeling is de evolutie van de computer zelf. Voorbeelden zijn (IT) virtualisatie en *System on Chip* (SoC)[21]. Virtualisatie is een techniek om fysieke bronnen - zoals een server, een besturingssysteem, een applicatie of een gegevensdrager - samen te kunnen voegen of te verplaatsen naar een ander hardware platform. Bij *System on Chip* worden alle onderdelen van een computersysteem op een enkele microchip of semi-conductor wafer gezet (denk bijvoorbeeld aan een de rekenfunctie, de grafische functie en geheugencapaciteit, maar ook NFC voor een betalingsfunctie). Dit is van belang bij mobiele of *embedded computing*. Mobiele apparaten worden daardoor steeds krachtiger en multifunctioneler, terwijl ze tegelijkertijd compact blijven.

3.5 Cluster 3: Het intelligente Web

Dit trendcluster gaat over alomtegenwoordige (*ubiquitous*) en altijd verbonden ICT-netwerken en apparaten en het 'slimmer worden' van het internet. Veel gebruikte begrippen als semantisch web, web 3.0 of het internet-der-dingen en het internet-of-content beschouwen we als vergelijkbaar. Het web wordt 'intelligenter' door bijvoorbeeld de ontwikkeling van het semantische web. Het semantisch web verbindt teksten en andere media (zoals foto's en video's) op basis van hun betekenis zodat ze makkelijker te vinden zijn. Het 'intelligente web' kan worden gezien als de volgende fase van de ontwikkeling van het internet (Web 3.0). Ook kan informatie toegevoegd worden aan virtuele en fysieke objecten[22], het 'internet-der-dingen'. Dit maakt het mogelijk dat de systemen achter de 'genetwerkte' apparaten – zonder menselijke tussenkomst – op de achtergrond autonoom complexe taken uitvoeren (ITU, 2005). Ook mens-computer interactie wordt met deze trends in verband gebracht (Cave et al, 2009). Dit cluster bouwt voort op de hiervoor beschreven clusters 'breedbandige convergerende infrastructuur' en 'utility computing'. Het onderscheidende verschil met deze twee clusters zit in de mogelijkheid voor de eindgebruiker om waarde (sociaal, economisch, maatschappelijk) te onttrekken aan de onderliggende technologieën die de kern vormen van de andere twee clusters.

[21] SoC verwijst naar de integratie van alle componenten van een computer of elektronisch system in een geintegreerd circuit (chip). Het kan digitale, analoge, gemixte signalen en vaak ook radio-frequentie functionaliteiten bevatten. http://en.wikipedia.org/wiki/System-on-a-chip
[22] Esmeijer, J. en Munck, de, S. (2009) Web, webber, webst, http://www.frankwatching.nl

Convergentie van applicaties
Hierbij gaat het om wat gebruiker kunnen doen met verschillende apparatuur die verbonden is met een infrastructuur, of het nu een smartphone, een TV of een computer betreft. Het gebruik is onafhankelijk van het apparaat en van de onderliggende infrastructuur. Voorbeelden van technologieën zijn hier: *streaming* en compressie protocollen en technologieën die het mogelijk maken om *high definition* (HD) multi-media aan een brede variatie van apparaten door te geven (Cave et al, 2009).

Meer, gemakkelijkere en betere sociale en creatieve tools
Er komen steeds meer tools die het mogelijk maken om informatie, intelligentie of content te delen. Voorbeelden op dit moment zijn YouTube (film/video delen), Twitter en Facebook (persoonlijke informatie delen), Wikipedia (kennis delen) of multimedia tools als pod-casting of vod-casting. Deze tools maken gebruik van uiteenlopende webtechnologie, meestal *open APIs* and *Service Orientated Architectures* (SOA) om eenvoudig nieuwe informatie met anderen te delen. Nieuwer is de *drag and drop* software engineering technologie die de ontwikkeling van – door gebruikers zelfgemaakte – applicaties verder zal vergemakkelijken (Cave et al, 2009). De hoeveelheid content stijgt door deze ontwikkeling explosief. Er ontstaan steeds meer diensten waar slimme algoritmes zijn ingebouwd om informatie op basis van persoonlijke voorkeuren of gedrag te filteren, *te personaliseren*, zodat relevante informatie sneller bij een gebruiker terecht komt (Pariser, 2011)[23].

Web 3.0 tools
Met web 3.0 wordt in het kort een fase van internetontwikkeling bedoeld die als het ware nieuwe 'functionaliteit' en intelligentie toevoegt, namelijk het (automatisch) uitvoeren van bewerkingen. Webtechnologieën, *netwerk computing tool*s en *distributed 'data web' tools*, zoals digitale archivering zijn methoden waardoor data via het web kan worden uitgegeven in herbruikbare en op afstand doorzoekbare formaten. Hieronder vallen ook technologieën die patronen kunnen afleiden, die bijvoorbeeld zijn gebaseerd op het bewerken en analyseren van grote hoeveelheden informatie van relevante websites (*cognitive computing*) (Cave et al, 2009). Via *smart searches* wordt informatie snel met elkaar in verband gebracht en aan de gebruiker gepresenteerd.

Lokalisatie van applicaties
Een nauw aan dit cluster gerelateerde technologische ontwikkeling (en daarom ga we er hier apart op in) is die van de locatiegebaseerde diensten. *Global Positioning System* (GPS) en satelliet locatietechnologie zullen zich verder ontwikkelen en worden aangevuld met de ontwikkeling van draadloze communicatietechnologieën. Deze applicaties zullen ook steeds verder evolueren in hun alomvattende aanwezigheid, bijvoorbeeld waar het gaat om de huidige koppeling aan de mobiele telefoon. Convergentie van infrastructuur zal ertoe leiden dat dit kan gaan gelden voor een veel groter aantal platformen. Behalve locatie zal op termijn ook omgevingsinformatie zoals beweging, gedrag etc. hierbij een rol gaan spelen (*context aware* informatie en diensten) (Cave et al, 2009). De toepassing van toegevoegde realiteit (*augmented reality*) past ook bij deze ontwikkeling. De gebruiker kan dan zo realistisch mogelijk achtergrondbeelden en informatie

[23] In zijn boek 'The Filter Bubble' beschrijft Pariser de positieve en negatieve aspecten van deze vorm van personalisatie die in steeds meer internetdiensten en –websites te vinden is.

activeren, waarbij data wordt geprojecteerd in het gezichtsveld van de gebruiker. Toepassingen zijn er voor ondersteuning bij complexe taken (van bijv. een monteur of arts), bij navigatie in vervoermiddelen of bij vermaak en onderwijs (bijv. historische context bij een voorwerp in een museum).

3.6 Cluster 4: Informatieverwerking

Technologieën voor de verzameling, opslag, transmissie, verwerking van data ontwikkelen zich snel (RAENG, 2007). Ze maken het mogelijk om sneller en eenvoudiger data te analyseren en maken zo nieuwe toepassingen mogelijk. Er worden nieuwe analysemogelijkheden ontwikkeld om de data te bewerken tot betekenisvolle en relevante informatie. Ook voor 'gewone' gebruikers komen hiervoor nieuwe toepassingen beschikbaar, (Cave, 2009). Visualisaties (*computer graphics*) worden hierbij ook steeds belangrijker.

Datamining, het vinden en analyseren van informatie
Hoeveelheden gegevens nemen explosief toe. Op het gebied van het vinden en bewerken van data tot bruikbare informatie, onder andere voor besluitvorming, wordt snelle vooruitgang geboekt. Het gaat dan om het ordenen, clusteren en analyseren van grote gegevensverzamelingen, op basis van (statistische) correlaties of patronen. Dit kan worden toegepast op grote hoeveelheden tekst (textmining), beeld (mediamining) of geluid (audiomining, m.n. spraakherkenning of gevaardreiging), maar ook op opinie of online sentimenten en gedrag. Met data mining software kunnen gegevens worden bewerkt en gecategoriseerd aan de hand van verschillende dimensies of invalshoeken, en kunnen de relaties tussen de onderscheiden categorieën worden geïdentificeerd. Voor het beschikbaar maken van internetcontent aan gebruikers, wordt door websites en internetdiensten steeds meer gebruik gemaakt van persoonlijke filters die op basis van geavanceerde algoritmes een selectie maken van content en dit aan gebruikers tonen.

Interfaces en representatie (agenttechnologie)
Een software agent is een intelligent programma, een intelligente virtuele entiteit, met de vrijheid om zelfstandig te handelen in opdracht en binnen de grenzen van een menselijke (legale) eigenaar. De agent handelt op basis van een profiel, informeert proactief en is in staat tot leren, dat wil zeggen dat het kan omgaan met de feedback van de eigenaar. Agenttechnologie is nauw verbonden met kennistechnologie (het vakgebied Kunstmatige Intelligentie). De agent kan ook anoniem zijn. In virtuele werelden neemt deze representatie een steeds centralere rol in. Mensen kunnen een reeks van verschillende (door henzelf aangestuurde) *avatars* gebruiken die ze in verschillende omgevingen gebruiken. Belangrijke ondersteunende technologieën hierbij zijn (biometrische) encryptietechnieken die veiliger identiteitsmanagement en authenticatie mogelijk maken.

Modellering en simulatie
Hierbij gaat het om het creëren van omgevingen waarbinnen nieuwe concepten kunnen worden ontwikkeld en getest of waarbinnen gedrag kan worden gemodelleerd of getraind. Voorbeelden hiervan zijn het modelleren van het gedrag van piloten in de Joint Strike Fighter (JSF), of het 3D visualiseren van het

missiegebied in Afghanistan (o.a. TNO Defensie en Veiligheid[24]). Modellering en simulatie worden steeds vaker verbonden met serious gaming, het leren in virtuele omgevingen in het bijzonder.

3.7 Cluster 5: Convergerende technologieën

Convergerende technologie bestaat uit de 'kruisbestuiving' tussen de (NBIC) disciplines nanotechnologie, biotechnologie, informatie- en communicatietechnologie en de cognitieve wetenschappen (Roco en Brainbridge, 2002). Soms wordt ook geavanceerde materiaalkunde onder de convergerende technologieën gerekend. Nieuwe toepassingen die hieruit voortkomen hebben verschillende transformaties (o.a. medische diagnose en behandelingen) en op termijn mogelijk zelfs reproductie van leven tot gevolg. Nanotechnologie (nano-electronica) en biotechnologie creëren bijvoorbeeld nieuwe typen sensoren (o.a. biosensoren en optische waarneming van nanodeeltjes). Nanotechnologie draagt ook bij aan de miniaturisering en energiezuinigheid van ICT-sensoren, zoals RFID-chips. Informatietechnologie biedt de verwerkingscapaciteit en visualisatietools om sensorinformatie van verschillende bronnen te gebruiken voor bijvoorbeeld risicoanalyse en -beoordeling. Neurowetenschappen en beeldtechnologie kunnen helpen bij het diagnoseproces in de (bio)medische wetenschap.

Convergerende technologie brengt diverse nieuwe toepassingen voort, waarvan menselijke 'verbeteringstechnologieën' of 'verbetergeneeskunde' vanuit een ethisch perspectief steeds vaker onderwerp van discussie zijn. De biomedische technologieën zijn gericht op het vergroten van de lichamelijke of geestelijke capaciteiten van de mens (brein-machine-interfaces) of op persoonlijke gezondheidsverbetering, veroudering en levensverlenging (o.a. regeneratieve geneeskunde, gentherapie, stamceltherapie, reprogenetica, neurale implantaten). Aan de andere kant creëren de convergerende technologieën een steeds slimmer wordende omgeving, waarin mensen en objecten voortdurend kunnen worden geanalyseerd, beoordeeld en zelfs gecontroleerd.

Biotechnologie en informatietechnologie
Biowetenschap en biotechnologie zijn in toenemende mate afhankelijk van informatietechnologie voor het vastleggen, analyseren, modelleren en visualiseren van data (bio-informatica). Computerberekeningen en –methoden, simulatie- en modelleringtechnieken spelen hier een belangrijke rol. Omgekeerd wordt ook ICT in toenemende mate beïnvloed door biotechnologie. In de IT wordt bijvoorbeeld gekeken naar hoe biologische mechanismen omgaan met hun natuurlijke omgeving om hiermee nieuwe methoden van data-analyse, modellerings- en simulatietechnieken te ontwikkelen (*computational biology*). Een ander voorbeeld is *swarm intelligence,* waarmee het gezamenlijke gedrag van gedecentraliseerde of zelforganiserende systemen wordt geanalyseerd of nagebootst. Biometrie waarbij gebruik wordt gemaakt van persoonseigen fysiologische eigenschappen om de identiteit van die persoon te kunnen verifiëren, is een ander relevant deelgebied.

Toepassingen op dit snijvlak zijn bijvoorbeeld biosensoren, biomarkers en bioactuatoren te benutten voor monitoring en diagnostiek. Of *Lab-on-a-chip,* kleine

[24] Zie ook http://www.tno.nl/content.cfm?context=kennis&content=techno&item_id=28

apparaten die een snelle analyse mogelijke maken voor bijvoorbeeld medisch of forensisch onderzoek. Bij 'in-situ-diagnostiek' maakt convergentie het bijvoorbeeld mogelijk om sensoren in het lichaam te plaatsen en ziekten en aandoeningen op te sporen nog voordat zich symptomen voordoen (OSI, 2006). Er worden *body area networks* ontwikkeld voor applicaties die de gezondheid van patiënten kunnen monitoren (Teeuw en Vedder, 2008).

Nanotechnologie en informatietechnologie
Nanotechnologie is een verzamelnaam voor technologieën die opereren op zeer kleine materialen, systemen of objecten (tussen 1 en 100 nm). Nano-electronica is het gebruik van nanotechnologie voor elektronische componenten, zoals transistors. Nano-photonica gebruikt ICT voor de ontwikkeling van fibre optics voor communicatie, optische dataopslag en in beeldtechnologie. ICT op zijn beurt beïnvloedt nanotechnologie met name op het gebied van simulatie- en modelleertechnieken (van Lieshout et. al., 2005). Nanosensoren creëren een gevoelige en bewuste omgeving die in staat is te interacteren met mensen, objecten en gebouwen (OST, 2006). Hieronder vallen ook zelfsturende infrastructuren die de conditie van objecten kunnen monitoren, waardoor zelfdiagnose (bijvoorbeeld bij dijkbewaking, sterkte van gebouwen of bruggen) mogelijk wordt (OSI, 2006). Een voorbeeld is het zogenaamde 'slimme stof' (*smart dust*), een draadloos netwerk dat bestaat uit hele kleine micro-elektromechanische sensoren (MEMS), robots of andere apparaten, die bijvoorbeeld licht, temperatuur of beweging kunnen detecteren.

Cognitiewetenschappen en informatietechnologie
Ook cognitiewetenschappen en informatietechnologie beïnvloeden elkaar wederzijds. Beeldverwerkingstechnologie (*brain imaging technology*), zoals fMRI's[25], is een duidelijk voorbeeld hoe ICT cognitiewetenschap mogelijk maakt. Een ander voorbeeld is simulatie van neurale netwerken door softwareprogramma's (ontwikkeling van cognitieve systemen en modellen). Neurale netwerken worden bijvoorbeeld ingezet om aardbevingen op te sporen. Kunstmatige intelligentie is een belangrijke discipline die cognitiewetenschappen en informatietechnologie combineert. Spraakherkenning is een voorbeeld van de invloed van cognitiewetenschap op ICT (mens-computer-interface).

Toepassingen zijn mens-brein-interfaces, waaronder *brain-fingerprinting* kan worden gerekend. Dit is een voor opsporing relevante, overigens controversiële forensische techniek die gebruik maakt van technieken om vast te stellen of bepaalde informatie in iemands hersenen is opgeslagen. Andere toepassingen betreffen cognitieve systemen (op basis van neurale netwerken en kunstmatige intelligentie) onder meer voor het voorspellen van gedrag. Ook zijn er veel ontwikkelingen op het gebied van de mens-computerbesturing en interactie, bijvoorbeeld via spraakherkenning of gezichtsherkenning.

[25] Dit staat voor Functional MRI or functional Magnetic Resonance Imaging, een techniek in het moderne hersenonderzoek waarbij de activiteit van de hersenen door middel van een computer zichtbaar wordt gemaakt in een drie-dimensionaal beeld (via *imaging and visioning*).

3.8 Effecten van trends in relatie tot overheidsdienstverlening

Voor vrijwel alle beschreven ICT trends en concepten geldt dat zij consequenties zullen hebben op overheidsdienstverlening en effecten zullen hebben op de bescherming van de persoonlijke levenssfeer. Hoewel er nog weinig bekend is over de precieze effecten bespreken we hier een aantal relevante gevolgen.

Betere dienstverlening en personalisatie
De geschetste technologische ontwikkelingen als data-explosie, snellere dataverwerking en –interpretatie en de vergaande mogelijkheden voor gepersonaliseerde dienstverlening, brengen nieuwe kansen en voordelen op het gebied van overheidsdienstverlening. De ICT-technologieën ondersteunen nieuwe vormen van dienstverlening en eGovernment waarin flexibiliteit, samenwerking (met andere overheidsorganisaties, maar ook met bedrijven, burgers en het maatschappelijk middenveld) en nieuwe, meer decentrale organisatiestructuren centraal staan (Frissen et al, 2007). De toepassing van de NBIC-technologieën en nieuwe typen sensoren creëren ook nieuwe mogelijkheden voor een open overheid/open data, waarbij overheden pro-actief de verzamelde ruwe data ter beschikking kunnen stellen aan bedrijven, individuen en maatschappelijke organisaties om daar waarde mee te creëren.

Ook overheden zelf zijn beter in staat relevante informatie voor beleid (zowel voor de agendabepaling als voor de uitvoering en handhaving) te verzamelen en toe te passen. Intelligente systemen produceren bruikbare informatie waardoor overheidsinstanties meer kansen krijgen om informatie beter af te stemmen op de omstandigheden van de burger en zo betere en geïntegreerde dienstverlening mogelijk kunnen maken. Dit maakt dat afstemming in ketens kan verbeteren en het biedt kansen om diensten te ontwikkelen die beter aansluiten op de speciale behoeften van specifieke individuen of groepen; het wordt makkelijker om maatwerk te leveren. Personificatie van elektronische diensten zal in de toekomst verder toenemen. We zien nu al voorbeelden, zoals de vooringevulde belastingaangifte of overheidsportals zoals mijnoverheid.nl waar de burger de gegevens die verschillende overheidsinstanties over hem/haar hebben geregistreerd, kan inzien.

Aan de andere kant duiden de technologische trends op een toenemende verknoping van diensten en informatiestromen. Het WRR rapport ‘iOverheid’ toont informatievervuiling binnen de overheid, waarin onduidelijk is wie verantwoordelijk is voor welke informatiestromen en waarin burgers, bedrijven en overheidsinstanties zelf ‘verstrikt raken in de datakluwen van de overheid’ (WRR, 2011).

Machtsrelaties
De nieuwe ontwikkelingen in ICT bieden ook nieuwe kansen voor burgers om meer invloed uit te oefenen op beleid en overheid. Dat kan impact hebben op de relatie overheid-burger. Groepen gebruikers worden door ICT steeds beter in staat gesteld om zich makkelijk en snel te organiseren en zo invloed uit te oefenen op elkaar en op de overheid (Huijboom et al 2009). Voorbeelden variëren van *fixmystreet.com* waar burger met behulp van mobiele telefoons ongeregeldheden (zoals overtollig vuilnis, graffiti of een uitstekende stoeptegel) direct kunnen melden bij hun gemeente (dit zal ook voor de overheid betekenen dat zij haar processen anders

zal moeten inrichten om hier adequaat op te kunnen reageren), tot grootschalige Facebook-acties van burgers om invloed uit te oefenen op politieke campagnes (zie bijvoorbeeld de campagne van toenmalige presidentskandidaat Obama), tot meer controle op uitvoering en handhaving van beleid (zoals Geluidsnet of Wikileaks). Burgers dwingen zo transparantie aan de kant van de overheid. Ook stelt nieuwe technologie burgers in staat zelf de acties van haar overheid te monitoren (sousveillance). De technologische mogelijkheden, met name die van het intelligente web, zullen deze ontwikkeling versterken.

Privacybescherming
Inherent aan de steeds verdere personalisatie is dat de onderliggende technologieën ook een significante impact kunnen hebben op de privacy van individuen als er niet zorgvuldig wordt omgegaan met de verzamelde data. De clusters laten een snelle ontwikkeling zien van technieken voor dataverzameling, -opslag en -verwerking. Personalisatie en meer gemak leveren, betekent inherent ook meer dataverzameling door de overheid over haar burgers. De toepassing van de nu al volwassen sensortechnologie en RFID-technologie, in combinatie met een toename in het aantal apparaten, objecten en actuatoren die altijd met het internet of netwerk verbonden zijn, zorgt voor een explosie van de hoeveelheid data. De toename in computerkracht, mede door nieuwe virtualisatietechnieken, en nieuwe technieken voor patroonherkenning en datamining zorgt dat deze grote hoeveelheden ook in korte tijd, en steeds vaker *real-time* geanalyseerd en toegepast kunnen worden. De moderne technologie creëert ook nieuwe typen data, zoals genetische gegevens (DNA), fysiologische gegevens (emoties) of medische gegevens (bloeddruk, insulinegehalte). De technologie biedt aldus uitgebreide mogelijkheden voor het aanleggen van gedetailleerde profielen van individuele, groepen en categorieën burgers. Toenemende dataverzameling en nieuwe typen van data (locatie, genetisch e.d) werkt deze ontwikkeling in de hand en creëert meer mogelijkheden voor het pro-actief handelen van de overheid waarbij van deze data en technieken gebruik wordt gemaakt.

Tenslotte moet erop worden gewezen dat opgeslagen data over individuen ook voor andere doelen en taken van de overheid dan e-dienstverlening kunnen worden gebruikt. De beschreven ICT-trends bieden een groeiend aantal mogelijkheden voor verregaande en intelligente surveillance. Een voorbeeld is het hiervoor beschreven *brainfingerprinting*. Ook nu zien we voorbeelden waar nieuwe technieken door de overheid worden ingezet voor surveillance en veiligheidsdoeleinden, zoals het toepassen van hoge tonen op plekken waar hangjongeren zich op houden en het inzetten van gezichtsherkenningssoftware in het openbaar vervoer van Rotterdam om overlast te kunnen beperken.

Kwetsbaarheid en complexiteit
De beschreven clusters van ICT-trends brengen ook nieuwe beveiligings- en aansprakelijkheidskwesties met zich mee. Steeds meer overheidsdiensten zullen een digitale component hebben en via online portals burgers worden aangeboden. De beveiliging van deze diensten is complex. De recente ontwikkelingen bij Diginotar onderstrepen dit. Ook de nieuwe wijze van het gebruik van computerkracht (zoals cloud computing of Software as a Service) creëert tal van onzekerheden: ten aanzien van de betrouwbaarheid van de dienst en onderliggende techniek, wie de eigenaar is van de opgeslagen en gebruikte data, wat er met de data wel en niet mag gebeuren, de mogelijkheid dat de

vertrouwelijkheid van de data in het geding komt en het risico dat de dienst niet beschikbaar is voor een langere periode als resultaat van technische storingen, vijandige acties of om juridische redenen. Deze kwesties raken direct aan de bescherming van persoonlijke gegevens van individuen. De opkomende *utility services* zijn in dat opzicht nog complexer dan de internet en databases die we vandaag kennen. Ook zal er een sterke behoefte blijven bestaan om de openheid van de cloud diensten te bewaren, inclusief interoperabiliteit en open standaarden.

De toenemende en steeds verdergaande digitalisering en informatisering binnen de overheid leidt tot veel en zeer complexe informatiestromen en een toenemende uitwisseling van gegevens tussen de publieke sector en de private sector (en binnen de publieke sector zelf). De WRR (2010) constateert dat in toenemende mate er een vernetwerking plaatsvindt van informatie, waar er sprake is van gezamenlijk gebruik en beheer van informatiesystemen door verschillende overheidsinstanties en het continue verrijking en samenstelling van informatie die uit verschillende bronnen (systemen) afkomstig is. De informatiestromen worden daardoor dusdanig complex dat het vaak onduidelijk is welke instantie waarvoor verantwoordelijk is en waarop aanspreekbaar is. De verantwoordelijkheidsverdeling voor de juiste verwerking van informatie is en wordt steeds diffuser in de toekomst. In de concrete vertaling van beleidslijnen naar de implementatie van informatiesystemen zal expliciet aandacht moeten zijn voor het vaststellen en bepalen van de verantwoordelijkheidsverdeling.

Conclusie
Geconcludeerd kan worden dat met de gesignaleerde trends de hoeveel data die over burgers wordt verzameld zeer waarschijnlijk verder toe zal nemen. Dat betekent dat het zorgvuldig afwegen en omgaan met die gegevens steeds belangrijker wordt om inbreuken op de persoonlijke levenssfeer te voorkomen**.** Het type data dat wordt verzameld, het type techniek of softwaresysteem dat wordt ingezet en het aantal overheidsorganisaties dat gebruik maakt van de gegevens bepalen mede hoe privacy-invasief een ICT-innovatie en is welke waarborgen nodig zijn om privacy te waarborgen. Dit hoofdstuk geeft daarmee de achtergrond en het belang weer van de ontwikkeling van een afwegingskader, dat inzicht biedt in de gevolgen van ICT-innovaties en de voorwaarden waaronder de inzet van Privacy by Design de legitimiteit en verantwoordelijkheid van de overheid kan vergroten.

4 Overheidsdienstverlening en privacybescherming

Om de theoretische en empirische analyses in de volgende hoofdstukken van noodzakelijke context te voorzien, gaan we eerst in op de begrippen privacy en elektronische dienstverlening door de overheid. Daarnaast volgt een beschrijving van Privacy by Design en de elementen die onder dit begrip vallen.

4.1 Privacy

Onder bescherming van privacy (zie ook Vedder, 2009) verstaan we activiteiten en maatregelen die erop gericht zijn om de toegang tot het individu in ruimtelijke, relationele en informationele zin te reguleren. Privacybescherming zoals hier onderzocht – namelijk in het kader van Privacy by Design – gaat uitdrukkelijk verder dan de bescherming van persoonsgegevens (dataprotectie). Bescherming van privacy is er uiteindelijk op gericht om de persoonlijke autonomie van mensen te beschermen of te vergroten en hun kwetsbaarheid (bijvoorbeeld voor materiële schade, discriminatie, stigmatisering) te verminderen of in elk geval niet verder te vergroten. Privacy is niet uitsluitend bedoeld om individuen te beschermen. De waarden achter privacy hebben ook belangrijke sociale dimensies. Privacy geeft de burger de mogelijkheid om zonder controle van buitenaf tot eigen meningen en voorkeuren te komen. Zo draagt zij bij tot de pluriformiteit en creativiteit in de samenleving en tot de bescherming en handhaving van de democratische rechtsstaat.

In Europa zijn de OECD privacy principes[26] en de Europese richtlijnen betreffende privacybescherming[27] van groot belang. Centraal in die principes en richtlijnen staat de principiële beschermwaardigheid van persoonsgegevens, d.w.z. gegevens die herleidbaar zijn tot een individuele persoon. De bescherming van die gegevens wordt op verschillende manieren nagestreefd. Voorop staat dat het individu in staat wordt gesteld controle uit te oefenen over wie er welke gegevens over hem of haar mag verzamelen, bewerken of opslaan. Dit gebeurt door het vereiste van toestemming, door inzage- en correctierechten, door regels die de transparantie bevorderen, door eisen van doelbinding (men geeft bijvoorbeeld toestemming voor een bepaald gebruik van gegevens en niet automatisch voor hergebruik of gebruik voor andere doeleinden) en door beheersvereisten (er moet bijvoorbeeld duidelijkheid worden geschapen over wie de verantwoordelijke is, wie de bewerker, over beveiligingsvoorschriften enz.). Privacy wordt in het debat dus een zaak van bescherming van gegevens over personen waarbij idealiter de centrale *locus of control* de individuen zijn op wie de gegevens betrekking hebben. Opgemerkt dient nogmaals te worden dat Privacy by Design zich niet beperkt tot de informationele dimensie van privacy.

[26] OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[27] Directive 2006/24/EC, Directive 95/46/EC en Directive 2002/58/EG.

Tabel 1: OESO privacyprincipes

- Beperking aan dataverzameling: er worden niet meer gegevens dan nodig voor het leveren van de dienst verzameld (tegenwoordig vaak geformuleerd als dataminimalisatie)
- Kwaliteit van data: opgeslagen data zijn accuraat, up-to-date en compleet
- Specificatie van het doel: vastleggen van het doel van dataverzameling
- Doelbinding: de verzamelde data mogen niet voor andere doeleinden worden gebruikt dan het vastgelegde doel
- Beveiliging van data: tegen ongeautoriseerde toegang, vernietiging, oneigenlijke openbaarmaking van data
- Openheid: de informatieverwerkende organisatie geeft openheid over ontwikkelingen, procedures en beleid ten aanzien van persoonlijke dataverzameling en - verwerking.
- Inzage en toestemming: een individu heeft het recht om de verzamelde informatie over hem/haar in te zien en moet worden geïnformeerd door de informatieverwerker over data die over hem/haar wordt verzameld
- Verantwoording: een dataverwerker moet verantwoording af kunnen leggen over het naleven van de eerder genoemde principes

Van belang is nog dat door de inwerkingtreding van het Verdrag van Lissabon (2009) het Handvest voor de rechten van de mens deel is gaan uitmaken van Europees recht. Artikel 8 van dit Handvest erkent de bescherming van persoonlijke data als een autonoom recht van het individu. Bovendien is in het Verdrag van Lissabon de bevoegdheid gecreëerd voor het aannemen van wetgeving met betrekking tot de bescherming van individuen voor wat betreft de verwerking van hun persoonlijke data en het vrije verkeer van deze data.[28] Op basis hiervan heeft de Commissie aangekondigd in 2011 met nieuwe wetgeving te zullen komen, met als doelstelling de huidige wetgeving te herzien opdat de bescherming van persoonlijke gegevens wordt versterkt.[29]

4.2 Elektronische dienstverlening door de overheid

Wat is elektronische dienstverlening door de overheid? Met “de overheid” verwijzen we in dit rapport naar organen van het nationale wereldlijke gezag. Het gaat daarbij om ministeries en diensten van de nationale overheid. Deze ministeries en diensten kunnen zelf elektronische diensten aanbieden (bijvoorbeeld het online verrichten van de jaarlijkse belastingaangifte). Maar ze kunnen de diensten ook aanbieden via private partijen. Naar verwachting zullen in de toekomst meer private of hybride partijen worden ingezet voor de uitvoering van traditionele overheidstaken. Zoals we later nog zullen zien zou dit bijkomende eisen voor de legitimiteit van en het vertrouwen in de overheid met zich mee kunnen brengen.

Onder elektronische dienstverlening verstaan wij hier in brede zin alle dienstverlening via elektronische netwerken zoals het huidige internet. In principe kan men hieronder zowel het eenzijdige verschaffen van informatie als alle vormen van transacties en communicatie met gebruikers vatten, maar wij beperken ons tot

[28] Zie artikel 16 van het Werkingsverdrag betreffende de Europese Unie.
[29] European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, COM(2010)609, p. 18.

transacties en communicatie waarbij de gebruiker gegevens – waaronder persoonsgegevens – aan de dienstverlener verschaft die in elk geval verder gaan dan alleen het IP-nummer van zijn computer door het simpele bezoek van de website. Onder dienstverlening verstaan wij niet alleen de dienst op zich maar ook de wijze waarop deze wordt aangeboden (gebruiksgemak, ontwerp site of formulier, e.d.). De diensten kunnen zeer verschillend van aard en complexiteit zijn. Ook kan het gaan om diensten die burgers helpen om aan hun wettelijke verplichtingen te voldoen (bijvoorbeeld belastingaangifte) of om een voorziening te verkrijgen (bijvoorbeeld huursubsidieaanvragen). Meestal bestaat er voor elektronische diensten een alternatief in de offline werkelijkheid (bijvoorbeeld papieren formulier invullen en insturen). Per elektronische dienst kan de offline evenknie echter verschillen in praktische verkieslijkheid.

4.3 Privacy by Design

We hebben gezien dat de mogelijkheden voor dataverzameling en -verwerking (en daarmee het aanbieden van persoonlijke diensten) in de toekomst alleen maar verder zal toenemen. Uit Brits onderzoek blijkt dat de generieke wetgeving op het gebied van dataprotectie vaak niet toereikend is om de doelen van elektronische dienstverlening en privacy goed te verenigen (Bellamy et. al., 2005).[30] De Britse toezichthouder op de bescherming van persoonsgegevens (de Information Commissioner's Office, ICO) stelt dat zowel publieke als private organisaties privacybescherming vaak benaderen als een minimale invulling van de dataprotectiewetgeving, waardoor zij belangrijke privacykwesties over het hoofd zien (ICO, 2008). Dit kan leiden tot kostbare en moeilijke 'reparaties' achteraf, imagoschade, en publieke weerstand tegen het systeem of dienst (ICO, 2008). De bescherming van privacy is bovendien vaak reactief; toezichthouders kunnen pas achteraf (na de ontwikkeling van een nieuw systeem of dienst) controleren of de dataprotectiewetgeving wordt nageleefd en eventuele boetes opleggen. In toenemende mate wordt daarom gekeken naar manieren om privacy op een proactieve wijze te beschermen. In de preambule van de EU Richtlijn 95/46 wordt bijvoorbeeld geëist dat passende technische en organisatorische maatregelen moeten worden genomen bij zowel het ontwerp als het gebruik van het nieuwe systeem.

Dit is precies de doelstelling van Privacy by Design: om in een zo vroeg mogelijk stadium na te denken over de mogelijke impact van de ICT innovatie op de privacy van burgers en om privacyrisico's te vermijden of zoveel mogelijk te minimaliseren. Dit betekent dat voordat een ICT-innovatie wordt geïmplementeerd wordt nagedacht over de noodzaak van vastlegging van persoonsgegevens, de wijze van gegevensbescherming, oplossingsrichtingen en bijbehorende kosten en baten (Koorn et al, 2004). Fundamentele privacyprincipes kunnen zo direct in het ontwerp van het IT-systeem én in de organisatie worden geïntegreerd. Privacybescherming is dan moeilijker te omzeilen, waardoor een sterkere en eenvoudiger controle op privacybescherming mogelijk is dan enkel door toezicht en handhaving van de dataprotectiewetgeving.

[30] Een discussie over de toereikendheid van de huidige wettelijke kaders ten aanzien van privacybescherming ligt buiten het bereik van deze studie. Voor meer informatie over dit onderwerp, zie Evaluatie Wet bescherming persoonsgegevens (kamerstuk 31 051, vergaderjaar 2010-11) en de brief van de regering aan de TK d.d. 29 april 2011 inzake haar voornemens tot wijziging van de Wet bescherming persoonsgegevens.

Transparantie is een belangrijk onderdeel van PbD. Alleen door het inzichtelijk maken van hoe er met privacyrisico's wordt omgegaan, zijn burgers in staat om controle uit te oefenen over hun eigen gegevens en waakzaam te zijn op de bescherming van persoonlijke gegevens. Het is daarom essentieel dat individuen duidelijk geïnformeerd zijn over hoe en door wie hun gegevens worden verzameld en gebruikt, om welke redenen, voor hoe lang en wat hun rechten zijn als zij toegang willen krijgen tot hun gegevens of als zij de gegevens willen verwijderen of rectificeren. Transparantie houdt in ieder geval in dat:

- informatie gemakkelijk toegankelijk is;
- gemakkelijk te begrijpen is;
- in duidelijke taal is verwoord.

Dat dit niet altijd het geval is blijkt uit een Eurobarometer onderzoek.[31] Uit een survey gehouden in 2009 onder het Europese publiek kwam naar voren dat de helft van de respondenten privacynotificeringen op websites 'erg' of behoorlijk onduidelijk vonden, niet transparant en moeilijk toegankelijk.

Een voorbeeld waarin Privacy by Design in de praktijk worden toegepast is de inzet van de *security scanner* op verschillende internationale vliegvelden. Dit apparaat scant passagiers op aanwezigheid van wapens en gevaarlijke stoffen. De scanner kan beelden van zeer hoge kwaliteit produceren van in feite het naakte lichaam. Men maakt op de vliegvelden gebruik van een techniek (een zogenaamde Privacy Enhancing Technology) om de beelden te vervagen en niet uniek identificeerbaar te maken. In sommige vliegvelden gaat men nog verder en wordt er ook rekening gehouden met data-opslag en de fysieke dimensie van privacy. Zo zit het personeel dat de beelden bekijkt op een andere fysieke locatie ('achterkamer') dan waar de passagiers door de scanners gaan ('frontlinie'), zodat het personeel dat de beelden bekijkt deze niet kan relateren aan de passagier. Als het personeel in de achterkamer een mogelijke afwijking of dreiging ontdekt, geven zij dit door aan het screening personeel (bij de passagiers) via een aparte grafische interface waar alleen die delen van het lichaam die om nader onderzoek vragen, worden getoond. Het personeel in de 'frontlinie' ziet niet de beelden van het hele lichaam. Extra informatie kan gedeeld worden via radiocommunicatie. De beelden worden niet opgeslagen of op enige wijze gedeeld of verstuurd naar andere partijen. Op deze manier wordt én in de techniek (het onherkenbaar maken van beelden) én in het bedrijfsproces (het niet opslaan van gevoelige gegevens) én in de fysieke omgeving (achterkamers separaat van waar passagiers worden gescand) Privacy by Design toegepast. Hiermee wordt aan een belangrijk uitgangspunt van PbD om privacybescherming in te bouwen zonder verlies van functionaliteit voldaan.

[31] Flash Eurobarometer No 282, beschikbaar op het internet via http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm

Hoewel de doelstelling van Privacy by Design op zich helder en functioneel is, is het allerminst duidelijk wat het precies omvat. Op dit moment ontbreekt zowel een eenduidige definitie van PbD als overeenstemming over de vraag welke elementen er onder vallen. In de wetenschappelijke literatuur is PbD geen gangbare term. De Canadese toezichthouder op de dataprotectiewetgeving Ann Cavoukian (2009) heeft de term in de jaren negentig geïntroduceerd na samenwerking met de Nederlandse toezichthouder (destijds de Registratiekamer) over toepassingsmogelijkheden van Privacy Enhancing Technologies (PET) en verwees naar het technisch inbouwen van privacybescherming in IT-systemen. Het begrip is daarna echter uitgegroeid tot een bredere benadering (Cavoukian, 2009), waarbij het niet alleen gaat om technische waarborgen, maar ook om waarborgen in bedrijfsprocessen en een omslag in bedrijfscultuur[32].

In dit rapport hanteren wij als stipulatieve definitie voor Privacy by Design:

Privacy by Design houdt in dat vanaf het (her)ontwerp en gedurende de gehele levenscyclus van een informatiesysteem (tot aan afbouw dan wel vervanging) met behulp van zowel technische als organisatorische maatregelen inbreuken op de persoonlijke levenssfeer worden vermeden

De stipulatieve definitie maakt duidelijk wat Privacy by Design inhoudt, maar geeft nog geen beeld welke maatregelen of instrumenten onder Privacy by Design vallen. Op basis van literatuuronderzoek hanteren we in dit project de volgende parameters voor Privacy by Design:

- Privacy Impact Assessments (privacyrisicobeoordelingen)
- Privacy in de organisatie
- Privacy Enhancing Technologies

Hierbij moet worden opgemerkt dat ook andere parameters kunnen worden genoemd, zoals privacy in de fysieke ruimte[33]. Wij hebben gekozen voor deze parameters, omdat deze het beste bij het onderzoeksobject (e-overheidsdiensten) van dit rapport passen.

[32] In 2010 hebben internationale toezichthouders op privacy en dataprotectiewetgeving een "Privacy by Design resolutie" aangenomen waarin PbD wordt omschreven als een holistisch concept dat kan worden toegepast in allerlei operaties van een organisatie, inclusief de informatie-technologie, bedrijfspraktijken, bedrijfsprocessen, fysieke omgeving en genetwerkte infrastructuur (Cavoukian, 2010).

[33] Zie voor meer informatie over de elementen van Privacy by Design: Lieshout, M. van, Kool, L., Schoonhoven, B. van, Jonge, de M. (nog te verschijnen) Privacy-by-Design: alternative for existing practices in safeguarding privacy? In: Info, 2011

4.3.1 Privacy Impact Assessments (PIA)

De eerste stap bij het toepassen van Privacy by Design is een goed beeld te krijgen van de mogelijke privacykwesties die de introductie van een (nieuw) IT-systeem of dienst teweeg brengt. Met een Privacy Impact Assessment (PIA) wordt ex ante een inschatting gemaakt van de privacyrisico's van het te ontwerpen informatiesysteem (risicoanalyse). Tevens wordt in kaart gebracht hoe deze risico's vermeden of verkleind kunnen worden. Een PIA wordt idealiter uitgevoerd vóór de implementatie van een IT-systeem en bij elke substantiële verandering in het systeem of in de omgeving van het systeem (ICO, 2009). Een belangrijk onderdeel van de PIA is participatie van belanghebbenden, waaronder de eindgebruikers. De organisatie kan zo ook anticiperen op eventuele risico's die niet voorzien waren op basis van algemene privacyprincipes en daarmee het vertrouwen van gebruikers verhogen en eventuele reputatieschade voorkomen. Op dit moment maken vooral Angelsaksische landen gebruik van PIA's. In sommige landen, waaronder Canada, is het uitvoeren van PIA voor overheidsinstanties verplicht. Bij de behandeling van de Evaluatie Wet bescherming persoonsgegevens is in de Eerste Kamer gepleit om voor elke nieuwe wet die de persoonlijke levenssfeer raakt een PIA uit te voeren (motie-Franken, vergaderjaar 2010-11, 31 051 D). Het Kabinet kondigde in een brief naar de Tweede Kamer in april 2011 aan dat ze de mogelijkheden voor het gebruik van Privacy Impact Assessments onderzoekt (TK 2010-2011). Dit sluit aan bij de Communicatie van de Europese Commissie betreffende dataprotectiewetgeving.[34]

Een PIA volgt een grondige en systematische methode voor de beoordeling van de risico's en onderzoekt manieren om de risico's te vermijden, verkleinen of beheersbaar te maken (zie bijvoorbeeld Wright, 2011 of Wright en de Hert, nog te verschijnen). Het helpt ook om juridische principes zoals doelbinding te vertalen naar concrete implementaties. Het brengt alle technologische, organisatorische, juridische en beleidsrisico's in kaart. Per categorie wordt bekeken hoe men de risico's kan vermijden of verkleinen. De meerwaarde van PIA is dat alle informatie wordt verkregen die een belangenafweging tussen enerzijds het belang van privacybescherming en anderzijds het belang van het informatiesysteem inzichtelijk maakt. Over de daadwerkelijke uitkomst van deze belangenafweging zegt de PIA niets: het is puur een procedureel instrument.

Voor RFID is er recent in Europa een PIA-raamwerk opgesteld. Wij beschrijven dit raamwerk hier omdat het inzicht biedt in wat een PIA inhoudt en welk proces er doorlopen moet worden. Het raamwerk wordt onderschreven door de Artikel 29 Werkgroep (Artikel 29 Werkgroep, 2011). De PIA is opgedeeld in twee fasen. De 'pre-assessment' fase beoordeelt een RFID-applicatie op privacygevoeligheid. Op basis hiervan wordt bepaald of een PIA op grote schaal ('full scale PIA') of een kleine PIA is vereist ('small scale PIA'). Fase 2 is de risicobeoordeling, die bestaat uit vier stappen:

- Karakterisering van de applicatie (data typen, datastromen, type technologie, manier van opslag, welke data wordt opgeslagen e.d.)
- Identificatie van risico's voor persoonsgegevens (beoordeling van de bedreiging, impact en kans dat de bedreiging daadwerkelijk optreedt, alsmede

[34] Zie ook WRR, *iOverheid*, rapport 86, 2011.

de impact van risico's in termen van het naleven van de Europese regelgeving omtrent privacy en dataprotectie)
- Identificatie en aanbeveling van beheersmechanismen (zogenaamde 'controls') voor de in de vorige stap vastgestelde risico's
- Documentatie van de resultaten van de PIA, inclusief de implementatie van beheersmechanismen in de applicatie en informatie over niet-geadresseerde risico's ('residual risk'), aan de desbetreffende autoriteit(en).

Elke stap wordt ondersteund door vaste templates beschreven in het PIA-raamwerk:
- Een sjabloon om de belangrijkste eigenschappen van de applicatie te beschrijven
- Een lijst van negen privacy 'doelen', afgeleid van de Europese dataprotectie richtlijn
- Een lijst van typische privacyrisico's, met beschrijving en voorbeelden
- Een lijst van voorbeelden van beheersmechanismen

4.3.2 *Privacy in de organisatie*

Om de legitimiteit van het informatiesysteem te verzekeren dient in de eerste plaats aandacht te worden besteed aan de inbedding van het systeem binnen de organisatie die er gebruik van maakt. Daarbij dient aansluiting te worden gezocht bij het wettelijk kader voor privacybescherming: welke verplichtingen heeft de beheerder van het informatiesysteem (in ons onderzoek: dienstverlenende instantie) uit het oogpunt van de bescherming van privacy en hoe is de beheerder aanspreekbaar?

Uit het Europese recht vloeit een aantal concrete verplichtingen voort. Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer daarvan is hier relevant. Een aantal van de verplichtingen die in deze richtlijn is opgenomen vereisen een bepaalde organisatie van een overheid, die te maken krijgt met de verwerking van persoonsgegevens. Allereerst is het beginsel van dataminimalisering vastgelegd: waar mogelijk streven naar maximale anonimiteit, zo min mogelijk gegevens en zo vroeg mogelijke verwijdering van data.[35] Hoewel hiervoor zoals we zullen zien technische oplossingen mogelijk zijn, moet de organisatie dit mogelijk maken en ondersteunen. Hetzelfde geldt voor de transparantie over de gegevensverwerking[36] en de beveiliging aan de hand van een privacyrisicoanalyse.[37] Dit geldt des te meer als het gaat om zaken als rechtmatigheid, zoals bijvoorbeeld het geven van toestemming m.b.t. de gegevensverwerking en de kwaliteit van de gegevens.[38] Zo kunnen persoonlijke gegevens automatisch worden vernietigd als een vooraf gestelde (en eventueel wettelijk omschreven) termijn is verlopen. Dit is uiteraard alleen mogelijk als de oorspronkelijke logica achter de geautomatiseerde besluiten bekend is, en kan worden omgezet in een technische oplossing.

[35] Art. 6(1)(b, c, e).
[36] Artikelen 6(1)(a), 10, 11.
[37] Artikelen 17.
[38] Zie bijvoorbeeld artikelen, 6, 7(a-f) en 8 lid 2,4,6.

In Nederland zijn de Europeesrechtelijke verplichtingen geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Deze wet is van toepassing op de volledig of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op handmatig beschikbare gegevens, voor zover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen (art. 2, lid 1). Samengevat vereist de Wbp explicitering van de verantwoordelijkheden voor de verwerking van persoonsgegevens en vereist hij een deugdelijke beveiligingsregie voor de opslag en verwerking van de betreffende gegevens.

Verantwoordelijke
Als 'verantwoordelijke' voor de gegevensverwerking noemt de Wbp degene die formeel-juridisch de zeggenschap over de verwerking heeft. Deze persoon is bevoegd doel en middelen vast te stellen en is tevens aansprakelijk. Het is meestal de rechtspersoon onder wiens bevoegdheid de operationele gegevensverwerking plaatsvindt. Dit laat onverlet dat het feitelijk beheer aan een ander ('bewerker') kan worden overgelaten. Op een 'verantwoordelijke' rust een beveiligingsplicht. Ter voorkoming van onrechtmatige verwerkingen of ter voorkoming van verlies van gegevens, moet een verantwoordelijke 'passende organisatorische en technische maatregelen' treffen. Een organisatorische maatregel is bijvoorbeeld het treffen van een regeling voor de toegang tot de gegevens. In een overzicht kan worden aangegeven welke functionaris tot welke gegevens toegang heeft. Zo'n voorbeeldmatrix is opgenomen in een van de rapporten, die in het kader van het Implementatieprogramma WGBO in juni 2004 zijn gepubliceerd.[39]

Grondslag van de verwerking
Voor elke handeling met persoonsgegevens geldt dat deze in overeenstemming moet zijn met wet en beginselen van behoorlijk bestuur. Het verzamelen van persoonsgegevens is alleen toegestaan als dat gebeurt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze gerechtvaardigde doeleinden komen in de praktijk overeen met een of meer van de grondslagen waarop elke verwerking van en handeling met persoonsgegevens moet berusten. Voor een gegevensverzameling zijn twee van deze gronden relevant: de toestemming van de cliënt en/of noodzakelijkheid voor de behartiging van een gerechtvaardigd belang. Een eenmaal gegeven toestemming kan bovendien altijd worden ingetrokken. Toestemming hoeft niet te worden gevraagd als kan worden beargumenteerd dat de gegevensverzameling "noodzakelijk" is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke (bijvoorbeeld dagelijks beheer van de reguliere bedrijfsactiviteiten, tijdsbesparing, minder fouten, soepeler declareren en meer klantvriendelijkheid, kostenbesparing) of van derden aan wie de gegevens worden verstrekt. Om rekening te houden met de privacy van cliënten kan bijvoorbeeld worden voorzien in een privacyreglement dat voor cliënten beschikbaar is en waarin de mogelijkheid is opgenomen om bezwaar te maken tegen deelname aan de gegevensverzameling.

[39] J.M.Witmer, R. de Roode, *Van wet naar praktijk. Implementatie van de WGBO. Deel 4 Toegang tot patiëntengegevens*, Utrecht 2004, bijlage 2, p. 73.

Wanneer men op rechtmatige wijze verzamelde persoonsgegevens wil gebruiken (verder verwerken), dan is dat uitsluitend toegestaan als dat in overeenstemming is met het oorspronkelijke doel van het verzamelen en verwerken. De Wbp kent uitdrukkelijk de mogelijkheid om de wettelijke voorschriften nader uit te werken in instrumenten van zelfregulering. Zoals reeds hierboven opgemerkt, kan een privacyreglement nuttig zijn voor de organisatie teneinde tegemoet te komen aan het privacybelang van de betrokkenen.

Meldingsplicht en informatieplicht
Voor alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens geldt op grond van de Wbp een meldingsplicht. Het gaat hier om een administratieve verplichting. Deze verplichting houdt in dat in principe alle verwerkingen, behalve handmatige verwerkingen, moeten worden aangemeld bij het College bescherming persoonsgegevens of bij een Functionaris voor de Gegevensbescherming (FG), als die binnen de branche of organisatie is benoemd. Naast handmatige verwerkingen hoeven ook verwerkingen die vallen onder het Vrijstellingsbesluit Wbp niet te worden aangemeld, mits deze voldoen aan de voorwaarden die in dat Vrijstellingsbesluit zijn aangegeven. Een vrijstelling van de meldingsplicht bestaat echter niet voor verwerkingen waarbij sprake is van gedeelde of gezamenlijke verantwoordelijkheid waarvan sprake kan zijn als ook andere bestuursorganen in het geding zijn.

Op de (gezamenlijke) verantwoordelijke(n) rust de verplichting om alle betrokkenen van wie gegevens worden vastgelegd te informeren over de identiteit van de verantwoordelijke(n) en het doel van de gegevensverzameling, alsmede nadere informatie te verschaffen voor zover dat nodig is uit een oogpunt van rechtmatige gegevensverwerking.

4.3.3 Privacy Enhancing Technologies

In aanvulling op de organisatorische maatregelen wordt steeds meer ingezet op technische middelen om privacy te garanderen. Privacy Enhancing Technologies (PETs) zijn technische instrumenten om privacyrisico´s te verkleinen of in zijn geheel te vermijden. Als zodanig vormen zij een belangrijk onderdeel van Privacy by Design. De term PET werd in 1995 voor het eerst gebruikt in een rapport van de Information and Privacy Commissioner in Ontario in Canada en de toenmalige Registratiekamer (Blarkom et. al. 2003). Het rapport verkende een nieuwe benadering voor het beschermen van privacy en toonde overigens aan dat systemen die geen tot weinig persoonlijke gegevens verzamelen dezelfde functionaliteiten kunnen hebben als systemen die veel data verzamelen (Hes en Borking, 1995). Daarvoor (in de jaren ’80) werd al door wetenschappers gewerkt aan cryptografische protocollen die anonieme en ontraceerbare communicatie mogelijk maken (Chaum, 1981). In 2007 publiceerde de Europese Commissie een Communicatie om het gebruik van PET te stimuleren en zo de schending van de dataprotectie moeilijker maken (EC, 2007). In Nederland werd bij de behandeling van de Wet persoonsbescherming in de Tweede Kamer al in 1999 de motie Nicolaï aangenomen. De regering werd hierin verzocht om de ontwikkeling en gebruik van PET te bevorderen door als innovatieve aanbesteder het voortouw inzake de inzet van PET te nemen bij haar eigen verwerking van persoonsgegevens (TK 1999-2000, 25891, nr. 31). Dit heeft onder andere geleid tot een onderzoek in welke overheidsprojecten PET kon worden toegepast (TNO, 2002; Borking, 2010). De

toepassing van PET bleek echter bij verschillende overheidsinstanties op weerstand te stuiten (Borking, 2010).

PETs zijn technologieën en maatregelen die zich richten op het elimineren of minimaliseren van de hoeveelheid gegevens die verzameld en opgeslagen worden over een individu (dataminimalisatie), het voorkomen van strijdigheid met privacyprincipes (zie hierboven) en het inzetten van controle-instrumenten voor gebruikers over informatie die over henzelf verzameld en gebruikt wordt. Deze technologieën kunnen in allerlei verschillende systemen en diensten worden toegepast. Veel online applicaties vragen bijvoorbeeld meer informatie dan strikt noodzakelijk is voor het leveren van een dienst. Het toepassen van dataminimalisatie beperkt het aantal identificerende gegevens over een individu zoveel mogelijk, bijvoorbeeld door niet naar leeftijd en/of geboortedatum te vragen, maar alleen te kijken of iemand meerderjarig is of niet. Een andere mogelijkheid is om de identiteitsgegevens los te koppelen van de overige gegevens die zijn vastgelegd over een persoon (het scheiden van gegevens), of om persoonlijke data direct na een transactie te vernietigen. Ook kan door middel van programmatuur worden afgedwongen dat het verstrekken van gegevens altijd voldoet aan het vigerende privacybeleid ('privacy policies') (Koorn et al, 2004). Onder algemene PET-maatregelen vallen bijvoorbeeld het beveiligen van gegevens, het versleutelen van gegevens, authenticatie- en autorisatiemanagement, strenge vormen van toegangsbeheer, e.d.

Privacybescherming dient volgens Cavoukian (2009) de standaardinstelling in een systeem of dienst te zijn (*privacy-by-default*). Dit betekent bijvoorbeeld dat wanneer een gebruiker een profiel aanmaakt op een sociale netwerksite, dit profiel standaard niet gedeeld wordt met anderen, tenzij de gebruiker deze instelling zelf veranderd. Een ander punt dat ook de Britse toezichthouder ICO (2008) benadrukt, is het inbouwen van privacybescherming in de totale levenscyclus van het systeem/dienst. Dit betekent dat niet alleen in de ontwerpfase wordt nagedacht over hoe privacy optimaal te beschermen, maar ook bij de implementatie en bij de beëindiging van het systeem: kunnen de data in het systeem bijvoorbeeld worden vernietigd[40]?

Bij de toepassing van PET staan vier mechanismen centraal:

1. Anonimiteit: de identiteit van een subject kan binnen een set van subjecten in een systeem of database niet worden vastgesteld.
2. Pseudonimiteit: een pseudoniem is een alias die niet in verband kan worden gebracht met de echte naam van een subject, maar gebruikt wordt om aan dat subject te relateren.
3. Onverbondenheid (*unlinkability*): een actie of verschijning van een subject in een systeem kan niet in verband kan worden gebracht met een andere actie van dit subject.
4. Onwaarneembaarheid (*unobservability*): een data-object of transfer is niet te zien voor partijen die niet betrokken zijn in de transactie (zoals onbevoegden of aanvallers) maar de betrokkenheid van de subjecten in de datatransfer zijn ook niet te zien voor iedere andere partij.[41]

[40] Dit sluit aan bij het idee van 'vergeten' of 'het recht om te worden vergeten' ('right to be forgotten') (zie bijvoorbeeld Reding, 2010).
[41] Pfitzmann en Hansen, 2009; Fritsch, 2009; Meta Group, 2005.

De vier mechanismen verminderen verschillende privacyrisico's. Onverbondenheid maakt het bijvoorbeeld technisch onmogelijk om verschillende data / transacties over een subject met elkaar te combineren (aggregatie). De mogelijkheid tot het uniek identificeren van een individu wordt beperkt door het toepassen van anonimiteit, pseudonimiteit of een combinatie van alle bovenstaande vormen die de vertrouwelijkheid van communicatie garandeert. De toepassing van deze mechanismen bij bijvoorbeeld beveiligingscamera's kan betekenen dat beelden van individuen die rechtstreeks worden weergegeven worden vervaagd. Unieke identificatie is dan niet meer mogelijk.

5 Legitimiteit, verantwoordelijkheid, vertrouwen en acceptatie

5.1 Inleiding

In dit hoofdstuk wordt op basis van conceptuele analyses en literatuuronderzoek in kaart gebracht welke factoren vertrouwen en acceptatie bij de burger en verantwoordelijkheid en legitimiteit van de betrokken overheden beïnvloeden. De resultaten van dit onderzoeksdeel worden meegenomen bij het opstellen van vragen in het empirische onderzoeksdeel. Ook dragen zij bij aan de vorming van het uiteindelijk beoogde afwegingskader.

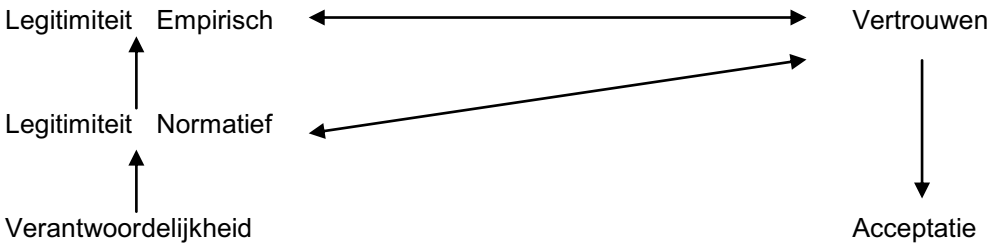
We beginnen met een nadere begripsbepaling. Aan de hand van stipulatieve definities van de noties verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie wordt de onderlinge samenhang van deze begrippen weergegeven en tegelijkertijd een compact overzicht gegeven van recente relevante literatuur. Daarna richten we ons specifiek op verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie rond elektronische dienstverlening door de overheid. Hier kan alvast worden opgemerkt dat onderzoek en literatuur over e-dienstverlening door de overheid in het licht van legitimiteit van die overheid tot nu toe ontbreekt voor zover zij niet direct of indirect wordt geïmpliceerd door het debat over vertrouwen en acceptatie. Tenslotte gaan we in op de rol die privacyoverwegingen spelen bij de verantwoordelijkheid, legitimiteit, vertrouwen en acceptatie rond e-dienstverlening door de overheid. Ook hier geldt hetzelfde *caveat* ten aanzien van bestaand onderzoek en literatuur.

5.2 Algemene begripsbepaling

De noties legitimiteit (“legitimacy”), verantwoordelijkheid (Engels: “accountability”), vertrouwen (“trust”, “confidence”) en acceptatie (“acceptance”, “adoption”) worden op soms meer, soms minder uiteenlopende wijze omschreven. De verschillen hangen af van het toepassingsgebied en de wetenschappelijke discipline waarin de noties als technische termen gebruikt worden. Zo zijn er bijvoorbeeld discrepanties te bespeuren tussen de manieren waarop vertrouwen wordt gedefinieerd in wetenschappelijke bijdragen over e-commerce (definities primair in termen van risicobeheersing) en over sociaal gedrag van mensen in groepen (definities primair in termen van gedrag en eigenschappen van individuen). Bij definities van legitimiteit zijn er verschillen tussen de politiek ethische (primair normatieve definities) en meer sociaal wetenschappelijk georiënteerde politicologische disciplines (primair empirische definities). Vaak ook is er sprake van overlap tussen de verschillende definities van de genoemde begrippen. Het doel van dit hoofdstuk is niet om met een universeel geldige definitie van de vier noties voor de dag te komen, maar om helder te krijgen wat de meest gangbare functionaliteiten van de termen zijn op vakgebieden en in wetenschappelijke debatten die relevant zijn voor elektronische dienstverlening van de overheid en de privacy van de burger. Het gaat daarbij vooral om achterliggende criteria, vragen, zorgen, idealen en andere aandachtspunten die experts in de actuele discussies als belangrijk aanmerken.

Het is duidelijk dat er belangrijke verbanden en overlappingen bestaan tussen de noties van verantwoordelijkheid en legitimiteit en vertrouwen en acceptatie. Deze verbanden en overlappingen bestaan tussen de vier afzonderlijke noties, maar ook tussen de begrippenparen verantwoordelijkheid-legitimiteit enerzijds en vertrouwen-acceptatie anderzijds. Zoals we verderop nog zullen zien, kan verantwoordelijkheid (*accountability*) een belangrijke voorwaarde vormen voor legitimiteit in moreel normatieve en juridische zin. Vertrouwen in een aanbieder en/of dienst of product blijkt vaak een belangrijke voorwaarde voor de acceptatie van een dienst of product. Feitelijk vertrouwen en acceptatie komen grotendeels overeen met wat we hieronder empirische legitimiteit zullen noemen. Tegelijkertijd zijn vertrouwen en acceptatie idealiter ook gebaseerd op legitimiteit in moreel normatieve en juridische zin. Hieronder zullen we verantwoordelijkheid en legitimiteit behandelen met nadruk op legitimiteit, en vertrouwen en acceptatie met nadruk op vertrouwen. Daarbij mag niet uit het oog worden verloren dat verantwoordelijkheid idealiter voorwaardenscheppend is voor legitimiteit, terwijl vertrouwen idealiter voorwaardenscheppend is voor acceptatie.

Bij de genoemde verbanden is er lang niet altijd sprake van noodzakelijke voorwaardelijkheid. Vertrouwen en acceptatie kúnnen gebaseerd zijn op legitimiteit, maar zij kunnen ook op heel andere overwegingen zijn gestoeld. Ook kunnen zij op bijkomende overwegingen – naast legitimiteit – gebaseerd zijn. Belangrijk is dat de legitimiteit van de aanbiedende overheid idealiter correspondeert met vertrouwen en acceptatie van de burger en omgekeerd.



5.3 Legitimiteit en verantwoordelijkheid

Legitimiteit is letterlijk de toestand of hoedanigheid van gelegitimeerd zijn. De term legitimiteit stamt van het Middeleeuws Latijnse *legitimatus,* voltooid deelwoord van *legitimare*: legitimeren. De term wordt in al zijn varianten in moderne talen primair geassocieerd met geboren zijn uit een erkend huwelijk en dientengevolge volle rechten en plichten bezitten als zoon of dochter. De Merriam-Webster Online Dictionary geeft als secundaire betekenissen voor het Engelse “legitimate” onder andere:

- precies zo zijn als bedoeld: niet vervalst of onecht.
- in overeenstemming met het recht of bestaande wettelijke vormen en vereisten of heersen krachtens of op grond van een strikt erfelijk recht.
- in overeenstemming met erkende beginselen of gedeelde regels en maatstaven.

In de politicologie wordt hierbij aangesloten, voor zover met het begrip legitimiteit het recht of de bevoegdheid om macht uit te oefenen wordt aangeduid. Daarbij wordt legitimiteit gebruikt in een meer globale of dispositionele betekenis en in een

meer locale of handelingsgebonden betekenis. In de eerstgenoemde betekenis wordt de betrokken overheid en haar handelen als geheel gekwalificeerd. In de laatstgenoemde betekenis gaat het om specifieke (typen of clusters van) handelingen. Zo kan een overheid over het geheel genomen wel legitiem zijn, maar incidenteel een *faux pas* maken uit een oogpunt van legitimiteit.

Empirische opvattingen
Vaak word een onderscheid gemaakt tussen empirische of descriptieve benaderingen en normatieve benaderingen van legitimiteit (Steffek, 2003; Bader, 1989). Normatieve benaderingen houden *idealen* voor (Held, 1999; Buchanan, 2004); empirische benaderingen draaien rond de *feitelijke* motieven en oorzaken van de perceptie van burgers van overheden als zijnde legitiem (Hurd, 1999; Franck, 1988; 1995; Bodansky, 1999; Hurrell, 2002; Clark, 2003).

Empirische benaderingen zijn meestal geïnspireerd door de Duitse socioloog Max Weber (1864-1920). Weber benadrukte het belang van het feitelijk geloof in legitimiteit als noodzakelijk element voor de legitimiteit van een overheid – overigens in aanvulling op gewoonte, maatschappelijk en persoonlijk voordeel en ideële motieven (Weber 1978, 213). Hedendaagse voorstanders van een empirische opvatting neigen er meestal toe om legitimiteit te beperken tot het criterium van juist geacht worden door een relevante referentiegroep. De tegenstelling normatief – empirisch is enigszins misleidend. In zowel normatieve als empirische benaderingen wordt legitimiteit gedefinieerd als een criterium of een verzameling criteria waaraan een overheid of een bestuursstructuur bij voorkeur moet voldoen. In zekere zin zijn beide benaderingen dus normatief. Desalniettemin gaat er een belangrijk verschil schuil achter de empirische en normatieve benadering.

Het verschil is dat de voorstanders van een empirische visie op zich niet geïnteresseerd zijn in het naar voren brengen van morele of andere normatieve criteria voor de acceptatie van een overheid. Hun eerste interesse ligt bij de psychologische, sociologische en politieke factoren en mechanismen die de perceptie van legitimiteit teweeg brengen. De morele of bijvoorbeeld juridische kwaliteit van die factoren en mechanismen is niet hun eerste zorg. Zij kunnen deze zien als middelen om acceptatie te veroorzaken. Maar dat hoeft niet per se. Evenmin zullen zij van mening zijn dat morele of juridische criteria altijd de boventoon moeten voeren bij de beoordeling van legitimiteit. In zekere zin zijn voorstanders van de empirische benadering vooral geïnteresseerd in legitimiteit als praktisch fenomeen en om redenen van politieke doelmatigheid en effectiviteit. Wat dit betreft gaapt er een diepe kloof tussen de voorstanders van de empirische visie en die van de normatieve benadering. De laatsten zijn voornamelijk geïnteresseerd in acceptatie door de burgers voor zover deze voldoen aan morele en juridische maatstaven.

Normatieve opvattingen: drie dimensies
De voorstanders van een normatieve benadering van legitimiteit zijn niet in de eerste plaats geïnteresseerd in de technische en empirische factoren die acceptatie van machtsuitoefening door overheden mogelijk maken. Veeleer zoeken zij een antwoord op de vraag: met welk recht oefent de overheid die macht uit? Tegen deze achtergrond is legitimiteit een diep gewortelde normatieve notie die doorgaans geassocieerd wordt met morele rechtvaardiging, legaliteit en representativiteit. Vaak

wordt één van deze dimensies verheven tot het definiërend element van (normatieve) legitimiteit: morele rechtvaardiging, overeenstemming met regels en procedurevoorschriften, of representativiteit voor de groep van mensen over wie of voor wie macht wordt uitgeoefend. Soms worden deze criteria door elkaar gehusseld – bijvoorbeeld door auteurs die – goed bedoeld – morele en juridische criteria vereenzelvigen. Tenslotte zijn er auteurs die bewust een multidimensioneel begrip van legitimiteit voorstaan in termen van morele, juridische en sociologische criteria (Beetham, 1991).

De twee laatstgenoemde dimensies, c.q. typen van criteria, hebben een primair procedureel karakter. Ze verwijzen niet *in directe zin* naar de mate waarin een overheid zich gedraagt in overeenstemming met waarden en idealen, zoals bijvoorbeeld menselijke waardigheid, persoonlijke autonomie, privacy, veiligheid enz. Zij verwijzen primair naar regels met formeel of informeel erkende status of naar enige vorm van instemming van of ondersteuning door de betrokken mensen.
De moreel normatieve dimensie bevat primair substantiële criteria en vereist dat het overheidshandelen kan worden gerechtvaardigd in termen van waarden en normen met een specifieke inhoud. Belangrijk is echter dat deze dimensie niet is beperkt tot substantiële criteria. Ze bevat eveneens criteria die eerder lijken te corresponderen met open, procedurele waarden en normen. Hierbij is bijvoorbeeld te denken aan een waarde als verantwoordelijkheid (zie onder). Ook kunnen de criteria in de morele dimensie procedurele criteria uit de overige dimensies veronderstellen of impliceren. Dat komt doordat voldoen aan de criteria in de sociale en juridische dimensie instrumenteel kan zijn voor het voldoen aan de criteria in de morele dimensie. Let wel: het gaat hier om een kunstmatig onderscheid. Overeenstemming met een wettelijke norm betreffende privacy, bijvoorbeeld, wordt uit een oogpunt van legitimiteit gescoord op de juridische dimensie waar het de overeenstemming met wettelijke voorschriften betreft. Voor wat betreft de inhoudelijke bescherming van de privacy wordt zij op de morele dimensie gescoord.

Belangrijk is nog, tot slot, om op te merken dat het bij een multidimensioneel begrip met meerdere en grondig verschillende criteria per dimensie zinvol is om te spreken van graden van legitimiteit, c. q. van meer of minder legitiem. Niet alleen kan een overheid of een overheidshandelen verschillend scoren op verschillende dimensies en verschillende criteria binnen die dimensies; de criteria kunnen gezien hun verschillend aard ook nog eens verschillend worden meegewogen in de kwalificatie.

Verantwoordelijkheid
Verantwoordelijkheid heeft een overheersend retrospectieve betekenis. Het staat voor de plicht of de bereidheid om verantwoording af te leggen: uitleg, verklaring of motivatie voor het eigen handelen of beleid. De rechtsfilosoof Hart (1968) legt uit dat verantwoordelijkheid daarnaast ook vaak in bijkomende betekenissen gebruikt wordt. Zo kent de term een prospectieve betekenis, als equivalent van plicht of taak. Ook een betekenis die dicht in de buurt komt van het begrip deugd is tamelijk courant. Verantwoordelijkheid als deugd is een stabiele karaktertrek of dispositie om vlot de morele aspecten van situaties te onderkennen en morele problemen adequaat tegemoet te treden. In deze laatste betekenis komt verantwoordelijkheid dicht in de buurt van morele sensitiviteit (Vedder, 2008). De begrippen van verantwoordelijkheid in de zin van bereidheid om verantwoording af te leggen en in de zin van morele sensitiviteit kunnen deel uitmaken van de morele dimensie van legitimiteit. Legitimiteit is echter meer dan verantwoordelijkheid.

E-dienstverlening en privacy
Voor het doel van dit rapport lijkt een multi-dimensionele benadering van legitimiteit het meest geschikt. Daarbij lijkt de morele dimensie in dit geval het meeste aandacht te vragen. In de politiek theoretische literatuur worden de juridische en sociale dimensie meestal in termen van respectievelijk staatsrechtelijkheid en democratietheorie bediscussieerd. Dat lijkt bij de hoofdkwestie van dit rapport minder urgent. We hebben het immers over elektronische dienstverlening door overheden binnen een staatsrechtelijk en democratisch bestel.

Waar het de legitimiteit betreft van Nederlandse overheden specifiek bij het aanbieden van elektronische diensten wordt de sociale dimensie in paragraaf 5.4 verder besproken onder de noemers “vertrouwen” en “acceptatie”. Aannemend dat de e–dienstverlening van overheden in Nederland zich binnen de door de wet gestelde perken begeeft lijkt ook de juridische dimensie weinig aandacht te hoeven krijgen. Elke beweging in de richting van betere privacybescherming van de burger kan zelfs als een extra legitimerende factor in de juridische dimensie worden beschouwd.

Tenslotte moet worden opgemerkt dat er geen empirisch bronnenmateriaal beschikbaar is waartegen mogelijke criteria voor de legitimiteit van overheden bij elektronische dienstverlening kan worden afgezet. In de volgende paragraaf zal blijken dat dit bij burgervertrouwen en –acceptatie van e-dienstverlening heel anders ligt.

5.4 Vertrouwen en acceptatie

Vertrouwen kan betrekking hebben op personen en organisaties enerzijds en dingen anderzijds. Bij de dingen kan men denken aan werktuigen en apparaten, maar ook aan data en informatie. Bij dingen is vertrouwen het geloof of de overtuiging dat zij de verwachtingen ten aanzien van het gebruik door de vertrouwende persoon zullen waarmaken. Bij werktuigen en gebruiksvoorwerpen is het vertrouwen sterk verbonden met hun betrekkelijk gemakkelijk vaststelbare functie. Bij gecompliceerde zaken als data en informatie zijn criteria voor betrouwbaarheid moeilijker vast te stellen maar desalniettemin specificeerbaar (Vedder, Wachbroit, 2003).

Bij personen en organisaties is vertrouwen het geloof of de overtuiging dat een persoon of organisatie met wie of waarmee direct of indirect enige vorm van interactie zal worden aangegaan zal waarmaken wat ervan of wat van hem verwacht wordt of wat hij beloofd heeft. In de sociale wetenschappen en de economische theorie bestaat de neiging om vertrouwen vooral te bestuderen als een dimensie van menselijk gedrag die helpt bij het mogelijk maken en bestendigen van maatschappelijke verbanden en samenwerking tussen mensen (Buskens, 1998; Doney e.a., 1998; James, 2002; Kipnis, 1996; Sztompka, 1999).

Vaak wordt het verband tussen vertrouwen enerzijds en onzekerheid en risico’s anderzijds gethematiseerd (Lewis, Weigert 1985; Kee, Knox, 1970). Dit komt uit in een tweespalt van positieve en negatieve benaderingen van vertrouwen. Sommigen definiëren vertrouwen vanuit een praktische invalshoek als een positieve verwachting ten aanzien van het gedrag van personen met wie moet worden

samengewerkt (Barber, 1983; Koller, 1988; Luhmann, 1979; Rotter, 1967). Anderen definiëren vertrouwen vanuit een beschouwend perspectief eerder in termen van de bereidheid om zich kwetsbaar op te stellen voor de mogelijkheid dat anderen niet aan verwachtingen voldoen (Doney, Cannon, & Mullen, 1998; Mayer, Davis, & Schoorman, 1995; Rosseau et al., 1998).

Bij de determinanten van vertrouwen moet worden gedacht aan factoren in de te vertrouwen persoon of organisatie of het te vertrouwen ding en aan factoren in degene die vertrouwt. Bij de factoren in de te vertrouwen persoon of entiteit moet in de eerste plaats gedacht worden aan *reputatie*. Hierbij gaat het om de goede naam en status die een persoon of de entiteit van oudsher heeft op basis van traditie of conventie of die is opgebouwd in korte of langere tijd door stabiele goede werking. Daarnaast kan het ook gaan om reputaties op grond van bijkomende eigenschappen zoals veiligheid, netheid enz. Vaak heeft de reputatie in beiderlei zin betrekking op de typische of specifieke functie of taak van de desbetreffende persoon of entiteit. De associatie met de hierboven besproken legitimiteit ligt voor de hand. Bij de overheid lijkt legitimiteit een minimale voorwaarde voor status en reputatie.

Bij de vertrouwende persoon gaat het om de *ervaring* met de te vertrouwen persoon of entiteit (Sztompka, 1999). Hierbij kan het gaan om eigen kennis van de goede naam en status en/of kennis van de relevante historie van de te vertrouwen persoon of entiteit. Daarnaast is volgens sommigen een algemene geneigdheid om te vertrouwen relevant. Sommige personen zouden meer genegen zijn tot vertrouwen dan anderen (Mayer, Davis, & Schoorman, 1995; Das & Teng, 2004; Gefen, 2000; Teo, Liu, 2007).

Vertrouwen kan echter ook worden vermeerderd of verminderd of helemaal teniet gedaan door *factoren buiten de te vertrouwen persoon of entiteit* en de vertrouwende persoon. Hierbij is bijvoorbeeld te denken aan de goede resultaten die van de interactie tussen de te vertrouwen persoon of entiteit en de vertrouwende persoon verwacht worden (Laufer, Wolfe, 1977). Maar ook de aan- of afwezigheid van formele of informele *reguleringsarrangementen* zoals recht en branchecodes speelt een grote rol.

E-dienstverlening en vertrouwen

Het vertrouwen van de gebruiker is essentieel voor het aangaan van commerciële transacties via internet (Buttner & Goritz, 2008; Everard & Galleta, 2005; Gefen, 2000; McKnight, Choudhury, Kacmar, 2002). Ook voor de acceptatie van elektronische dienstverlening door de overheid is vertrouwen van onmisbaar belang (Belanger, Carter, 2008; Carter, Belanger, 2005; Colesca, Dobrica, 2008; Lean et al., 2009).

In de context van online dienstverlening kan een onderscheid worden gemaakt tussen factoren in de te vertrouwen persoon of organisatie die een online dienst aanbiedt enerzijds, factoren in de vertrouwende gebruiker anderzijds en externe factoren. Daar komen in de online context echter nog factoren van de bemiddelende technologie bij, waaronder veiligheid en gebruiksgemak.

Allereerst is van belang de algemene reputatie van de aanbieder. Volgens verscheidene auteurs over commerciële transacties op het internet is algemene reputatie vooral van belang voor gebruikers die zelf nog geen ervaring hebben opgedaan met de aanbieder (Chen, 2006; Kim, Ferrin, & Rao, 2003; Koufaris & Hampton-Sosa, 2004; McKnight et al., 2002). Zoals hierboven al opgemerkt lijkt bij de overheid legitimiteit een minimale conditie voor reputatie en status. Ten tweede lijkt het gebruiksgemak van een website of applicatie het vertrouwen bij de gebruiker te vergroten (Bart et al., 2005). Dit lijkt wederom vooral het geval bij nieuwe gebruikers die nog geen ervaring hebben opgedaan met de aanbieder (Chau, Hu, Lee, Au, 2007). Onoverzichtelijkheid en ingewikkelde navigatie lijkt de gebruiker onzeker te maken en angstig voor technische fouten (Flavian et al., 2006).

Wat de gebruiker betreft lijkt vooral algemene ervaring met het internet van belang voor het vertrouwen in een aanbieder. De onderzoekers zijn het er echter niet over eens of de invloed van internetervaring positief is (Corbitt, Thanasankit, & Yi, 2003), of juist negatief (Aiken & Bousch, 2006; Jarvenpaa, Tractinsky, & Saarinen, 1999). Hetzelfde beeld geeft ook de factor van geneigdheid tot vertrouwen in de gebruiker. Sommige onderzoeken laten zien dat dit het vertrouwen in online aanbieders vergroot (Gefen, 2000; Teo & Liu, 2007). Anderen betwijfelen dit (Koufaris, Hampton-Sosa, 2004). Ook is aangetoond dat positieve ervaringen bijdragen tot groter vertrouwen in de desbetreffende aanbieder (Pavlou, 2003; Casalo et al., 2007; Flavian et al., 2006; Yoon, 2002).

Naast vertrouwen kunnen de voordelen van een elektronische dienst of transactie er natuurlijk ook simpelweg toe bijdragen dat gebruikers een dienst of transactie accepteren. Naast besparingen in tijd en energie (geen fysieke verplaatsing nodig) lijken in het geval van elektronische overheidsdiensten ook behulpzaamheid en overzichtsverbetering van complexe taken bij te dragen tot acceptatie (Lee, Rao, 2009).

Privacy

Het verband tussen het nemen van privacybeschermende maatregelen door aanbieders en het vertrouwen van gebruikers is nog niet intensief onderzocht. Dat bezorgdheid over de eigen privacy een rol speelt bij het vertrouwen van de gebruiker is een aanname die nog maar met weinig empirisch onderzoek onderbouwd is (Hoffman e.a., 1999; Al-Awadhi, Morris, 2009). Volgens sommige onderzoekers wordt de bezorgdheid veroorzaakt door een gebrek aan inzicht in de manier waarop de betrokken aanbieders omgaan met de persoonsgegevens (Reagle, Cranor, 1997). Anderen menen dat de bezorgdheid te maken heeft met het onvermogen om te verhinderen dat andere organisaties zich toegang verschaffen tot de eigen gegevens (Hoffman, Novak, peralta, 1999). Weer anderen zien als belangrijkste oorzaak de angst van de gebruiker dat zijn gegevens wel eens voor heel andere doelen gebruikt kunnen worden dan die waarvoor hij ze afstaat (Culnan, Armstrong, 1999)

De aanwezigheid van privacy-verklaringen op een site lijkt het vertrouwen van gebruikers te vergroten (Lauer & Deng, 2007; Meinert et al., 2004; Pan & Zinkhan, 2006), hoewel dergelijke verklaringen nauwelijks worden gelezen (Arcand et al., 2007; Jensen et al., 2005; Meinert et al., 2004). Aanwijzingen dat de aanbieder zich extra moeite getroost om met behulp van technologische middelen, zoals PETs en

authenticatieinstrumenten, transacties te beveiligen lijkt het vertrouwen van in elk geval nieuwe gebruikers te vergroten (Koufaris, Hampton-Sosa, 2004). Dergelijke aanwijzingen dragen meer bij tot het vertrouwen dan privacyverklaringen (Belanger, Hiller, & Smith, 2002).

Wanneer gebruikers een aanbieder vertrouwen, lijkt hun bereidheid om (persoonlijke) gegevens aan hem te verschaffen groter te worden (Belanger, Hiller, & Smith; McKnight, Choudhury, & Kacmar, 2002). De bereidheid om (persoonlijke) gegevens prijs te geven kan echter ook toenemen wanneer de gebruiker de voordelen van de transactie belangrijker vindt dan verlies van privacy (Berendt, Gunther, Spiekermann, 2005; Norberg & Dholakia, 2003; Culnan, Bies, 2003; Olivero, Lunt, 2004). In het geval van de overheid als aanbieder gaat het bij die voordelen om tijds- en energiebesparing, doelmatigheid of hulp bij complexe taken. Ook de aanwezigheid van een algemeen reguleringskader inzake privacy en gegevens bescherming lijkt bij te dragen tot de acceptatie van online diensten (Geest en Beldad, 2010; Bellman et al., 2004).

5.5 Samenvatting

De begrippenparen legitimiteit en verantwoordelijkheid en vertrouwen en acceptatie hangen nauw samen. Verantwoordelijkheid van de overheid is een voorwaarde voor haar legitimiteit (in normatieve zin); vertrouwen is een voorwaarde voor acceptatie. Ook hangt legitimiteit (zowel in normatieve als empirische zin) samen met acceptatie. Daar komt bij dat vertrouwen in het geval van e-dienstverlening door de overheid idealiter (mede) gebaseerd is op overheidslegitimiteit in normatieve zin.

Legitimiteit kent empirische en meer normatieve definities. Bij empirische definities draait het om de feitelijke perceptie van legitimiteit. Bij meer normatieve definities gaat het erom of de overheid voldoet aan normatieve criteria. Gezien ons voorwerp van onderzoek gaan we uit van een multidimensionele definitie van normatieve legitimiteit: een definitie in termen van acceptatie of ondersteuning, legaliteit en overeenstemming met inhoudelijke morele criteria. In een multidimensonele definitie van normatieve legitimiteit voeren morele criteria de boventoon. Criteria uit de juridische en sociale dimensie zijn instrumenteel voor het voldoen aan morele criteria. Legaliteit, transparantie en het streven naar instemming en steun van betrokken burgers kunnen bijvoorbeeld worden opgevat als invullingen van de verantwoordelijkheid van de overheid.

Het bestaande onderzoek naar legitimiteit is vooral theoretisch en conceptueel analytisch van aard. Vertrouwen is zowel op meer theoretisch niveau als empirisch onderzocht. Vertrouwen is de aanname dat een persoon of organisatie zich in de toekomst zal gedragen zoals men verwacht, c.q. zoals hij of zij beloofd heeft. Vertrouwen is onmisbaar voor samenwerking en maatschappelijke projecten.

Vertrouwen is gebaseerd op factoren in de te vertrouwen instantie en op factoren in de vertrouwende persoon. Wat het eerste betreft is de reputatie van de instantie relevant. Bij e-dienstverlening aan nieuwe cliënten blijkt reputatie erg belangrijk. Als de overheid de dienstverlener is, lijkt legitimiteit een minimale voorwaarde voor haar reputatie. In het empirisch onderzoek in het volgende hoofdstuk verwijzen sommige deelnemers hier naar door aan te geven dat ze online overheidsdiensten

vertrouwen omdat de overheid gebonden is aan strikte wetgeving. Gebruiksgemak en overzichtelijkheid lijken voor iedereen – dus niet alleen beginnelingen – een belangrijke rol te spelen, net als indicaties over de beveiliging van een site of transacties. In het volgende hoofdstuk zullen we bijvoorbeeld zien dat sommige deelnemers aan het empirisch onderzoek het gebruik van DigiD ervaren als extra beveiliging van hun gegevens waardoor ze meer vertrouwen krijgen in de online dienstverlening van de overheid. Veiligheidsindicaties lijken weer belangrijker voor het vertrouwen dan bijvoorbeeld privacyverklaringen. Deze laatste spelen wel een rol, maar dus niet zo'n grote. Bovendien worden ze zelden gelezen. Uit het empirisch onderzoek blijkt daarnaast dat herhaaldelijke meldingen over privacy- of beveiligingsincidenten van een bepaalde online dienst, het vertrouwen dan ook kan verminderen en zelf kan leiden tot het verlaten van de dienst.

De vertrouwende persoon vertrouwt meer als hij positieve ervaringen met een bepaalde dienstverlener en diens dienstverlening heeft. Zijn vertrouwen wordt niet per se groter naarmate hij meer ervaring met het internet in het algemeen heeft. Zijn geneigdheid om anderen te vertrouwen in het algemeen lijkt ook geen eenduidige garantie op te leveren dat hij dienstverleners eerder of meer vertrouwt.

Buiten de factoren in de te vertrouwen instantie en de vertrouwende persoon blijken nog andere elementen van belang voor de acceptatie van (elektronische) dienstverlening. In de eerste plaats gaat het daarbij om de voordelen die de dienstverlening oplevert – bijvoorbeeld besparing van tijd en energie en de vereenvoudiging van complexe taken. Ook de aanwezigheid van een wettelijk kader kan bijdragen tot acceptatie. Zo lijkt aanwezigheid van wettelijke regelingen rond privacy en gegevensbescherming de risicoperceptie rond het afstaan van persoonlijke gegevens ten behoeve van de dienstverlening te verkleinen en daardoor de acceptatiegraad te verhogen.

6 Empirisch onderzoek

6.1 Inleiding

Dit hoofdstuk geeft verslag van het verrichte empirisch onderzoek. De centrale vragen voor het empirisch onderzoek zijn:

- Hoe percipiëren burgers en de overheid de relaties tussen privacybescherming, vertrouwen en acceptatie enerzijds en doelmatigheid, effectiviteit anderzijds?
- Hoe beschouwen burgers de inzet van Privacy by Design met het oog op de acceptatie van de toepassing hiervan en het vertrouwen in de overheid?

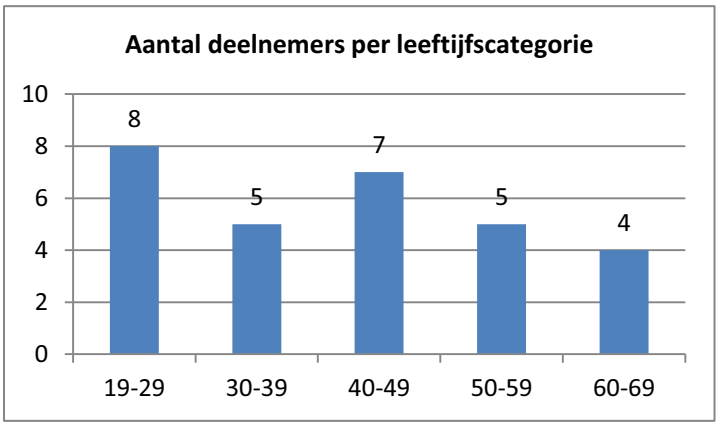
6.2 Methode

Het empirisch materiaal is verzameld via focusgroepen.[42] Deze wijze van gegevensverzameling is een kwalitatieve vorm van onderzoek en geeft inzicht in de diversiteit van kennis, meningen, redeneringen en attitudes van personen ten opzichte van bepaalde fenomenen om deze beter te doorgronden. Een focusgroep bestaat uit vijf tot twaalf mensen die bepaalde eigenschappen gemeen hebben. Dit kan heel breed zijn (zoals personen die het Nederlands burgerschap hebben) tot heel specifiek ('personen die gebruik maken van product X'). De resultaten van de focusgroep worden vergeleken met tenminste twee andere focusgroepen en begeleid door een moderator, luisteraar en observant (in dit onderzoek door één moderator en door één luisteraar/observant). De vragen zijn van te voren vastgesteld in een logische en begrijpelijke volgorde voor de deelnemers. Er worden alleen open vragen gesteld. De focusgroepen beginnen met een introductie in het onderwerp, de vragen zijn voornamelijk bedoeld om de deelnemers op hun gemak te stellen en een open sfeer te creëren. Naarmate de focusgroep vordert, worden de vragen meer specifiek over het onderwerp Privacy by Design. Het gaat bij focusgroepen niet om het bereiken van consensus, maar om het boven tafel krijgen van meningen, gedachten, redeneringen, gevoelens, gedragingen en dergelijke.

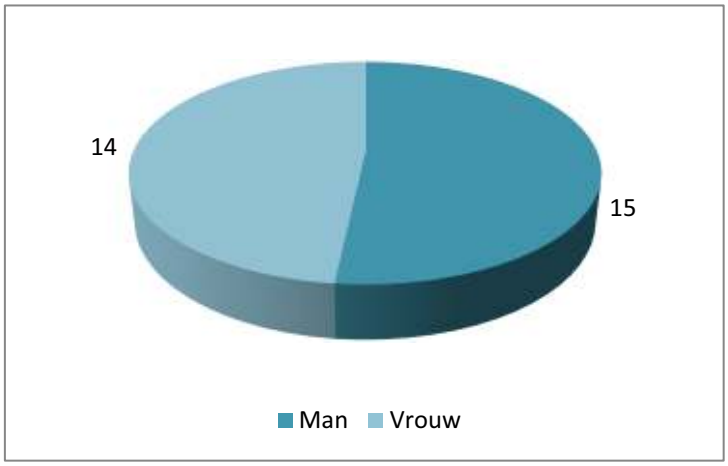
In dit onderzoek is voor deze methode gekozen, omdat er nog relatief weinig bekend is over het concept Privacy by Design, zeker waar het gaat om de perceptie van burgers hiervan, als ook over de relatie tussen privacybescherming, vertrouwen en acceptatie en effectiviteit. Dit maakt het uitvoeren van kwantitatief onderzoek, bijvoorbeeld middels een grootschalige survey, zeer moeilijk. Focusgroepen zijn kwalitatief van aard lenen zich daarom goed voor het verkennen van verschillende afwegingen, redeneringen en motivaties van burgers hierover te verkennen. Het nadeel van focusgroepen als onderzoeksmethode is dat de onderzoeksresultaten niet representatief zijn voor de hele populatie (de Nederlandse bevolking in dit geval). De resultaten dienen gevalideerd te worden middels een representatieve steekproef.

[42] Daarnaast lag het in de bedoeling een expert-seminar te organiseren, waarin experts uit de kring van overheid en wetenschap de preferenties van de focusgroepen krijgen voorgelegd. Dit seminar is opgezet en aangekondigd, maar is vanwege beperkte aanmeldingen vervangen door vier individuele diepte-interviews met experts, met als doel het concept afwegingskader (zie hoofdstuk 7) te toetsen.

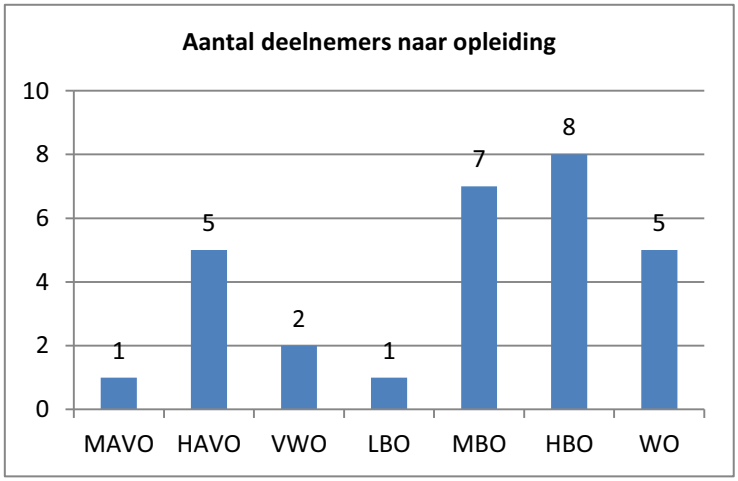
Voor dit onderzoek zijn drie heterogene focusgroepen georganiseerd met een doorsnee van de Nederlandse bevolking als deelnemers. Binnen de focusgroepen is gestreefd naar een zo goed mogelijke verdeling van leeftijd, opleiding, geslacht en activiteiten op internet. In totaal zijn 30 personen met behulp van een respondentenbureau uitgenodigd om deel te nemen aan het onderzoek, waarvan één zich heeft afgemeld. Het onderzoek is uitgevoerd met 29 deelnemers, met gemiddeld 10 deelnemers per groep. De focusgroepen vonden 's avonds plaats om de heterogeniteit en beschikbaarheid van de deelnemers te bevorderen. Figuren 3, 4 en 5 tonen het overzicht van het aantal deelnemers en de verdeling over leeftijd, geslacht en opleiding. De focusgroepsdiscussies zijn aangevuld met individuele vragenlijsten om zo ook per deelnemer inzicht te krijgen in zijn/haar mening en attitude.



Figuur 3 Aantal deelnemers en verdeling naar leeftijd



Figuur 4 Aantal deelnemers en verdeling naar geslacht



Figuur 5: Aantal deelnemers en verdeling naar opleiding

De resultaten zijn systematisch geanalyseerd door een analyse per groep te maken en vervolgens deze onderling te vergelijken. De resultaten tonen sterke overeenkomsten voor alle drie de groepen. De resultaten geven een beeld van mogelijke redeneringen, meningen en houding van Nederlandse burgers ten opzichte van de toepassing van Privacy by Design. Nader vervolgonderzoek is nodig om de gevonden resultaten op een kwantitatief niveau onder een representatieve groep Nederlanders te valideren. Het is op basis van dit onderzoek niet mogelijk om definitieve antwoorden te geven over de relatie tussen Privacy by Design en vertrouwen.

Het programma van de focusgroepen is ontworpen om de in de inleiding genoemde vragen te beantwoorden. Tabel 2 toont de verschillende onderdelen van het programma. Deze worden hieronder toegelicht. In Bijlage 1 is het gedetailleerde programma van de focusgroep te vinden. In Bijlage 2 zijn de gebruikte vignetten en vragenlijsten te vinden. De focusgroepen zijn met toestemming van de deelnemers opgenomen (audio) en uitgewerkt tot de onderstaande analyse (paragraaf 6.3).

Centraal in de focusgroepen staat de perceptie van burgers van Privacy by Design, en meer specifiek de verschillende elementen van Privacy by Design en de relaties tussen privacy, vertrouwen en legitimiteit van overheidsdienstverlening. De verschillende elementen van PbD zijn omschreven in hoofdstuk 4. De concepten privacy, vertrouwen, acceptatie en legitimiteit en mogelijke onderlinge relaties zijn omschreven in hoofdstuk 5. Per focusgroep worden zeven onderdelen besproken die betrekking hebben op de toepassing van PbD:

1. *Vertrouwen in online en acceptatie van online (overheids-)dienstverlening*: Het eerste onderwerp gaat over vertrouwen in online (overheids-)dienstverlening en gebruik van online overheidsdienstverlening. Waarom maakt men wel of niet gebruik van online overheidsdiensten? Welke overwegingen spelen hierbij een rol (denk aan tijdwinst, gemak, maar mogelijk ook privacy-overwegingen)? Er wordt een vergelijking gemaakt tussen vertrouwen in publieke of overheidsdienstverlening en commerciële dienstverlening om te onderzoeken of er verschillen optreden en wat de achterliggende redenen zijn.

2. *Gepercipieerde veiligheid van online (overheids-)dienstverlening*: Kennen burgers bepaalde risico's toe aan online dienstverlening en waarom wel of niet? Welke risico's zijn dat? Ook hier wordt een vergelijking gemaakt tussen overheidsdienstverlening en commerciële dienstverlening.
3. *Privacy by Design*: In het derde onderdeel wordt Privacy by Design in zijn geheel met de deelnemers besproken; de volgende onderdelen bespreken elk PbD element apart. De deelnemers krijgen twee voorbeelden voorgelegd, in voorbeeld 1 is PbD niet toegepast, in voorbeeld 2 zijn alle drie de elementen van PbD toegepast (een privacy impact assessment, organisatorische elementen en privacybeschermende technologie). Een van de weinige bestaande voorbeelden van PbD waarin al deze elementen worden toegepast, is het voorbeeld van de security scanner (Cavoukian, 2009; zie voor een volledige beschrijving paragraaf 4.3) die op verscheidene internationale luchthavens wordt toegepast. Daarom wordt de security scanner hier als voorbeeld gebruikt.
4. *Privacy Impact Assessment*: Met een PIA wordt van te voren een inschatting gemaakt van de privacyrisico's van het te ontwerpen informatiesysteem (risicoanalyse) en hoe deze te verkleinen of te vermijden. Het is echter onbekend welke effect PIAs hebben op het vertrouwen in, en acceptatie van, dienstverlening door burgers. Hoe percipiëren burgers de uitvoering van een uitgevoerde PIA? Doet een PIA het vertrouwen in de dienstverlening en instantie toenemen? Of leidt communicatie over mogelijke risico's tot afnemend vertrouwen?
5. *Privacy by Design in de organisatie*: Om de legitimiteit van het informatiesysteem te verzekeren, zal aandacht moeten worden besteed aan de inbedding van het systeem in de organisatie die er gebruik van maakt. Voor PbD is het van belang dat de organisatie uitvoering geeft aan de wettelijke eisen die worden gesteld aan de bescherming van de privacy: welke verplichtingen heeft de beheerder van het informatiesysteem (in ons onderzoek: dienstverlenende instantie) en hoe is deze aanspreekbaar? De aanwezigheid van een wettelijk kader kan bijdragen tot acceptatie van elektronische dienstverlening door de overheid. Zo kan de aanwezigheid van wettelijke regelingen rond privacy en gegevensbescherming de risicoperceptie van het afstaan van persoonlijke gegevens ten behoeve van de dienstverlening verkleinen en daardoor de acceptatiegraad verhogen. In dit onderdeel wordt gekeken welk effect de wettelijke verplichtingen hebben op vertrouwen in en acceptatie van online dienstverlening. Omdat de Europese wetgeving op het punt staat te worden geactualiseerd (2011), zal bovendien rekening worden gehouden met deze toekomstige wetgeving. Samengevat vereist deze wetgeving explicitering van de verantwoordelijkheden voor de verwerking van persoonsgegevens en vereist ze een deugdelijk beveiligingsregie voor de opslag en verwerking van de betrokken gegevens. Voor burgers is dus met name van belang dat duidelijk is wie zij kunnen aanspreken en waarvoor.
6. *Privacybevorderende technologieën*: een ander element van PbD is het gebruik van privacybeschermende technologie, ofwel Privacy Enhancing Technologies (PETs). Dit zijn technologieën en maatregelen die zich richten op het elimineren of minimaliseren van de hoeveelheid gegevens die verzameld en opgeslagen worden over een individu (dataminimalisatie), het voorkomen van strijdigheid met privacyprincipes en het inzetten van controle-instrumenten voor gebruikers

over informatie die over henzelf verzameld en gebruikt wordt. Het gebruik van PETs is echter vaak 'onzichtbaar' voor burgers. Het is niet bekend hoe burgers deze technologie percipiëren en welk effect toepassing ervan heeft op het vertrouwen van burgers in de dienstverlening en dienstverlenende instantie en de acceptatie daarvan.

7. *Specifieke toepassingen van privacytechnologie*: hier worden verschillende voorbeelden van PET-toepassingen besproken, waaronder het gebruik van anonieme credentials op (identiteits)smart cards.

Tabel 2 Overzicht programma focusgroepen

Onderdeel	Tijd	Duur	Methode
0. Kennismaking (opening)	19.00-19.10	10 min	Voorstelronde
1. Gebruik, vertrouwen en acceptatie online overheidsdiensten	19.10-19.25	5 min 10 min	- Stellingformulier - Groepsdiscussie
2. Risico's van online diensten	19.25-19.40	5 min 10 min	- Stellingformulier - Groepsdiscussie
3. Privacy by Design	19.40-20.00	10 min 10 min	- Uitleg + voorbeeld - Groepsdiscussie
4. Privacy risicobeoordelingen (PIA)	20.00-20.15	5 min 10 min	- Vignetten - Groepsdiscussie
5. Verantwoordelijkheden bij dienstaanbieders (organisatie, proces, transparantie)	20.15-20.30	5 min 10 min	- Stellingformulier - Groepsdiscussie
6. Privacytechnologieën (PETs)	20.30-20.45	5 min 10 min	- Uitleg + voorbeeld - Groepsdiscussie
7. Specifieke toepassingen privacytechnologie	20.45-21.00	5 min 10 min	- Uitleg + voorbeeld - Groepsdiscussie
Totaal		120 minuten	

6.3 Analyse resultaten focusgroepen

6.3.1 Gebruik en vertrouwen in online diensten

De deelnemers zijn bekend met verschillende online overheidsdiensten. Zij hebben de meeste ervaring met de online diensten van de Belastingdienst (zoals het digitaal invullen en aanleveren van de Belastingaangifte). Weinig deelnemers (vijf van de 29) hebben in het afgelopen jaar tenminste 1 keer gebruikt gemaakt van de (online) diensten van het Kadaster. Dit geldt ook voor het UWV, waar negentien deelnemers aangeven geen ervaring te hebben met de online diensten van deze instantie. De meeste deelnemers ervaren online overheidsdiensten als snel en gemakkelijk en maken daarom ook gebruik van de diensten. Een enkele deelnemer geeft aan persoonlijk contact zeer op prijs te stellen en maakt daarom geen gebruik van de diensten. Privacyoverwegingen lijken geen rol te spelen bij de beslissing om wel of niet een online overheidsdienst te gaan gebruiken, gemak en snelheid zijn belangrijkere factoren. Een deelnemer merkt het volgende op: '*online of offline maakt toch niet uit, er is toch één grote achterliggende database?*' Overheden zien het offline aanbieden en online aanbieden van haar diensten vaak als twee aparte alternatieven. Deze opmerking maakt duidelijk dat burgers dit, als het gaat om vertrouwen, mogelijk anders zien. De achterliggende infrastructuur (database) bestaat in zowel de offline als de online variant.

Deelnemers geven aan veel vertrouwen te hebben in internetbankieren, de Belastingdienst en online overheidsdiensten in het algemeen. Als redenen geven deelnemers op dat zij er vanuit gaan dat de overheid zorgvuldig met persoonlijke gegevens van burgers omgaat. Tijdens de discussie brengen de deelnemers DigiD ter sprake. Het gebruik van DigiD ervaren sommige deelnemers als een extra beveiliging van hun gegevens waardoor ze meer vertrouwen krijgen in de online dienstverlening van de overheid. Sommige deelnemers vertrouwen de overheid juist minder dan bedrijven. Zij geven aan dat bedrijven een commercieel belang hebben om klanten te behouden en daardoor extra gemotiveerd (ten opzichte van de overheid) zijn om zorgvuldig om te gaan met persoonlijke gegevens van klanten. Sommige deelnemers betwijfelen of de overheid voldoende expertise in huis heeft om gegevens goed te beveiligen.

'Bedrijven moeten wel [data goed beschermen, red], als ze een slechte reputatie krijgen dan hebben ze geen klanten meer.'

Een andere deelnemer geeft aan dat er negatieve berichten in het nieuws zijn geweest over de overheid en gegevens van burgers die 'op straat zijn komen liggen', USB-sticks die zijn verloren e.d. Dat heeft hun vertrouwen aangetast. Dit geldt ook voor bedrijven. Sommige deelnemers geven aan dat hun vertrouwen in internetbankieren wordt aangetast door de berichtgeving van banken zelf over verstuurde *phishing* e-mails en de herhaalde waarschuwingen op de website van de bank of via persoonlijke e-mails over veilig internetbankieren (bijvoorbeeld het niet afgeven van TAN-codes). Dit is een interessant gegeven als het gaat om het vergroten van transparantie naar burgers over mogelijke risico's en privacy-incidenten – een belangrijk onderdeel van Privacy by Design. Het is dus mogelijk dat meer transparantie leidt tot een lager vertrouwen van burgers in de dienst en zelfs het niet meer gebruiken van de dienst.

Slechts weinig deelnemers hebben vertrouwen in sociale media. Als reden geven zij op dat deze diensten hun gegevens mogelijk voor commerciële doeleinden gebruiken, de diensten zijn negatief in het nieuws geweest en dat de gegevens mogelijk gemakkelijk te 'kraken' zijn. Dit wil niet zeggen dat ze de dienst ook niet gebruiken. Sommige deelnemers denken dat er voor de overheid strengere regelgeving bestaat dan voor commerciële bedrijven zoals Facebook of Hyves (zie citaat onder). Dit neemt niet weg dat ze sociale media wel gebruiken. Sommige deelnemers geven hiervoor als verklaring dat ze het voordeel dat sociale media opleveren wel waarderen en dat ze oppassen met wat zij op hun profielpagina plaatsen. Een enkele deelnemer merkt op dat 'ze niks te verbergen heeft' en de diensten daarom toch gebruikt.

'Ik weet dat de Nederlandse wetgeving zo is dat Nederlandse overheidsdiensten nooit heel erg misbruik zullen maken want er is strikte regelgeving. Maar voor Facebook is veel minder strikte regelgeving.'

6.3.2 Risico's van online diensten

Uit de focusgroepen komt geen eenduidig beeld naar voren als het gaat om zorgen om online privacy. Iets minder dan de helft van de deelnemers (dertien) geeft aan zich geen zorgen te maken over hun privacy op internet, tien deelnemers maken zich wel zorgen (zes deelnemers antwoorden neutraal). Vijftien deelnemers geven aan het (helemaal) eens te zijn met de stelling 'mijn gegevens zijn veilig bij de

overheid'. Acht deelnemers zijn het hiermee (helemaal) oneens en zes deelnemers antwoorden neutraal.

Deelnemers geven aan dat recente nieuwsberichten, bijvoorbeeld over de OV-chipkaart en het biometrisch paspoort hun vertrouwen heeft doen afnemen. Een aantal deelnemers geeft aan dat ze eigenlijk niet goed weten of hun gegevens veilig zijn, maar dat ze daar wel vanuit gaan en er ook op vertrouwen dat de overheid dit goed heeft geregeld. Een aantal deelnemers verwijst naar mogelijke politieke ontwikkelingen sinds de aanslagen in de Verenigde Staten '9/11'. Zij hebben nu vertrouwen in de overheid, maar stellen dat dit vertrouwen afhankelijk is van (toekomstige) politieke ontwikkelingen.

'Er komt te vaak in het nieuws dat er weer informatie gelekt is etc'
'[Ik vertrouw de overheid, red] iets minder na de ov-kaart, hackers, het vingerafdrukkenpaspoort en in gegevensopslag. Ze [de systemen, red] vormen toch een risico'
De intenties zijn meestal goed, maar het [wat er uiteindelijk mee gebeurt, red] is afhankelijk van politieke ontwikkelingen. Bovendien kan in de toekomst een nieuwe wet alles onderuit halen in naam van algemene veiligheid'

De deelnemers zijn bekend met verschillende risico's van internet, zoals de mogelijkheid van virussen, diefstal van gegevens door hackers, opgegeven gegevens kunnen gebruikt worden voor andere doelen en gegevens kunnen worden doorverkocht aan derde partijen. Sommige deelnemers wijzen op risico's van sociale netwerksites, het niet of moeilijk kunnen verwijderen van online informatie, de lange bewaartermijn van gegevens in databases en de groeiende hoeveelheid databases.

'Ik houd niet van enquêtes invullen, zodra je iets invult ben je de klos, dan krijg je allemaal aanbiedingen daarvan.'
'Wat ik vooral van databanken een potentieel gevaar vind, ik vertrouw het nu wel, maar ik weet niet of ik het over tien jaar nog vertrouw. Ik weet gewoon niet hoe de wereld dan is.'

Voor sommige deelnemers leidt de kennis over risico's ook tot bepaalde acties. Zo letten de meeste deelnemers op de aanwezigheid van een beveiligde verbinding als ze gebruik maken van online diensten (vooral internetbankieren en webwinkels). Privacyverklaringen worden (zoals ook uit de literatuur bekend) weinig gelezen door de deelnemers. De deelnemers geven aan dit pas te gaan lezen als ze een site of bedrijf niet kennen. De privacyverklaringen worden te lang en te moeilijk bevonden. Deelnemers die privacyverklaringen wel lezen, geven aan dat ze de verklaring voornamelijk scannen en niet zorgvuldig lezen. De bekendheid en reputatie van de aanbieder speelt een belangrijke rol in het vertrouwen in overheidsinstanties en bedrijven. Bij online overheidsdiensten geven deelnemers aan hier minder op te letten omdat ze hier minder vrezen voor (financiële) risico's en omdat ze er op vertrouwen dat de overheid zorgvuldig met hun gegevens omgaat (meer dan bedrijven).

'Ik ga ervan uit dat ze [de overheid, red] er goed mee omgaat, anders kan je helemaal niemand meer vertrouwen en dan wordt het [gebruik maken van online diensten, red] lastig'.

6.3.3 *Privacy by Design*

In dit onderdeel werd de deelnemers twee situaties (zie Bijlage 1) voorgelegd over de inzet van een security scanner op luchthaven (met of zonder toepassing van Privacy by Design). Hoewel de focus in dit onderzoek ligt op online overheidsdienstverlening is de security scanner een van de weinige, duidelijke voorbeelden van Privacy by Design dat al in de praktijk wordt toegepast. In situatie twee is een risicobeoordeling uitgevoerd (een privacy impact assessment) en wordt er gebruik gemaakt van privacybeschermende technologie om niet de volledige 3D-scan van het lichaam te tonen, maar een vast silhouet. Ook is in situatie twee een duidelijk aanwezig aanspreekpunt in het geval van klachten of vraag (een sticker duidelijk zichtbaar op het apparaat). De deelnemers is gevraagd wat hen opvalt, wat ze goed of slecht vinden en wat ze prettig of juist niet prettig vinden.

Figuur 6: Overzicht van voorgelegde situaties: met en zonder PbD

In de discussie benoemen de deelnemers voor- en nadelen van beide situaties. Deze betreffen in eerste instantie alleen het gebruik van wel of geen privacybeschermende technologie. Bij aanvang van de discussie geven de meeste deelnemers de voorkeur aan de privacyvriendelijke scanner. Deze houdt meer rekening houdt met privacy en lichamelijke integriteit van passagiers. In de discussie die volgt gaan sommige deelnemers echter twijfelen aan de effectiviteit van de privacyvriendelijke security scanner. Na afloop van de discussie kiezen de meeste deelnemers daardoor toch voor situatie één.

'Ik vind 1 geen optie. Als je het hebt over integriteit van je lichaam, het enige wat je echt bezit, dan moet je daar heel prudent mee omgaan.'

'Bij de eerste situatie is het iets te specifiek wat betreft het lichaam van de persoon. (…) Daarentegen kan het wel een precieze plek aangeven waar iets verstopt is.'

'Ik ga er vanuit dat het allebei even veilig is. Dat neem ik aan, dan heb ik voorkeur voor 2. Ik vind 1 niet minder veilig, maar minder prettig, ze staan dwars door je kleding heen te kijken.'

'Die jongen die het vliegtuig wilde opblazen, zo iemand zou ik liever door 1 dan door 2 willen laten gaan.'

‘Dat zou er toch bij 2 ook uitgekomen zijn, daar vertrouw ik tenminste op.’

De deelnemers die twijfelen over de effectiviteit van de software in situatie twee wijzen er op dat de software (in plaats van een beveiligingsbeambte, een mens) de analyse maakt; in situatie twee is men afhankelijk van de software. De deelnemers hebben minder vertrouwen in de software dan in de beveiligingsbeambten als het gaat om hoe goed ze in staat zijn verdachte zaken op te sporen. Sommigen wijzen op de mogelijke voordelen van software dat software geen vooroordelen kent. Situatie twee wordt (h)erkend als privacyvriendelijker, maar wordt minder effectief geacht. Deelnemers maken dus een afweging tussen de (verwachte) effectiviteit van de dienst en de verwachte privacybescherming.

‘Bij die eerste kun je precies zien waar het [verdachte zaken, red] is en wat het is. Wat vind je veiliger? Niet je lichaam zien of dat je heel nauwkeurig ziet waar het wapen of iets dergelijks zit. Die tweede houdt rekening met de privacy van de passagier, je ziet niet alle vetrollen. Maar wat is belangrijk? Voor mij, dat je precies kunt detecteren.’

‘Die tweede laat alleen zien wat de computer herkent.’

‘Bij situatie 2 ben je afhankelijk van wat er ingevoerd is in de computer. Als er een fout in het systeem zit, gaat de computer niet af.’

‘Bij 2 ligt de verantwoordelijkheid bij de programmeur, bij de 1e bij de persoon. Dat [situatie 1, red] vind ik prettiger.’

‘Het lijkt me onverstandig dat de software dat doet [de scan beoordelen, red], die gaat misschien hele voor de hand liggende dingen over het hoofd zien. Je moet heel erg in software vertrouwen dan.’

‘[Situatie, red] twee neemt eventueel het vooroordeel weg van beveiligingsambtenaar. Het verschil tussen een oud dametje of iemand met een terroristenlook, een mens beoordeelt daarop, een systeem niet.’

De meeste deelnemers achten de privacyvriendelijke optie minder effectief dan de ‘gewone’ optie. Ze hebben meer vertrouwen in het menselijk oordeel dan het oordeel van de software. Dit resultaat is van belang voor de inzet van Privacy by Design, en meer specifiek de inzet van PET: welke beslissingen zal de software maken, wat voor effect heeft dit op het vertrouwen van burgers in het systeem en op de acceptatie van burgers van het systeem?

Als er geen nieuwe argumenten of redenen uit de groep komen, vragen de onderzoekers de deelnemers of hen nog andere verschillen zijn opgevallen. Dan wijzen een aantal deelnemers op de aanwezigheid van de sticker die vermeldt waar burgers terecht kunnen in het geval van klachten en vragen. De meeste deelnemers ervaren dit als prettig, een enkeling beschouwt het meer als ‘een doekje voor het bloeden’. Geen van de deelnemers brengt de risicobeoordeling ter sprake.

‘Je hebt wel bij 2 dat je kunt bellen als je klachten hebt, op zich vind ik dat wel positief. Dan heb je het gevoel dat je voor je rechten kunt staan. Er kan niet zomaar over mij worden geoordeeld.’

'Dat bellen is een doekje voor het bloeden, echt een schaamlap. Je moet toch altijd je bezwaren kunnen uiten als je vindt dat er dingen fout gaan.'

'Dat je dat nummer kunt bellen is fijn.'

'Ja, dat is keurig.'

6.3.4 *Privacy Impact Assessments*

In dit onderdeel krijgen de deelnemers drie verschillende situaties (zie voor een volledig overzicht Bijlage 1) te lezen over de uitvoering van PIA's door de overheid bij de introductie van een nieuwe online dienst. Er wordt in de situaties onderscheid gemaakt tussen het aantal risico's, of het rapport alleen risico's identificeert of ook mogelijke oplossingen beschrijft, of het rapport openbaar is en hoe gebruikers als zij de dienst bezoeken op de resultaten van de PIA worden gewezen.

Situatie 1.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan tien privacyrisico's, waarvan twee als zeer ernstig beoordeeld zijn. De ontwikkelaars hebben het ontwerp van de online overheidsdienst op basis van de geïdentificeerde risico's aangepast zodat de privacyrisico's zijn verkleind. Het rapport waarin de privacyrisico's worden beschreven, is openbaar gemaakt.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de gebruiker kort gewezen worden op het onderzoek.

Situatie 2.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan twintig privacyrisico's en oplossingen om deze risico's te verkleinen. De ontwikkelaars hebben het ontwerp van de online overheidsdienst volgens de suggesties in het rapport aangepast zodat de privacyrisico's zijn verkleind. Het rapport waarin de privacyrisico's en de oplossingen worden beschreven, is openbaar gemaakt.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de burger gewezen worden op het onderzoek en de gemaakte aanpassingen, met een link naar het rapport. Ook de algemene informatie over hoe de instantie om zal gaan met de gegevens die van burgers verzameld worden, staat op de homepage vermeld.

Situatie 3.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan vijftien privacyrisico's, waarvan één als zeer ernstig is beoordeeld. De ontwikkelaars hebben het ontwerp van de online overheidsdienst volgens de suggesties in het rapport aangepast zodat de privacyrisico's zijn verkleind. Het rapport, waarin de privacyrisico's worden beschreven en oplossingen voor de risico's worden aangedragen, is niet openbaar.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de gebruiker kort gewezen worden op het onderzoek.

Ook hier wijzen deelnemers op diverse voor- en nadelen van verschillende situaties. Veel deelnemers zijn positief over de uitvoering van een PIA, maar hoe daarover gecommuniceerd moet worden verschillen de meningen. Een aantal deelnemers vindt het openbaar maken van de PIA prettig en soms zelfs noodzakelijk, andere deelnemers wijzen op de mogelijke risico's van het openbaar maken. Zij zijn bang dat kwaadwilligen misbruik maken van een dergelijk rapport omdat het laat zien waar de zwakheden zitten in het systeem. De deelnemers geven niet aan dat inzicht in de risico's van het systeem een averechts effect kan hebben op hun vertrouwen.

Wat ik van eerste twee wel vind is dat de risico's worden beschreven en openbaar gemaakt, dat breng mensen die kwaadwillenden op ideeën. Ik zou daarom voor 3 kiezen.

Bij situatie 1, vooral het zinnetje dat de risico's openbaar gemaakt worden, dan denk ik goh dat moet je vooral doen [cynisch, red]. Dat is hetzelfde als je voordeur openzetten en dan de hele dag van huis gaan. Dat vind ik een beetje raar. Degene die het willen doen het toch wel maar het brengt mensen op ideeën.

Ik vind de tweede het beste. Er wordt eerst gecontroleerd voordat het online gaat, zodat mensen het [de privacyrisico's van de dienst, red] kunnen checken. Het staat gelijk vermeld op de homepage, dat vind ik beter. Dat je gelijk ziet nou hier staat het.

Informatie achterhouden kan niet, de overheid is van ons allemaal.

De meeste deelnemers kiezen voor situatie twee, waarin het PIA rapport openbaar is en er ook zichtbaar aandacht aan wordt besteedt als gebruikers de site van online dienst bezoeken. Ze geven ook aan dat ze waarschijnlijk niet zelf het rapport gaan lezen, meestal omdat ze verwachten omdat het te moeilijk voor hun zal zijn. Het feit dat er een openbaar rapport is, betekent voor een aantal deelnemers dat andere instanties het onderzoek kunnen beoordelen en op die manier privacy gewaarborgd wordt.

Ik heb een voorkeur voor situatie 2. Het feit dat alles openbaar is, dat je kunt nalezen, dat je weet wat er met je gegevens gebeurt. ik zou het misschien globaal nalezen, alleen de conclusie. Ik vind het vooral belangrijk dat het openbaar is.

Ik heb er geen interesse in. Het feit dat ze het transparant maken is voor mij een teken dat ze er goed aan gedacht hebben.

Ik vind het fijn als het openbaar is, of ik er zelf wat mee kan weet ik niet.

Ik denk dat je wel bij zo'n link gaat kijken, als ie [de link naar PIA rapport, red] er niet is denk je er niet over na. Als ie [de link naar PIA rapport, red] er toch is, gaan veel mensen toch kijken.

Ik verwacht iets heel anders. Als zoiets openbaar gemaakt wordt, heb je altijd groepen, een soort Consumentenbond, die dat uitpluist, en dan zegt die hebben uit hun neus zitten peuteren, zo wordt dat beschermd. Jij en ik, wij kunnen dat niet uitpluizen.

Verder is de deelnemers gevraagd wanneer, voor welke systemen of diensten, een PIA zou moeten worden uitgevoerd. Aanvankelijk geven deelnemers aan dat iedere organisatie, zowel overheid als bedrijven, altijd een PIA zouden moeten uitvoeren.

Tijdens de discussie wijzigen sommige deelnemers echter op de kosten die daaraan verbonden zijn. Dan wordt in de discussie accent gelegd op overheidstrajecten (zoals diensten waar BSN mee gemoeid is, of publieke diensten zoals het biometrisch paspoort, OV-chipkaart). Sommige deelnemers concluderen dat het voor bedrijven niet altijd noodzakelijk is om een PIA uit te voeren (als ze moeten prioriteren) omdat zij daar een keuze hebben of ze de dienst wel of niet gebruiken. Deze redenering komt in alle drie de groepen terug. Daarnaast wordt het burgerservicenummer door de deelnemers als een gevoelig persoonsgegeven beschouwd, waardoor ze het belangrijker vinden als daar een dergelijke beoordeling wordt uitgevoerd.

In ieder geval moet de overheid dit doen, op sites waar persoonsgegevens worden ontsloten.

Ik kan de overheid niet uitkiezen, ik kan wel Sony buitensluiten en gaan xboxen, maar ik kan niet kiezen tussen DigiD en iets anders.

Voor alles met het BSN. Kijk, bij de Wehkamp weten ze mijn BSN nummer niet.

Bij bedrijven is niet echt noodzakelijk, daar heb je keuze. Je kunt mee doen ja of nee.

Als je afhankelijk bent, zoals bij de NS en de belastingdienst. Je kunt wel naar de C1000 als je de bonuskaart van Albert Heijn niet wilt.

De deelnemers is ook gevraagd of het voor hun vertrouwen uitmaakt wie de PIA uitvoert. In de huidige benadering voert de organisatie die een nieuw IT-systeem of dienst wil introduceren de PIA zelf uit. Een aantal deelnemers vindt niet dat dit door de organisatie die de dienst aanbiedt moet worden gedaan, omdat ze een ‘eigen beoordeling' niet zouden vertrouwen. Dit is van belang, omdat de huidige PIA-raamwerken er vanuitgaan dat de PIA wordt uitgevoerd door de organisatie die de nieuwe dienst ontwikkeld.

Sommige deelnemers twijfelen, in het geval van overheidsdiensten, of de overheid voldoende kennis in huis heeft, om zelf de beoordeling te kunnen uitvoeren. Anderen willen liever dat een onafhankelijke organisatie, zoals de toezichthouder (het CBP) de beoordelingen uitvoert.

‘Misschien kan de overheid het niet, die hebben de expertise niet, die gaan ze dan inhuren. (…) Ik vind dat de overheid die expertise in huis zou moeten hebben. je moet overheid kunnen vertrouwen, ik heb minder vertrouwen in een externe partij.’

‘Ik ken geen instanties die dat [een PIA, red] dan zouden moeten maken.’

‘Het moet in principe een onafhankelijke organisatie zijn.’

‘Het liefst onafhankelijk instantie. Een bedrijf kan nooit zichzelf controleren.’

6.3.5 *Privacy in de organisatie: verantwoordelijkheden van dienstaanbieders*

De meeste deelnemers (vijfentwintig) geven aan dat zij op de hoogte zijn van de Wet bescherming persoonsgegevens. Het noemen van een aantal waarborgen, rechten of plichten uit deze wet blijkt echter een stuk lastiger.

Ik weet dat er waarborgen zijn, maar niet wat precies.’

'Het is [voor mij, red] voldoende om te weten dát er iets in de wet staat.'

Veel deelnemers weten niet waar ze terecht kunnen als ze vragen of klachten hebben over de verwerking of opslag van persoonlijke gegevens bij het gebruik van online diensten, bijvoorbeeld als er om meer gegevens wordt gevraagd dan noodzakelijk lijkt. Een aantal deelnemers geeft aan er voor te kiezen om de dienst niet te gebruiken. Sommigen laten weten de informatie wel te geven. Een deelnemer noemt in de discussie de Ombudsman. Dit wordt door de andere deelnemers in de groep beaamd als mogelijk punt waar ze terecht zouden kunnen. Een deelnemer noemt het College Bescherming Persoonsgegevens. Ook als het gaat om het gebruik van overheidsdiensten weten de meeste deelnemers (26) niet bij welke instantie ze terecht kunnen. Drie deelnemers kunnen een instantie noemen, dit zijn de Ombudsman, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het College Bescherming Persoonsgegevens.

'Als ik het niet vertrouw stop ik met mijn gegevens invullen en delete ik alles. Ik zou niet weten bij wie ik moet zijn, heb dit [aanspreken van verantwoordelijke, red] dus nog nooit gedaan.'

'Nog nooit gedaan, eventueel zou ik aankloppen bij Kohnstamm, maar dan moet het me wel erg tegenstaan wat er is gebeurd. En dat kost veel energie.'

'Ik heb geen flauw idee bij wie ik moet aankloppen.'

De deelnemers zijn verdeeld als het gaat om de vraag of online dienstaanbieders (bedrijven en overheid) voldoende om toestemming vragen voor het gebruik van persoonlijke gegevens. Twaalf deelnemers geven aan dat dit voldoende gebeurt, vijftien deelnemers zijn van mening dat dit niet het geval is. De deelnemers zijn niet op de hoogte van de meldingsplicht voor gegevenswerkende bedrijven, maar de meesten geven aan, als zij hiervan op de hoogte worden gesteld, dat ze dit positief en noodzakelijk vinden, hoewel ze van mening zijn dat een dergelijke meldingsplicht hen geen zekerheid biedt of dienstverlenende instanties daadwerkelijk zorgvuldig en volgens de wet met hun gegevens zullen omgaan. Ook vragen de deelnemers zich af in hoeverre de melding betekent dat de toezichthouder ook controleert of de gemelde gegevensverwerking volgens de wet is. Ze vinden dat een meldingsplicht alleen niet voldoende is, er zou ook gecontroleerd moeten worden of de verwerking van persoonlijke gegevens daadwerkelijk aan de wet voldoet.

' Ik vind het goed, dan is er wat controle, of in elk geval een poging tot controle.'

'Als er dan ook nog echt gecontroleerd wordt, Facebook kan ook zeggen dat ze gegevens willen opslaan om een kerstkaart te sturen.'

Met het oog op de herziene dataprotectierichtlijn in Europa is de deelnemers ook gevraagd naar hun mening over een mogelijk verplichte melding in het geval van gestolen of anderszins gecompromitteerde gegevens (de *data breach notification*). De deelnemers staan hier positief tegenover en het zou de deelnemers meer vertrouwen in de dienstverlenende instantie geven. Ze zijn zich echter ook bewust van de mogelijke keerzijde, als er teveel of te vaak melding wordt gemaakt van gelekte gegevens kan dit een negatief effect hebben op hun vertrouwen in de desbetreffende instantie. Voor sommige deelnemers is het belangrijk dat er niet alleen gemeld wordt in het geval van incident, maar dat daar ook een sanctie (zoals een boete) aan gekoppeld is. Voor anderen is 'name en shame' voldoende. Een

deelnemer geeft aan dat te vaak om toestemming vragen mogelijk op dezelfde manier ook averechts kan werken.

'Je hele image [van de dienstverlenende instantie, red] gaat eraan. Het kost geld, dus ze worden wel wakker.'

"Ik denk dat het zichzelf reguleert. Als zij [dienstverlenende instanties] de hele tijd incidenten hebben gaan bedrijven vanzelf wel iets doen.'

'Als ze daar behulpzaam mee zijn wekt dat vertrouwen, als ze uitleggen het waren slimme hackers, daar kunnen we niks aan doen, dat vind ik sympathiek. Dat is beter dan [een privacy-incident] onder de pet te houden.'

Ook is de deelnemers gevraagd naar de optie om een Privacy Officer verplicht aan te stellen. De deelnemers geven aan dat wel op prijs te stellen, zeker gezien de ontwikkelingen in de 'digitale wereld' en voor de 'extreme' gevallen, zoals het Elektronisch Patiënten Dossier of Facebook) maar er wordt getwijfeld aan de haalbaarheid van het idee. Deelnemers redeneren dat een Privacy Officer ook extra kosten voor een organisatie betekent.

Het lijkt me wel goed, maar het kost extra geld.

In het extreme geval, zoals Facebook en zoals het elektronisch patiëntendossier daarvoor lijkt het me wel nuttig.

Ik weet niet hoeveel dat inhoudt, oh dan huren we even iemand en geven we het een naam. Ik wil liever dat bedrijven dat uit eigen belang willen doen, niet omdat er een wetje is dat zegt dat je dat moet doen.

Het zou zichzelf wel terug kunnen verdienen bij bedrijven misschien. Maar bij de overheid, bij iedere publieke dienst, dan kost het de belastingbetaler ook wel veel geld.

6.3.6 *Privacybeschermende technologie*

In dit onderdeel hebben de onderzoekers de deelnemers verschillende voorbeelden van privacybeschermende technologie (PET's) voorgelegd, waaronder het anonimiseren van gegevens, strengere toegangscontrole, het pas opslaan van camerabeelden als dat 'nodig' is, bijvoorbeeld in bejaardentehuizen als de software detecteert dat een bewoner gevallen is, of in de openbare ruimte op het moment dat er een rel ontstaat, en het werken met 'credentials' zodat alleen bepaalde identiteitsgegevens worden overhandigd (bijvoorbeeld voor het kopen van alcohol of tabak wordt alleen zichtbaar of een persoon wel of niet ouder is dan achttien).

Deelnemers vinden het moeilijk om over PET's in zijn algemeenheid te praten enna te denken. Ze gaan in de discussie steeds in op de in de introductie genoemde voorbeelden. Per voorbeeld hebben de deelnemers meer informatie nodig om te begrijpen hoe de technologie werkt. Het voorbeeld van het pas opslaan van camerabeelden op het moment dat er iets 'mis' is, wordt niet goed begrepen. De discussie gaat over de vraag of het überhaupt nodig is dat er een camera wordt geplaatst in plaats van over het verschil tussen wel of geen privacybeschermende technologie. Na verdere uitleg van de onderzoekers en de vraag welke situaties wenselijk worden gevonden, verschilt dit erg per deelnemer. In de discussie over 'credentials' twijfelen de deelnemers aan het nut ervan. Ze denken dat jongeren erg

gemakkelijk van pas kunnen wisselen als de volledige identiteitsinformatie niet zichtbaar is.

Jongeren zijn zo slim, die nemen het pasje van [naam andere deelnemer, red], want die is groter. Als je aan de bar alleen de leeftijd ziet, wie zegt dat [naam andere deelnemer, red] niet mij is. Aan de foto op je ID kunnen ze nog zien dat jij het bent.

Het anonimiseren van gegevens wordt goed begrepen door de deelnemers al wordt er getwijfeld of de gegevens daadwerkelijk anoniem zijn. In de discussie merkt men op dat dit een kwestie van vertrouwen is.

Vertrouwen is een lastig punt, ik wil het aannemen, maar het blijft een aanname. Als je iets doet met uniek identificeerbare gegevens, wie weet wordt dat later gekoppeld, dan was het ooit anoniem, maar blijkt het achteraf niet anoniem.

Per voorbeeld en per deelnemer verschillen de meningen over de wenselijkheid van privacybeschermende technologie. Het is daarom niet mogelijk om op basis van deze resultaten een uitspraak te kunnen doen over de wenselijkheid van privacybeschermende technologie in zijn algemeenheid. Wel wordt duidelijk dat privacybeschermende technologie vaak lastig te begrijpen is voor de deelnemers. Overheden en bedrijven die dit toepassen en willen communiceren aan burgers of klanten zullen hier rekening mee moeten houden.

6.3.7 Specifieke toepassing van privacybeschermende technologie

In het laatste onderdeel leggen de onderzoekers de deelnemers één specifiek voorbeeld van privacybeschermende technologie voor, een elektronische gezondheidskaart (op een Duits voorbeeld geïnspireerd) die werkt op basis van *credentials* en waar burgers zelf kunnen kiezen welke informatie zij op de kaart zetten. Opvallend is het enthousiasme in alle drie de groepen over de kaart. Waar de andere voorbeelden met wat scepsis worden ontvangen, geven veel deelnemers aan deze kaart direct te willen gebruiken. In de discussie blijkt dat de oorzaak ligt in het ‘vrije keuze’ element. Het spreekt de deelnemers zeer aan dat ze zelf kunnen kiezen welke informatie op de kaart komt en met wie ze dit kunnen delen. Sommige deelnemers twijfelen wel of dit wel handig is, bijvoorbeeld als mensen er voor kiezen cruciale medische informatie niet op de kaart te zetten.

6.3.8 Afronding van de bijeenkomsten

Ter afsluiting is de deelnemers de vraag voorgelegd wat zij de overheid zouden adviseren als het gaat om online dienstverlening en het beschermen van privacy van burgers. Veel deelnemers geven aan zorgvuldige opslag van gegevens belangrijk te vinden en zien graag dat de overheid meer informatie geeft over hoe privacy van burgers is/wordt gewaarborgd en dit (beter) communiceert aan burgers. Transparantie over opslag, gebruik en verwerking van gegevens, en zorgvuldige omgang met gegevens is een belangrijke factor voor het vertrouwen van deelnemers in de dienstverlening van de overheid. Eén deelnemer noemt de mogelijkheid om gegevens te kunnen verwijderen en verwijst daarmee naar de recente discussie over ‘the right to be forgotten’.

‘Meer bekend maken hoe ze het geregeld hebben, de PR kan beter.’

'Openheid is belangrijk, dat je weet wat er speelt en wat de privacyproblemen zijn.'

Zorgvuldigheid. Dat je wel goed bepaalt wie van de overheid toegang heeft, wie het controleert, waar het voor wordt gebruikt. ik ben niet bang voor opslag, maar voor onzorgvuldig gebruik. Daar kan het misgaan.

Dat de overheid een knop heeft waarmee gegevens verdwijnen? Het moet deletebaar zijn.

6.4 Conclusies

De focusgroepen laten zien dat burgers verschillend reageren op de *afzonderlijke parameters* van Privacy by Design. De verschillende elementen lijken daarmee elk een ander effect op vertrouwen en acceptatie te hebben. Vooral die elementen van Privacy by Design die de transparantie van gegevensverwerking door de overheid vergroten, lijken een positief effect te hebben op vertrouwen. Dit zijn o.a. het uitvoeren en publiceren van een PIA en organisatorische maatregelen zoals het geven van toegankelijke informatie over de gegevensverwerking, het duidelijk vragen van toestemming daarvoor en een eenvoudig te vinden contactpunt bij de organisatie (in het geval van vragen of klachten). Het laten uitvoeren van de PIA door een onafhankelijke organisatie lijkt een positief effect te hebben op vertrouwen. Het uitvoeren van een PIA voor overheidsdiensten lijkt voor burgers extra van belang, omdat daar vaak geen alternatieve dienstverlener is, burgers vaak verplicht zijn de dienst af te nemen (zoals de OV-chipkaart, vingerafdrukken in het paspoort e.d.) en de verzamelde gegevens gevoeliger worden geacht.

Wettelijke verplichtingen die de verantwoordelijkheden van organisaties vastleggen/vergroten – en het actief uitdragen van de naleving daarvan – kunnen ook positief bijdragen aan vertrouwen van burgers in diensten, zoals de meldplicht bij het CBP voor de verwerking van gegevens, de 'data breach notification' en sterk onafhankelijk toezicht. Voor sommige transparantie-elementen van PbD lijkt er ook een omgekeerd effect te kunnen optreden. Indien privacy-incidenten vaak voorkomen en organisaties hier burgers actief van op de hoogte houden, kan dit juist leiden tot een verminderd vertrouwen in de dienst, en uiteindelijk verminderde acceptatie van de dienst. Dit kan ook gelden voor PIA's, indien organisaties zoals de Consumentenbond of het College Bescherming Persoonsgegevens kritisch oordelen over de uitgevoerde PIA en de mate waarin geconstateerde risico's zijn geadresseerd.

Het technische element van Privacy by Design – de privacybeschermende technologie – is moeilijk te begrijpen voor de deelnemers uit de focusgroepen. De privacybeschermende technologie is niet goed te doorgronden voor een leek en wordt als een soort "black box" ervaren. De burger kan dus zelf niet goed inschatten wat deze technologie nu echt bijdraagt. In het voorbeeld van de security scanners twijfelen de deelnemers aan de effectiviteit van de privacyvriendelijke oplossing en geeft men zelfs uiteindelijk de voorkeur aan de niet-privacyvriendelijke oplossing. Het 'simpelweg' inbouwen van privacytechnieken in overheidsdienst leidt dus niet per definitie tot een hogere acceptatie van de dienst.

Het toepassen van privacybeschermende technologie kan mogelijk wel indirect leiden tot meer vertrouwen en acceptatie. Als we aannemen dat het toepassen van privacybeschermende technologie bij een dienst leidt tot een afname van privacy-incidenten, dan wordt hiermee ook de kans op verlies van vertrouwen verkleind. De deelnemers geven immers aan dat negatieve berichtgeving (zoals over privacy-incidenten) een negatieve invloed heeft op hun vertrouwen in dienstverlening. Treden dergelijke incidenten minder vaak op, dankzij technologische bescherming, dan kan dit tot minder vertrouwensverlies leiden.

De ‘black-box’ eigenschappen van privacybeschermende technologie, roept ook vragen op over hoe de toepassing van deze technologie het beste gecommuniceerd kan worden naar burgers. De wijze van communicatie kan invloed hebben op de mate van acceptatie van de dienst. Nader onderzoek zal moeten uitwijzen of en welke vorm van communicatie acceptatie van privacyvriendelijke technieken kan vergroten. Privacybeschermende technologie die meer keuzes voor gebruikers toelaat (iets dat zichtbaar en tastbaar is voor gebruikers) lijkt in ieder geval een positief effect te hebben op vertrouwen en acceptatie.

Onze bevindingen uit de focusgroepen geven een eerste indicatie van mogelijke redeneringen en effecten van de relatie tussen de inzet van Privacy by Design, verantwoordelijkheid en legitimiteit, effectiviteit en vertrouwen en acceptatie. Er is nader kwantitatief onderzoek nodig om deze bevindingen onder een representatieve groep van de Nederlandse bevolking om meer inzicht in deze relaties te krijgen.

7 Afwegingskader Privacy by Design

7.1 Inleiding

In dit hoofdstuk komt de laatste, in hoofdstuk twee geformuleerde deelvraag aan de orde: Hoe kunnen de resultaten van het onderzoek worden vertaald naar een afwegingskader voor beleidsmakers?

Privacy by Design biedt de overheid de mogelijkheid om op een systematische manier privacybescherming in te bouwen in (nieuwe) overheidsdiensten. Het empirisch onderzoek wijst echter uit dat Privacy by Design – in de ogen van de burger – leidt tot meer vertrouwen en acceptatie van e-overheidsdienstverlening. Uit het empirisch onderzoek kunnen samengevat de volgende conclusies worden getrokken:

- PET's zijn moeilijk te doorgronden en lijken door deelnemers niet altijd even effectief te worden geacht, waardoor toepassing van PET niet zonder meer leidt tot meer vertrouwen en hogere acceptatie;
- PIA's lijken een positief effect te hebben op het vertrouwen en acceptatie. Uit de focusgroepen komen geen situaties naar voren waar PIA's een negatief effect zouden kunnen hebben op vertrouwen en acceptatie. Wel geven burgers aan zich zorgen te maken over de openbaarmaking van PIA's omdat kwaadwilligen mogelijk misbruik kunnen maken van de geconstateerde kwetsbaarheden. Tegelijkertijd vinden deelnemers het wel belangrijk dat een dergelijke analyse wordt uitgevoerd.
- Wetgeving en organisatorische elementen die zichtbaar zijn voor de burger lijken een positief effect te hebben op vertrouwen waar deze maatregelen zichtbaar zijn of worden gemaakt aan burgers (zoals een herkenbaar aanspreekpunt, de *data breach notification*, daaraan gekoppelde sancties, openheid over gegevensverwerking, toegeven van mogelijke fouten). Het positieve effect van maatregelen die de transparantie over gegevensverwerking verhogen, kan worden aangetast op het moment dat het betekent dat er veel incidenten zichtbaar worden voor burgers (bij wijze van spreken: 1 keer een fout toegeven is sympathiek, bij 10x ben je een kluns);
- Keuze, controle en zeggenschap van burgers in de dienst: meer zeggenschap bij burgers zelf lijkt positief effect te hebben op vertrouwen en adoptie.

De ene eOverheidsdiensten is echter de andere niet. Uitvoeringsprojecten bij de overheid kunnen sterk verschillen in de mate van complexiteit, omvang en maatvoering. Daarom dient, alvorens het hierna volgende beoordelingsinstrument te hanteren, het desbetreffende project eerst te worden geïdentificeerd. Dat kan met behulp van de volgende vragen:

- Wat is de doelstelling, reikwijdte en rationale van het project?
- Worden er in het project/te ontwikkelen systeem nieuwe informatietechnologieën toegepast die een substantiële impact op de persoonlijke levenssfeer van burgers kunnen hebben (zoals biometrie, gezichtsherkenning, locatiebepaling, profilering e.d.)?
- Worden er in het te ontwikkelen/implementeren systeem persoonsgegevens verwerkt en op welke schaal?
- Zijn er meerdere overheidsinstanties bij de ontwikkeling, implementatie of uitvoering van het informatiesysteem betrokken of worden er gegevens

gebruikt, verzameld of verwerkt van of bij andere uitvoeringsinstanties of private organisaties?

7.2 Afwegingskader

Een afwegingskader is een instrument in handen van een overheidsorganisatie die (delen van) haar dienstverlening met behulp van ICT wil institutionaliseren, en daarbij Privacy by Design (PbD) toepast.

Het afwegingskader heeft betrekking op eOverheidsdiensten en is niet bedoeld voor het veiligheidsdomein. De vraag is aan welke condities of toepassingsvoorwaarden PbD, in welke vorm dan ook, en gelet op de resultaten van het empirisch onderzoek, moet voldoen. Deze toepassingsvoorwaarden hebben betrekking op de volgende elementen of aspecten:

I Condities voor vertrouwen in en acceptatie van overheidsdienstverlening;
II Condities voor verantwoordelijkheid ('accountability', d.w.z. zich goed kunnen verantwoorden).

Beiden zijn voorwaarden voor vertrouwen en acceptatie van overheidsdienstverlening (door middel van ICT) en hangen nauw met elkaar samen, waarbij de condities voor verantwoordelijkheid generieke voorwaarden zijn en de condities voor vertrouwen en acceptatie specifieke voorwaarden zijn.

I *Condities voor verantwoordelijkheid*

a. Het standaard vooraf uitvoeren van een Privacy Impact Assessment en het herhalen van een PIA bij substantiële wijziging van informatiesystemen en –processen of wetgeving.[43] De PIA karakteriseert het IT-systeem (datatypen, datastromen, opslag en verwerking van gegevens), identificeert privacyrisico's en bijbehorende beheersmechanismen[44].
b. Het aanstellen van een (part-time) Privacy Officer/Gegevens Functionaris in de betreffende overheidsorganisatie, die tot taak heeft toezicht uit te oefenen op het functioneren van de dataverwerkers c.q. contactambtenaren en tot wie burgers toegang hebben indien zij naar hun mening niet adequaat worden geholpen door de dataverwerkers c.q. contactambtenaren[45].
c. Actieve voorlichting van de overheidsorganisatie over alle aspecten van het ICT-instrument aan de doelgroep.
d. Het helder positioneren van de betreffende ICT-dienstverlening en de uitvoerende overheidsinstantie ten opzichte van andere publieke en private dienstverleners en de sociale media: Welke overheidsorganisatie is aanbieder van dienst en waarvoor wordt de dienst gebruikt?

[43] De PIA kan de toetsen in het Integrale Afwegingskader (IAK) van het Rijk en de daarbij behorende uitvoeringstoetsen verrijken (zie Rijksoverheid, 2010)
[44] Hierbij kan gebruik worden gemaakt van bestaande PIA-raamwerken en zogenaamde 'templates'.
[45] Een Privacy Officer heeft een ander aandachtsgebied dan de Information Officer die belast is met de besturing en beheersing van grootschalige ICT-projecten binnen de overheid en de positionering en kwaliteit van informatiemanagement en in 2009 binnen de ministeries zijn aangesteld.

e. Burgers standaard inzage geven in alle gegevens die op hem/haar betrekking hebben en hoe deze worden verwerkt.[46]
f. Duidelijke afspraken, afbakening en communicatie naar de burgers over: i) van welke gegevens wordt gebruik gemaakt (nieuwe verzameling of wordt er gebruik gemaakt van bestaande databases van andere overheidsorganisaties), ii) welke andere (overheids-)organisaties maken gebruik van de verzamelde gegevens, iii) waar worden de gegevens bewaard en iv) welke organisatie is voor welke dataverzamelingen verantwoordelijk?

II *Condities voor vertrouwen in en acceptatie van overheidsdienstverlening*
g. Het standaard realiseren van dataminimalisatie en datavernietiging als het doel waarvoor de gegevens zijn verzameld is bereikt.
h. Accuraatheid, up-to-date zijn en compleetheid van de opgeslagen data.
i. Heldere, specifieke en eenduidige formulering van het doel van de dataverzameling.
j. Het afdwingen van doelbinding[47] en overige privacyprincipes in de volledige levenscyclus van het systeem en de uitvoering van constante controles daarop.
k. Adequate beveiliging van de data, inclusief de technische uitwerking daarvan.
l. Het inbouwen van technische privacywaarborgen waar dit van toepassing is, zoals anonimiteit, pseudonimiteit, onverbondenheid, onwaarneembaarheid.
m. Het beschikbaar stellen van voldoende expertise in beveiliging.
n. Het beschikbaar stellen van instrumenten aan 'data-subjecten' om datasporen te kunnen volgen binnen de organisatie.
o. Openheid over geconstateerde privacy-incidenten en communicatie over de genomen maatregelen naar burgers.[48]
p. De aanwezigheid van een sterke onafhankelijke toezichthouder die controleert in hoeverre regelgeving omtrent privacy en dataprotectie wordt nageleefd.

Indien aan deze 16 condities is voldaan, kan de conclusie worden getrokken dat de betreffende overheidsorganisatie (i.c. haar bestuurders/beleidsmakers) beschikt over een ICT-overheidsdienstverlening die de kwalificatie 'trusted technology' verdient. Dat is een technologie waarin op overtuigende wijze privacy, vertrouwen, verantwoordelijkheid en acceptatie zijn gerepresenteerd.

Tot slot dient nog te worden nagegaan of en hoe deze 'trusted technology' kan worden ingevoerd of kan functioneren, zonder dat afbreuk wordt gedaan aan de effectiviteit en doelmatigheid van de overheidsdienstverlening. De criteria hiervoor zijn geformuleerd aan de hand van de volgende vragen, waarop de beleidsmakers een expliciet antwoord moeten geven:

a. Botst de concrete toepassing van de technologie met condities die de legitimiteit van het systeem (condities onder I) zichtbaar maken of vergroten? Zo ja, om welke condities gaat het?

[46] Een voorbeeld hiervan is mijnoverheid.nl. Ook bij de OV-chipkaart is het sinds kort mogelijk voor reizigers om hun gegevens in te zien.
[47] Hierbij moet worden opgemerkt dat het doel van het systeem kan veranderen als de wettelijke basis is veranderd (door wijziging van wet of het aannemen van een nieuwe wet).
[48] In de volgende wetswijziging van de Wet bescherming persoonsgegevens zal hiervoor een meldpunt worden ingericht.

b. Botst het zichtbaar maken of vergroten van de legitimiteit op zijn beurt met de oorspronkelijk nagestreefde belangen van de dienstverlening?
c. Zijn de uitgewerkte condities voor verantwoordelijkheid (condities onder II) aanvaardbaar uit een oogpunt van kostenefficiëntie?

Literatuur

Aiken, K. D., & Bousch, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the contextspecific nature of internet signals. *Journal of the Academy of Marketing Science*, 34, 308–323.

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a website's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, 31(5), 661−681.

Artikel 29 Werkgroep (2011) *Opinion 9/2011 on the revised industry proposal for a privacy and data protection impact assessment framework for RFID Applications*. 00327/11/EN, WP 180. Geadopteerd op 12 februari 2011.

Bader, Veit (1989) Max Webers Begriff der Legitimität. Versuch einer systematisch-kritischen Rekonstruktion. In Max Weber heute. Erträge und Probleme der Forschung. Edited by Johannes Weiss. Frankfurt am Main: Suhrkamp.

Barber, B. (1983). *The logic and limits of trust. New Jersey*: Rutgers University Press.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, 69, 133-152.

Beetham, David (1991) *The legitimation of power*. London: Macmillan.

Belanger, F. & Carter, L. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems*, 17, 165-176.

Belanger, F., Hiller, J.S., & Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11, 245–270.

Beldad A., De Jong, M., & Steehouder, M. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites. *Government Information Quarterly,* 26(4), 559-566.

Beldad, A., De Jong, M., & Steehouder, M. (2010). Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. *Government Information Quarterly*, 27(3), 238-244.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International differences in information privacy concerns: a global survey of consumers. *The Information Society*, 20, 313-324.

Berendt, B., Gunther, O., & Spiekermann, S. (2005). Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM* 48:101-106.

Bodansky, Daniel (1999) The legitimacy of international governance: A coming chal-lenge for international environmental law? *American Journal of International Law* 93 (3), 596-624.

Bolchini, D., He, Q., Anton, A. I., & Stufflebeam, W. (2004). 'I need it now': improving website usability by contextualizing privacy policies. In N. Koch, P. Fraternali, & M. Wirsing (Eds.), ICWE 2004, LCNS 3140 (pp. 31−44). Heidelberg, DE: Springer-Verlag.

Buchanan, Allen (2003) *Justice, legitimacy, and self-determination: Moral foundations for international law*. Oxford: Oxford university Press.

Buskens, V. (1998). The social structure of trust. *Social Networks*, 20, 265–289.

Buttner, O.B. & Goritz, A.S. (2008). Perceived trustworthiness of online shops. *Journal of Consumer Behavior*, 7, 35-50.

Carens, Joseph H. (2000) *Culture, citizenship, and community: A contextual exploration of justice as evenhandedness.* Oxford: Oxford University Press.

Carens, Joseph H. (2004) A contextual approach to political theory. *Ethical Theory and Moral Practice* 7, no. 2: 117-132.

Carter, L., F. Belanger (2004). The influence of perceived characteristics of innovating on e-government adoption. Electronic Journal of e-Government, 2(1), 11-20. Available online at www.ejeg.com.

Carter, L., F. Bélanger (2008)Trust and Risk in E-Government adoption. *The Journal of Strategic Information Systems*, 17 (2), 165-176

Casalo, L. V., Flavian, C., & Guinaliu, M. (2007). The influence of satisfaction, perceived reputation and trust on a consumer's commitment to a website. *Journal of Marketing Communications*, 13(1), 1–17.

Chen, C. (2006). Identifying significant factors influencing consumer trust in an online travel site. *Information Technology and Tourism*, 8, 197–214.

Choudrie, J., Raza, S., & Olla, P. (2009). Exploring the issues of security, privacy, and trust in e-government: UK citizens' perspectives. *Proceedings of the Fifteenth Americas Conference on Information Systems*, San Francisco, California, 6-9 August 2009, 1-9.

Colesca, S.E. & Dobreca, L. (2008). Adoption and use of e-government services: The case of Romania. *Journal of Applied Research and Technology*, 6(3), 204-216.

Corbitt, B. J., Thaasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. In *Electronic Commerce Research and Applications*, 2, 203–215.

Culnan, M.J. & Bies, R.J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues* 59(2): 323-342.

Das, T. K., & Teng, B. S. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology*, 19(1), 85–116.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the influence of national culture on the development of trust. *Academy of Management Review*, 23(3), 601–620.

Edwards, Michael (1999) Legitimacy and values in NGOs and voluntary organisations: Some sceptical thoughts. In *International perspectives on voluntary action: Reshaping the third sector.* Edited by David Lewis. London: Earthscan.

European Commission (2011) Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011. http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

Everard, A. & Galleta, D.R. (2005). How presentation flaws affect perceived site quality, trust, and intention purchase from an online store. *Journal of Management tnformation Systems,* 22(3), 55-95.

Flavian, C., Guinaliu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction, and consumer trust on website loyalty. Information & Management, 43, 1–14.

Franck, Thomas M. (1988) Legitimacy in the international system. *American Journal of International Law* 82 (4), 705-759.

Fu, J. R, C.K. Farn, W.P. Chao (2006), Acceptance of electronic tax filling: a study of taxpayer intentions, *Information & Management*, 43(1), 109-126

Gefen, D. (2000). E-commerce: The roles of familiarity and trust. *Omega*, 28, 725–737.

Gershtenson, J., J. Ladewig, D. L. Plane (2006), *Parties, Institutional Control, and Trust in Government*, *Social Science Quarterly* 87(4) 882-902

Hart, H.L.A. (1968), *Punishment and Responsibility.* Oxford/New York: Oxford University Press

Held, David (1999) The transformation of political community: Rethinking democracy in the context of globalization. In *Democracy's Edges*, edited by Ian Shapiro, and Casiano Hacker-Cordón. Cambridge: Cambridge University Press: 84-111.

Hinde, S. (2005) No state can exist without the confidence of people, *Computer Fraud & Security,* 8, Pages 18-20

Hurd, Ian (1999) Legitimacy and authority in international politics. *International Organisation* 53 (2), 379-408.

Hurrell, Andrew (2002) "There are no rules" (George W. Bush): International order after September 11. *International Relations* 16, 185-204.

James, H. S. (2002). The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness. *Journal of Economic Behavior & Organization*, 47, 291–307.

Jarvenpaa, S. L., Tractinsky, N.,& Saarinen, L. (2002). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2), Available online at http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html.

Jensen, C. and Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. *CHI 2004 Vienna, Austria :* 471-478.

Jensen,C., Potts, C.,&Jensen,C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63, 203−227.

Karvonen, K. (2000). The beauty of simplicity. *CUU '00 Arlington*, Virginia, ACM, 85-90.

Kee, H. W., & Knox, R. E. (1970). Conceptual and methodological consideration in the study of trust and suspicion. *Journal of Conflict Resolution*, 14(3), 357–366.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2003). A study of the effect of consumer trust on consumer expectations and satisfaction: The Korean experience. *In Proceedings of the 5th international conference on electronic commerce* (pp. 310–315). Pittsburg, PA.

Kipnis, D. (1996). Trust and technology. In R. M. Kramer & T. R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 39–50). Thousand Oaks, CA: Sage Publications Inc.

Koller, M. (1988). Risk as a determinant of trust. Basic and Applied Social *Psychology*, 9(4), 265–276.

Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, 41, 377–397.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, 6, 323–331.

Laufer, R.S. & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33(3):22-42.

Lean, O.K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). Factors influencing intention to use e-government services among citizens in Malaysia. *International Journal of Information Management*, 29(6), 458-475.

Lee, J. and H.R. Rao (2009), Task complexity and different decision criteria for online service acceptance: A comparison of two e-government compliance service domains, *Decision Support Systems* 47, 4, 424-435.

Lieshout, M. van, Kool, L., Schoonhoven, B. van, Jonge, de M. (nog te verschijnen) Privacy-by-Design: alternative for existing practices in safeguarding privacy? In: *Info*, Vol 13, Issue 6, 2011

Luhmann, N. (1979). *Trust and power*. Chichester: John Wiley.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organization trust. *Academy of Management Review*, 20(3), 709–734.

McKnight, D. H., Choudhoury, H., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems*, 11, 297–323.

Meinert, D. B., Peterson, D. K., Criswell, J. R., & Crossland, M. D. (2004). Would regulation of website privacy policy statements increase consumer trust? *Informing Science Journal*, 9, 123−142.

Merriam-Webster Online Dictionary (2006) Legitimate. http://www.m-w.com/dictionary/legitimate.

Eerste Kamer (2010-2011) Motie Lid Franken. Evaluatie Wet bescherming persoonsgegevens. 31 051 D, 17 mei 2011.

Morgeson, F.V., Van Amburg, D., & Mithas, S. (2010). Misplaced trust? Exploring the structure of the e-government-citizen trust relationship. *Journal of Public Administration Research and Theory*, doi:10.1093/jopart/muq006.

Norberg, P.A. & Dholakia, R.R. (2004). Customization, information provision and choice: what are we willing to give up for personal service? *Telematics and Informatics* 21: 143-155.

Olivero, N. and Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology* 25:243-262.

Oliviero, Melanie Beth, and Adele Simmons (2002) Who's minding the store? Global civil society and corporate responsibility. In *Global Civil Society Yearbook* 2002. Edited by Marlies Glasius, Mary Kaldor, and Helmut Anheier. Oxford: Oxford University Press.

Pan, Y. and Zinkhan, G.M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing* 82(4): 331-338.

Pavlou, P. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 17(3), 101–134.

Petty, R.E. & Cacioppo, J.T. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York, NY: Springer-Verlag.

Phelan, C. (2006) *Public Trust and Government Betrayal*, *Journal of Economic Theory* 130(1), 27-43

Geest, T. van der en Beldad, A. (2010) *Citizens' trust in e-government and DigiD.* Rapport Universiteit Twente.

Reding, V. (2010) *Building Trust in Europe's Online Single Market*. SPEECH/10/327, Brussels, 22 June 2010.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, 35(4), 651–665.

Rosseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: Across-discipline view of trust. Academy of Management Review, 23(3), 393–404.

Rijksoverheid (2010) Het Integraal Afwegingskader voor beleid en regelgeving.

Salam, A. F., Iyer, L., Palvia, P., & Singh, R. (2005). Trust in e-commerce. Communications of the ACM, 48(2), 73–77.

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. Journal of Strategic Information Systems, 11, 325–344.

Steffek, Jens (2003) The legitimation of international governance: A discourse approach. *European Journal of International Relations* 9 (2), 249-275.

Sztompka, P. (1999). Trust: A sociological theory. Cambridge: Cambridge University Press.

Teo, T. S. H., & Liu, J. (2007). Consumer trust in e-commerce in the United States, Singapore, and China. Omega, 35, 22–38.

Tolbert, C.J., K. Mossberger (2006), The Effects of E-Government on Trust and Confidence in Government.

Tweede Kamer (2010-2011) *Verwerking en bescherming persoonsgegevens*. Brief van de staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties. 32 761, nr. 1, 29 april 2011.

Vedder, A., R. Wachbroit, (2003) Reliability of information on the Internet: Some distinctions. *Ethics and Information Technology*, *5*, 211-215.

Vedder, A. (2008) Responsibilities for Information on the Internet. In: Himma, K. and Tavani, H. (eds.), *The Handbook of Information and Computer Ethics.* Hoboken NJ (etc.) John Wiley and Sons: 2008, pp. 339-359 ISBN 978-0-471-79959-7

Vu, K. P. L., Chambers, V., Garcia, F. P., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R., & Proctor, R. (2007). How users read and comprehend privacy policies. In M. J. Smith, & G. Salvendy (Eds.), Human Interface, Part II, HCII 2007 (pp. 802−811). Berlin: Springer.

Warkentin, M., D. Gefen, P.A. Pavlou, M.G. Rose, *Encouraging citizen adoption of e-government by building trust*, 2002:

Weber, Max (1978) Economy and society. Berkeley: University of California Press.

Wright, D. (2011) Should PIA's be mandatory? *Communications of the ACM*, Vol. 54, No. 8, August 2011

Wright, D. and de Hert, P., *Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy*, Springer, Dordrecht, 2012 (nog te verschijnen)

WRR (2011) *iOverheid*. Nr. 86. Amsterdam University Press.

Yang, P. (2007) *Government Behaviour and Trust: The Case of China. Cato Journal,* 27(3), 359-372.

Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. Journal of Interactive Marketing, 16(2), 47–63.

Bijlage 1 – Programma focusgroepen

1. Gebruik, vertrouwen & acceptatie online overheidsdiensten

Per deelnemer formulier met aantal vragen en de opdracht om deze in te vullen (zie bijlage).
Groepsdiscussie om uitslag, opinies en achterliggende redeneringen te bespreken.

Individuele vragen:

- Hoe vaak heeft u in het afgelopen jaar gebruik gemaakt van één of meerder online diensten van onderstaande overheidsinstanties?
- Hoeveel vertrouwen heeft u in onderstaande instanties en waarom?

Groepsdiscussie:

- Maakt iedereen weleens gebruik van online overheidsdiensten? Wie niet?
- Wat zijn (positieve en negatieve) ervaringen met de gebruikte diensten? *Moderators: eventueel voorleggen: reputatie, snelheid, toegankelijkheid, onbekendheid, begrijpelijkheid, vertrouwen/betrouwbaarheid, aanwezigheid van privacyverklaringen?*
- Wat zijn de belangrijkste voor- en nadelen van deze diensten?
- Welke diensten vertrouwen jullie wel/niet? Waarom?(Hoe) hebben eerdere ervaringen met online diensten hier een rol in gespeeld?
- Als je kijkt naar online diensten in het algemeen (ook webshoppen, internetbankieren): Waardoor raken jullie vertrouwen kwijt in een online dienst? En waardoor zou je meer vertrouwen krijgen?

2. Betrouwbaarheid & online privacy

Per deelnemer formulier met aantal vragen en de opdracht om deze in te vullen (zie bijlage).
Groepsdiscussie om uitslag en opinies te bespreken.

Individuele stellingen:

- Ik let op de aanwezigheid van een privacyverklaring als ik gebruik maak van een online dienst van de overheid
- Ik let op de aanwezigheid van een beveiligde (https) verbinding
- Wanneer ik bepaalde gegevens moet invullen bij een online overheidsdienst, is het is mij duidelijk hoe de overheid omgaat met deze gegevens (bijvoorbeeld waar de overheid deze gegevens voor gebruikt, waar de gegevens worden opgeslagen of met wie (welke andere instanties) de gegevens worden gedeeld)?
- Als u (enigszins) weet hoe de overheid omgaat met uw gegevens: kunt u aangeven waar u deze kennis heeft opgedaan (bijvoorbeeld online, in een folder, van iemand gehoord, ...)?
- Onder privacy op internet versta ik ……..
- Op internet maak ik me geen zorgen over mijn privacy
- Mijn persoonlijke gegevens zijn veilig bij de overheid
- Ik denk dat de wet mijn privacy voldoende beschermd

Groepsdiscussie:

- Kunt u bepaalde risico's noemen van online dienstverlening met het oog op de veiligheid?
  Maakt u zich zorgen over deze risico's?
  Weet u hoe de overheid omgaat met de bescherming tegen deze risico's?
  Maakt ze hierbij gebruik van technologie? Om wat te doen? Is dat voldoende?
- Wat verstaan jullie onder privacy? Wat is belangrijk/noodzakelijk voor de overheid om persoonlijke gegevens te beschermen?

Moderators: Eventueel voorbeelden geven van privacy-aspecten op internet (als groep niet met antwoorden komt)

3. Privacy by Design

Groepsdiscussie met behulp ppt-slides en vignetten (voorbeeldcase: security scanner)

Groepsdiscussie:

- Hebben jullie weleens gehoord van Privacy by Design?
- Wat denken jullie dat het zou kunnen betekenen?

Moderator: uitleg over Privacy by Design, aan de hand van voorbeelden/vignetten (zie bijlage)

Privacy by Design is een manier om al bij het ontwerp van een nieuwe dienst of informatiesysteem na te denken over mogelijke privacyrisico's. Het probeert ook deze risico's zoveel mogelijk te vermijden of te verkleinen. Dit gebeurt op 3 manieren:

1. Risicobeoordelingen: voor het ontwerp wordt onderzoek gedaan naar de mogelijke risico's. De analyse kijkt ook naar hoe deze risico's vermeden kunnen worden, bijvoorbeeld door bepaalde technologie te gebruiken. [voorbeeld]
2. Verantwoordelijkheden: In de organisatie die de dienst aanbiedt, wordt gekeken hoe de verwerking van gegevens geregeld is en wie waarvoor verantwoordelijk is en daarvoor aanspreekbaar is. [voorbeeld]
3. Technologie: met behulp van technologie wordt gekeken hoe er zo min mogelijke persoonlijke gegevens kunnen worden verzameld, of worden gegevens geanonimiseerd. [voorbeeld]

Vragen groepsdiscussie:

- Wat valt op? Wat vinden jullie wel/niet goed?
  Moderators: eventueel uitvragen: wel/niet opslag gegevens, wel/niet geanonimiseerd, analyse door apparaat/analyse door beveiligingsmedewerker
- Waar voelen jullie het prettigst bij? [mening: nuttig, noodzakelijk, handig, overbodig, veilig, duur…]
- Denken jullie dat dit al gebeurt (wordt toegepast)?
- Wanneer is privacy by design wel/niet nuttig? Bijvoorbeeld bij bepaalde diensten/doelgroepen wel/niet (zoals de overheid, sociale netwerken, internetbankieren)?

4. Privacy by Design: risicobeoordelingen (Privacy Impact Assessments)

Groepsdiscussie met behulp van uitleg en scenario's

Voor moderator: langs de lijnen transparantie en wie PIA uitvoert [openbaar/niet openbaar, CBP/organisatie zelf, aantal risico's, informatie op de website van de overheidsdienst]

Vragen groepsdiscussie:

- Wat valt op na het lezen van de voorbeelden?
- Welk voorbeeld spreekt jullie het meeste aan? Waarom?
- Wat zien jullie als voor- en nadelen van dergelijke beoordelingsrapporten?
- Creëert zo'n beoordelingsrapport / risicobeoordeling wel/geen vertrouwen?
- Maakt het verschil wie de beoordelingsrapport maakt? Wie vinden jullie dat het rapport moet uitvoeren?
- Moet het rapport openbaar zijn? Zouden jullie de rapporten 'in het echt' ook lezen? Waarom wel/niet? Of is het voldoende dát het rapport is uitgevoerd?
- Wanneer zou zo'n beoordeling moeten worden uitgevoerd? Verplicht voor elk systeem? Alleen bij gevoelige gegevens?
- Zou de uitvoering van zo'n beoordeling voor u doorslaggevende reden zijn om gebruik te maken van de dienst?

5. Privacy by Design: Verantwoordelijkheden van de dienstaanbieder

Per deelnemer formulier met aantal vragen en de opdracht om deze in te vullen (zie bijlage).

Groepsdiscussie om uitslag en opinies te bespreken.

Vragen groepsdiscussie:

- Weten jullie dat in de wet een aantal waarborgen staan om uw persoonsgegevens te beschermen? Kunnen jullie er een aantal noemen? [zoals doelbinding, dataminimalisatie, inzage, toestemming, correctie]
- Als jullie adviseur zou zijn bij de overheid over haar online dienstverlening, wat zou je haar adviseren als het gaat om transparantie over gegevensverwerking [en de wettelijke verplichtingen]? Zou je bijvoorbeeld een risicobeoordeling online plaatsen op de website? Hoe zou je omgaan met informatie en toestemming?
- De wet heeft een meldingsplicht opgenomen voor alle geautomatiseerde verwerkingen van persoonsgegevens. Dat betekent dat als uw persoonsgegevens worden gebruikt door een online dienst, deze moeten worden gemeld bij het College Bescherming Persoonsgegevens (CBP) of bij een Functionaris voor de Gegevensbescherming (FG) als die binnen een branche of organisatie benoemd is. Vindt u dat een prettig idee? Stelt u het op prijs een notificatie te ontvangen als uw gegevens worden bewerkt, aan derden worden doorgegeven, verloren zijn gegaan, of zijn veranderd?
- Neemt door deze notificatie het vertrouwen in en de acceptatie van de dienstverlening toe of ziet u juist af van de online dienstverlening en keert u terug naar de offline dienstverlening?
- Hecht u er waarde aan dat een organisatie een privacycertificatie heeft<uitleg/voorbeeld>? Beïnvloedt het werken met een privacy certificatie uw beslissing om gebruik te maken van de online dienstverlening?

- Vinden jullie dat dienstaanbieders nog meer zouden moeten doen? Bijvoorbeeld een directeur aannemen die verantwoordelijk is voor alles wat met privacy en de verwerking van persoonlijke gegevens te maken heeft?

6. Privacy by Design: privacybeschermende technologieën
Groepsdiscussie met behulp van uitleg (ppt-slides) en voorbeelden

Vragen groepsdiscussie:
- Acht u het wenselijk dat overheidsdienstverlening dit soort technieken inzet om uw persoonsgegevens te beschermen? Waarom wel/waarom niet?
- Dit soort technologie is vaak moeilijk te begrijpen en te doorgronden (hoe werkt het precies?). Het is ook niet zichtbaar met het blote oog. Vertrouwt u als zodanig op dit instrument? En vertrouwt u organisaties die zeggen deze technieken te gebruiken? Waarom wel/niet?
- Vergroot het uw vertrouwen als een website zou vermelden dat de website en dienst is ontworpen met privacytechnologie? Bent u dan wel/niet eerder bereid om persoonlijke gegevens af te staan?
- Bent u van mening dat privacytechnologie een zeer belangrijke manier is om privacy op het internet te beschermen? Waarom wel, waarom niet?

7. Specifieke toepassingen van privacybeschermende technologieën
Groepsdiscussie aan de hand van voorbeelden.

Vragen groepsdiscussie voorbeeld:
- Stel Nederland introduceert eveneens dit systeem. Zou u deze kaart willen aanschaffen? Waarom wel, waarom niet? Wat geeft de doorslag?
- Denkt u dat deze kaart meer of minder bescherming van uw privacy biedt dan het huidige systeem? Waar komt dat door?
- Vertrouwt u erop dat alleen u zeggenschap heeft over wie toegang heeft tot de gegevens die op de kaart staan en de overdracht van gegevens? Bijvoorbeeld als u naar een medisch specialist gaat en u hem/haar toestemming geeft om alleen die gegevens te zien die relevant zijn voor de behandeling die u moet ondergaan?
- Stel er wordt een biometrische component (zoals digitale gezichtsherkenning of digitale vingerafdrukken) toegevoegd om toegang te krijgen. Vergroot of verkleint dat uw vertrouwen in de kaart?

Slotvraag:
- Denk u dat toekomstige technologische ontwikkelingen de veiligheid en bescherming van uw persoonsgegevens in gevaar kunnen brengen? Waaraan denkt u dan?

Bijlage 2 - Vragenlijsten

1. Gebruik, vertrouwen en acceptatie online diensten

Hieronder staan stellingen en vragen over uw gebruik van online diensten en de betrouwbaarheid daarvan. U krijgt vijf minuten om het formulier in te vullen. Hierna zullen we de vragen en stellingen met de groep bespreken.

1. Hoe vaak heeft u in afgelopen jaar (ongeveer) gebruik gemaakt van een of meerdere online diensten van onderstaande overheidsinstanties?								
Kruis het vakje aan dat de situatie het best weergeeft. Het meest linkervakje [1] betekent dat u het afgelopen jaar geen gebruik heeft gemaakt van online diensten van deze organisatie, het meest rechtervakje [5] betekent dat u het afgelopen jaar vaak gebruik heeft gemaakt van online diensten van deze organisatie.								
Gemeente(loket) – denk aan registratie geboorte, trouwen, overlijden, verhuizing, aanvraag vergunningen (verbouwen, parkeren), identiteitsbewijs, rijbewijs, uittreksel GBA	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker 0**
Kadaster – denk aan kadastrale kaart, koopjaar huis/vastgoed, grootte huis/vastgoedobject, koopsom, eigenaar	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker 0**
Belastingdienst – denk aan belastingaangifte, autobelasting, woning, eigendom en vermogen, toeslagen (huur, zorg)	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker 0**
UWV (Uitvoeringsinstituut Werknemersverzekeringen) – denk aan aanvragen uitkering (werkloosheid, ziekte, arbeidsongeschiktheid)	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker 0**
DUO - Informatie Beheer Groep – denk aanvragen/stopzetten studiefinanciering, ov-chipkaart aanvragen/stopzetten	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker 0**

(*Indien van toepassing*) **Een andere overheidsdienst die ik online bezoek is: .....**	**Geen ervaring met online dienst**	**0**	**0**	**0**	**0**	**0**	**Veel ervaring met online dienst**	**Weet niet zeker** **0**

2. In hoeverre vertrouwt u erop dat er bij de online diensten van de onderstaande organisaties zorgvuldig omgegaan wordt met uw persoonsgegevens*, en waarom?

***Persoonsgegevens geven informatie over een bepaald persoon. U kunt hierbij denken aan naam en adres, maar ook aan IQ, politieke voorkeur, gezondheid en financiële situatie.**

Kruis het vakje aan dat de situatie het best weergeeft. Het meest linkervakje [1] betekent dat geen vertrouwen heeft in de online diensten van deze organisatie, het meest rechtervakje [5] betekent dat u veel vertrouwen heeft in de online diensten van deze organisatie.

Overheidsorganisaties (algemeen)	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden:							
Belastingdienst	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden:							
UWV (Uitvoeringsinstituut Werknemersverzekeringen)	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden:							
DUO - Informatie Beheer Groep	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden:							

……							
Internetbankieren	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden: **.....** **.....** **……** **……**							
Internetwinkelen (bv. bol.com, wehkamp.nl, ...)	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden: **.....** **.....** **……** **……**							
Sociale media (bv. Hyves, LinkedIn, Facebook)	**Geen vertrouwen**	**0**	**0**	**0**	**0**	**0**	**Veel vertrouwen**
Reden: **.....** **.....** **……** **……**							

2. Risico's van online diensten

Hieronder staan stellingen over risico's van online diensten. U krijgt vijf minuten om het formulier in te vullen. Hierna zullen we de vragen en stellingen met de groep bespreken.

Stelling 1: Ik let op de aanwezigheid van een privacyverklaring als ik gebruik maak van een online dienst van de overheid						
Kruis het vakje aan dat de situatie het best weergeeft. Het meest linker vakje betekent dat u nooit op de aanwezigheid van een beveiligde verbinding let, het meest rechter vakje betekent dat u dit altijd doet.						
Nooit	**0**	**0**	**0**	**0**	**0**	**Altijd**
Kruis het vakje aan dat de situatie het best weergeeft. Het meest linker vakje betekent dat u nooit op de aanwezigheid van een privacyverklaring let, het meest rechter vakje betekent dat u dit altijd doet.						
Waarom wel/niet? **.....** **.....** **……** **……..**						
Stelling 2: Ik let op de aanwezigheid van een beveiligde (https) verbinding						
Kruis het vakje aan dat de situatie het best weergeeft. Het meest linker vakje betekent dat u nooit op de aanwezigheid van een beveiligde verbinding let, het meest rechter vakje betekent dat u dit altijd doet.						
Nooit	**0**	**0**	**0**	**0**	**0**	**Altijd**
Waarom wel/niet? **.....** **.....** **……** **……..**						
Stelling 3: Wanneer ik bepaalde gegevens moet invullen bij een online overheidsdienst, is het is mij duidelijk hoe de overheid omgaat met deze gegevens (bijvoorbeeld waar de overheid deze gegevens voor gebruikt, waar de gegevens worden opgeslagen of met wie (welke andere instanties) de gegevens worden gedeeld)						
Kruis het vakje aan dat de situatie het best weergeeft. Het meest linker vakje betekent dat u nooit op de aanwezigheid van een beveiligde verbinding let, het meest rechter vakje betekent dat u dit altijd doet.						
Nooit	**0**	**0**	**0**	**0**	**0**	**Altijd**
Als u (enigszins) weet hoe de overheid omgaat met uw gegevens: kunt u aangeven waar u deze kennis heeft opgedaan (bijvoorbeeld online, in een folder, van iemand gehoord, ...)? **.....** **.....** **……** **……..**						

Er zijn op dit moment veel discussies gaande over online privacy in relatie tot nieuwe technologische ontwikkelingen (denk bijvoorbeeld aan sociale netwerken, OV-chipkaart, Elektronisch Patienten Dossier of het biometrisch paspoort). Hierbij is vaak de vraag wat privacy nu eigenlijk inhoudt. Wat betekent online privacy voor u?

Vul op de puntjes kort in wat u onder online privacy verstaat.

Stelling 4: Onder online privacy versta ik:

.....
.....
……
……..

……
……..

Stelling 5: Ik maak me geen zorgen over mijn privacy op internet

Kruis het vakje aan dat uw mening het best weergeeft. Het meest linkervakje betekent dat u het helemaal oneens bent met de stelling, het meest rechtervakje betekent dat u het helemaal eens bent met de stelling.

Helemaal mee oneens	**0**	**0**	**0**	**0**	**0**	**Helemaal mee eens**

Waarom wel/niet?

.....
.....
……
……..

……
……..

Stelling 6: Mijn persoonlijke gegevens zijn veilig bij de overheid

Kruis het vakje aan dat uw mening het best weergeeft. Het meest linkervakje betekent dat u het helemaal oneens bent met de stelling, het meest rechtervakje betekent dat u het helemaal eens bent met de stelling.

Helemaal mee oneens	**0**	**0**	**0**	**0**	**0**	**Helemaal mee eens**

Waarom wel/niet?

.....
.....
……
……..

……
……..

3. Privacy by design

Hieronder worden twee situaties beschreven die over dezelfde toepassing gaan: de security scanner. Dit apparaat wordt ingezet op vliegvelden om passagiers te scannen op mogelijk gevaarlijke stoffen en wapens. Lees onderstaande verhalen zorgvuldig door. U krijgt hiervoor 5 minuten. Probeer u in te leven in de situatie en bedenk wat u van de beschreven situaties vindt. Hierna zullen we de verhalen in de groep bespreken.

Situatie 1.	**Situatie 2.**
Bas werkt als beveiligingsmedewerker op Schiphol. Hij controleert met behulp van de security scanner passagiers op de aanwezigheid van mogelijk gevaarlijke of verboden stoffen, producten en wapens. Bas begeleidt passagiers naar de scanners. Als een passagier in de scanner staat, ziet Bas binnen twee seconden 3D-beelden waarop het lichaam van de passagier te zien is (zoals te zien is op de afbeelding). Hij ziet precies de lichaamscontouren van de passagier en kan op de 3D-beelden zien of de passagier gevaarlijke of verboden producten bij zich draagt. Het beeld staat zo dat de passagier de scan ook ziet. Als Bas iets verdachts ziet in de scan, fouilleert hij de passagier. Als hij niks verdachts ziet in de scan, laat Bas de passagier doorlopen.	Ook Anna is beveiligingsmedewerker op Schiphol en ook zij controleert passagiers met behulp van een security scanner. Ze werkt met een nieuw type scanner, die is ontworpen op basis van een vooraf uitgevoerde analyse van privacyrisico's. Anna begeleidt de passagiers naar de scanner, waar binnen twee seconden een scan wordt gemaakt. Anna en de passagier kunnen de scan zelf niet zien. Als er een verdacht voorwerp wordt gedetecteerd op de scan, krijgt Anna een signaal. De scanner toont Anna dan een standaardpoppetje (zoals te zien op de afbeelding) met de plaats van het mogelijk verdachte voorwerp. Anna kan dan de passagier fouilleren. Op de scanner zit een sticker, waarop de passagier kan zien wie hij kan bellen als hij klachten heeft over de scanprocedure.

4.Risicobeoordelingen: privacy impact assessment

Hieronder staan drie mogelijke situaties over het uitvoeren van risicobeoordelingen. U krijgt 10 minuten om de situaties door te lezen. Probeer u in te leven in de situatie en bedenk wat u van de beschreven situaties vindt, wat valt u op, wat vindt u wel of niet goed? Hierna zullen we de verhalen in de groep bespreken.

Situatie 1.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan tien privacyrisico's, waarvan twee als zeer ernstig beoordeeld zijn. De ontwikkelaars hebben het ontwerp van de online overheidsdienst op basis van de geïdentificeerde risico's aangepast zodat de privacyrisico's zijn verkleind. Het rapport waarin de privacyrisico's worden beschreven, is openbaar gemaakt.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de gebruiker kort gewezen worden op het onderzoek.

Situatie 2.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan twintig privacyrisico's en oplossingen om deze risico's te verkleinen. De ontwikkelaars hebben het ontwerp van de online overheidsdienst volgens de suggesties in het rapport aangepast zodat de privacyrisico's zijn verkleind. Het rapport waarin de privacyrisico's en de oplossingen worden beschreven, is openbaar gemaakt.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de burger gewezen worden op het onderzoek en de gemaakte aanpassingen, met een link naar het rapport. Ook de algemene informatie over hoe de instantie om zal gaan met de gegevens die van burgers verzameld worden, staat op de homepage vermeld.

Situatie 3.
Er is onderzoek gedaan naar de introductie van een nieuwe online overheidsdienst. In het onderzoeksrapport staan vijftien privacyrisico's, waarvan één als zeer ernstig is beoordeeld. De ontwikkelaars hebben het ontwerp van de online overheidsdienst volgens de suggesties in het rapport aangepast zodat de privacyrisico's zijn verkleind. Het rapport, waarin de privacyrisico's worden beschreven en oplossingen voor de risico's worden aangedragen, is niet openbaar.

De dienst wordt volgende week gelanceerd. Op de homepage van de dienst zal de gebruiker kort gewezen worden op het onderzoek.

5. Privacy by Design: Verantwoordelijkheden van de dienstaanbieder

Hieronder staan vragen over uw gebruik en de betrouwbaarheid van online diensten. U krijgt vijf minuten om ze te beantwoorden. Hierna zullen we de vragen met de groep bespreken.

Vraag 1: In de wet staat een aantal waarborgen om uw persoonsgegevens te beschermen. Deze waarborgen geven u als het ware de garantie dat de online diensten uw privacy niet schenden en dat dienstaanbieders dus zorgvuldig met uw persoonsgegevens omgaan. Bent u daarvan op de hoogte? Omcirkel wat van toepassing is. **Ja / Nee**
Vraag 2: In de wet staat bijvoorbeeld dat voor de verwerking van persoonsgegevens degene om wie het gaat om toestemming moet worden gevraagd. Gebeurt dit volgens u voldoende? Omcirkel wat van toepassing is. **Ja / Nee**
Vraag 3: Zou u vertrouwen in de dienstverlenende instantie wel/niet toenemen als u vaker wordt geïnformeerd, om toestemming wordt gevraagd en/of als u de mogelijkheid krijgt om uw toestemming weer in te trekken? Omcirkel wat van toepassing is. **Ja / Nee**
Vraag 4: Wat doet u als u om meer informatie (persoonlijke gegevens) wordt gevraagd dan nodig lijkt? Weet u bij wie u dan moet aankloppen? Heeft u dit weleens gedaan? Waarom wel/niet? .... …… …….. .... …… ……
Vraag 5: Weet u wie u bij de overheid moet aanspreken wanneer u informatie wilt over het beheer van uw gegevens, als u deze wilt raadplegen of verifiëren? Heeft u dit wel eens gedaan? Waarom wel/niet? .... …… …….. .... …… ……