

Andersson Elffers Felix

**Media-analyse
Identiteitsmanagement
Eindrapport**

Utrecht, 17 december 2013
GB154/eindrapport identiteitsmanagement



Inhoud

1	Samenvatting	3
1.1	Bevindingen	4
1.2	Beschouwing op landsniveau	4
1.3	Suggesties voor verdere ontwikkeling van het debat over ID-management	5
2	Inleiding	7
2.1	Aanleiding onderzoek	7
2.2	Vraagstelling	8
2.3	Afbakening	8
2.4	Methodologie en aanpak	8
2.5	Leeswijzer	9
3	Analyse kernonderwerpen	10
3.1	Identiteitsfraude	10
3.2	eID	14
3.3	Biometrisch paspoort	16
4	Analyse ondersteunende onderwerpen	21
4.1	NSA/PRISM	21
4.2	Behavioral profiling	24
4.3	Elektronisch patiëntendossier	27
4.4	Slimme meter	30
4.5	Passagiersgegevens	34
5	Samenvatting per onderwerp	38
5.1	Kernonderwerpen: ID-management	38
5.2	Ondersteunende onderwerpen	38
6	Beschouwing per land	40
6.1	Nederland	40
6.2	Duitsland	40
6.3	Spanje	40
6.4	Groot-Brittannië	41
6.5	Zweden	41
6.6	Vlaanderen	41
7	Suggesties	42
7.1	Kritische houding en evenwichtig debat	42
7.2	Regionale aanpak kan debat nuanceren	43
7.3	Radicale openheid voor meer vertrouwen	43
7.4	Schaalvoordelen door integrale visie	43
7.5	Publiek-private samenwerking	44
7.6	Doorontwikkeling eID	44
8	Bijlagen	45
8.1	Onderzoeksvragen	46
8.2	Methode onderzoek	47
8.3	Expertlijst	51
8.4	Data	52

1 Samenvatting

In de huidige genetwerkte en gedigitaliseerde samenleving is identificatie van groot belang. Veel dagelijkse handelingen van Nederlandse burgers zijn gekoppeld aan identiteitsgegevens, zoals pinbetalingen, mobiel bellen, internetten en reizen met het openbaar vervoer. Hiermee ontstaat de noodzaak identiteitsgegevens verantwoord te beheren.

Dit rapport bespreekt de stand van zaken op het gebied van identiteitsmanagement, of ID-management in een aantal Europese landen, waaronder Nederland. Identiteitsmanagement heeft betrekking op hoe individuen, overheden en private partijen identiteitsgegevens beheren. Bij het beheren en beveiligen van identiteitsgegevens hebben deze partijen verschillende belangen en verantwoordelijkheden en moeten ze zich tot elkaar verhouden. De manier waarop deze relatie wordt ingevuld kan onderwerp van discussie zijn. De NSA affaire die zich op dit moment ontwikkelt toont de urgentie van deze discussie aan: wat is de verantwoordelijkheid van de overheid in het beheren van identiteitsgegevens van burgers? In hoeverre moet de private sector hierbij toegelaten worden? Hoe zelfredzaam kunnen burgers geacht worden te zijn in het beschermen van hun eigen identiteitsgegevens?

Het onderzoek dat ten grondslag ligt aan dit rapport is door Andersson Elffers Felix (AEF) uitgevoerd voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, in het kader van het interdepartementale programma 'identiteit op orde.' Om de maatschappelijke discussie over ID-management te doorgronden heeft het ministerie van BZK AEF gevraagd een media-analyse uit te voeren over hoe de discussie over ID-management in Nederland en een vijftal andere Europese landen is gevoerd vanuit de perspectieven van techniek, privacy, vertrouwen en veiligheid. In dit rapport presenteert AEF haar bevindingen.

In de vormgeving van dit onderzoek is onderscheid gemaakt tussen een aantal 'kernonderwerpen' die direct gerelateerd zijn met ID management, en een aantal 'ondersteunende' onderwerpen die van belang zijn in het duiden van ontwikkelingen in ID management:

- Kernonderwerpen over ID-management:
 - Identiteitsfraude
 - Het elektronisch identiteitsbewijs (de eID)
 - Het biometrische paspoort
- Ondersteunende onderwerpen
 - Het NSA schandaal
 - 'Behavioral profiling,' het in kaart brengen van online handelingen van burgers door de private sector
 - Het elektronisch patiëntendossier
 - De slimme energiemeter
 - Het opslaan en delen van passagiersgegevens door overheden.

Deze onderwerpen hebben de afgelopen jaren tot maatschappelijke discussie geleid in de onderzochte landen. Door een vergelijkende analyse van de media in de verschillende landen kan het discours in Nederland beter geduid worden.

1.1 Bevindingen

Op het gebied van de kern- en ondersteunende onderwerpen heeft het onderzoek geleid tot de volgende bevindingen:

- **Kernonderwerpen: ID-management**
 - **Identiteitsfraude** is nadrukkelijk in Nederland en Groot-Brittannië onderwerp van discussie. Waar in Nederland de overheid zich vooral met het strafbaar stellen van identiteitsfraude bezighoudt, richten andere landen zich meer op preventie en eigen verantwoordelijkheid van burgers.
 - Wat betreft de **eID** loopt Nederland achter bij Vlaanderen, Duitsland, Zweden en Spanje. Over het algemeen wordt de eID echter weinig gebruikt in deze landen.
 - Vergeleken met andere landen lijkt het Nederlandse debat over het **biometrisch paspoort** een meer principiële insteek te hebben, gericht op vermeende privacy-schendingen. In het buitenland wordt over het algemeen pragmatischer omgegaan met biometrie. Deze pragmatische houding staat een kritisch debat over de verhouding tussen privacy en veiligheid overigens niet in de weg.
- **Ondersteunende onderwerpen**
 - Het debat over de afluisterpraktijken van de **NSA** kent de grootste nationale verschillen. Dit houdt verband met de verschillende manier waarop de landen al dan niet in eigen persoon met de afluisterpraktijken geconfronteerd werden.
 - Op het gebied van **behavioral profiling** wordt het debat in Nederland eenzijdig negatief gevoerd. In andere landen is er meer ruimte voor de positie van internetbedrijven en hun belangen, en hoe behavioral profiling onderdeel is van functioneel internetgebruik.
 - Wat betreft het **elektronisch patiëntendossier** is er in Nederland bovengemiddeld veel aandacht voor privacy in het debat. In Duitsland speelt dataveiligheid een belangrijker rol, terwijl landen als Vlaanderen, Zweden en Spanje meer aandacht besteden aan de technologische vooruitgang die gepaard gaat met een elektronisch patiëntendossier.
 - De **slimme energiemeter** is door het felle privacydebat in Nederland minder snel ingevoerd dan in de andere onderzochte landen. Tegelijkertijd blijkt dat in de landen waar slimme meters wel grootschalig ingevoerd zijn, de toegevoegde waarde van dergelijke meters voor energiebeapring in de praktijk tegenvalt.
 - Het debat over de **overdracht van passagiersgegevens** speelt zich af op het snijvlak tussen staatsveiligheid en privacy van individuele burgers. In Groot-Brittannië lijkt staatsveiligheid in dit debat de overhand te hebben, terwijl in Nederland en Duitsland vooral het privacy-aspect van deze afweging aan bod is gekomen. De overige onderzochte landen staan op een gelaten manier in dit debat.

1.2 Beschouwing op landsniveau

De volgende stap in het onderzoek is het doortrekken van deze bevindingen naar een horizontale beschouwing op landsniveau, waarin uiteengezet wordt hoe de uitkomsten van het onderzoek zich verhouden tot culturele en socio-economische verschillen tussen landen.

- **Nederland**

In Nederland is **privacy de meest nadrukkelijke kernwaarde** in (vrijwel) elke maatschappelijke discussie omtrent ID-management. Iedere ontwikkeling die gepaard gaat met identiteit en technologische vooruitgang wordt direct aan het schenden van privacy gekoppeld. Echter, deze principiële aandacht voor privacy wordt te weinig geconcretiseerd. Dit maakt privacy in het Nederlandse debat **een relatief ongedefinieerd begrip**, wat een meer inhoudelijke discussie op het snijvlak van privacy, veiligheid, technologische vooruitgang en vertrouwen in de weg lijkt te zitten.

- **Duitsland**

In Duitsland lijkt van de onderzochte landen de meeste ruimte te zijn voor **een inhoudelijk maatschappelijk debat** over ID-management. Binnen de gebieden van privacy, veiligheid, technologische vooruitgang en vertrouwen is er zowel in de media als onder burgers in Duitsland sprake van een **grote maatschappelijke betrokkenheid en inhoudelijke kennis**. De media faciliteren het forum waarop de inhoudelijke discussie plaatsvindt.

- **Spanje**

De maatschappelijke houding ten opzichte van ID-management in Spanje lijkt enigszins **afwachtend** te zijn. Over het algemeen is er in berichtgeving vooral aandacht voor **technologische vooruitgang** en de **rol van de private sector** op het gebied van ID-management. Deze nadruk op technologie en het bedrijfsleven lijkt echter ook gebonden te zijn aan de politieke oriëntatie van media en deskundigen.

- **Groot-Brittannië**

In Groot-Brittannië staat **de overheid nadrukkelijk op afstand** wanneer het gaat om het beschermen van identiteitsgegevens van burgers. Dit wordt met name aan de private sector gelaten. Daarnaast is de overheid een stuk actiever in **het beschermen van (nationale) veiligheid ten koste van privacy en zelfbeschikking** van burgers. Ook kenmerkt het Britse maatschappelijk debat zich door een **cynische houding** ten opzichte van de overheid in het faciliteren van ID-management, wat een inhoudelijke discussie over nut en noodzaak in de weg staat.

- **Zweden**

Opvallend aan Zweden is, dat identiteitsmanagement in verhouding **weinig aanleiding voor publieke discussie** is. Het Zweedse principe van **radicale openheid vanuit de overheid** lijkt voor minder achterdocht te zorgen in de Zweedse samenleving. Omdat de overheid veel informatie aan burgers geeft, is het voor burgers ook makkelijk om veel persoonlijke informatie aan de overheid toe te vertrouwen.

- **Vlaanderen**

In Vlaanderen worden debatten op het gebied van identiteitsmanagement relatief nuchter gevoerd. Over het algemeen is er veel aandacht voor de technologische vooruitgang, en blijven kritische geluiden vanuit bijvoorbeeld een privacy-perspectief achterwege. Wat daarnaast opvalt is de succesvolle integrale aanpak die in Vlaanderen nagestreefd wordt in het faciliteren van ID-management. Ten slotte heeft de verregaande regionalisering van openbaar bestuur in Vlaanderen als gevolg dat de implementatie van ID-management projecten ook een regionaal plaatsvindt, waardoor nationale debatten een genuanceerd karakter hebben.

1.3 **Suggesties voor verdere ontwikkeling van het debat over ID-management**

Deze suggesties zijn geformuleerd in de vorm van prikkelende stellingen die de afzonderlijke bevindingen van dit onderzoek overstijgen. Met deze suggesties wordt beoogd discussie op gang te brengen binnen beleidskringen, over hoe het maatschappelijke debat omtrent ID management in Nederland zich constructief verder zou kunnen ontwikkelen.

- **Een kritische houding ten opzichte van ID-management hoeft een evenwichtig debat niet in de weg te staan.**

De staat van het maatschappelijke debat in Duitsland toont aan dat het mogelijk is om een genuanceerd en afgewogen discussie te voeren over ontwikkelingen in ID-management. In een dergelijk stelsel bieden de media een forum waar verschillende belangen en meningen

samenkomen, en waar burgers zich kunnen laten informeren over onderwerpen op het spectrum van privacy, veiligheid, technologische vooruitgang en vertrouwen in overheid en private sector. Hier kan dan nog steeds een kritische houding uit voortkomen, maar dit is dan wel een kritische houding vanuit een goed geïnformeerd perspectief.

- **Een regionale implementatie van ID-managementprojecten kan een nuancerend effect op nationale debatten hebben.**

Uit de ervaringen in Vlaanderen blijkt dat een regionale implementatie van ID-managementprojecten de angel haalt uit principiële debatten op nationaal niveau. Regionale implementatie voorkomt niet dat er controverses ontstaan, maar de afhandeling van dergelijke controverses kan dicht bij de burger plaatsvinden. Het Nederlandse bestuurlijke systeem is minder verregaand geregionaliseerd dan het geval is in Vlaanderen. Dit wil echter niet zeggen dat het onmogelijk is om bijvoorbeeld gemeenten meer ruimte en vrijheid te geven bij de invoering van toekomstige toepassingen van ID-management.

- **Radicale openheid van informatie kan een succesvolle strategie zijn om meer vertrouwen in de overheid te wekken bij het ontwikkelen van ID-managementprojecten voor burgers.**

Vertrouwen werkt twee kanten op, zo toont Zweden aan: een overheid die verwacht dat de gemiddelde burger niets te verbergen heeft, komt geloofwaardiger over wanneer zij als overheid zelf te kennen geeft niets te verbergen te hebben. Openheid van zaken vanuit de overheid wekt vertrouwen onder burgers.

- **Een integrale visie op ID-management die verder gaat dan afzonderlijke thema's kan voor schaalvoordelen zorgen.**

ID-management lijkt in Nederland versnipperd te zijn geraakt over een verscheidenheid aan dossiers. Discussies over het elektronisch patiëntendossier, slimme meters, het biometrisch paspoort en identiteitsfraude zijn in bepaalde mate een herhaling van zetten. Het is echter wel degelijk mogelijk om een meer integrale aanpak na te streven, waarin verschillende dossiers aan elkaar gekoppeld kunnen worden. Het is onwenselijk wanneer ID-management in de perceptie van burgers vooral bekend staat als een middel van de overheid om zo veel mogelijk persoonsgegevens op te slaan, en die teneur heeft het debat in Nederland op dit moment wel.

- **Succesvolle publiek-private samenwerking is belangrijk om ID-management onder burgers te stimuleren.**

Succesvol gebruik van ID-management in de dagelijks praktijk lijkt voor een groot gedeelte afhankelijk te zijn van in hoeverre de private sector aangesloten is aan ontwikkelingen. Wanneer burgers weinig praktische toepasbaarheid zien van een dergelijk ID-management systeem, dan zal gebruik in de praktijk tegenvallen. Deze stelling kan onderschreven worden door ervaringen in Duitsland en Spanje, waar technisch goed functionerende ID-managementprojecten door achterblijvend gebruik nu als mislukt beschouwd worden.

- **Bij het doorontwikkelen van de eID in Nederland liggen veel kansen voor een succesvolle implementatie.**

Vrijwel alle bovenstaande suggesties kunnen toegepast worden op de ontwikkeling van de eID in Nederland. Voor veel Nederlandse burgers is de eID nog een onbekend begrip. Daarom is er nu nog in verregaande mate de mogelijkheid voor de overheid om initiatief te nemen tot het invoeren van de eID die succesvolle implementatie nastreeft.

2 Inleiding

2.1 Aanleiding onderzoek

Identiteitsmanagement, of ID-management, heeft betrekking op hoe individuen, overheden en private partijen omgaan met identiteitsgegevens. In de netwerksamenleving waarin we leven worden identiteitsgegevens op grote schaal opgevraagd, verwerkt en uitgewisseld. Of het nu gaat om internetbankieren, een vlucht boeken, een ziekenhuis bezoeken of simpelweg browsen op het internet, communicatie van (digitale) identiteitsgegevens speelt een rol om al deze handelingen te faciliteren.

Identiteitsgegevens worden voor veiligheidsdoeleinden gebruikt, maar kunnen ook verhandeld worden of toegepast voor illegale praktijken. Binnen dit spectrum wordt het beheren van identiteitsgegevens noodzakelijk, zodat burgers controle kunnen houden over hun eigen identiteit. Hier hebben zowel overheden als burgers zelf een verantwoordelijkheid, en de verhouding van overheid en individu in deze verantwoordelijkheid kan onderwerp van discussie zijn.

Maatschappelijke discussies over ID-management kunnen zich toespitsen op vele gebieden. Het aan het licht komen van het NSA schandaal, heeft recentelijk bijvoorbeeld tot ophef geleid over het op grote schaal bespioneren van burgers wereldwijd, en de onmacht van burgers om hun identiteitsgegevens te beschermen. Media in binnen- en buitenland berichten bijna dagelijks over hoe technologische ontwikkelingen zich verhouden tot identiteit, privacy, veiligheid, vrijheid en vertrouwen in de overheid en private sector. Wat begon met de discussies omtrent de uitwisseling van passagiersgegevens bij intercontinentale vluchten tussen Europa en de Verenigde Staten is inmiddels een breed discours geworden met onderwerpen als het biometrisch paspoort, het elektronisch patiëntendossier, identiteitsfraude, behavioral profiling, et cetera.

Binnen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is er eveneens aandacht voor het onderwerp van ID-management. Een van de relevante activiteiten op dit gebied is het interdepartementale programma 'Identiteit op Orde' waarbij het ministerie samenwerkt met het ministerie van Veiligheid en Justitie aan een integrale visie op identiteitsmanagement.¹

Om de maatschappelijke discussie over ID-management te doorgronden heeft BZK Andersson Elffers Felix (AEF) gevraagd een media-analyse uit te voeren over hoe de discussie over ID-management in Nederland en een vijftal andere Europese landen is gevoerd vanuit de perspectieven van techniek, privacy, vertrouwen en veiligheid. In dit rapport presenteert AEF de bevindingen van dit onderzoek.

¹ Mobiele identificatie, zelfbeschikking en gecontroleerde koppeling van gegevens een visie op Identiteit in 2025 en vier pijlers voor identiteitsbeleid.

2.2 Vraagstelling

De vraagstelling van de verkenning luidt: Hoe ziet het politieke en maatschappelijke discours op het terrein van techniek, privacy, vrijheid, vertrouwen en veiligheid met betrekking tot ID-management in Nederland en verschillende andere landen er uit sinds 2001?

Deze centrale vraagstelling heeft u verder onderverdeeld in een aantal sub-vragen. Deze sub-vragen vallen uiteen in de volgende drie clusters:

- Duiding media-analyse (argumenten, maatschappelijke gebeurtenissen, relevante culturele achtergronden)
- Rol stakeholders (burger, private partijen, overheid)
- Vertaling nationale discourses in concrete maatregelen en beleid en lessen voor Nederland.²

2.3 Afbakening

Voor de afbakening van de verkenning is het belangrijk stil te staan bij het doel van de verkenning, de doorlooptijd en de keuze van landen voor de casestudies.

Het doel van de verkenning is om op hoofdlijnen het discours over ID-management in Nederland en vijf andere landen te schetsen. Dit ter voorbereiding en ondersteuning van het debat zoals dit in de Tweede Kamer en in de media gevoerd zal worden. Naast Nederland werden in overleg met de opdrachtgever de volgende vier landen gekozen, en een landsdeel: Duitsland, Spanje, Engeland, Zweden en Vlaanderen. Hierbij gaat het om landen die qua discours en beleid voldoende aanknopingspunten bieden voor Nederland. Dit betekent echter niet dat de bevindingen één-op-één op Nederland van toepassing zijn, maar naar de Nederlandse context vertaald moeten worden.

De verkenning kende een korte doorlooptijd. Binnen twee maanden moesten voor de zes gekozen landen casestudies opgesteld worden over de breedte van het onderwerp ID-management, terugkijkend op de laatste 10 jaar.

Het doel van de verkenning, in combinatie met het korte tijdsframe, drukt een belangrijke stempel op de onderzoekscontext, met name wat betreft het belang van diversiteit aan bevindingen en het contextualiseren van de resultaten. Het gaat niet om het extraheren van argumenten, overwegingen en sentimenten maar om het in kaart brengen hiervan tegen de achtergrond van relevante culturele, historische en economische omstandigheden.

2.4 Methodologie en aanpak

De media-analyse werd geoperationaliseerd door middel van een longlist en een shortlist van relevante onderwerpen op het gebied van identiteitsmanagement. In de offerte had AEF een longlist opgenomen bestaande uit twaalf onderwerpen met betrekking tot ID-management, die in de laatste jaren in de internationale media uitvoerig besproken zijn. Aan het begin van het project werd deze longlist in overleg met de opdrachtgever teruggebracht tot een shortlist met acht onderwerpen. Hierin is geprobeerd een evenwichtige keuze van onderwerpen te maken met een goede verdeling tussen de

² Zie bijlage voor alle sub-vragen.

kernwaarden technologie, privacy, vrijheid, vertrouwen en veiligheid. Daarnaast is, gezien de focus op ID-management van dit onderzoek, een onderscheid aangebracht tussen kernonderwerpen die direct raken aan de focus van het onderzoek, en ondersteunende onderwerpen die in mindere mate van toepassing zijn op ID-management, maar wel van belang zijn binnen het spectrum van techniek, privacy, vertrouwen en veiligheid. De onderstaande shortlist van onderwerpen is niet bedoeld als een uitputtende en complete lijst op het gebied van identiteitsmanagement, techniek, privacy, vertrouwen en veiligheid, maar heeft de insteek van een breed palet aan relevante thema's waaruit inzichten voort kunnen komen die bijdragen aan een integrale visie op identiteit voor de overheid.

- Kernonderwerpen: ID-management
 - Identiteitsfraude
 - eID
 - Biometrisch paspoort
- Ondersteunende onderwerpen
 - Het NSA schandaal
 - 'Behavioral profiling' van individuen door bedrijven als google en Facebook
 - Elektronisch patiëntendossier
 - Slimme energiemeters
 - Verzamelen en delen van passagiersgegevens tussen landen.

Met behulp van hiermee corresponderende Boolean zoektermen zijn vervolgens de belangrijkste (inter)nationale databanken voor een gedegen media-analyse doorzocht. Naast LexisNexis waren dit GoPress voor Vlaamse bronnen en Retriever voor Zweedse bronnen. Na aanscherping en een tweede uitvraag van de databanken zijn zo per land en onderwerp datasets verkregen. Deze datasets zijn vervolgens geanalyseerd en gekwantificeerd. Bij de analyse is voor alle landen en onderwerpen dezelfde format gebuikt om tendensen en correlaties tussen landen en onderwerpen zo inzichtelijk mogelijk te maken. De resultaten zijn getoetst en aangevuld door middel van telefonische interviews met nationale experts.³

2.5 Leeswijzer

In hoofdstuk 2 worden de belangrijkste bevindingen uit de casestudies per kernonderwerp benoemd, de ondersteunende onderwerpen volgen in hoofdstuk 3. Hoofdstuk 4 bevat een samenvatting op basis van deze case studies. In hoofdstuk 5 kiezen wij vervolgens een breder perspectief in de vorm van een beschouwing op landenniveau: hoe is in de onderzochte landen ID-management ingericht? Op basis van de samenvatting en beschouwing, komen wij ten slotte in hoofdstuk 6 tot suggesties voor toekomstig beleid. De bijlagen bevatten naast de gesprekspartners voor het toetsen van de bevindingen nog uitgebreide informatie over de toegepaste terminologie en over de statistieken. De statistieken zelf zijn in een apart bijlagenboekje opgenomen.

³ Zie de bijlage voor een uitgebreide beschrijving van de methodologie en een overzicht van de nationale experts.

3 Analyse kernonderwerpen

Dit hoofdstuk bespreekt de belangrijke bevindingen die voortkomen uit ons onderzoek. Per onderwerp wordt hetzelfde format aangehouden, corresponderend met de sub-vragen van het onderzoek. Na een korte omschrijving van het onderwerp wordt eerst het debat in Nederland tot nu toe beschreven. Vervolgens worden de belangrijkste trends uit het buitenland benoemd. Ten slotte worden hieruit de belangrijkste aandachtspunten voor de toekomstige ontwikkeling in Nederland beschreven.

De centrale vraagstelling van het onderzoek (“Hoe ziet het politieke en maatschappelijke discours op het terrein van techniek, privacy, vertrouwen en veiligheid met betrekking tot ID-management in Nederland en verschillende andere landen er uit sinds 2001?”) alsmede de sub-vragen hierbij komen bij ieder deelonderwerp dynamisch aan bod. Dit wil zeggen dat in de beantwoording van de onderzoeksvragen gekozen is voor het aanstippen van de voor elk onderwerp meest relevante bevindingen op het gebied van de centrale vraagstelling en relevante sub-vragen, in plaats van een meer strikte en schematische aanpak.

3.1 Identiteitsfraude

Algemene Inleiding

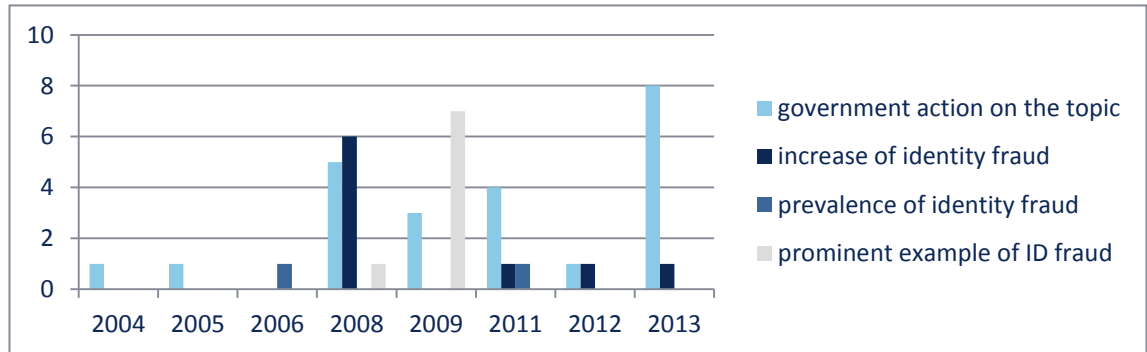
Identiteitsfraude vindt plaats wanneer de identiteitsgegevens van een individu worden gebruikt om fraude te plegen. In veel gevallen gaat het om nietsvermoedende burgers, wiens identiteit gebruikt wordt door criminelen om geld wit te wassen, sociale voorzieningen te misbruiken, vervolging te ontlopen, of criminele activiteiten als mensenhandel of terrorisme te faciliteren. Ook kan identiteitsfraude gebruikt worden bij stalking en aantasting in eer en goede naam.

Al zolang mensen zich als iemand anders voordoen, wordt identiteitsfraude gepleegd. De toegenomen digitalisering van de samenleving, gecombineerd met een verregaande mondialisering, heeft er echter toe geleid dat de omvang en mogelijke gevolgen van identiteitsfraude sterk zijn toegenomen.

Het Nederlandse debat tot nu toe

In Nederland staat het onderwerp identiteitsfraude sinds ongeveer 2004 op de publieke agenda. Er is voor identiteitsfraude bijzonder veel aandacht geweest in de media. Deze aandacht concentreert zich met name op drie gebieden: (1) het beschrijven van schrijnende gevallen, (2) melding maken van de overheid die actie wil ondernemen, en (3) het informeren van burgers over wat ID fraude inhoudt.

Tussen deze drie typen nieuwsitems lijkt een verband te liggen. Met enige regelmaat kondigt de overheid aan identiteitsfraude aan te willen pakken (‘Politie bindt strijd aan met id-fraude’, *Het Parool*, 7 augustus 2008). Vervolgens komen schrijnende gevallen in het nieuws (‘Je raakt je leven kwijt, als je identiteit wordt gestolen’, *de Volkskrant*, 22 november 2008), en hiermee gepaard komen onderzoeken uit over hoe vaak identiteitsfraude voorkomt (‘Identiteit is aantrekkelijke buit’, *Het Parool*, 1 september 2011). Hierdoor ontstaat dan vervolgens een nieuwscyclus op het gebied, wanneer de overheid wederom actie onderneemt tegen identiteitsfraude (‘Kabinet pakt identiteitsfraude harder aan’, *Financieele dagblad*, 7 september 2011).



Figuur 1: aanleiding voor berichtgeving over identiteitsfraude door de jaren heen in Nederland, in aantallen nieuwsitems

In de bovenstaande grafiek is duidelijk te zien dat hoewel al sinds 2004 het tegengaan van identiteitsfraude door de overheid in het nieuws komt, berichtgeving over de toename van identiteitsfraude en schrijnende gevallen van identiteitsfraude gehandhaafd blijft. De focus ligt in berichtgeving met name op de verhouding tussen burgers en de publieke sector: wat de overheid kan doen om identiteitsfraude tegen te gaan.

Het beeld binnen de social media bevestigt het beeld van de media-analyse. Schrijnende gevallen en slachtoffers worden uitgelicht. Vergeleken met de andere onderwerpen is er bij het onderwerp identiteitsfraude meer aandacht voor de veiligheid dan voor privacyschending.



Figuur 2: tag cloud identiteitsfraude 2009-heden (15463 berichten)

Initiatieven tot preventie van identiteitsfraude komen met regelmaat voor, in zogenaamde how-to artikelen ('Succesvolle id-fraude zelden opgemerkt: tips om id-fraude te voorkomen', *Nederlands Dagblad*, 7 augustus 2008). Uit de berichtgeving blijkt dat de overheid zich daarentegen meer op sancties tegen identiteitsfraude richt en minder op voorlichting van burgers over wat ze zelf kunnen doen om identiteitsfraude te voorkomen ('Justitie zet vingerscan in tegen identiteitsfraude', *AD*, 8 september 2011; Stelen identiteit zwaar bestraft, *De Telegraaf*, 3 juni 2013).

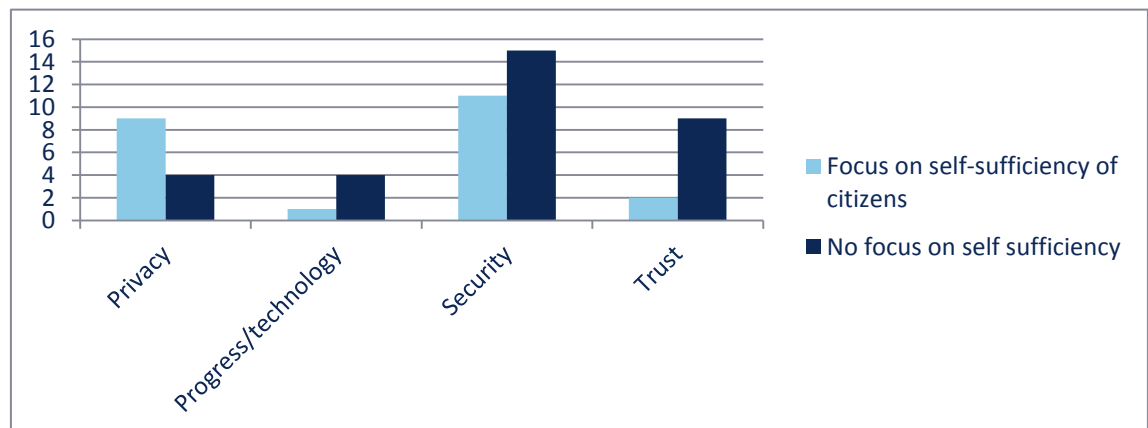
Belangrijkste trends en ontwikkelingen in het buitenland

De berichtgeving over identiteitsfraude in Duitsland lijkt op de situatie in Nederland, al is het Duitse debat een stuk recenter dan in Nederland. Hoewel de overheid aankondigt maatregelen te (willen) nemen tegen identiteitsfraude ('Innenministerium warnt vor Identitätsdiebstahl im Internet', *VDI Nachrichten*, 6 mei 2010), verschijnen nog steeds met

enige regelmaat alarmerende artikelen over de sterke toename van identiteitsdiefstal onder Duitsers ('Deutschen wird immer öfter die Identität gestohlen', *Die Welt*, 13 augustus 2013). Beschrijving van schrijnende gevallen zoals in Nederland gebeurt, lijken te ontbreken.

Een interessant gegeven in de Zweedse berichtgeving over identiteitsfraude, is dat de rol van de private sector in het mogelijk maken en voorkomen van deze vormen van fraude veel breder wordt uitgemeten ('Dataintrång har blivit en affärsida', *Sydsvenskan*, 5 november 2011). Meer dan in Nederland is er vervolgens aandacht voor hoe private data door wetgeving beter beschermd kunnen worden tegen identiteitsdiefstal ('Dataintrång: Lagring av uppgifter kan sakna lagstöd', *Sydsvenskan*, 7 juni 2013).

Groot-Brittannië lijkt van de onderzochte Europese landen, inclusief Nederland, het meeste te kampen met identiteitsfraude ('UK worst in Europe for identity fraud; Britons are more at risk of having identities stolen than any other nation in Europe, experts have warned,' *the Telegraph*, 1 oktober 2012). Volgens de Britse media is dit vooral te wijten aan organisaties die slordig omgaan met identiteitsgegevens van hun klanten, die door criminelen eenvoudig gehackt of uit prullenbakken gehaald kunnen worden ('A Gift to a Fraudster; Medical files dumped in crates...Easy access to bank records...Data Protection chief discovers appalling breaches of your personal details in Government department', *Daily Mail*, 1 augustus 2008). Het lijkt alsof het antwoord op identiteitsfraude door de Britse coalitieregering vooral aan de private sector wordt gelaten. De regering blijft opvallend stil over het onderwerp, terwijl de oppositie kritischer is ('A Labour government would make identity fraud a specific criminal offence for the first time [...] if the party wins the next general election, Yvette Cooper will pledge', *the Telegraph*, 25 september 2013). Vanuit de private sector is echter misbruik gemaakt van deze verantwoordelijkheid in het aanpakken van identiteitsfraude. Er is veel berichtgeving over malafide verzekeringspolissen tegen identiteitsfraude, wat geleid heeft tot grote publieke verontwaardiging ('The Banks That Cash in on Your ID Fraud Fears', *The Daily Mail*, 23 februari 2011). Door het wantrouwen in de private sector en de afwezigheid van de publieke sector in het debat over identiteitsfraude, hebben de media het op zich genomen om het publiek te informeren over de gevaren van identiteitsfraude, en te wijzen op wat burgers zelf kunnen ondernemen ('How to prevent identity fraud', *The Guardian*, 17 oktober 2006; 'How to stop them using your name', *The Mirror*, 4 augustus 2008).



Figuur 3: kernwaarden in Britse berichtgeving, gecorreleerd met aandacht voor zelfredzaamheid, in aantal nieuwsitems

In Spanje manifesteert berichtgeving over identiteitsfraude zich op twee manieren: allereerst op het gebied van financiële frauduleuze handelingen waar individuen en banken het slachtoffer worden ('Los bancos dan la batalla contra la suplantacion de personalidad; A 6.000 euros de media por victima, el robo de identidad supone el 44% de las estafas cometidas en Espana', *Cinco Dias*, 9 juni 2008), en het aannemen van iemand anders identiteit op sociale media, vooral onder kinderen en tieners ('Los menores suplantados no piden ayuda; El robo de identidad tiene los efectos psicológicos más duros en los adolescentes', *El Periodico*, 13 juli 2011). In beide gevallen vermelden artikelen dat de Spaanse wetgeving dusdanig achterloopt op deze ontwikkelingen dat het lastig is om passend te vervolgen voor politie en openbaar ministerie. Initiatieven om identiteitsfraude tegen te gaan komen daarom met name vanuit de private sector en pressiegroepen ('Librería Lucas Rojas y Fellowes inician una campaña contra el fraude de robo de identidad', *Diario de Cordoba*, 19 oktober 2013).

In Vlaanderen is beperkt aandacht voor de gevaren van identiteitsfraude. Het maatschappelijke debat op dit gebied is dus nog sterk in ontwikkeling. Het is echter opvallend dat een aanzienlijk aantal nieuwsberichten de nadruk legt op preventieve maatregelen die burgers zelf kunnen nemen ("Ga niet op aanbod via mail in," *De gazet van Antwerpen*, 27 mei 2013). Ook wordt vanuit de private sector initiatief genomen om burgers te informeren over de gevaren van identiteitsfraude. Zo lanceerde een bank een succesvolle YouTube campagne over het onderwerp (Internetfilmje over identiteitsfraude: op naar 200.000 kijkers, *De Morgen*, 12 juli 2013). Een mogelijke verklaring voor deze situatie is als volgt: gezien het relatieve succes van de Belgische eID-kaart, het digitale identiteitsbewijs dat gebruikt kan worden bij vele publieke en private identificatiedoelinden, is identiteitsfraude een relatief zeldzaam fenomeen in Vlaanderen. Banken en andere private partijen besteden aandacht aan preventie, omdat zij in veel gevallen opdraaien voor de schade die burgers lijden wanneer identiteitsfraude plaatsvindt.

Aandachtspunten en implicaties voor Nederland in de toekomst

Vergeleken met andere Europese landen wordt er in Nederland en Groot-Brittannië opvallend veel bericht over identiteitsfraude. Tegelijkertijd lijkt het niet alsof identiteitsfraude in Nederland zo veel vaker voorkomt dan in bijvoorbeeld Spanje of Duitsland. In Groot-Brittannië daarentegen, lijkt identiteitsfraude op een veel grotere schaal plaats te vinden dan elders in Europa. Een groot gedeelte van de berichtgeving in Nederland behelst het beschrijven van schrijnende gevallen, dit is in de andere landen vrijwel geheel afwezig in het publieke debat.

Twee duidelijke lessen blijken uit de internationale vergelijking: allereerst lijkt het alsof de Nederlandse overheid zich te veel op sanctionering richt, en te weinig op preventie. Hoewel er veel initiatieven zijn geweest om identiteitsdiefstal zwaarder te straffen, wordt de zorg om de gevolgen van dergelijke fraude niet minder. Het weerbaarder maken van burgers lijkt urgenter te zijn. In het verlengde daarvan, kan de private sector sterker betrokken worden in het debat over identiteitsfraude. Vlaanderen en Zweden tonen aan dat de private sector actief kan bijdragen aan preventiemaatregelen, zodat er minder last op de schouders van de overheid hoeft te liggen. Het aanpakken van identiteitsfraude volledig overlaten aan de private sector lijkt in Groot-Brittannië geen succes te zijn geweest.

3.2 eID

Algemene Inleiding

De elektronische identiteitskaart, ofwel eID, is een met een chip uitgerust identiteitsbewijs ter grootte van een creditcard dat gebruikt kan worden voor online- en offline identificatie. Veel meer dan het biometrische identiteitsbewijs, dat vooral als controlemechanisme dient, draait het bij de eID om dienstverlening. Burgers gebruiken hun eID bijvoorbeeld om zich te identificeren bij banken en zorgverleners, of bij gemeentelijke loketten. Tegelijkertijd kunnen burgers zich met behulp van een eID-lezer online identificeren, op een vergelijkbare manier als bij internetbankieren.

Het Nederlandse debat tot nu toe

Vergeleken met alle andere onderwerpen in dit rapport, staat de ontwikkeling van de eID in Nederland het meest in de kinderschoenen. Hoewel er al geruime tijd ervaring is met de DigiD, wil de overheid de stap zetten naar een fysiek pasje in de vorm van een eID. Met de eID wordt aldus de (online) dienstverlening van de DigiD uitgebreid naar offline functionaliteiten die naast identificatie met de overheid zelf, nadrukkelijker ook gebruikt kunnen worden voor dienstverlening vanuit de private sector ('Plasterk presenteert de eID als opvolger van DigiD' *De Volkskrant*, 11 april 2013).

Wat betreft de eID is Nederland dus nog voor een groot gedeelte *terra incognita*. Het begrip is in de volksmond nog niet of nauwelijks bekend. Op de sociale media zijn er in totaal slechts 75 berichten. Daarom is het bijzonder interessant om te onderzoeken hoe de ontwikkeling van de eID verlopen is in Europese landen waar deze dienstverlening wel al beschikbaar is. Met name Spanje, Vlaanderen en Duitsland bieden interessante voorbeelden. Uit de sociale media-analyse blijkt dat men in Nederland tot nu toe voornamelijk het Vlaamse voorbeeld citeert.

Uit de sociale media-analyse blijkt dat een toonaangevend acteur op het gebied van de eID Platform Identity Management Nederland (PIMN) is. Ze hebben 12% van de berichten geschreven, PIMN is dus een invloedrijke speler.

Auteur	Berichten	Volgers	Invloed
1. pimn1	9	359	2,1
2. GertManeschijn	5	106	1,5
3. Céécile van Voorst	3	x	x
4. CreAim	2	x	x
5. elf	2	x	x
6. HF_Opdrachten	1	411	0,7
7. lVBennekom	1	68	1,7
8. OpenKortenhoef	1	428	3,7
9. RichardBladEZ	1	126	1,2
10. _Amstelveen	1	1.001	0,8

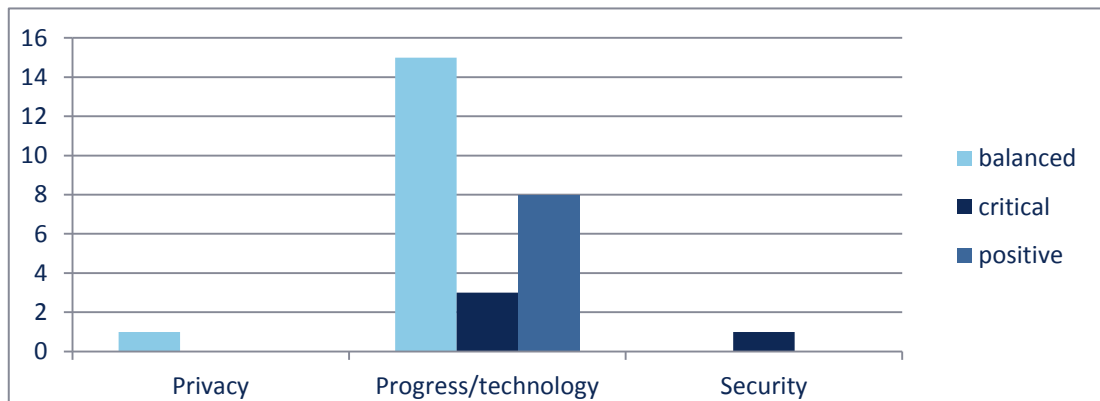
Figuur 4 Auteurs van de nieuwsberichten "eID" (75 berichten)

Belangrijkste trends en ontwikkelingen in het buitenland

Vlaanderen heeft van de onderzochte landen de meeste ervaring met de eID. Al vanaf de eeuwwisseling ontstaan in Vlaanderen initiatieven om digitale identificatie en bijbehorende dienstverlening te faciliteren ('E-government neemt vanaf eind volgend jaar concreet gestalte' *Het Laatste Nieuws*, 10 februari 2001).

Een belangrijke sociaal-culturele factor die in Vlaanderen invloed heeft gehad op de invoering van de eID, is het sterk regionale karakter van openbaar bestuur in België. Vlaamse gemeenten kunnen daarom opereren binnen een aanzienlijke bandbreedte bij het invoeren van de eID. Dit maakt dat ze relatieve vrijheid hebben bij de kosten, ingangsdatum en het ‘aanprijzen’ van de eID op een manier die dicht bij de burger staat. De centrale Belgische overheid speelt niet of nauwelijks een rol in berichtgeving omtrent de eID, en dit is in vergelijking met andere Europese landen een bijzonderheid. Hierdoor lijkt het alsof de eID op nationaal niveau ook nooit een heet hangijzer heeft kunnen worden. Hoewel er wel degelijk aanloopproblemen zijn geweest bij het invoeren van de eID (‘Al meer dan 40.000 elektronische identiteitskaarten teruggestuurd met kapotte chip’ *Het Nieuwsblad*, 26 maart 2009), leiden deze situaties niet tot hoogoplopende politieke discussies, maar worden op lokaal bestuurlijk niveau afgehandeld.

De berichtgeving in Vlaanderen heeft inhoudelijk een hoog ‘how-to’ gehalte: de eID wordt geïntroduceerd, met uitleg over hoe deze functionaliteit precies toegepast kan worden (‘Waarvoor dient uw eID?’ *De Tijd*, 21 januari 2012). Hoewel er wel degelijk ruimte is voor kritische geluiden, zijn privacy en veiligheid als kernwaarden in de berichtgeving vrijwel geheel afwezig. Dominant in berichtgeving is daarentegen de technologische vooruitgang die de eID met zich meebrengt. Daarnaast lijkt de invoering van een eID voor kinderen haast meer aandacht te krijgen dan de eID voor volwassenen.



Figuur 5: kernwaarden en tenor van berichtgeving in Belgische nieuwsmedia over de eID, in aantal nieuwsitems

De rol van de private sector in de ontwikkeling van de eID is aanwezig in Vlaanderen. Hoewel de eID met name gezien wordt als dienstverlenend tussen burger en overheid, is het ook inmiddels gemeengoed voor Vlamingen om hun eID te gebruiken bij (bijvoorbeeld) het afsluiten van een telefoonabonnement. In Duitsland is eveneens geprobeerd de private sector aan te laten sluiten bij het ontwikkelen van de eID, en een breed product voor identificatie en dienstverlening aan burgers te bieden. Het lijkt er echter op dat het stevige publieke debat omtrent de eID en privacyzorgen (‘Elektronischer Personalausweis; Neuer Chip: Deutsche fürchten um ihre Daten’ *Hamburger Abendblatt*, 28 oktober 2010) ertoe geleid hebben dat de private sector niet aangehaakt is bij het door ontwikkelen van de kaart. Hiermee lijkt een situatie te zijn ontstaan waarin de eID geheel geïmplementeerd is in Duitsland, maar dat de functionaliteit van de eID onderbenut wordt (‘Der elektronische Personalausweis könnte das ohne Verlust an Sicherheit verhindern. Doch er wird nicht genutzt’ *Die Welt*, 27 november 2012).

In Spanje, daarentegen, is de eID vanaf het begin nadrukkelijk een publiek-private samenwerking geweest. Het gebruiksgemak dat gepaard gaat met de eID, en het verminderen van administratieve rompslomp wordt gezien als een belangrijk voordeel van de kaart ('El DNI electronico permitira hacer gestiones desde casa' *El Mundo*, 12 februari 2004). Opvallend genoeg is de invoering van de eID in Spanje een sterk gepolitiseerd proces geweest: het publiek-private karakter van de kaart werd als een uitwas van de centrumrechtse regeringspartij 'Partido Popular' gezien, en kritiek op de kaart kwam met name vanuit de linkse oppositie. Uit de meer recente berichtgeving blijkt echter dat de invoering van de eID in Spanje niet het gewenste effect gehad heeft: net zoals in Duitsland wordt de 'e' component van de eID relatief weinig gebruikt door Spaanse burgers ('Cuatro millones de españoles tienen ya el DNI electrónico, pero apenas lo usan', *El Pais*, 11 juni 2008).

Zweden biedt voor Nederland wellicht eveneens een interessante case study, aangezien de invoering van de eID daar iets vooruitloopt op de Nederlandse planning. De invoering van de eID lijkt voornamelijk weinig controversieel te zijn, en met name gericht te zijn op de technologische voordelen die de eID biedt ten opzichte van andere identificatievormen ('Lagförslag ska göra fler e-legitimationer valbara', *It i varden*, 4 april 2013). In Groot-Brittannië lijken er geen plannen te zijn op korte termijn een eID in te voeren.

Aandachtspunten en implicaties voor Nederland in de toekomst

Met het ontwikkelen van de eID voor Nederland ligt er, meer dan op andere hier beschreven onderwerpen, een kans voor de overheid om lering te trekken uit ervaringen uit het buitenland met de eID. In Spanje, Vlaanderen en Duitsland is er al sinds geruime tijd eID-dienstverlening beschikbaar, zij het met gemengd succes.

Het valt op dat in Duitsland en Spanje, ondanks forse investeringen van de overheid, relatief weinig gebruik wordt gemaakt van de vele functionaliteiten die de eID biedt. In Duitsland lijkt de afwezigheid van de private sector debet te zijn aan deze situatie, maar in Spanje lijkt een sterke publiek/private samenwerking niet veel betere resultaten geboekt te hebben. Er zijn er in Spanje grootschalige campagnes opgezet om Spanjaarden te wijzen op de voordelen van hun eID ("En marcha una campaña para fomentar el DNI electrónico en Castilla-La Mancha, donde ya lo tienen 418.000 personas" *La Verdad*, 17 oktober 2009). Wellicht is het interessant de uitkomst van deze campagnes met Spaanse collega's te bespreken.

Vlaanderen vormt overduidelijk een 'best practice' scenario voor het invoeren en toepassen van de eID. De invoering van de kaart is voorspoedig verlopen, zonder maatschappelijke discussie over veiligheid of privacy. De gefaseerde, regionaal-georiënteerde invoering van de eID die in Vlaanderen heeft plaatsgevonden, kan echter niet eenvoudig gerepliceerd worden in Nederland. Van alle onderzochte landen heeft in Vlaanderen de private sector bovendien het meest succesvol aangesloten bij de doorontwikkeling van de eID.

3.3 Biometrisch paspoort

Algemene Inleiding

Biometrische gegevens zijn unieke eigenschappen verbonden aan het menselijk lichaam, aan de hand waarvan personen geïdentificeerd kunnen worden. Het gaat hier zowel om fysiologische karakteristieken, zoals vingerafdrukken, DNA-structuur, irisstructuur, geur en gezichtskenmerken, als gedragseigenschappen zoals stem en motoriek.

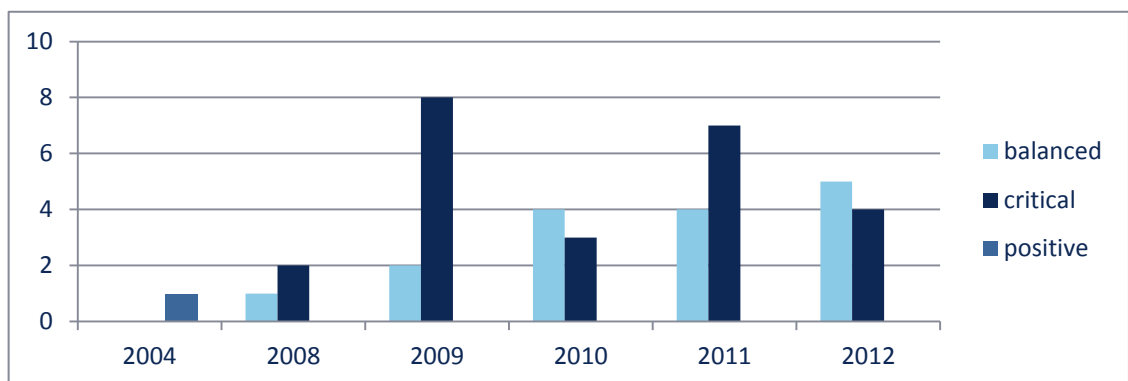
Fysiologische eigenschappen, en met name vingerafdrukken, worden sinds lange tijd gebruikt ter identificatie. Het is echter een redelijk recente ontwikkeling dat biometrische gegevens gekoppeld worden aan identiteitsbewijzen. Het gaat in dit geval om elektronische chips in paspoorten en andere identiteitsbewijzen, die biometrische gegevens van de eigenaar van het reisdocument bevatten - meestal in de vorm van vingerafdrukken en/of irisscans. Indien gewenst kan daarom met vingerafdruk- of irisscanners gecontroleerd worden of de identiteit van de eigenaar van een reisdocument ook overeenstemt met de identiteit van de persoon die het reisdocument in bezit heeft.

Het vastleggen en delen van biometrische gegevens door overheden is onder de aandacht gekomen na de aanslagen van 11 september 2001. Inmiddels zijn reisdocumenten van vrijwel alle westerse landen uitgerust met biometrische gegevens. Dit roept echter vragen op over de beveiliging van deze gegevens, en de uitwisseling ervan tussen landen.

Het Nederlandse debat tot nu toe

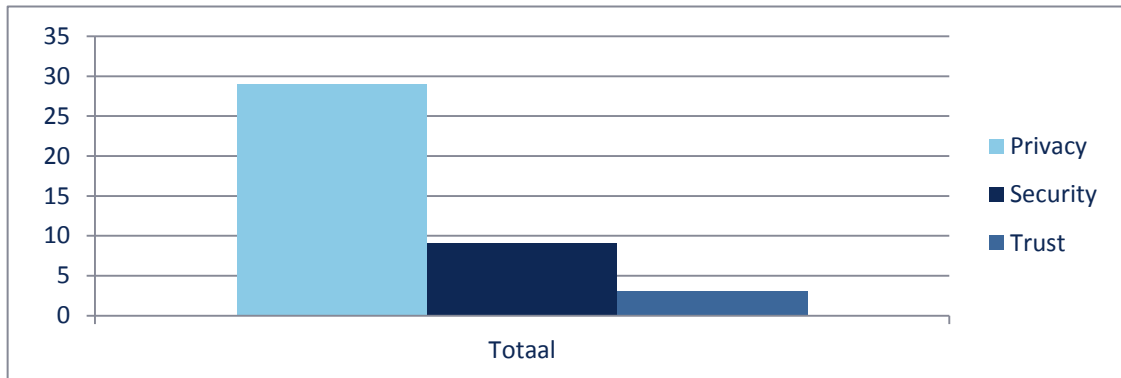
Uit de berichtgeving omtrent het biometrisch paspoort in Nederland blijkt een progressie van scepsis over nut en noodzaak van biometrische gegevens verwerkt in reisdocumenten, naar twijfel of de overheid biometrische gegevens veilig en verantwoord kan beheren.

Wanneer bekend wordt dat de Nederlandse overheid biometrische gegevens van burgers op wil slaan, ontstaat een levendige discussie in de nieuwsmidia. De teneur van deze discussie is overwegend negatief ('Biometrie ernstige bedreiging privacy', *Trouw*, 24 juli 2008) en argwanend ('Een nieuw paspoort? Dan ook je vingerafdruk afgeven. Al die vingerafdrukken komen in een database. Niks aan de hand, zegt de overheid. Waarom geloven we dat eigenlijk?' *NRC-Next*, 18 september 2009).



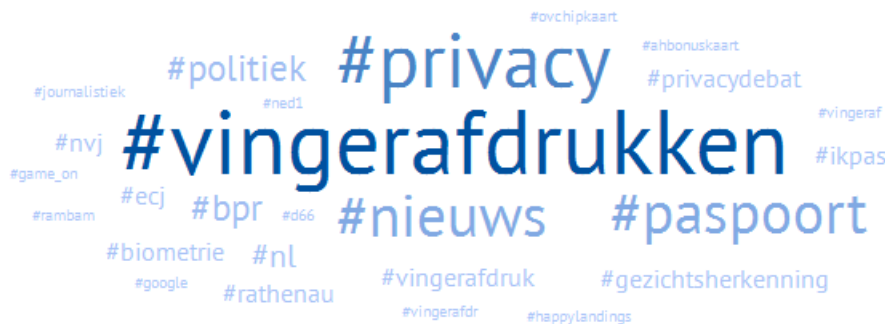
Figuur 6: teneur van nieuwsberichten in Nederlandse nieuwsmidia door de jaren heen, in aantallen nieuwsitems

De privacy van burgers staat centraal in de discussie, meer dan bijvoorbeeld de veiligheid van opgeslagen gegevens. Verhalen van principiële weigeraars - personen die weigeren biometrische gegevens af te staan bij het aanvragen van een reisdocument - worden breed uitgemeten. Het voornemen om vingerafdrukken dan wel irisafbeeldingen centraal op te slaan, en vervolgens te delen met buitenlandse instanties leidt tot argwaan.



Figuur 7: kernwaarden in Nederlandse nieuwsmedia over biometrisch paspoort, in aantallen nieuwsitems

In het debat over het biometrische paspoort op social media is de nadruk op privacy duidelijk zichtbaar. Er zijn geen discussies op het gebied ‘#veiligheid’ of ‘#digitale veiligheid.’ De technologische trend is voornamelijk gericht op vingerafdrukken omdat burgers deze momenteel moeten leveren bij de aanvraag van een nieuw paspoort. Met oog op de toekomst is de voornaamste trend gezichtsherkenning.



Figuur 8: Meest gebruikte hashtags in biometrisch paspoort discussie (2.246 berichten)

De Nederlandse overheid lijkt zich in beperkte mate te laten leiden door het publieke debat. Pas onder grote publieke druk worden eerdere beslissingen op vingerafdrukken op te nemen in het paspoort uitgesteld, maar nadrukkelijk niet afgesteld. Hierdoor lijkt een beeld in de media te ontstaan van een centrale overheid die vasthoudt aan een discutabele maatregel (‘Vingerafdruk in paspoort veel te snel ingevoerd’ *Volkskrant*, 29 februari 2012).

Belangrijkste trends en ontwikkelingen in het buitenland

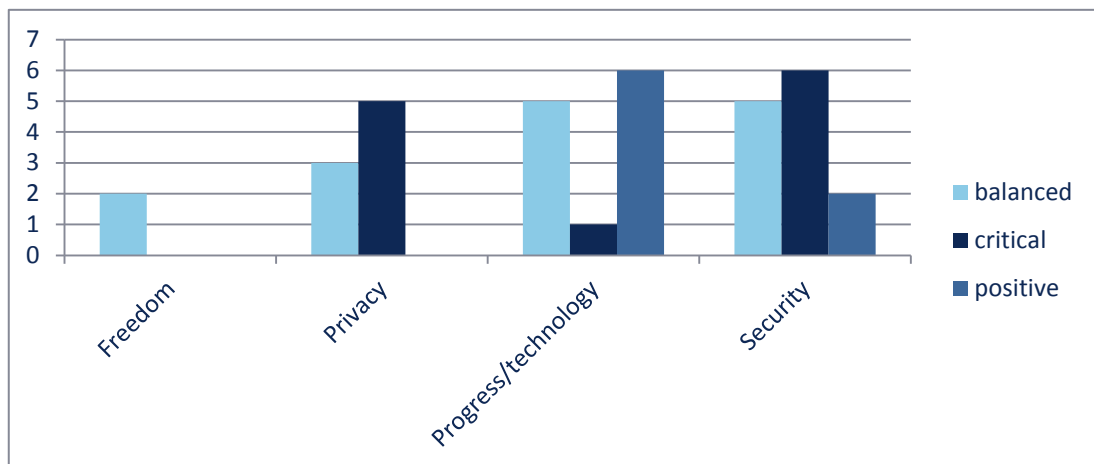
Vergeleken met andere Europese landen nemen de Nederlandse nieuwsmedia een redelijk extreme mening in over het biometrisch paspoort. Het Zweedse debat over biometrie is inhoudelijk verwant aan het Nederlandse: er is ook hier vooral veel aandacht voor de rol van de Verenigde Staten en EU in het verzamelen van gegevens, echter zonder de sterke argwaan die uit de Nederlandse berichtgeving blijkt.

In landen als Vlaanderen en Spanje is de toon van het debat positiever dan in Nederland, vanwege een nadruk op veiligheid en technologische vooruitgang. Hoewel de daadwerkelijke invoering van het biometrisch paspoort in Vlaanderen traag op gang kwam,

lijken de Belgen zichzelf te zien als een Europese voortrekker op het gebied van opslag van biometrische gegevens. Biometrie wordt geïntegreerd als een middel om identiteitsfraude tegen te gaan ('De veiligste sleutel ben je zelf' *de Standaard*, 19 januari 2006), en hoewel er wel degelijk ruimte is voor kritische kanttekeningen ('Blind vertrouwen in biometrie' *de Tijd*, 27 juli 2002) blijft de teneur van het publieke debat zoals weerspiegeld door de media overwegend positief.

In Spanje overheerst pragmatisme ten opzichte van biometrie. Naar aanleiding van het voorkomen van terroristische aanslagen wordt geconcludeerd dat het opslaan en delen van biometrische gegevens kan bijdragen aan de bestrijding van terrorisme. Opvallend in het Spaanse debat is de aandacht voor de private sector, de bedrijven die het mogelijk maken biometrische gegevens te verwerken. Vanuit een interesse in technologische vooruitgang wordt het gemak benadrukt van biometrische gegevens bij identificatie.

Ook in Duitsland speelt de private sector een opvallende rol, vooral aangezien bedrijven in de biometrische industrie grote werkgevers in Duitsland lijken te zijn. Dit neemt overigens niet weg dat het debat in Duitsland van alle onderzochte landen het meest evenwichtig gevoerd wordt. De introductie van biometrische gegevens op identiteitsbewijzen heeft in Duitsland in bepaalde mate sociale onrust met zich meegebracht, en zelfs protestmanifestaties ('Neue Reisepässe passen Datenschützern nicht' *die Tageszeitung*, 5 december 2007). Dit heeft echter een gebalanceerd maatschappelijk debat niet in de weg gestaan: biometrie is een technologische vooruitgang die kan bijdragen aan het verhogen van de staatsveiligheid, maar hiervoor dienen persoonsgegevens te worden gedeeld. De Duitse media hechten er vervolgens meer belang aan dat biometrische gegevens veilig worden opgeslagen, dan dat het om privacygevoelige persoonsgegevens gaat.



Figuur 9: kernwaarden in Duitse berichtgeving over biometrisch paspoort, in aantallen nieuwsitems

Tegelijkertijd is er in Duitsland ook nadrukkelijk discussie over de (gestegen) prijs van biometrische paspoorten ('Zwei Fingerabdrücke im Chip; Missbrauch wird erschwert, der Preis steigt' *Hamburger Abendblatt*, 20 oktober 2007). In Groot-Brittannië is de prijs van nieuwe biometrische paspoorten eveneens een nadrukkelijk aspect van de discussie ('Axe Id Card, Save £1.3bn' *Daily Mail*, 7 mei 2009). Daarnaast staan de Britten over het algemeen kritisch tegenover het biometrisch paspoort door de gebrekkige communicatie vanuit de overheid over het opslaan en verwerken van gegevens. Hierdoor ontstaat in de media het beeld dat biometrische gegevens een geld verspillend en schimmig

overheidsproject is dat gebruikt wordt om burgers te controleren ('ID cards: Surveillance creep' *The Guardian*, 28 juni 2005).

Aandachtspunten en implicaties voor Nederland in de toekomst

In vergelijking met het publieke debat over het biometrisch paspoort in het buitenland, valt in het Nederlandse debat een aantal zaken op.

Over het algemeen heeft het debat in de ons omringende landen, en dan met name Vlaanderen, Zweden, Duitsland en Spanje, een pragmatischere insteek: biometrie is *here to stay*, en brengt voordelen met zich mee op het gebied van identificatie en werkgelegenheid - Gemalto, een wereldleider op het gebied van verwerking van biometrische gegevens, is bijvoorbeeld gevestigd in Amsterdam.

Dit neemt niet weg dat er in deze landen niet kritisch wordt gekeken naar het verwerken van biometrische gegevens. Deze kritiek spitst zich toe op de veiligheid die al dan niet gepaard gaat met het opslaan en delen van biometrische gegevens. Dit lijkt een meer praktische kritische houding dan een vrijwel exclusieve focus op privacy zoals die uit het Nederlandse debat naar voren komt. Kritiek op een vermeend gebrek aan dataprotectie is veel beter te faciliteren door concrete maatregelen op het gebied van beveiliging.

Het risico bestaat dat het debat in Nederland de richting opgaat van Groot-Brittannië, waar het biometrisch paspoort wordt gezien als één van de vele dure en mislukte overheidsprojecten op het gebied van IT. In Nederland zijn de tendensen van een dergelijke richting al zichtbaar.

4 Analyse ondersteunende onderwerpen

De analyse voor de ondersteunende onderwerpen wordt omgekeerd chronologisch geanalyseerd, beginnend bij het meest recente debat. De vorm van de analyse is gelijk aan die van de kernonderwerpen uit hoofdstuk 3: een algemene inleiding, gevolgd door het Nederlandse debat, waarna trends en ontwikkelingen in het buitenland geanalyseerd worden. Hierop volgt een korte conclusie met aandachtspunten voor Nederland in de toekomst.

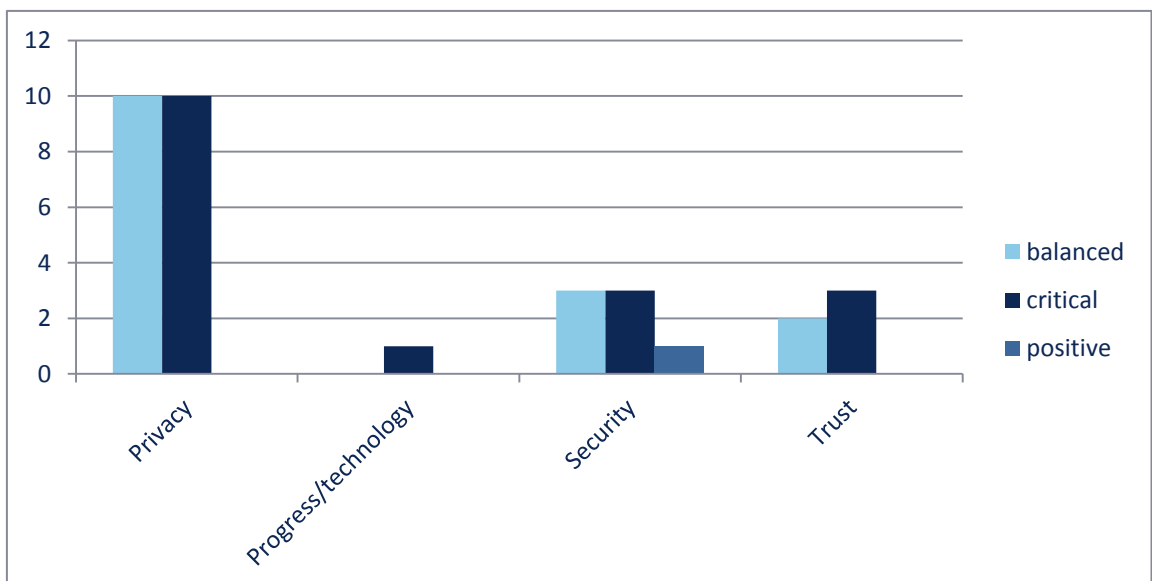
4.1 NSA/PRISM

Algemene Inleiding

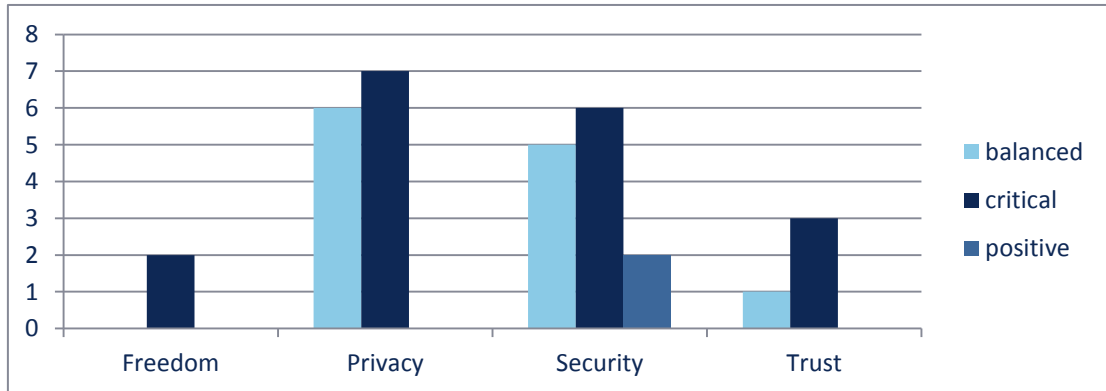
Het media-discours over de Amerikaanse afluisterdienst National Security Agency (NSA) en het door deze organisatie gebruikte programma PRISM is het meest recente debat dat bij de media-analyse werd betrokken. Tot de onthullingen in juni 2013 door Edward Snowden wisten weinig mensen over het bestaan van het programma PRISM, of over de vergaande illegale aftappraktijken van de NSA. PRISM is een programma dat door de NSA sinds 2007 wordt gebruikt om inlichtingen over personen te vergaren uit gegevens van een reeks grote Amerikaanse internetbedrijven. Na juni bleven de onthullingen elkaar opvolgen. Zo werd in oktober bekend dat de NSA 1,8 miljoen Nederlandse telefoonnummers heeft afgetapt, binnen een maand tijd 70,3 miljoen Franse telefoontjes heeft onderschept en in 2010 het e-mailaccount van de toenmalige Mexicaanse president Felipe Calderon heeft gehackt. Met het bekend worden van het afluisteren van de mobiele telefoon van de Duitse premier Angela Merkel - met wetenschap van Obama - heeft het schandaal een nieuw hoogtepunt bereikt.

Het Nederlandse debat tot nu toe

Bij de beschrijving van het Nederlandse discours tot nu toe is het belangrijk om zich te realiseren dat de geanalyseerde bronnen nog geen artikelen omvatten die zijn verschenen nadat bekend is geworden dat de NSA ook in Nederland telefoonnummers heeft afgetapt. Deze informatie werd pas 28 oktober 2013 bekend.



Figuur 10: teneur Nederlandse berichtgeving over het NSA schandaal, in aantal nieuwsitems



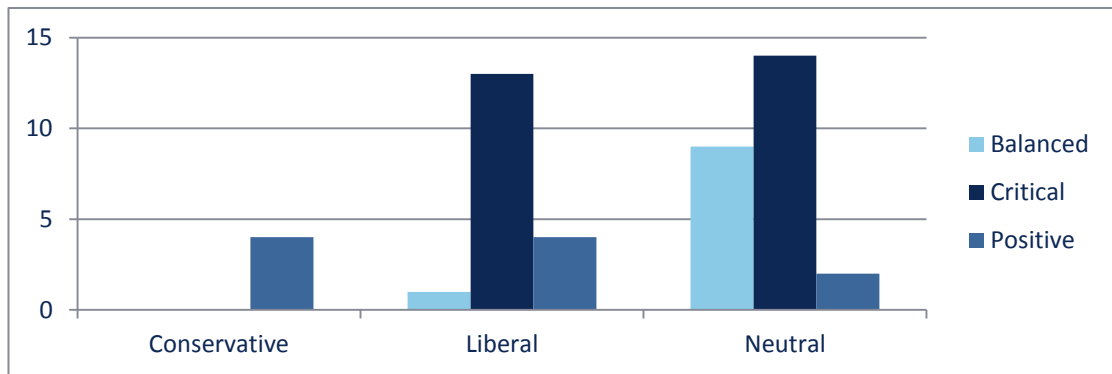
Figuur 12: teneur van berichtgeving over het NSA schandaal in Duitsland, in aantal nieuwsitems

In Duitsland gaat het debat vooral over de bescherming van de privacy van de burger; hoe deze weer gegarandeerd kan worden en welke rol de staat hierin heeft. Er is een roep voor meer regelgeving op het gebied van (online) beveiliging, zowel door de Duitse overheid als ook door Brussel. Er wordt een grote rol gezien voor de private sector bij de beveiliging van data. Ook worden kansen genoemd voor de Duitse IT branche op het gebied van versleutelingstechnieken ('NSA-Debatte Chance für deutsche IT-Industrie', *Die Welt*, 10-08-13). Veel bronnen bevatten praktische tips voor de burgers over hoe hij zijn privacy (beter) kan beschermen. Bijvoorbeeld door middel van versleuteling, door het overstappen naar Duitse e-mailproviders et cetera.

Het debat in Vlaanderen is als kritisch-realistisch te beschrijven. Men is zonder twijfel kritisch over de afluisterpraktijken maar beschouwt deze tegelijkertijd als niet te vermijden. Veiligheidsdiensten als de NSA zullen linksom of rechtsom aan de data komen die ze willen hebben. Naast deze algemene lijn is er een splitsing tussen de publieke en de private sector. Wat het laatste betreft wordt vaak de ongeïnteresseerdheid van burgers bekritiseerd: burgers lijken steeds minder bezorgd over de mogelijkheid afgetapt te worden. Maar het eigenlijke debat vindt met betrekking tot de publieke sector plaats. Hiervoor zijn twee verklaringen: enerzijds het gemak van het verzamelen van data van individuen. Anderzijds het feit dat een van de belangrijkste Belgische bedrijven, de telecomoperator Belgacom, sinds 2010 door de Britse inlichtingendienst afgetapt werd. Via toegang tot routers van de telecomoperator kon de GCHQ gesprekken afluisteren, waaronder ook diverse internationale organisaties die in Brussel zijn gevestigd. Als gevolg van de Belgacom spionage besteden Vlaamse media veel aandacht aan de publieke sector. Bedrijven komen in opstand; accepteren dergelijke afluisterpraktijken niet. Er wordt vaak aan de regering geappelleerd om stevig op te treden ('Hoog tijd voor een geloofwaardig veiligheids- en privacybeleid', *De Tijd*, 18 september 13).

Het discours in Engeland verschilt fundamenteel van het discours in Nederland en de andere lidstaten. In het begin waren de media terughoudend in de berichtgeving, ook toen de rol van de Britse inlichtingendienst steeds duidelijker werd. Enkel de links-liberale Guardian heeft herhaaldelijk en gedetailleerd bericht over de Snowden documenten. Hierop werd heftig gereageerd, niet alleen door de overheid maar ook door de conservatief-rechtse media. De Guardian zou met zijn onthullingen de strijd tegen het terrorisme in gevaar brengen en het leven van mensen op het spel zetten. ('Yes, Big Brother is watching you, But for a good reason', *The Sunday Telegraph*, 9 juni 2013). Toch is er ook in Engeland een verandering te zien in de mate van acceptatie van de algemeenheid met betrekking tot het

monitoren en verzamelen van persoonsgegevens. De grote bereidheid na 9/11 om maatregelen te aanvaarden die inzage in persoonsgegevens en het monitoren ervan mogelijk maken, verandert. Het aantal mensen dat de huidige mate van afluistering buiten alle proporties vindt groeit. Een van de belangrijkste onderwerpen van het debat is wat de juiste verhouding is tussen veiligheid en bescherming van persoonsgegevens en hoe een betere en transparantere verhouding kan worden bereikt tussen veiligheid en privacy. Aandachtspunt hierbij is de mate van informatie die de veiligheidsdiensten moeten geven over hun activiteiten om voor meer transparantie te zorgen.



Figuur 13: teneur berichtgeving in Britse media aan de hand van politieke signatuur, in aantal nieuwsitems

Met betrekking tot het nemen van maatregelen is er de roep om wetgeving en beleid aan te passen, zowel nationaal/bilateraal (VK en VS) als ook op het niveau van de EU. Het beleid op basis van de Regulation of Investigatory Powers Act (RIPA) en de voorgestelde Communications Data Bill wordt gezien als te algemeen voor een proactieve omgang met de technologische vooruitgang en groeiende mogelijkheden om data te verzamelen. Technologie wordt vooral als inbreuk faciliteren gezien, niet in termen van het bieden van oplossingen. Er wordt dus anders dan in Duitsland weinig soelaas gezien in private partijen en de IT-branche.

Aandachtspunten en implicaties voor Nederland in de toekomst

Het einde van de onthullingen rondom de NSA en andere inlichtingendiensten is nog niet in zicht. Duidelijk is echter al dat het schandaal vergaande gevolgen zal hebben voor de toekomstige omgang met privacy en de bescherming van identiteitsgevoelige gegevens. Er valt niet meer te ontkennen dat het gebruik van het internet/mobiele telefonie voor het uitwisselen van informatie niet veilig is. In Nederland is nog maar kort bekend dat ook hier telefoons afgeluisterd worden. Hierdoor is het debat tot nu toe vooral vanuit verontwaardiging gevoerd over het aantasten van de privacy, en nog niet vanuit een realistisch pragmatisme dat meer de focus legt op de nodige maatregelen en oplossingen zoals de mogelijkheden die de IT sector biedt, aangescherpte regelgeving, voorlichting voor burgers over een zo veilig mogelijke omgang met internet en (mobiele) telefonie.

4.2 Behavioral profiling

Algemene Inleiding

Een cookie is een bestand dat websites achterlaten bij de gebruiker. Cookies kunnen meerdere doeleinden hebben. In eerste instantie waren cookies er om bepaalde gegevens op te slaan voor een browser zodat gebruikersinstellingen bewaard blijven voor een volgende sessie. Tracking cookies zijn cookies die het surfgedrag van de gebruiker

bijhouden en daar advertenties op aanpassen. De technische term voor dit volgedrag is 'behavioral profiling.'

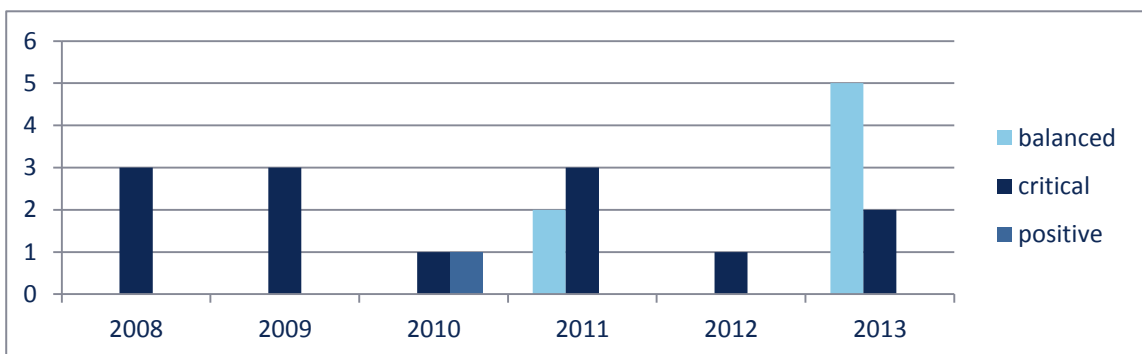
Het is tegenwoordig in steeds betere mate mogelijk om de identiteit van gebruikers te koppelen aan het surfgedrag. In het geval van bijvoorbeeld zwangerschap is het belangrijk als adverteerders daar zo snel mogelijk op in kunnen spelen. Cookies kunnen hier bij helpen.

Er is al sinds de jaren 1990 een internationaal debat over de cookies. Toen werd er in de browser een mogelijkheid geprogrammeerd om de instellingen voor de cookies zelf aan te kunnen passen. Het werd daardoor mogelijk om alle cookies te weren of allemaal toe te staan. Probleem: er zijn veel websites die niet functioneren zonder het gebruik van cookies.

Het Nederlandse debat tot nu toe

Als de eerste berichtgeving over de mogelijkheden van cookies in 2008 naar buiten komt, wordt benadrukt dat je geen privacy meer hebt op het net. Er wordt vaak op een objectieve manier vermeld op welke manieren de cookies het surfgedrag van de gebruiker bijhouden. Uiteindelijk melden de artikelen wat adverteerders met de gegevens kunnen doen ('Internet verradt uw koopgewoontes: Hoe bedrijven het zoek- en surfgedrag van consumenten gebruiken voor specifieke aanbiedingen en advertenties', *NRC next*, 12 november 2008).

EU wetgeving heeft getracht de adverteerders een halt toe te roepen en de gebruiker meer inzicht te geven in het gebruik van cookies door de verschillende websites. Het gevolg was dat bijvoorbeeld sites van de publieke omroep een scherm presenteerden met de vraag of de gebruiker cookies wil accepteren van de website. Deze wet die voor de gebruiker ingesteld is werd over het algemeen door de gebruiker als vervelend ervaren. De negatieve sentimenten zijn vooral te zien bij de social media-analyse. De negatieve geluiden houden aan totdat in 2013 de wetgeving afgezwakt wordt. Gebruikers kunnen, vanaf dat moment, direct naar de website zonder eerst in een apart scherm een keuze te moeten maken ('Kamp zegt versoepeling toe van de Cookiewet', *Financieele Dagblad*, 1 april 2013).



Figuur 14: teneur van Nederlandse berichtgeving over behavioral profiling door de jaren heen, in aantal nieuwsitems

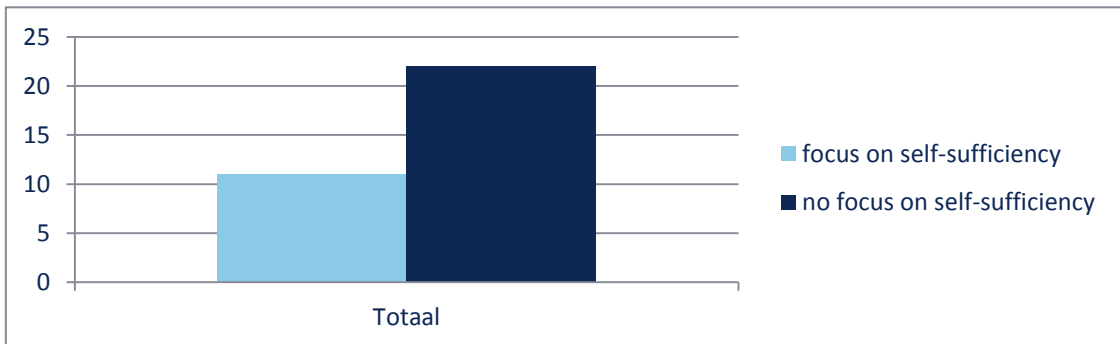
De Nederlandse media gebruiken regelmatig de term 'gluren' ('Adverteerder op web gluurt mee', *NRC*, 15 juni 2006). Dit is ook de manier waarop wij het debat behandelen. Als er begluurd wordt, dan komt meteen het klassieke beeld boven van iemand die een gordijntje opzij schuift en iemand anders bekijkt zonder dat deze persoon het weet. Gluren is een inbreuk op de privacy waar je in principe weinig aan kunt doen.

Belangrijkste trends en ontwikkelingen in het buitenland

Het kenmerkende aan het debat in de andere landen is dat het in de meeste gevallen inhoudelijker is. Er worden meer termen genoemd (zoals ISP of HTML5) en meerdere verschillende toepassingen voor de cookies. In Duitsland is er bijvoorbeeld een artikel dat ook benadrukt hoe cookies bij de verkiezingsstrijd in de VS ingezet zijn ('Mit Cookies fängt man Wähler; KLIKKS Das wird der erste datengesteuerte US-Wahlkampf, sagen Wahlwerber. Am Dienstag zeigt sich, was das heißt', *Die Tageszeitung*, 3 maart 2012).

Verder wordt er in alle landen melding gemaakt van de EU wetgeving in 2011. Deze wet wordt in ieder land bekritiseerd. Er zijn voornamelijk kritische geluiden met een enkele positieve uitzondering. Opvallend in de kritiek is de Spaanse kritiek die vooral gericht is aan Duitsland omdat de rapporteur Duits was. Spanjaarden vinden de rapporteur niet objectief omdat Duitsers veel waarde hechten aan privacy. De kritiek van de Spaanse media is gericht op hoe webadverteerders last hebben van de nieuwe cookiewetgeving. ('La nueva ley 'anticookies' amenaza la publicidad en la Red (The new law 'anticookies' threatens Web advertising)', *El Pais*, 14 april 2012)

Dat Duitsers veel waarde hechten aan privacy is duidelijk te zien aan het feit dat bijna de helft van de artikelen de zelfredzaamheid bevorderen van de burgers. Deze artikelen equiperen burgers hun privacy zelf te beschermen, ze leggen het stap voor stap uit. ('Cookies ausschalten: Wie man seine Daten schützt', *Handelsblatt*, 16 september 2011)



Figuur 15: De Duitse focus op zelfredzaamheid in berichtgeving over behavioral profiling, in aantal nieuwsitems.

Van de ene kant is er de roep om meer bescherming tegen bedrijven zoals Google en Facebook die gegevens opslaan, maar van de andere kant is de wet die dit zou moeten beschermen niet goed ontvangen. Dit beeld is voor alle landen herkenbaar.

Het discours in Groot-Brittannië is genuanceerder, het weegt nog af of het gericht adverteren een kwalijke zaak is voor de burger of niet. Britse media kijken ook naar de voordelen van wat de bedrijven doen. Consumenten hoeven geen lange zoektochten naar specifieke producten te ondernemen. Gericht adverteren zorgt voor veel tijdswinst ('Media: Internet advertising: Targeted advertising: Timesaver or digital foot in the door?: In an age of surveillance, we are bound to worry about targeted online advertising. Can the industry convince the public it isn't spying on them?', *The Guardian*, 3 november 2008).

Aandachtspunten en implicaties voor Nederland in de toekomst

In Nederland heerst vooral het idee dat we begluurd worden, dat schetst een passief beeld. Er is als gevolg daarvan geen manifestatie van zelfredzaamheid van burgers, wat eigenlijk vreemd is. Aan de ene kant hechten Nederlanders blijkbaar veel aan hun privacy, en aan de andere kant doen burgers blijkbaar weinig om hun privacy te beschermen.

Een ander aspect van de discussie dat onderbelicht wordt, zijn de belangen van adverteerders. Groot-Brittannië en Spanje nemen het ook op voor de markt en zien de markt niet louter als kwaad. De discussie is genuanceerder in deze landen, het verdient aanbeveling een soortgelijke strategie te volgen. Op dit moment reageert de Europese politiek slechts op geluiden uit de privacy- of de markthoek zonder een vaste lijn te volgen.

Cookies zijn noodzakelijk om goed te surfen, in het Nederlandse debat wordt er nog te weinig onderscheid gemaakt tussen de verschillende cookies. Er wordt over het algemeen stelling genomen voor of tegen cookies. Het merendeel is tegen cookies, wetgeving zou verscherpt kunnen worden als er precies omschreven wordt welk soort cookies inbreekt op de privacy.

4.3 Elektronisch patiëntendossier

Algemene Inleiding

Met de opkomst van de digitale media is het delen van gegevens via netwerken verbeterd. Het elektronisch patiëntendossier (EPD) is een databank van persoonlijke zorggegevens die voor zorgverleners inzichtelijk is. Het archief gaat van papier naar digitaal, de ontwikkeling van een digitale infrastructuur heeft daarbij een grote rol. Specifieke inlogcodes voor zorgverleners beveiligen de toegang.

Het EPD biedt vooral voordelen op het gebied van de acute zorgverlening. Er hoeven minder vragen gesteld te worden per persoon, de medische geschiedenis is direct inzichtelijk en dat scheelt tijd die van levensbelang kan zijn.

Het Nederlandse debat tot nu toe

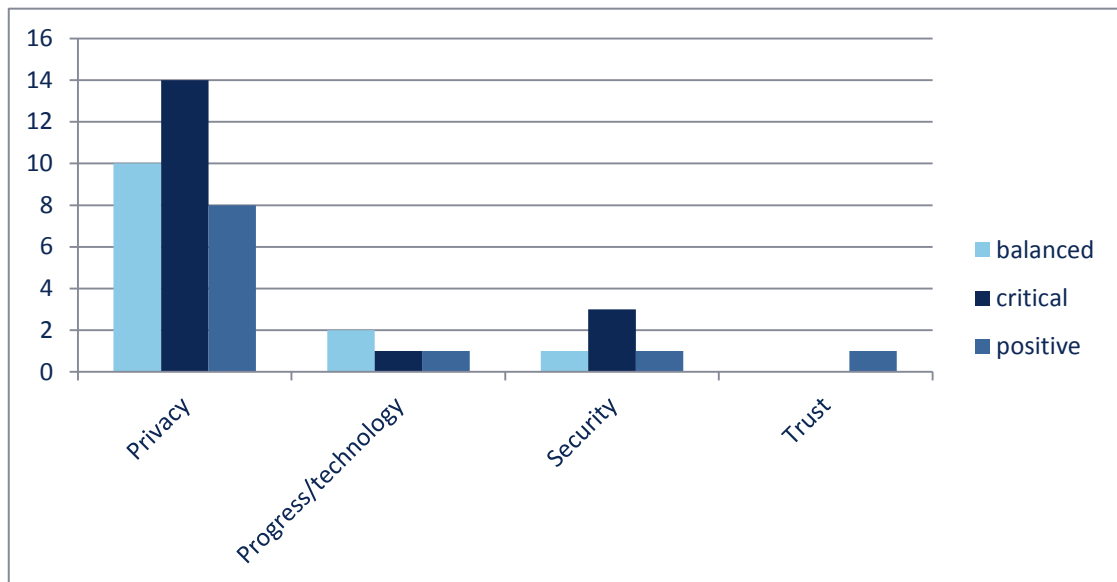
Sinds de introductie van het EPD in november 2008 zijn er geluiden die waken voor de privacy van de patiënt. Dat men angst heeft voor privacyschending en het delen van gegevens, heeft vaak te maken met de angst dat de gegevens bij de verzekeraars terecht komen en vervolgens tegen de patiënt gebruikt worden ('Patiëntengegevens voor het grijpen', *Trouw*, 10 december 2009). Verzekeraars zouden met behulp van de medische gegevens nieuwe persoonlijke premies vast kunnen stellen die duurder uit kunnen vallen.

Een ander argument tegen privacyschending is principieel. Door de geschiedenis heen hebben artsen de eed van Hippocrates af moeten leggen voor zij als arts beginnen. Dit bindt de artsen aan de doelen van hun beroep en zorgt voor het vertrouwen dat wij hebben in onze artsen. In de originele eed staan enkele passages die betrekking hebben op de privacy. Informatie over veiligheidslekken van het systeem stellen dus direct de betrouwbaarheid van de eed aan de kaak.

In de Tweede Kamer is een wetsvoorstel aangenomen dat het EPD gefaseerd in zou voeren vanaf november 2008. In 2010 werd de wet echter door de Eerste Kamer unaniem verworpen, naar aanleiding van de vermeende veiligheidslekken.

Edith Schippers heeft gestreden voor een doorstart van het EPD, ditmaal in de vorm van een vrijwillige overgang. ('Schippers belooft: EPD wordt veilig', *Algemeen Dagblad*, 30 november 2012). Alleen met expliciete toestemming van de patiënt worden de gegevens gedeeld in het dossier. Toch is er op deze plannen veel weerstand met wederom privacyschending als het grootste tegenargument. Tot op heden hebben ongeveer een miljoen burgers toestemming gegeven voor de opname van hun gegevens in het EPD.

De voorstanders van het EPD wijzen op de tijdswinst die geboekt kan worden met de database. In nood zal de beschikbaarheid van medische gegevens artsen niet alleen in staat stellen sneller hun werk te doen, sterker nog, zij kunnen ook hun diagnose op meer data baseren. Er wordt in een enkel geval zelfs geclaimd dat de privacy in het geval van het elektronische dossier beter gewaarborgd is dan bij de papieren versie ('Elektronisch patiëntendossier zegen voor privacybescherming,' *Financieele Dagblad*, 19 januari 2009).



Figuur 16: Overzicht van de kernwaarden in de discussie in Nederland omtrent het EPD, in aantallen nieuwsitems

Aangedragen alternatieven voor het EPD betreffen bijvoorbeeld een systeem waardoor burgers zelf controle houden over hun medische gegevens. Software creëert hier een beveiligde omgeving die alleen met een persoonlijke sleutel te bereiken is. Deze vorm van 'privacy by design' benadrukt de zelfredzaamheid van burgers. Een politieke drijfveer voor de doorstart en positief beleid voor het EPD is de aangelegde infrastructuur van 300 miljoen. Het is opvallend hoe vaak er gewezen wordt op de nadelige gevolgen van privacyschending in vergelijking met de voordelen.

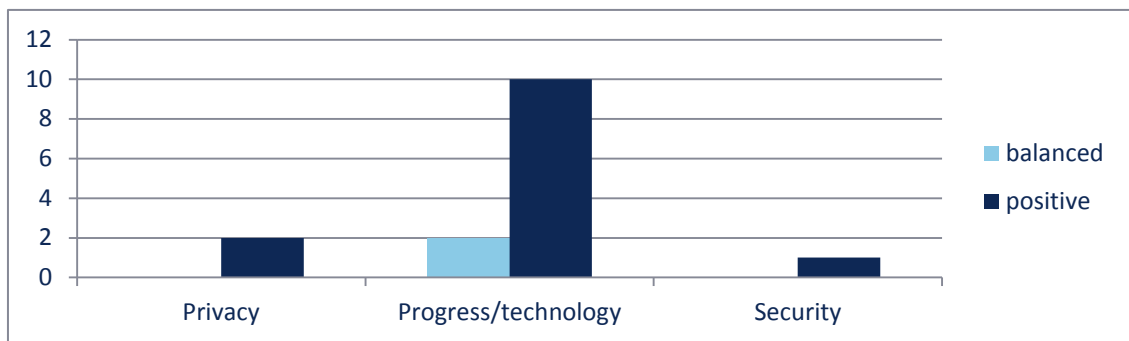
Belangrijkste trends en ontwikkelingen in het buitenland

Vergeleken met de andere Europese landen richt Nederland zich nadrukkelijk op privacy in de discussie omtrent het EPD.

In Spanje zijn de privacyoverwegingen minimaal en ondergeschikt aan het financiële gewin dat er te behalen is door het systeem. Omdat het land fors moet bezuinigen is het economische argument doorslaggevend voor een snelle invoering van het EPD. De meeste artikelen prijzen de voordelen van de technologische vooruitgang die een EPD mogelijk maakt.

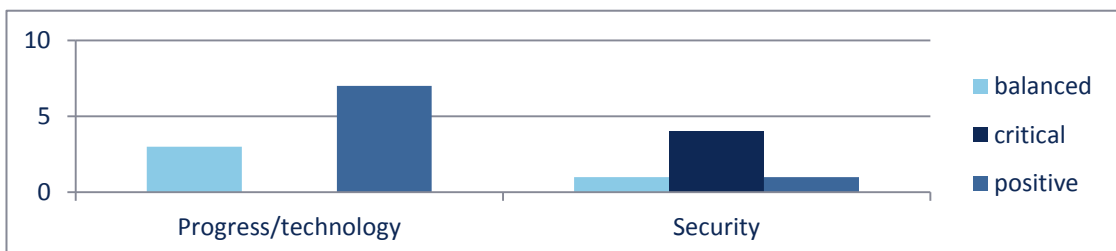
Groot-Brittannië is daarentegen meer met het privacyvraagstuk bezig dan Spanje. In een recente affaire waarbij het ministerie van Volksgezondheid anonieme gezondheidsgegevens doorverkocht heeft aan verzekeringsmaatschappijen, is privacy een nadrukkelijk punt van discussie. De vraag wordt eveneens gesteld of medische gegevens gekoppeld kunnen worden aan bepaalde personen door inlichtingendiensten. In dat geval zouden algoritmen er voor kunnen zorgen dat de data niet meer anoniem zijn. De media zijn over het algemeen echter positief over de veiligheid van de data.

In Vlaanderen is het debat ongeveer hetzelfde als in Spanje, de technologische vooruitgang en het financiële gewin worden geprezen. Sterker nog, in Vlaanderen heeft men het vrijwel nooit over de mogelijke privacy schendingen. Alleen de positieve aspecten worden benadrukt.



Figuur 17: kernwaarden en teneur in Vlaamse berichtgeving omtrent EPD, in aantal nieuwsitems

Het Duitse discours heeft een heel ander verloop. Duitse media zijn vooral bezig met de veiligheid van hun gegevens, en voeren het debat daarmee op een meer pragmatische manier dan in Nederland. Veiligheid gaat vooraf aan technologische vooruitgang is het credo in Duitsland. Het EPD is inmiddels ingevoerd, maar gekeken wordt naar betere beveiliging door de medische gegevens op een zorgpas, verwant aan de eID te zetten. Op deze manier heeft de burger meer keuze of zijn/haar gegevens gedeeld worden door meerdere zorginstellingen of verzekeraars.



Figuur 18: kernwaarden en teneur in Duitse berichtgeving omtrent EPD, in aantal nieuwsitems

Aandachtspunten en implicaties voor Nederland in de toekomst

Nederland kan van ieder bovengenoemd land een les leren. De les van Spanje is dat er nadrukkelijk gekeken wordt naar de economische aspecten van de technologische vooruitgang. Op het gebied van privacy dient de naïeve houding van Groot-Brittannië vermeden te worden, kijken naar veiligheid en privacy schendingen zoals in Duitsland verdient meer aanbeveling. De Duitse grondtoon is constructiever dan de Nederlandse, dat is vooral te zien aan de nadruk op veiligheid in plaats van privacy.

De Duitse media gebruiken vaak de term '*Datenschützer*'. De term betekent letterlijk gegevensbeschermers. In Nederland is daarentegen de term 'privacy-waakhond' gebruikelijker. Het verschil zit in het veiligheidsaspect waar Duitsland meer mee bezig is dan Nederland. Een waakhond zal waarschuwen, een gegevensbeschermers zal zich eerder bezighouden met het proces na het waarschuwen. De focus zou in de media en binnen organisaties meer op de term veiligheid kunnen komen dan op privacy. Linksom of rechtsom, Nederland zal mee moeten gaan met de tijd, maar zal de privacy in gedachten moeten houden. De zorgpas van Duitsland kan hiervoor oplossing bieden.

4.4 Slimme meter

Algemene Inleiding

Na smartphones en smartTV is er nu de slimme meter. Een technologische vooruitgang in de meterkast die al het energieverbruik digitaal inzichtelijk maakt. Door het inzichtelijk maken van het energieverbruik wordt gehoopt dat mensen minder energie zullen verbruiken en dat het installeren van een slimme meter de CO₂ uitstoot verder zal reduceren. De doelstelling van de EU is om voor 2020 bij 80% van de huishoudens een slimme meter geïnstalleerd te hebben.

De slimme meter heeft ook voordelen bij het monitoren van het opwekken van energie. Als consumenten zonne- of windenergie opwekken dan is het voordeel hiervan met een slimme meter veel inzichtelijker - consumenten zien wat ze zelf verdienen aan de stroom die ze opwekken. Een andere financiële prikkel die van de slimme meter uitgaat is het verschaffen van meer zekerheid over de hoogte van energierekeningen. Burgers zullen minder vaak voor onaangename verrassingen komen te staan bij het ontvangen van de rekening.

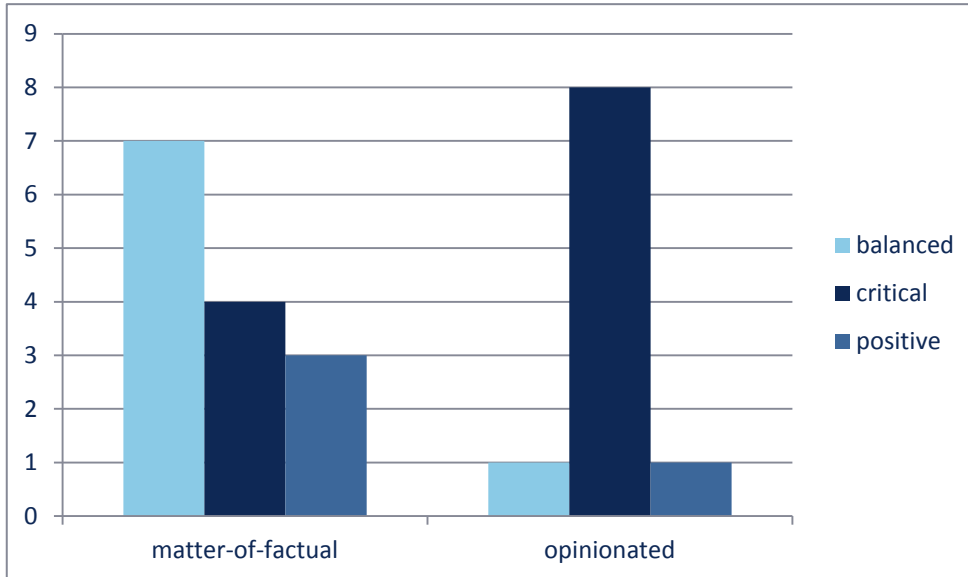
De toevoer van energie zal door toenemende opwekking van duurzame energie uit zon, wind en biomassa onregelmatiger en met meer pieken te maken krijgen.

Energieleveranciers kunnen met de kennis van het energieverbruik en via het medium van de slimme meter in de toekomst laten zien wanneer deze pieken zijn. Door aanpassingen van de prijs van energie aan de piekmomenten kan energie bespaard worden.

Het Nederlandse debat tot nu toe

In mei 2008 begint het debat over de slimme meter in de media. De aanleiding is een plan om de slimme meter verplicht in te voeren in Nederland. Het apparaat zal op ieder moment in verbinding staan met de energieleverancier. Het zal ook mogelijk zijn om op afstand de stroom af te sluiten in het geval van wanbetaling of overbelasting van het stroomnet.

Vanaf het wetsvoorstel zijn er uitsluitend kritische berichten die wijzen op de inbraak op de privacy. ('Zeg, doucht u altijd zo lang?; Slimme meter bedreigt privacy', NRC next, 2 juli 2008) Er wordt in deze berichten vooral benadrukt wat de negatieve gevolgen zijn van de inbreuk op de privacy.



Figuur 19: Slimme meter debat in NL

Via de slimme meter is al het energiegebruik van gebruikers te zien, aan de hand waarvan het gemakkelijk is om het leefpatroon van iemand in huis af te leiden. Belanghebbenden zouden aan de hand van het gebruik van gas kunnen zien wanneer iemand kookt. Het verbruik van warm water kan aangeven wanneer men doucht of de afwas doet. Als iemand veel water tegelijk gebruikt wordt dan is de WC doorgespoeld, als dat vaker gebeurt dan normaal kan de meter concluderen dat er iets mis is met zijn gezondheid. Nog een ander gevolg: dieven kunnen eenvoudig zien of er iemand thuis is of niet ('Energimeter is handig voor dieven en terroristen', *De Volkskrant*, 21 maart 2009).

Een schrikbeeld zoals dit komt vaak terug in de Nederlandse berichtgeving. Dit beeld wordt ingezet in de roep om privacy en het wordt gebruikt om pogingen te ondersteunen om het wetsvoorstel dat de slimme meter verplicht stelt tegen te houden. Dit gebeurt uiteindelijk ook als de Eerste Kamer in april 2009 tegenstemt ('Eerste Kamer: Verplichte energiemeter tast privacy aan', *Trouw*, 8 april 2009).

Sociale media laten zien dat de berichten steeds meer gericht zijn op technologische vooruitgang en minder op privacy. Gebruikers zijn over het algemeen bezig met de nieuwste modellen en technologische ontwikkelingen op het gebied van slimme energiemeters. Dat is te zien aan de vele vermeldingen op de site '*tweakers.net*.' Kritische berichtgeving met betrekking tot de privacy en de werking is te zien aan de berichten op de sites van '*Kassa*' en '*Radar*.'

Website	Bereik	Berichten
1. www.nuijij.nl		184
2. tweakers.net		139
3. www.telegraaf.nl		50
4. www.groeneluis.nl		39
5. weblogs.nrc.nl		31
6. www.energievastgoed.nl		28
7. gathering.tweakers.net		27
8. www.trosradar.nl		24
9. www.security.nl		21
10. kassa.vara.nl		21

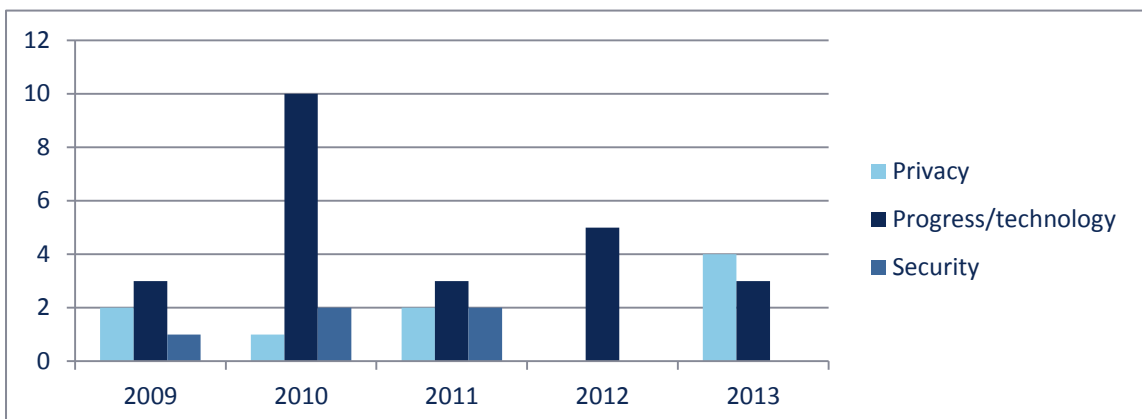
Figuur 20: Slimme energiemeter, bronnen (2.471 berichten)

Naar aanleiding van het tegenstemmen door de Eerste Kamer is de wet aangepast zodat het gebruik van de slimme meter vrijwillig wordt. Ondanks dat de berichtgeving na deze aanpassing gematigd positiever wordt zijn er nog steeds veel artikelen die de nadruk op het schrikbeeld en de inbreuk op de privacy leggen ('Slimme meters: pas op met privacy', *Algemeen Dagblad*, 12 juni 2012). Uiteindelijk komt er strenge wetgeving voor de beveiliging van de gegevens.

Belangrijkste trends en ontwikkelingen in het buitenland

Door de EU regelgeving heeft ieder land op een bepaald punt de verplichte invoering van de slimme meter overwogen. Het verschilt echter per land wat voor bezwaren ontstaan bij het gebruik van slimme meters, en wanneer deze bezwaren ontstaan.

Duitsland is het enige land waar het debat over de slimme meter pas begon nadat de meter al landelijk was ingevoerd. De houding in de artikelen is van een gematigd positieve naar een gematigd negatieve houding gegaan. Bij het schetsen van schrikbeelden zoals in Nederland ligt meer de nadruk op veiligheid en databescherming dan privacy ('Dann schalten Hacker die Lichter aus', *Die Zeit*, 29 april 2010). Na de NSA onthullingen van Edward Snowden in 2013 wordt bijvoorbeeld gewaarschuwd dat de NSA beschikking heeft tot de gegevens van de Duitse slimme meters ('Ein Bild aus tausend Spuren; In Zukunft verraten unzählige vernetzte Geräte den Spionen intime Details aus unserem Alltag - ganz automatisch', *Die Zeit*, 1 augustus 2013). Pas in een later stadium van het debat komt privacy dus in beeld, nadat technologische vooruitgang en veiligheid lang dominant waren in het Duitse debat.



Figuur 21: Dominante kernwaarden in Duitse debat over de slimme meter, in aantal nieuwsitems

In Vlaanderen wordt vooral gekeken naar de kosten die niet doorberekend mogen worden aan de consument. De invoering gaat heel zorgvuldig met meerdere pilots die geëvalueerd worden. De conclusie in Vlaanderen is dat de gewone Vlaming weinig energie zal besparen met de slimme meter, de voordelen zijn vooral voor eigenaren van zonnepanelen en grootverbruikers ('Slimme meter niet slim voor gewone man', *Gazet van Antwerpen*, 12 september 2011).

In Spanje wordt de slimme meter eenvoudigweg ingevoerd en worden alleen de voordelen benadrukt. Zweden begint in 2010 de voordelen te herkennen maar er ontstaat geen debat. Nederland is over het algemeen een voorloper in het discours. In Groot-Brittannië zijn ongeveer dezelfde ontwikkelingen als in Nederland gaande. Er wordt in de Britse media ook verwezen naar hoe de invoering in Nederland is verlopen. Privacy is een groot argument, maar het kostenargument weegt het zwaarst. Opvallend is wel dat de burgers zich weinig bewust zijn van het debat ('Majority of UK unaware of smart meters, research shows', *The Guardian unlimited*, 22 augustus 2012).

De kosten en de inefficiëntie bij het gebruik van zonnepanelen zorgen voor een negatieve houding tegenover de slimme meter in de onderzochte Europese landen. Privacy-schending is een argument dat ook op de achtergrond meespeelt in het buitenland. Waarschijnlijk gaan veel landen het voorbeeld van Nederland volgen om het gebruik van de slimme meter op vrijwillige basis in te voeren. Duitsland probeert zelfs de Europese regelgeving terug te draaien omdat het apparaat niet de geanticiperde kostenbesparing oplevert.

Aandachtspunten en implicaties voor Nederland in de toekomst

Het voordeel van het verloop van het debat in Nederland is dat de slimme meter niet verplicht ingevoerd is, terwijl de andere landen veel hebben geïnvesteerd in een snufje dat uiteindelijk niet de kostenbesparing oplevert die beloofd was, ook op het gebied van duurzame energievoorziening.

Toch focust het Nederlandse debat zich meer op de privacy en te weinig op de voordelen. In het geval dat de slimme meter wel een succes was geweest, dan had Nederland nu sterk achtergelopen op de Europese ontwikkelingen. Het is interessant om te kijken naar het Vlaamse verloop, hier is door pilots in te voeren aangetoond dat de slimme meter van beperkt nut is. Nederland heeft minder ruimte voor experimenten en blijft principieel afwijzend.

Het privacy-argument dat Nederland, Groot-Brittannië en Duitsland in een later stadium gebruiken heeft na de onthullingen van de NSA een betere onderbouwing gekregen. Nederland is alert geweest op het gebied van privacy en plukt daar nu de vruchten van.

In de toekomst is het afwachten of de Europese regelgeving aangepast wordt. Verder is het gebruik van wind- en zonne-energie niet hoog in Nederland en heeft het gebruik van de slimme meter daarom minder voordelen. Het huidige beleid waarin mensen zelf kunnen kiezen voor de slimme meter lijkt voorlopig aan te bevelen. Toch is het belangrijk om in de toekomst meer te kijken naar de voordelige gevolgen die de meter kan hebben.

4.5 Passagiersgegevens

Algemene Inleiding

Het afstaan van passagiersgegevens gaat over de verplichting van luchtvaartmaatschappijen om op verzoek van overheden gegevens over hun passagiers af te staan. Het initiatief hiervoor kwam vanuit Amerika na de terreuraanslagen op 9/11. Het delen van passagiersgegevens moet ervoor zorgen dat het veiligheidsrisico voor luchthavens en vliegvelden beter ingeschat kan worden. Dit neemt niet weg dat de Verenigde Staten en de Europese Unie touwtrokken over de inhoud van de te verstrekken passagiersgegevens. De wens van de VS om ook informatie te ontvangen over dieetwensen, religie et cetera gaat de Europese lidstaten te ver.

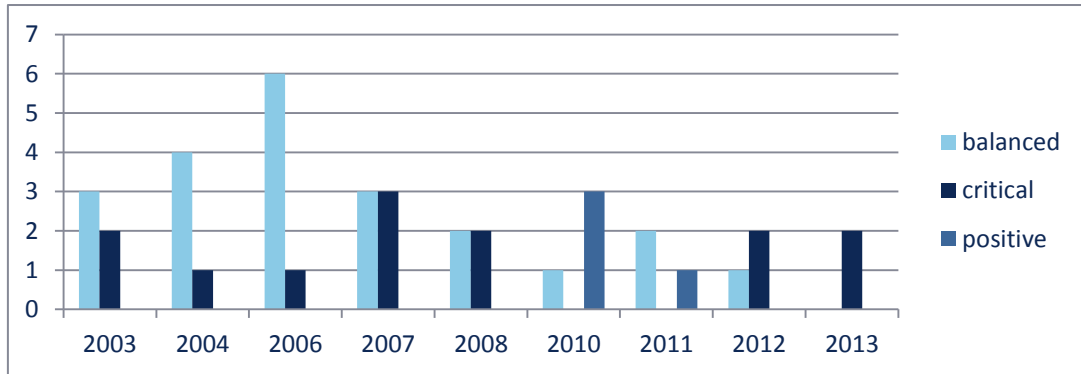
Ook binnen de EU wordt gewerkt aan gemeenschappelijke regels op grond waarvan de lidstaten nationale systemen voor de verwerking van passagiersgegevens moeten opzetten. De commissie werkt op dit moment aan een richtlijn aan de hand waarvan luchtvaartmaatschappijen de EU-lidstaten gegevens moeten verstrekken over de passagiers die de EU in- of uitreizen. De richtlijn is omstreden omdat ze het bewaren van passagiersgegevens voor vijf jaar en Profiling met PNR-gegevens toestaat. Op dit moment is de toekomst van de richtlijn nog niet duidelijk.

Het Nederlandse debat tot nu toe

In Nederland wordt de berichtgeving over het afstaan van passagiersgegevens enkel vanuit het perspectief van de privacy gevoerd. De teneur van de berichtgeving is echter in ontwikkeling: In de periode tot 2006 was de teneur van de berichtgeving vooral feitelijk. Er werd bericht over het getouwtrek tussen de Amerikaanse visie (“afstaan passagiersgegevens essentieel voor het bestrijden van terreur”) en de Europese visie (“afstaan passagiersgegevens zo beperkt mogelijk uit privacyoverwegingen”), (‘EU waakt over privacy van passagiers’, *Financieele Dagblad*, 9 september 2003). Wel is er een kritische onderstroom in de berichtgeving. (‘Reiziger naar VS levert zijn privacy in’, *de Volkskrant*, 10 januari 2003).

In de jaren 2007-2008 wint de kritische stroom aan positie. De berichtgeving wordt emotioneler; er spreekt meer verontwaardiging uit de berichtgeving (‘Op 4a zit een homo, op 16d een veganist; Vergaande registratie VS van luchtreizigers’, *NRC Next*, 7 September 2007; ‘Verdenkingen die nergens op slaan; Bezwaren tegen levering van passagiersgegevens aan VS’, *Trouw*, 27 augustus 2007).

Toch is het pas vanaf 2012 dat de kritische berichtgeving de overhand krijgt (‘Run op personalia EU-reiziger’, *Parool*, 20 april 2012; ‘Als het fout gaat, moet jij je onschuld maar zien te bewijzen’, *NRC Handelsblad*, 31 januari 2012). Dit is des te interessanter aangezien de berichtgeving tot 2010 vooral feitelijk is, en in 2010 en 2011 zelfs positief (‘VS willen meer inzage in gegevens passagiers’, *Financieele Dagblad*, 5 november 2010; ‘EU wil waarborg privacy reizigers’, *Spits*, 3 februari 2011).



Figuur 22: Teneur van het debat over afstaan van passagiersgegevens in Nederland door de jaren heen, in aantal nieuwsitems

Qua argumenten voor het delen van passagiersgegevens staat één punt centraal: het verijdelen van terroristische aanslagen. Dit argument wordt herkend in de berichtgeving maar er wordt een aantal tegenargumenten genoemd die pleiten voor een heel zorgvuldige afweging voor de mate van het afstaan van gegevens: het belangrijkste is uiteraard dat de uitwisseling indruist tegen de bescherming van onze privacy; vooral in de mate en vorm zoals gewenst door de VS (inclusief gegevens over dieet, seksuele geaardheid, religie maar ook het lange tijd bewaren van de gegevens). Andere argumenten zijn de onnodige arrestaties die het gevolg zijn van profiling op basis van passagiersgegevens en het feit dat het beschikbaarstelling veel administratieve lasten met zich meebrengt.

De aanslagen van 11 september 2001 zijn zonder enige twijfel de belangrijkste gebeurtenis in het debat. Echter, te zien is dat met het verloop van tijd de invloed van 9/11 wat afzwakt. Binnen Europa is de voortgang omtrent de richtlijn over het verstrekken van passagiersgegevens inmiddels ook een 'gebeurtenis' geworden dat het debat medebepaalt. Dit verklaart ook de ontwikkelingen in het discours in Nederland van redelijk feitelijk tot 2008, positief in de jaren 2009 en 2010 en overwegend kritisch na 2010. De EU wordt gezien als ambassadeur en strijder voor de bescherming privacygegevens in Nederland.

Auteur	Berichten	Invloed
1. SophieintVeld	85	26,7
2. Eerste Kamer der Staten-Generaal	34	×
3. I.W. Opstelten	23	×
4. zegmaarpatrik	22	21,3
5. ANP	21	×
6. D66	16	34,9
7. persd66brussel	16	9,6
8. KLM	16	16,1
9. René Schoemaker	15	×
10. Gerard Schouw	15	×

Figuur 23: Auteurs passagiersgegevens (1.728 berichten)

Sophie in 't Veld en D66 zijn binnen Nederland de actoren met de meeste invloed binnen dit debat. In de overige debatten is de aanwezigheid van D66 minder sterk. Toch is D66 de partij met de meeste hits bij de social media-analyse. In de bovenstaande grafiek zijn de helft van de auteurs gerelateerd aan D66. (Sophie in 't Veld, 'zegmaarpatrik,' D66, persd66brussel en Gerard Schouw). Onder het kopje 'invloed' zijn vier van de vijf actoren met een hoge invloed gerelateerd aan D66.

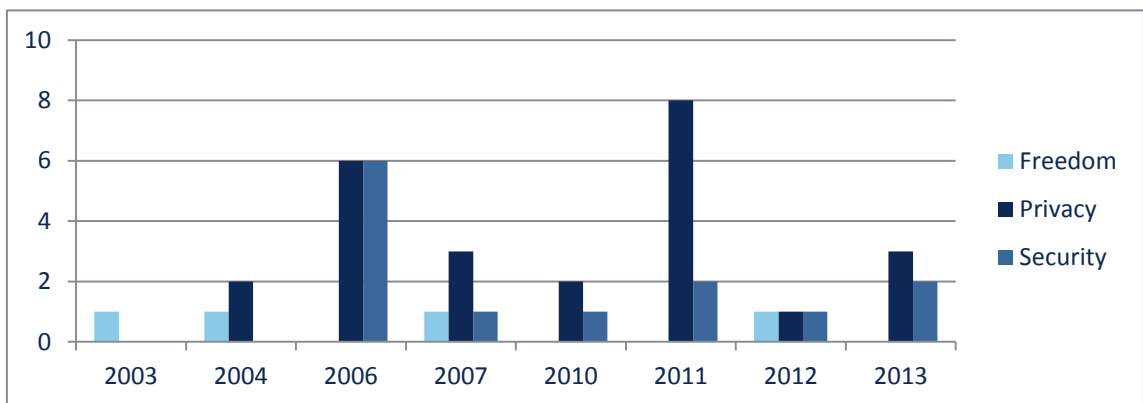
Dit uitgangspunt blijft onveranderd maar in de laatste jaren komt er steeds meer frustratie over het getouwtrek met de VS en de vergaande eisen van de EU.

Belangrijkste trends en ontwikkelingen in het buitenland

Ook in de andere lidstaten volgt de berichtgeving de ontwikkelingen in Brussel nauwlettend. Samen met 9/11 is de Europese richtlijn over het verstrekken van passagiersgegevens daarmee de belangrijkste 'gebeurtenis' die het debat bepaalt. Het discours in de andere landen is echter genuanceerder dan in Nederland: het perspectief van (het beschermen van de) privacy is minder dominant. Ook veiligheid en vrijheid zijn belangrijke invalshoeken.

Duitsland en Engeland nemen de meest extreme posities in het debat in.

Duitsland is het land waar het discours het meest kritisch is over het afstaan van passagiersgegevens en ook het meest principieel gevoerd wordt. Dit is te verklaren met de geschiedenis van Duitsland, specifiek de Tweede Wereldoorlog en de desastreuze gevolgen van de registratie van persoonsgegevens van Joden. Anders dan in Nederland wordt het debat dan ook in eerste instantie gevoerd vanuit het perspectief van veiligheid, wat vervolgens gekoppeld wordt aan privacy ('Der gläserne Passagier ist der Willkür ausgeliefert; Der skandalöse Transfer sensibler Fluggastdaten an US-Sicherheitsbehörden verstößt gegen Bürgerrechte und Europäischen Datenschutz', *Frankfurter Rundschau*, 8 augustus 2004).



Figuur 25: Kernwaarden in het Duitse debat over het afstaan van passagiersgegevens door de jaren heen, in aantallen artikelen

Overall in de Duitse media is de teneur dat de VS de EU onder druk zetten bij het sluiten van akkoorden over het afstaan van passagiersgegevens en dat de overeenkomsten tegen de Europese burgerrechten indruisen. De berichtgeving is als genuanceerd te bestempelen, consequenties van gebeurtenissen worden vaak uitgebreid beschreven, zoals de berichtgeving over het oordeel van het Europese Hof van Justitie over de nietigverklaring van het omstreden akkoord tussen de EU en de VS in mei 2006 ('Pyrrhussieg für das Europaparlament und den Datenschutz; Der Europäische Gerichtshof erklärt Vertrag über Weiterleitung von Fluggastdaten in die USA für nichtig - Nun hat Amerika freie Hand', *Stuttgarter Zeitung*, 31 mei 2006).

De 'Bundesbeauftragte für den Datenschutz' is de belangrijkste persoon in de berichtgeving. Zijn activiteiten en uitingen worden nauw gevolgd ('Fluggast-Daten sollen besser geschützt werden; Bundesdatenschutzbeauftragter Schaar für neue Verhandlungen

der Europäer mit den USA', Berliner Zeitung, 13 juni 2006 of USA behalten Zugriff auf Europas Fluggastdaten Datenschutzbeauftragter Schaar rügt neues EU-Abkommen, *Berliner Zeitung*, 19 november 2011).

In Engeland is de berichtgeving over het algemeen neutraal. De belangrijkste perspectieven van waaruit het delen van passagiersgegevens wordt besproken zijn veiligheid en privacy. Veiligheid wordt hier echter anders geladen dan in Duitsland. Het gaat om de veiligheid van de staat en het afstaan van passagiersgegevens wordt dan ook vooral gezien als een waardevol instrument voor politie en justitie in de strijd tegen het terrorisme en ernstige misdaad ('Airline passengers' sensitive data to be handed to US; Millions of airline customers' personal data will be handed over to the United States after MEPs voted for new laws that it's claimed are vital to tackle terrorism', *The Telegraph*, 19 april 2012).

In de andere drie landen, Vlaanderen, Spanje en Zweden ligt het debat tussen deze bandbreedtes, waarbij het nog interessant is te vermelden dat in Vlaanderen het debat heel zakelijk en feitelijk gevoerd wordt. Er wordt simpelweg bericht over lopende ontwikkelingen, over het algemeen zonder hieraan een waardeoordeel te koppelen. Of dit te maken heeft met de eigen politieke onrust over splitsing tussen Vlaanderen en Wallonië of een meer pragmatische benadering van onderwerpen waarop de EU actief is en men als klein land weinig input heeft, is hier niet te zeggen.

Aandachtspunten en implicaties voor Nederland in de toekomst

In Nederland lijkt het debat opgeslokt te worden door het perspectief van privacy. Zodra privacy in het geding komt, lijkt een genuanceerder beeld niet mogelijk. Voor een meer objectiever en genuanceerder debat helpt de blik naar de oosterburen: Hier gaat het debat vooral over de veiligheidsrisico's die de schending van de privacy met zich mee brengen. Veiligheid is de reden dat men niet wil dat de privacy geschonden wordt. In Nederland is het gevaar voor de veiligheid onderbelicht, en gaat het meer om het principe van de privacy.

Op dit onderwerp zijn er geen directe beleidsmaatregelen of interventies die als voorbeeld voor Nederland kunnen dienen. Gezien de rol van de EU is de nationale handelingsruimte beperkt.

5 Samenvatting per onderwerp

In dit laatste hoofdstuk brengen wij de bevindingen uit de hoofdstukken 2 en 3 samen, en distilleren hieruit een samenvatting per onderwerp.

5.1 Kernonderwerpen: ID-management

- **Identiteitsfraude**
Nederland en Groot-Brittannië spannen de kroon wat betreft berichtgeving of identiteitsfraude. In Groot-Brittannië lijkt het fenomeen echter veel vaker voor te komen dan in Nederland. In de omgang met identiteitsfraude lijkt de Nederlandse overheid zich veel te richten op straffen, en minder op preventie. In landen als Vlaanderen en Spanje wordt nadrukkelijker gewezen op de gevaren van identiteitsfraude om de zelfredzaamheid van burgers te vergroten.
- **eID**
In Nederland is er, vergeleken met Vlaanderen, Duitsland en Spanje, relatief weinig ervaring met de eID. In deze drie landen, met uitzondering van Vlaanderen, wordt de eID echter bijzonder weinig gebruikt door burgers. De crux om gebruik te bespoedigen lijkt te liggen bij het betrekken van de private sector in het door ontwikkelen van de eID kaart: in Vlaanderen wordt de eID op relatief grote schaal gebruikt bij identificatie en authenticatie voor het afsluiten van overeenkomsten met dienstverleners uit de private sector.
- **Biometrisch paspoort**
Vergeleken met de andere onderzochte landen lijkt het Nederlandse debat over biometrie een meer principiële insteek te hebben in de vorm van privacy. In met name Vlaanderen, Zweden, Duitsland en Spanje wordt pragmatischer omgegaan met biometrie, wat overigens een kritische houding op het gebied van databeveiliging niet in de weg staat. Het publieke debat over biometrische gegevens in Groot-Brittannië valt op door de hoge mate van cynisme over publieke IT projecten.

5.2 Ondersteunende onderwerpen

- **NSA/PRISM**
Het debat over de afluisterpraktijken van de NSA kent de grootste nationale verschillen. Dit is ook niet vreemd, gezien de verschillen in betrokkenheid van de nationale inlichtingendiensten en de manier waarop de landen al dan niet in eigen lijve met de afluisterpraktijken geconfronteerd werden.

In Nederland wordt het debat principieel gevoerd met nadruk op het privacy-aspect. Er is nog weinig aandacht voor concrete oplossingen. Ook is er in vergelijking met de andere landen relatief weinig aandacht voor de zelfredzaamheid van burgers en mogelijkheden voor een zo veilig mogelijke omgang met internet en (mobiele) telefonie.

- **Behavioral profiling**
Ook op dit gebied wordt het debat in Nederland eenzijdig gevoerd. Cookies worden over het algemeen als slecht afgeschilderd, terwijl ze essentieel zijn in het faciliteren van functioneel gebruik van het internet. In landen als Spanje en Groot-Brittannië is er meer ruimte voor de positie van internetbedrijven en hun belangen. Daarnaast is er in Nederland, net zoals bij identiteitsfraude, meer nadruk op sanctionering dan op zelfredzaamheid.

- Elektronisch patiëntendossier
Ook bij het elektronisch patiëntendossier valt op dat er in Nederland bovengemiddeld veel aandacht is voor privacy in het debat en minder voor dataveiligheid. Dit in tegenstelling tot bijvoorbeeld Duitsland, waar de discussie over het uitwisselen van patiëntengegevens meer inhoudelijk en minder ideologisch wordt gevoerd. In andere landen, zoals Spanje, Vlaanderen en Zweden, is er vooral aandacht voor de vooruitgang en het gemak dat gepaard gaat met een elektronisch patiëntendossier.
- Slimme meter
De nadruk op privacy in het Nederlandse debat over de slimme energiemeter, en de hieruit resulterende vertraging van invoering, heeft een onverwacht voordeel gehad ten opzichte van invoering van de meter in het buitenland. Namelijk: door verplichte en gehaaste invoering in het buitenland is de slimme meter daar mislukt. Het huidige beleid in Nederland waarin burgers zelf kunnen kiezen voor de slimme meter heeft vooralsnog goed uitgepakt. In het buitenland lijkt er echter beduidend meer aandacht te zijn voor de voordelen die de meter kan bieden.
- Passagiersgegevens
Het debat over de overdracht van passagiersgegevens speelt zich af op het snijvlak tussen staatsveiligheid en privacy van individuele burgers. In Groot-Brittannië lijkt staatsveiligheid in dit debat de overhand te hebben, terwijl in Nederland en Duitsland vooral het privacy-aspect van deze afweging aan bod gekomen. In Nederland wordt dit debat op principiële niveau gevoerd. Tegelijkertijd is de invloed van het nationale debat op daadwerkelijke besluitvorming beperkt - beleid op dit gebied komt immers met name vanuit de EU.

6 Beschouwing per land

Tot nu toe is het onderzoek over ID-management vooral ‘verticaal’ vormgegeven, op basis van de onderzochte kernonderwerpen en ondersteunende onderwerpen. Dit hoofdstuk, daarentegen, besteedt aandacht aan beschouwingen op ‘horizontaal’ niveau. Hoe loopt, tussen de verschillende onderwerpen door, het maatschappelijk debat over ID-management langs de lijnen van privacy, veiligheid, technologische vooruitgang en vertrouwen in overheid en de private sector?

6.1 Nederland

Over het algemeen genomen, en in vergelijking met de andere onderzochte landen, blijkt dat in Nederland privacy de meest nadrukkelijke kernwaarde is in (vrijwel) elke maatschappelijke discussie omtrent ID-management. Iedere ontwikkeling die gepaard gaat met identiteit en technologische vooruitgang wordt direct aan het schenden van privacy gekoppeld, vaak zonder dat de principiële aandacht voor privacy wordt geconcretiseerd. Dit maakt privacy in het Nederlandse debat een relatief ongedefinieerd begrip, wat een meer inhoudelijke discussie op het snijvlak van privacy, veiligheid, technologische vooruitgang en vertrouwen in de weg lijkt te zitten. Het zou te ver gaan om de ideologische discussie in Nederland op het gebied van privacy aan de rol van media te wijten. Echter, in vergelijking met andere onderzochte landen, met name Duitsland, blijkt dat de Nederlandse media zich weinig constructief opstellen in debatten omtrent ID-management. Traditionele journalistieke waarden als hoor en wederhoor lijken minder van toepassing wanneer het om vermeende privacy-schendingen gaat. Hiermee gaat de nuance verloren in maatschappelijk relevante debatten over, bijvoorbeeld, de verhouding tussen veiligheid en privacy.

6.2 Duitsland

In Duitsland lijkt er, van alle onderzochte landen, het meeste ruimte te zijn voor een evenwichtig maatschappelijk debat over ID-management. Binnen de gebieden van privacy, veiligheid, technologische vooruitgang en vertrouwen is er in Duitsland sprake van een grote maatschappelijke betrokkenheid en inhoudelijke kennis. De media faciliteren het forum waarop deze inhoudelijke discussie plaatsvindt. Hoewel Duitsland strenge privacywetgeving kent, en privacy een belangrijke kernwaarde is voor veel Duitsers, is er wel degelijk ruimte voor tegengeluiden in het maatschappelijk debat: (nationale) veiligheid, technologische vooruitgang, en het succes van de private sector in bijvoorbeeld de biometrische industrie. Discussies die raken aan ID-management zijn over het algemeen genuanceerd, inhoudelijk en niet-ideologisch.

6.3 Spanje

De maatschappelijke houding ten opzichte van ID-management in Spanje lijkt enigszins afwachtend te zijn. Waar in landen als Duitsland en Nederland veel kritische aandacht is voor de rol van de EU en VS in het uitwisselen van identiteitsgegevens, worden dergelijke ontwikkelingen in Spanje met afstand gadeslagen. Over het algemeen lijkt er in Spanje veel aandacht te zijn voor technologische vooruitgang en de rol van de private sector op het gebied van ID-management. Deze nadruk op technologie en het bedrijfsleven lijkt echter ook gebonden te zijn aan politieke oriëntatie: vanuit rechts-conservatieve hoek wordt publiek-private samenwerking in het verwerken of beschermen van identiteitsgegevens nadrukkelijk ondersteund, terwijl Spanjaarden met een links-progressieve politieke oriëntatie van nature kritischer lijken te staan ten opzichte van dergelijke ontwikkelingen.

6.4 Groot-Brittannië

Groot-Brittannië is in veel opzichten een uitzondering ten opzichte van de andere onderzochte landen naar aanleiding van het maatschappelijke debat over ID-management. Deze uitzonderingspositie uit zich op drie manieren. Allereerst staat de overheid nadrukkelijk op afstand wanneer het gaat om het beschermen van identiteitsgegevens van burgers. Dit wordt met name aan de private sector gelaten, en dit lijkt met weinig succes te gebeuren - de aanpak van identiteitsfraude is hier een goed voorbeeld van. Tegelijkertijd, en ten tweede, is de overheid een stuk actiever in het beschermen van (nationale) veiligheid ten koste van privacy en zelfbeschikking van burgers, en de media, met uitzondering van *the Guardian*, zijn hier weinig kritisch bij. Ten slotte kenmerkt het Britse maatschappelijk debat zich door een cynische houding ten opzichte van de overheid in het faciliteren van ID-management. IT projecten geïnitieerd door de overheid worden bij voorbaat door de media beschouwd als gedoemd te mislukken, wat een inhoudelijke discussie over nut en noodzaak in de weg staat.

6.5 Zweden

Opvallend aan Zweden is, dat identiteitsmanagement in verhouding weinig aanleiding voor publieke discussie is. Over wat in andere landen gevoelige dossiers zijn, zoals biometrie en het elektronische patiëntendossier, wordt in Zweden vooral vanuit het perspectief van technologische vooruitgang geredeneerd. Van de felheid die het maatschappelijk debat in Duitsland of Nederland kenmerkt, lijkt in Zweden veel minder sprake te zijn. Daarnaast streeft Zweden traditioneel een cultuur van openheid na. Het zogenaamde "offentlighetsprincipen" is stevig verankerd in de Zweedse cultuur: alle overheidsdocumenten zijn in principe voor iedereen toegankelijk, en de belastingaangiften van Zweedse burgers zijn openbaar beschikbaar. Dit principe van radicale openheid vanuit de overheid lijkt voor minder achterdocht te zorgen in de Zweedse samenleving. Omdat de overheid veel informatie aan burgers geeft, is het voor burgers ook makkelijk om veel persoonlijke informatie aan de overheid toe te vertrouwen.

6.6 Vlaanderen

In Vlaanderen worden debatten op het gebied van identiteitsmanagement relatief nuchter gevoerd. Dit staat in sterk contrast met de vaak emotionele toon van vergelijkbare debatten in Nederland. Over het algemeen is er veel aandacht voor de technologische vooruitgang die bijvoorbeeld biometrie, elektronische patiëntendossiers en slimme meters met zich meebrengen, en blijven kritische geluiden vanuit bijvoorbeeld een privacy-perspectief achterwege. Wat daarnaast opvalt is de integrale aanpak die in Vlaanderen nagestreefd wordt in het faciliteren van ID-management: de eID, gekoppeld met biometrische gegevens, worden nadrukkelijk gepositioneerd als een strategie om identiteitsfraude aan te pakken. Deze aanpak lijkt succesvol te zijn: de eID wordt op aanzienlijke schaal gebruikt, en identiteitsfraude lijkt een minder groot maatschappelijk probleem te zijn dan in Nederland en Groot-Brittannië. Ten slotte lijkt het alsof de verregaande regionalisering van openbaar bestuur in Vlaanderen ervoor zorgt dat de implementatie van ID-management projecten ook een regionaal karakter heeft. Hierdoor worden mogelijke controverses ook op regionaal niveau afgehandeld, waardoor nationale debatten een genuanceerd karakter hebben.

7 Suggesties

Dit rapport heeft een uiteenzetting gegeven van het publieke debat omtrent ID-management in vijf Europese landen, waaronder Nederland. Op het gebied van identiteitsfraude, de eID, het biometrische paspoort als kernonderwerpen, en de aanvullende onderwerpen NSA, behavioral targeting, EPD, slimme meter en passagiersgegevens is het discours in Nederland, Vlaanderen, Groot Brittannië, Zweden, Spanje en Duitsland geanalyseerd.

De acht onderzochte onderwerpen raken elkaar nadrukkelijk, of liggen in elkaars verlengde. Het delen van passagiersgegevens met de Verenigde Staten staat in verband met de spionagepraktijken die tot het NSA schandaal geleid hebben. De eID kan eveneens biometrische gegevens bevatten, en beide toepassingen kunnen gebruikt worden om identiteitsfraude tegen te gaan.

Daarnaast blijkt uit de beschouwing van hoofdstuk zes een verscheidenheid aan socio-economische, politieke en culturele fenomenen die in de onderzochte landen invloed hebben gehad op het publieke debat omtrent ID-management.

Dit laatste hoofdstuk bouwt voort op de samenvatting uit hoofdstuk 4, en de beschouwing uit hoofdstuk 5. Op basis van de bevindingen van dit onderzoek kan een aantal suggesties aangedragen worden voor de rol die het ministerie van BZK aan kan nemen in het maatschappelijke debat over ID-management in Nederland.

7.1 Kritische houding en evenwichtig debat

Een kritische houding ten opzichte van ID-management hoeft een evenwichtig debat niet in de weg te staan

De staat van het maatschappelijke debat in Duitsland toont aan dat het mogelijk is om een genuanceerd en afgewogen discussie te voeren over ontwikkelingen in ID-management. In een dergelijk stelsel bieden de media een forum waar verschillende belangen en meningen samenkomen, en waar burgers zich kunnen laten informeren over onderwerpen op het spectrum van privacy, veiligheid, technologische vooruitgang en vertrouwen in overheid en privat sector. Hier kan dan nog steeds een kritische houding uit voortkomen, maar dit is dan wel een kritische houding vanuit een goed geïnformeerd perspectief.

Een 'forumfunctie' zoals in Duitsland hebben Nederlandse nieuwsmedia in mindere mate. Berichtgeving in de Nederlandse media op het gebied van ID-management is over het algemeen opiniërend, met een sterke en ideologische nadruk op het privacy-aspect. Er bestaat een zekere achterdocht richting de overheid, gevoed door slechte ervaringen met het biometrische paspoort, slimme meters, en het elektronisch patiëntendossier. Hier lijkt een kans voor de overheid te liggen om ID-management in de toekomst op een andere manier in te richten: door de discussie op te zoeken, en vanaf het begin openheid van zaken te geven, kan bijgedragen worden aan een constructief debat in de samenleving over de voortgang van ID-management. Burgers uitgebreid informeren via de media over ID-management leidt waarschijnlijk tot minder achterdocht en een beter ingevoerd debat.

7.2 Regionale aanpak kan debat nuanceren

Een regionale implementatie van ID-managementprojecten kan een nuancerend effect op nationale debatten hebben

Uit de ervaringen in Vlaanderen blijkt dat een regionale implementatie van ID-managementprojecten de angel haalt uit principiële debatten op nationaal niveau. Regionale implementatie voorkomt niet dat er controverses ontstaan, maar de afhandeling van dergelijke controverses kan dicht bij de burger plaatsvinden. Hierdoor dringen discussies over, bijvoorbeeld, kapotte chips in eIDs, niet door tot het nationale publieke debat.

Het Nederlandse bestuurlijke systeem is minder verregaand geregionaliseerd dan het geval is in Vlaanderen. Dit wil echter niet zeggen dat het onmogelijk is om bijvoorbeeld gemeenten meer ruimte en vrijheid te geven bij de invoering van toekomstige toepassingen van ID-management. Zeker wanneer het de bedoeling is dat de private sector meer aansluiting zoekt bij dergelijke ontwikkelingen, zijn lagere overheden de meer natuurlijke partners van het bedrijfsleven bij de implementatie van slimme meters of patiëntendossiers. De centrale overheid kan zich zo richten op haar veiligheidstaak in het beschermen van persoonsgegevens.

7.3 Radicale openheid voor meer vertrouwen

Radical openheid van informatie kan een succesvolle strategie zijn om meer vertrouwen in de overheid te wekken bij het ontwikkelen van ID-management projecten voor burgers

Vertrouwen werkt twee kanten op, zo toont Zweden aan: wanneer de overheid burgers vertrouwt en openheid van zaken geeft, zijn burgers ook eerder geneigd om de overheid te vertrouwen. Nu is de Zweedse *high-trust society* niet eenvoudig te repliceren in Nederland, en dat is wellicht ook niet geheel wenselijk in een geglobaliseerde en genetwerkte wereld. Dit wil echter niet zeggen dat geen voorbeeld genomen hoeft te worden aan een radicaal open overheid. Een overheid die verwacht dat de gemiddelde burger niets te verbergen heeft, komt geloofwaardiger over wanneer zij als overheid zelf te kennen geeft niets te verbergen te hebben. Openheid van zaken vanuit de overheid wekt vertrouwen onder burgers.

7.4 Schaalvoordelen door integrale visie

Een integrale visie op ID-management die verder gaat dan afzonderlijke thema's kan voor schaalvoordelen zorgen

ID-management lijkt in Nederland versnipperd te zijn geraakt over een verscheidenheid aan dossiers. Discussies over het elektronisch patiëntendossier, slimme meters, het biometrisch paspoort en identiteitsfraude zijn in bepaalde mate een herhaling van zetten. Hierdoor blijft het maatschappelijke debat steken in een eerste, vaak privacy-gerelateerde reactie op technologische ontwikkelingen op het gebied van ID-management vanuit de overheid.

Het is echter wel degelijk mogelijk om een meer integrale aanpak na te streven, waarin verschillende dossiers aan elkaar gekoppeld kunnen worden. Zo tonen ervaringen uit Vlaanderen aan dat de aanpak van identiteitsfraude gekoppeld kan worden aan de ontwikkeling van de eID en het biometrisch paspoort. Wanneer burgers inzien dat ID-management ook (en vooral) bijdraagt aan hun eigen mogelijkheid om persoonsgegevens beter te beschermen, zou er minder scepsis hoeven te ontstaan. Het is onwenselijk wanneer

ID-management in de perceptie van burgers vooral bekend staat als een middel van de overheid om zo veel mogelijk persoonsgegevens op te slaan, en die teneur heeft het debat in Nederland op dit moment wel.

7.5 Publiek-private samenwerking

Succesvolle publiek-private samenwerking is belangrijk om ID-management onder burgers te stimuleren

Een nieuw ID-management kan technisch perfect zijn, en de data van gebruikers bijzonder goed beveiligd hebben. Wanneer burgers echter weinig praktische toepasbaarheid zien van een dergelijk ID-management systeem, dan zal gebruik in de praktijk tegenvallen. Deze stelling kan onderschreven worden door ervaringen in Duitsland en Spanje, waar technisch goed functionerende ID-managementprojecten door achterblijvend gebruik nu als mislukt beschouwd worden. Succesvol gebruik van ID-management in de dagelijks praktijk lijkt voor een groot gedeelte afhankelijk te zijn van in hoeverre de private sector aangesloten is bij ontwikkelingen.

Binnen de private sector is er veel kennis en ervaring aanwezig over het beschermen van persoonsgegevens, en het faciliteren van dienstverlening aan de hand van gedigitaliseerde persoonsgegevens. Ook kan de private sector bijdragen aan het creëren van maatschappelijk draagvlak om zelfredzaamheid en digitale geletterdheid te stimuleren: banken hebben er net zo veel belang bij dat burgers zorgvuldig met hun persoonsgegevens omgaan als overheden. Ten slotte is de verankering van ID-management in het dagelijks leven van burgers in hoge mate afhankelijk van de private sector. Wanneer burgers hun identiteitsgegevens op een uniforme manier kunnen gebruiken bij het aangaan van overeenkomsten, het afnemen of verlenen van diensten, zal deze praktijk naar verwachting spoedig gebruikelijk worden in de samenleving.

7.6 Doorontwikkeling eID

Bij het doorontwikkelen van de eID in Nederland liggen veel kansen voor een succesvolle implementatie

Vrijwel alle bovenstaande suggesties kunnen toegepast worden op de ontwikkeling van de eID in Nederland. Voor veel Nederlandse burgers is de eID nog een onbekend begrip. Daarom is er nu nog in verregaande mate de mogelijkheid voor de overheid om initiatief te nemen tot het invoeren van de eID die een aantal noodzakelijke randvoorwaarden voor succesvolle implementatie nastreeft. Op basis van dit rapport zijn deze randvoorwaarden de volgende: (1) implementeer de eID vanuit een perspectief van een open overheid; (2) zoek nadrukkelijk het maatschappelijke debat op; (3) verbind de eID op een integrale manier aan andere onderwerpen op het gebied van ID-management, zoals het tegengaan van identiteitsfraude; (4) betrek de private sector in ontwikkeling en toepassing; en (5) maak gefaseerde, regionale implementatie mogelijk waarbij lokale overheden een rol van betekenis spelen.

8 Bijlagen

8.1 Onderzoeksvragen

De hoofdvraag luidt:

Hoe ziet het politieke en maatschappelijke discours op het terrein van techniek, privacy, vrijheid, vertrouwen en veiligheid met betrekking tot ID-management in Nederland en verschillende andere landen er uit sinds 2001?

De hoofdvraag is verder uitgesplitst in elf sub-vragen:

- a Welke argumenten, overwegingen en sentimenten rondom privacy en veiligheid worden naar voren gebracht in de discussie?
- b Welke maatschappelijke gebeurtenissen, overheidsmaatregelen en (uitspraken van) personen zijn toonaangevend geweest in het discours?
- c Welke culturele aspecten – tradities, waarden, symbolen – hebben het discours in de greep gehad?
- d Op welke aspecten focust de discussie zich in de diverse landen?
- e Hoe krijgt de rol en de zelfredzaamheid van de burger een plaats in de discussie op het terrein van techniek, privacy en veiligheid met betrekking tot ID-management?
- f Hoe krijgt de rol van private partijen een plaats in de discussie op het terrein van techniek, privacy en veiligheid met betrekking tot ID-management?
- g Hoe krijgt de rol van de overheid een plaats in de discussie op het terrein van techniek, privacy en veiligheid met betrekking tot ID-management?
- h In hoeverre hebben biometrie en technologische vernieuwingen een vaste positie gekregen in het systeem van identiteitsmanagement binnen de diverse landen?
- i Welke conclusies zijn er politiek getrokken op basis van de discussie?
- j Welke consequenties heeft de discussie gehad? Geef aan of er een vertaling naar concrete maatregelen is gemaakt. Zo ja, geef een korte opsomming van de maatregelen.
- k De discussies (en conclusies) in de verschillende landen overziend: welke lessen zijn hier voor Nederland uit te trekken? Denk hierbij aan lessen in termen van: als je x wilt bereiken, let dan op deze aspecten, steek de discussie dan zo in et cetera.

Deze sub-vragen zijn verschillend in niveau en kunnen als volgt geclusterd worden:

Het eerste cluster omvat de deelvragen a - d. Hierbij gaat het om de eigenlijke mediadiscours analyse, inclusief de maatschappelijke duiding.

De volgende drie deelvragen e - g zoomen nader in op de rol van de verschillende stakeholders in de discussie: de rol van de burger, de private partijen en die van de overheid. Belangrijk aandachtspunt hierbij is de zelfredzaamheid van de burger.

Het laatste cluster sub-vragen h - k vraagt naar de vertaling van de verschillende nationale discussies in concrete maatregelen en beleid. En de lessons learned en implicaties voor Nederland.

8.2 Methode onderzoek

In wat volgt beschrijven wij kort de gehanteerde methodologie voor het verzamelen, categoriseren en analyseren van data. Eveneens besteden wij kort aandacht aan eerste resultaten, teneinde een beter inzicht te geven in de toegevoegde waarde van ons onderzoek voor BZK.

Dataverzameling

Startpunt in het onderzoek was het vaststellen van de shortlist aan onderwerpen op het gebied van identiteitsmanagement. Aan de acht geselecteerde onderwerpen hebben wij vervolgens Boolean zoektermen gekoppeld, op basis waarvan gezocht kan worden in nieuwsdatabases. Hierover hebben wij BZK reeds bericht in een memo dd. 25 september 2013.

Deze zoektermen hebben wij vervolgens ingevoerd in LexisNexis en equivalente nieuwsdatabanken zoals GoPress, en op basis van de binnengekomen resultaten mogelijk verfijningen op de termen toegepast. In het geval van de Nederlandse, Vlaamse en Duitse bronnen hebben wij vervolgens een sub-selectie van de resultatenlijsten gemaakt, waarin wij dubbelingen of onjuiste resultaten verwijderd hebben. Voor de Britse, Zweedse en Spaanse bronnen heeft onze partner Matrix deze sub-selectie gemaakt.

Nexis®: Display Bibliographic References

Page 1 of 2

Display Bibliographic References Help

Houd u er rekening mee dat deze citations niet gegarandeerd nauwkeurig zijn. Bewerk en check uw citations voordat u ze gebruikt in uw bibliografische pagina.

<p>"British Gas contract creates 600 jobs as smart-meter roll-out begins; Company boss says technology will cut £65 a year from bills, and dismisses privacy fears GOOD NEWS BRITAIN." <i>The Daily Telegraph (London)</i>, September 16, 2013 Monday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business</p>
<p>"British Gas contract creates 600 jobs as smart meter roll-out begins; Energy smart meter manufacturer Landis+Gyr is to create 600 new UK jobs after landing a £600m contract to supply more than 10m meters for British Gas." <i>telegraph.co.uk</i>, September 16, 2013 Monday 6:00 AM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"THE NEW REVIEW: Discover: THE NETWORKER: Why smart meters might not be so clever after all." <i>The Observer (England)</i>, August 16, 2013 . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Vodafone loses out to Telefonica in smart meter race: Spanish group wins £1.5bn government contracts Capita beats G4S for management of system." <i>The Guardian (London) - Final Edition</i>, August 15, 2013 Thursday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Offer energy use displays, say MPs." <i>Express Online</i>, July 27, 2013 Saturday 12:17 AM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"The global surge online: What it might mean for your business." <i>City A.M.</i>, June 6, 2013 Thursday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"British families at risk from smart meters, campaigners tell MPs; Smart energy meters offered to every British home could be as dangerous as a 'bullet from a rifle' because of the radiation they emit, campaigners have told MPs." <i>telegraph.co.uk</i>, April 24, 2013 Wednesday 3:59 PM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"A home run for renewables." <i>Guardian Unlimited</i>, December 1, 2012 Saturday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Majority of UK unaware of smart meters, research shows." <i>Guardian Unlimited</i>, August 22, 2012 Wednesday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"National: Home energy smart meters are a threat to data privacy." <i>The Observer (England)</i>, July 1, 2012 . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"National: Home energy smart meters threaten privacy." <i>The Observer (England)</i>, July 1, 2012 . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"SMART METERS IN OUR HOMES WILL LEAVE US OPEN TO CYBER ATTACK." <i>DAILY MAIL (London)</i>, June 9, 2012 Saturday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Government plans to install smart meters in our homes; will leave us open to cyber attack." <i>MHIOnline</i>, June 9, 2012 Friday 10:40 PM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Are smart meters a good idea?; Jeff Howell answers readers' home maintenance questions. This week: a focus on smart meters." <i>telegraph.co.uk</i>, May 30, 2012 Wednesday 5:39 PM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"A BUILDER GIVES IT TO YOU STRAIGHT; rouble with the boiler? Rogue traders? Or a tricky do-it-yourself job? Jeff gives on-the-level advice and answers your home maintenance questions." <i>The Sunday Telegraph (London)</i>, May 27, 2012 . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"THE WEEK IN WESTMINSTER." <i>The Daily Telegraph (London)</i>, April 23, 2012 Monday . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Are smart meters worth it?; The Government are promoting smart meters as being eco-friendly and good value options. But are they really right, asks Sarah Lonsdale." <i>telegraph.co.uk</i>, February 22, 2012 Wednesday 5:45 PM GMT . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"HOW TO BE GREEN AND STAY SANE; Want to trim your bills, update your home and do your bit for the planet? Sarah tests the latest eco products and sorts the facts from the fads. This week: getting the measure of smart meters." <i>The Sunday Telegraph (London)</i>, February 12, 2012 . Date Accessed: 2013/10/01. www.lexisnexis.com/nl/business.</p>
<p>"Questions remain over Big Brother smart meters; Comment." <i>The Daily Telegraph (London)</i></p>

Figuur 26: Fragment LexisNexis subselectie onderwerp 'slimme meter' voor Groot-Brittannië

Hiermee ontstaat een bruikbare dataset per onderwerp en per land, die vervolgens gecategoriseerd en geanalyseerd kan worden.

Categorisatie en analyse

TOPIC	COUNTRY	Date (publication)	Title	Source name	Source type	Highbrow/lowbrow	Political affiliation
Behavioral Targeting	Spain						
SUMMARY							
1) Overall arguments, considerations and sentiments:							
2) Defining events/policies/debate leaders:							

Figuur 27: Overzicht van lege spreadsheet

Voor deze fase van het onderzoek hebben wij een uitgebreide Engelstalige spreadsheet geproduceerd per onderwerp en per land, wat neerkomt op 40 spreadsheets in totaal. Deze spreadsheets maken het mogelijk de verzamelde data te categoriseren en te kwantificeren, zodat het mogelijk wordt tendensen in en correlaties tussen nieuwsitems inzichtelijk te maken.

De data zijn gegroepeerd aan de hand van dertien categorieën, bestaand uit een combinatie van invulvelden en drop-down menu's:

TOPIC	COUNTRY	Date (publication)	Title	Source name	Source type	Highbrow/lowbrow	Political affiliation
Behavioral Targeting	Spain						
SUMMARY							
1) Overall arguments, considerations and sentiments:							
2) Defining events/policies/debate leaders:							

Figuur 28: Dertien categorieën in de spreadsheet

1. Date (publication)
Please fill in the publication date of an entry here in the date format dd-mm-yy
2. Title
Please fill in the title of an entry here, i.e. "new prime minister elected"
3. Source name
Please fill in the source name of each entry here, i.e. "the Guardian"

4. Source type
Pick one option from the drop-down menu:
Newspaper
Magazine
TV
Radio
5. Highbrow/lowbrow
Pick one option from the drop-down menu:
Highbrow
Lowbrow
This column is meant to distinguish highbrow sources (i.e. the Times) from lowbrow sources (i.e. the Daily Star)
6. Political affiliation
Pick one option from the drop-down menu:
Liberal
Conservative
Neutral
7. factual/opinionated
Pick one option from the drop-down menu:
matter-of-factual
Opinionated
8. Focus
Pick one option from the drop-down menu:
Privacy
Security
Trust
Freedom
Progress/technology
These options designate the general theme of each particular entry, i.e., does the entry focus on privacy of citizens; or their security; or trust in government/private sector; or freedom of citizens; or technological progress. When more than one option applies, pick the most dominant one.
9. agent→principal
Pick one option from the drop-down menu:
Government→private sector
Government→citizens
Private sector→citizens
These options designate the basic relation between actors per entry: does the entry concern the relation between government and private sector; or the relation between government and citizens; or the relation between private sector and citizens. When more than one options apply, pick the most dominant one.
10. Self-sufficiency citizens?
Pick one option from the drop-down menu:
Focus on self-sufficiency of citizens
No focus on self-sufficiency
These options designate whether or not the entry mentions the self-sufficiency of citizens, i.e. if and how citizens themselves can play an active role in the management or protection of private data, digital identity, etc.
11. Connected to event?
Please fill in if the entry is connected to a relevant event, for instance the 9/11 attacks or the 2012 Olympics. Please make sure to use consistent terminology on each worksheet.
12. Relevant values/sentiments
Please fill in what values or sentiments are important in the entry, for instance "distrust of technology" or "state security is more important than privacy ." Please make sure to use consistent terminology on each worksheet.
13. Overall view
Pick one option from the drop-down menu:
Positive
Critical
Balanced
Overall, is the entry positive, critical or balanced regarding the topic discussed?

Hiernaast hebben wij per spreadsheet een aantal kwalitatieve velden opgenomen om de algemene tendens van het onderwerp per land samen te vatten:

	A	B	C	D	E	F	G	H
1	TOPIC	COUNTRY						
2	Behavioral Targeting	Spain						
3	SUMMARY		Date (publication)	Title	Source name	Source type	Highbrow/lowbrow	Political affiliation
4	1) Overall arguments, considerations and sentiments:							
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22	2) Defining events/policies/debate leaders:							
23								
24								
25								
26								
27								

Figuur 29: Kwalitatieve velden

1. Overall arguments, considerations and sentiments
Please summarize the dominant arguments, considerations and sentiments for this topic, in order to give an overall view that can be used as input for the final report.
2. Defining events/policies/debate leaders
Please summarize the dominant events/policies/debate leaders for this topic, in order to give an overall view that can be used as input for the final report.
3. Cultural aspects shaping the debate
Please summarize national cultural elements that have played a role in the development of this topic, in order to give an overall view that can be used as input for the final report.
4. Manifestation of self-sufficiency of citizens
Please summarize to what extent self-sufficiency of citizens in safeguarding their privacy/digital identity has played a role in this topic, in order to give an overall view that can be used as input for the final report.
5. Role of public and private sector in debate
Please summarize how the public and private sector factor into this topic, in order to give an overall view that can be used as input for the final report.
6. Political follow-up based on debate
Please summarize what political conclusions have been drawn from the debate on this topic, in order to give an overall view that can be used as input for the final report.
7. Policy-related consequences based on debate
Please summarize if the debate on this topic has led to any consequences in terms of policy making, in order to give an overall view that can be used as input for the final report.
8. Lessons for the Netherlands
Please summarize what relevant lessons can be learned from this topic, in this country, in order to give an overall view that can be used as input for the final report

Verwerking gegevens

Als laatste stap hebben wij verbanden aangebracht binnen de spreadsheets met behulp van de beperkte kwalitatieve functionaliteit die de dataset en software (Excel) toelaat. Hieruit hebben wij de lopende tekst gedistilleerd. Gezien de internationale samenwerking bij dataverzameling en data-analyse zijn de teksten in de grafieken Engelstalig. Onze bevindingen hebben wij vervolgens getoetst bij onafhankelijke, nationale experts op het gebied van ID-management en de andere besproken onderwerpen. Daarnaast hebben wij voor de Nederlandse bronnen ook sociale media onderzocht om sentimenten uit de nieuwsmedia te peilen.

8.3 Expertlijst

Ter controle van onze bevindingen hebben wij per land met een expert uit de wetenschap op het gebied van ID-management, en beleid omtrent persoonsgegevens en databeveiliging gesproken.

- Nederland: prof. dr. Corien Prins, Universiteit van Tilburg
- Vlaanderen: mr. Brendan van Alsenoy, Katholieke Universiteit Leuven
- Duitsland: prof. dr. Gerrit Horning, Universität Passau
- Groot-Brittannië: dr. Angela Daly, Swinburne University of Technology
- Spanje: dr. Pablo Ibañez-Colomo, London School of Economics
- Zweden: dr. Måns Svensson, Lund University

8.4 Data

Onderstaand vindt u ter illustratie de statistiek voor het onderwerp identiteitsfraude in Nederland. In verband met de omvang zijn de statistieken opgenomen in een apart bijlagenboekje.

TOPIC	COUNTRY												
Identity fraud	Netherlands												
SUMMARY	Date (publication)	Title	Source name	Source type	Highbrow/lowbrow	Political affiliation	factual/opinionated	Focus	agent→principal	Self-sufficiency citizens?	Connected to event ?	Relevant values/sentiments	Overall view
1) Overall arguments, considerations and sentiments: Voor het onderwerp identiteitsfraude is bijzonder veel aandacht geweest in de media. Deze aandacht concentreert zich met name op drie gebieden: (1) het beschrijven van schrijnende gevallen, (2) melding maken van de overheid die actie wil ondernemen, en (3) het informeren van burgers over wat ID fraude inhoudt. Het is opvallend dat de overheid al sinds het begin van het debat voornemens is actie te ondernemen, maar dat dit blijkbaar niet voldoende is om de zorgen in de media weg te nemen. Daarbij blijkt uit het mediaoverzicht een wantrouwen richting de overheid, die niet voldoende in staat zou zijn om op te treden	03-07-13	Stelen identiteit zwaar bestraft; Lange gevangenisstraf of hoge boete	De Telegraaf	newspaper	lowbrow	conservative	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	triggered by hate crime	balanced
	03-07-13	Kamer: Fraude met identiteit strafbaar	reformatorisch dagblad	newspaper	highbrow	conservative	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	phenomenon warrants intervention	balanced
	10-06-13	ID-fraude op vakantie	Spits	newspaper	lowbrow	neutral	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	summer holiday season	raising awareness	critical
	07-06-13	Fraude met identiteit neemt elk jaar toe	de Volkskrant	newspaper	highbrow	liberal	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	critical
	07-06-13	Twee miljoen Nederlanders ooit slachtoffer ID-fraude	Trouw	newspaper	highbrow	liberal	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	critical
	15-04-13	Vijf vragen over Maatregelen tegen identiteitsfraude	NRC/NRC.Next	newspaper	highbrow	neutral	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	critical
	12-04-13	Eén kopietje van je paspoort en je identiteit is gejat	NRC/NRC.Next	newspaper	highbrow	neutral	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	critical
	09-04-13	ID-fraude twee keer zo groot	De Telegraaf	newspaper	lowbrow	conservative	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	balanced
	05-04-13	Bijna gesloopt door identiteitsfraude	reformatorisch dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	government action on the topic	Kafkaesque situation	critical
	25-02-13	Criminelen hebben het steeds vaker op onze identiteit	de Volkskrant	newspaper	highbrow	liberal	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	increase of identity fraud	raising awareness	balanced

Andersson Efficers Felix

en klachten niet serieus neemt.	gemunt'												
	15-02-13	Aangifte identiteitsfraude	de Volkskrant	newspaper	highbrow	liberal	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	TV show	n.a.	balanced
	20-03-12	Meer meldingen van identiteitsfraude	metro	newspaper	lowbrow	neutral	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	n.a.	balanced
	12-01-12	Identiteitsfraude in Nederland	NRC/NRC.Next	newspaper	highbrow	neutral	opinionated	Security	Government→citizens	focus on self-sufficiency	increase of identity fraud	raising awareness	critical
	25-10-11	Klantgegevens bekend na hacken http://cheaptickets.nl	NRC/NRC.Next	newspaper	highbrow	neutral	opinionated	Security	private sector→citizens	no focus on self-sufficiency	hacking of popular website	n.a.	balanced
	17-09-11	Kabinet pakt id-fraude aan	AD	newspaper	lowbrow	neutral	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	balanced
	07-09-11	Kabinet pakt identiteitsfraude harder aan	Financieel Dagblad	newspaper	highbrow	conservative	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	balanced
	08-09-11	Justitie zet vingerscan in tegen identiteitsfraude	AD	newspaper	lowbrow	neutral	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	prevalence of identity fraud	importance for rule of law	balanced
	01-09-11	Identiteit is aantrekkelijke buit	Parool	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	government action on the topic	Kafkaesque situation	critical
	02-04-11										technological solution to prevent credit card fraud	n.a.	balanced
	25-02-11	SmartSwipe tegen identiteitsfraude	De Telegraaf	newspaper	lowbrow	conservative	matter-of-factual	Security	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	balanced
	22-02-11	Identiteitsfraude strenger aangepakt	Financieel Dagblad	newspaper	highbrow	conservative	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	balanced
	12-01-11	Vader krijgt na id-fraude toch geld van huisverkoop	AD	newspaper	lowbrow	neutral	matter-of-factual	Security	Government→citizens	no focus on self-sufficiency	court case	Kafkaesque situation	critical
	24-08-10	Alarmerende stijging van identiteitsfraude	AD	newspaper	lowbrow	neutral	matter-of-factual	Security	citizens→citizens	no focus on self-sufficiency	increase of identity fraud	lack of government action	critical
	29-09-09	Identiteitsfraude; Netwerk zomerserie Kafka in de Polder	De Telegraaf	newspaper	lowbrow	conservative	opinionated	Trust	Government→citizens	no focus on self-sufficiency	TV show	Kafkaesque situation	critical
25-09-09	Fraude identiteit 170 keer gemeld	de Volkskrant	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	government action on the topic	Kafkaesque situation	critical	
25-09-09	Fouten ministerie bij identiteitsfraude	de Volkskrant	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens	no focus on self-	prominent example of	Kafkaesque situation	critical	

2) Defining events/policies/debate leaders: Om de zoveel tijd komen onderzoeken uit over hoe vaak ID fraude voorkomt, en komen schrijvende verhalen in het nieuws. Hierdoor ontstaat dan vervolgens een nieuwscyclus op het gebied.

Andersson Efficers Felix

										sufficiency	ID fraud		
25-09-09	Jaren de dupe na diefstal id; 'We weten nog niet hoe hoog, de claim zal zeker in de miljoenen lopen'	Parool	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	Kafkaesque situation	critical
25-09-09	Fraude met identiteit zakenman	Nederlands Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	Kafkaesque situation	critical
25-09-09	Rijk maakt excuus na identiteitsfraude	reformatorisch dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	Kafkaesque situation	critical
25-09-09	Einde nachtmerrie in zicht; Excuses minister aan slachtoffer van identiteitsfraude	Spits	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	Kafkaesque situation	critical
02-07-09	Sinds december 144 meldingen van identiteitsfraude bij meldpunt - Opeens heb je een strafblad	AD	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens		focus on self-sufficiency	government action on the topic	raising awareness	critical
03-07-09	Nederlanders laconiek over identiteitsfraude	De Telegraaf	newspaper	lowbrow	conservative	matter-of-factual	Trust	Government→citizens		focus on self-sufficiency	government action on the topic	raising awareness	critical
17-04-09	Minister Hirsch Ballin hekelt 'onjuist' rapport over identiteitsdiefstal - Justitie kraakt ombudsman	AD	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	lack of government action	critical
16-3-2009	Machteloos bij diefstal van identiteit	AD	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens		no focus on self-sufficiency	prominent example of ID fraud	Kafkaesque situation	critical
22-11-08	Je raakt je leven kwijt, als je identiteit wordt gestolen'	de Volkskrant	newspaper	highbrow	liberal	opinionated	Trust	Government→citizens		focus on self-sufficiency	prominent example of ID fraud	lack of government action	critical
08-10-08	Centraal meldpunt voor identiteitsfraude	metro	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens		focus on self-sufficiency	government action on the topic	raising awareness	critical
07-10-08	Slachtoffers identiteitsfraude in de kou	Spits	newspaper	lowbrow	neutral	opinionated	Trust	Government→citizens		focus on self-sufficiency	increase of identity fraud	lack of government action	critical
27-08-08	Slachtoffer moet onschuldig bewijzen; Identiteitsfraude; Diefstal van	Trouw	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens		focus on self-sufficiency	increase of identity fraud	raising awareness	critical

3) Cultural aspects shaping the debate: wantrouwen richting overheid zit diep.

Andersson Efficers Felix

persoonsgegevens
blijkt soms jaren later

08-08-08	Agent getraind op identiteitsfraude	Spits	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	critical
07-08-08	Politie bindt strijd aan met id-fraude	Parool	newspaper	highbrow	liberal	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	critical
07-08-08	Succesvolle id-fraude zelden opgemerkt								focus on self-sufficiency	increase of identity fraud	raising awareness	critical
07-08-08	Tips om id-fraude te voorkomen	Nederlands Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	critical
26-03-08	Overeenkomst: Strengere controle op identiteitsfraude	Nederlands Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	critical
21-03-08	Identiteitsdiefstal op internet is griezeligst!	metro	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	increase of identity fraud	raising awareness	critical
03-03-08	Bestrijd identiteitsfraude met preventie	Financieel Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	increase of identity fraud	raising awareness	critical
02-02-08	Voorkom identiteitsfraude	reformatoisch dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	increase of identity fraud	raising awareness	critical
14-03-05	Campagne tegen identiteitsfraude	Financieel Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	focus on self-sufficiency	government action on the topic	raising awareness	critical
05-06-04	Identiteitsfraude strenger aangepakt	AD	newspaper	lowbrow	neutral	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	government action on the topic	raising awareness	critical
18-10-08	Geen groot risico; Minder dan de helft van de Nederlanders denkt slachtoffer te kunnen worden van identiteitsfraude	Financieel Dagblad	newspaper	highbrow	conservative	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	increase of identity theft	raising awareness	critical
11-11-06	IDENTITEITSFRAUDE: DUBBELGANGERS	Elsevier	magazine	highbrow	conservative	matter-of-factual	Trust	Government→citizens	no focus on self-sufficiency	prevalence of identity fraud	importance for rule of law	balanced

<p>4) Manifestation of self-sufficiency of citizens: het is opvallend dat met name de media hier op inzetten. De overheid lijkt zich te beperken tot reactief optreden.</p>
<p>5) Role of public and private sector in debate: de publieke sector is met name aan zet hier, over private oplossingen wordt niet of nauwelijks gesproken.</p>
<p>6) Polical follow-up based on debate: er zijn voortdurend initiatieven vanuit politiek en regering, vaak gebaseerd op media aandacht voor schrijnende gevallen. Hier blijft het dan vervolgens bij, een coherente, niet ad-hoc aanpak lijkt te ontbreken.</p>
<p>7) Policy-related consequences based on debate: ministerie, politie en justitie nemen voortdurend initiatieven en zetten het punt op de agenda. Hiermee wordt de aandacht voor het probleem echter niet minder.</p>

8) Lessons for the Netherlands: Nu neemt de media vooral het voortouw in preventie. Dit zou meer vanuit de overheid kunnen komen.