



Eerste Kamer der Staten-Generaal

Staatssecretaris van Veiligheid en Justitie
De heer mr. F. Teeven
Postbus 20301
2500 EH Den Haag

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00
fax 070-312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 12 april 2011

betreft vragen ter voorbereiding debat 17 mei 2011

ons kenmerk 147654.01U

Geachte heer Teeven,

De leden van de vaste commissies voor Justitie en BZK/AZ hebben op 23 november 2010 besloten een beleidsdebat te willen voeren met de regering over de rol van de overheid m.b.t. de digitale opslag, verwerking en uitwisseling van persoonsgegevens in relatie tot de privacy van burgers. Daarbij willen zij vraagstukken als doelbinding, de kwaliteit van het ICT-ontwerp/databestand en bescherming van persoonsgegevens en de rechtsbescherming voor burgers aan de orde stellen. Dit debat willen zij voeren naar aanleiding van het rapport van de commissie Brouwer-Korf, de kabinetsreactie¹ daarop en het schriftelijk overleg² dat daarover is gevoerd. De leden van de vaste commissies voor Justitie en BZK/AZ hebben tevens besloten de leden van de vaste commissies voor OCW, VWS en de JBZ-Raad bij het debat en de voorbereiding daarvan te betrekken.

Op 21 februari jl. hebben de leden van deze vijf commissies in het kader van de voorbereiding van het debat een expertmeeting gehouden met experts van de Algemene Rekenkamer, de Europees Toezichthouder voor de Gegevensbescherming, het College bescherming persoonsgegevens, de Wetenschappelijke Raad voor de Regering en het Rathenau Instituut.³ Tijdens de expertmeeting is er (onder meer) gesproken over de door vernoemde instanties relevante gepubliceerde rapporten (waaraan in deze brief meermalen wordt gerefereerd).⁴ In 2008 hield de vaste commissie voor Justitie al eerder een expertmeeting over de gegevensbescherming.⁵

In het kader van de voorbereiding op het debat op 17 mei a.s. willen de leden van de fracties van het **CDA**, de **PvdA**, de **SP** en **GroenLinks** vragen en opmerkingen aan u voorleggen. De

¹ Kamerstukken II 2009/10, 31051, 5.

² Kamerstukken I 2009/10, 31 051, A.

³ Kamerstukken I 2010/11, 31 051, B.

⁴ Rapport van de commissie Brouwer-Korf, *Gewoon doen, bescherming van veiligheid en persoonlijke levenssfeer*, 3 november 2009, Kamerstukken II 2008/09, 28684, 199 met bijlage; Rapport van de Adviescommissie Informatiestromen Veiligheid, *Data voor daadkracht: gegevensbestanden voor veiligheid: observaties en analyse*, april 2007; Rathenau Instituut, *Databases: over ICT-beloftes, informatiehonger en digitale autonomie*, december 2010; Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, maart 2011; Rathenau Instituut, *Check in/ check uit: de digitalisering van de openbare ruimte*, mei 2010.

⁵ Kamerstukken I 2007/08, 31 200 VI, F.



datum 12 april 2011

ons kenmerk 147654.01U

blad 2

SP-fractie sluit zich bij alle vragen en opmerkingen van de PvdA-fractie aan. Ook wordt er een commissievraag aan u voorgelegd.

1. Visie regering en reactie op rapporten

1.1 Visie regering

De leden van de commissies vragen de regering op welke terreinen er al gebruik gemaakt wordt van datamining of -profilering of op welke terreinen zij van plan is daarvan gebruik te gaan maken? De indruk bestaat dat via Europese voorstellen het gebruik van profielen geïntroduceerd wordt, terwijl daar in het verleden in Nederland altijd terughoudend over gesproken is.

De leden van de **CDA**-fractie vragen de regering of het juist is dat de overheid streeft naar een consolidatie van datacentres? Wat zijn de concrete voordelen daarvan mede gelet op de beheersbaarheid en kwetsbaarheid voor een ongestoorde en verantwoorde informatievoorziening?

Kan de regering bij benadering aangeven aan de leden van de **SP**-fractie hoeveel databanken er door de overheid zijn of worden opgebouwd en hoe die met elkaar verknoopt en gekoppeld zijn? Heeft de regering hier zelf nog overzicht over? Acht de regering het zinnig om hierover zo nu en dan te reflecteren en zichzelf hierover kritisch te bevragen?

Wat is de visie van de regering op de verantwoordelijkheid van de overheid voor de 'iSamenleving'? In de epiloog van het WRR rapport lezen de leden van de **PvdA**-fractie immers dat de overheid niet alleen verantwoordelijk is voor het eigen gebruik van ICT, maar ook systeemverantwoordelijkheid heeft voor de ontwikkeling van de informatiesamenleving, met inbegrip van de informatiemacht van mondiale spelers als Google, Facebook en Apple. Erkent de regering deze rol en verantwoordelijkheid van de overheid? Op welke wijze is de regering als 'iOverheid' voornemens inhoud en vorm te geven aan haar systeemverantwoordelijkheid voor de 'iSamenleving'? Op welke wijze zal de overheid voor haar burgers opkomen ten opzichte van private partijen zoals Google, Facebook of Apple? Hoe hanteert de regering het dilemma zoals geformuleerd door John Naughton in the Guardian: "Live with the WikiLeaksable world or shut down the net, it's your choice."?

De leden van de **PvdA**-fractie vragen de regering naar de rol die zij kan toekennen aan interactie met burgers via web 2.0. In het schriftelijk overleg volgend op de kabinetsreactie over het rapport van de commissie Brouwer-Korf⁶ stelt de regering dat web 2.0 nog een relatief nieuw fenomeen betreft, waarvan de kansen en bedreigingen nog niet duidelijk zijn. Er zou meer ervaring en expertise nodig zijn voor het inzetten van web 2.0 door de overheid. Is de regering anno nu - voorjaar 2011 - nog steeds deze mening toegedaan? Zo nee, wat is dan het actuele standpunt? Wat is het beeld dat de regering heeft van de wijze waarop burgers actief zijn op de vele toepassingen van het internet? Is het niet de hoogste tijd de burger veel meer interactief te betrekken in allerlei maatschappelijke processen via de digitale middelen? Meer in het algemeen bezien: acht de regering actieve inbreng van de samenleving, groepen en individuele burgers niet onmisbaar bij de verdere ontwikkeling van de iOverheid en de iSamenleving?

⁶ Kamerstukken I 2009/10, 31 051, A.



datum 12 april 2011

ons kenmerk 147654.01U

blad 3

In de Europese Commissie combineert commissaris Viviane Reding de portefeuille Justitie met Grondrechten en Burgerrechten. Tijdens de selectiehoorzittingen sprak zij zich uit dat het tijd werd dat we de veiligheid niet voortdurend laten voorgaan op de gerechtigheid. Ook gaf zij aan dat dataprotectie hoofdprioriteit zou moeten zijn. De leden van de **SP**-fractie signaleren met haar een onbalans tussen het bewaken van de veiligheid en het recht van de burger op bescherming van zijn persoonlijke levenssfeer. Is de regering dat met ons eens? Zo ja, op welke manier gaat zij de balans terug brengen? Indien de regering het niet met deze leden eens is, dan ontvangen zij graag een gemotiveerde toelichting op dit punt.

Wat is de mening van de regering over de spreekwoordelijke overheidsmissers, in de vorm van onhaalbare deadlines en kostbare mislukkingen als het gaat om grootschalige ICT projecten? Dit is toch meermaals door de ARK gesignaleerd, zo constateren de leden van de **PvdA**-fractie.

ICT projecten van de overheid zijn vaak te zeer *ICT driven*, zo constateren de leden van de **SP**-fractie. Ze zijn te ambitieus en te complex en worden te laat opgeleverd en ze kosten teveel geld. We kennen allemaal de voorbeelden van de OV-chipkaart en het landelijk EPD. In zijn algemeenheid wordt van technologie teveel verwacht, terwijl men technische problemen onderschat. Kan de regering zich vinden in deze analyse?

1.2 *Reactie regering rapporten*

Het rapport 'Data voor daadkracht' behandelt expliciet de spanning tussen veiligheid en privacy. Het is niet gebleken, dat de regering is ingegaan op de observaties en aanbevelingen, die in dit rapport zijn vermeld. De leden van de **CDA**-fractie vernemen graag het standpunt van de regering met betrekking tot deze onderwerpen. Meer in het bijzonder zou volgens hen moeten worden ingegaan op de knelpunten die in het rapport zijn gesignaleerd rond het proces van het inwinnen van gegevens uit verschillende gekoppelde (externe) databases. De knelpunten doen zich voor bij de vragers van gegevens, bij de organisaties die deze gegevens moeten leveren en in het proces van bevraging. Deze knelpunten leiden bij de adviescommissie tot het oordeel dat de totaliteit van verschillende systemen in de keten niet voldoet aan de criteria inzake de grondslag - zoals vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid - voor de verwerking van gegevens uit andere bestanden of databases. In hoofdstuk 5 doet de adviescommissie een vijftal aanbevelingen die voor de burger en het bedrijfsleven van groot belang lijken. Ondanks het feit dat het rapport van 2007 dateert, is het vraagstuk nog steeds actueel en de aanbevelingen ook. Een regeringsstandpunt lijkt dan ook niet overbodig.

In het hoofdrapport met de titel 'iOverheid' signaleert de WRR dat *de facto* en bijna ongemerkt samenhangende informatiestromen het karakter van de overheid domineren, waarmee nieuwe mogelijkheden - maar ook afhankelijkheden en kwetsbaarheden - voor zowel de overheid als haar burgers ontstaan. De leden van de **PvdA**-fractie constateren ook dat er desalniettemin in de dagelijkse praktijk allerminst vanuit een samenhangende visie wordt bestuurd, en overheidsinitiatieven tot digitalisering, met bijbehorende informatiestromen binnen de verschillende sectoren, geïsoleerd van elkaar worden ontwikkeld. Herkent de regering dit beeld en welke stappen is zij van plan hier tegen te ondernemen?



datum 12 april 2011

ons kenmerk 147654.01U

blad 4

Bij de behandeling van het wetsvoorstel ter invoering van het BSN⁷ in 2007 hebben de leden van de **PvdA**-fractie met nadruk gevraagd naar een algemeen, ex ante toetsingskader voor sectorale regelingen voor de toepassing het BSN. De regering verwees naar nadere uitwerking in een later stadium - ex post dus - in de sectorale toepassingen. Heeft de regering intussen kennis genomen van relevante passages in deel twee van de WRR verkenning 'De staat van informatie'?⁸ Daar worden immers de Verwijsindex Risicjongeren en het EPD aan de hand van de beginselen in het toetsingskader langs gelopen en voorzien van op onderdelen zeer kritische kanttekeningen. Het rapport 'Databases: over ICT beloftes, informatiehonger en digitale autonomie' van het Rathenau Instituut bevat ook case studies van de OV-chipkaart, het EPD, het elektronisch Kinddossier, klantenprofielen, het Schengen Informatie Systeem en het GBA. De conclusie van het rapport is: "Alles bij elkaar genomen schetsen de case studies een vrij onthutsend beeld van wat er in de praktijk mis kan gaan bij het gebruik van databases, en deze risico's hangen samen met de keuzes die worden gemaakt over de architectuur van de betreffende database." Had de regering al kennis genomen van deze conclusie? Hoe kwalificeert de regering deze verdere invulling met daarin de handvaten voor professionals, zoals die tot dusverre heeft plaatsgevonden in de sectorale uitwerking? Welke gevolgtrekkingen en consequenties verbindt de regering aan deze bevindingen voor de eigen regulerende rol van de overheid in de digitale samenleving?

In de verkennende studie van de WRR 'Rolverdeling tussen Overheid en Burger bij Bescherming van Identiteit', lezen de leden van de **PvdA**-fractie onder meer dat er wordt geconcludeerd dat privacy niet een gepasseerd station is voor burgers, burgers een strakkere regie van de overheid wensen bij het gebruik van het BSN in het maatschappelijk verkeer, en dat de respondenten inzage willen hebben in hun elektronische dossiers, zodat ze gegevens kunnen corrigeren en kunnen zien wie gegevens bewerkt en inziet. Wat is de reactie van de regering op deze bevindingen? Overweegt de regering nadere maatregelen? Zo ja, van welke aard en richting? Het Rathenau Instituut heeft in de expertmeeting van 21 februari jl. gewezen op de noodzaak van meer aandacht voor risico's van databases en voor de positie van de burger, omdat vooral de burger de dupe dreigt te worden. Welke conclusies verbindt de regering aan deze uitkomsten voor de gewenste rol van de overheid?

Het rapport 'Check in/Check uit' van het Rathenau Instituut beschrijft de technische realisatie van herroepbare privacy door het verstrekken van een nummer aan gebruikers van informatie-systemen, waarmee zij een digitale identiteit opbouwen. De koppeling tussen dat nummer en de data, die direct herleidbaar zijn tot de fysieke identiteit van de persoon, kan worden versleuteld en slechts onder strikte voorwaarden worden vrijgegeven. Een partij beheert het systeem met alleen anonieme nummers, terwijl een andere partij alleen de sleutel beheert tussen dat nummer en de persoon. De politie is de derde actor. Deze is alleen onder strikt omschreven voorwaarden gemachtigd de sleutel te krijgen. Een dergelijk protocol maakt het publieke debat over de voorwaarden bij het vrijgeven van gegevens mogelijk. Per geval wordt er nu data gevorderd, die een willekeurige ongecontroleerde termijn worden bewaard, soms (veel) langer dan wettelijk toegestaan. De publieke discussie zou te meer relevant zijn omdat het ook gaat om het vrijgeven van gegevens voor preventieve opsporing, zo constateren deze leden. Wat is de reactie van

⁷ Wetsvoorstel 30 312 (Wet algemene bepalingen burgerservicenummer).

⁸ WRR, *De staat van informatie*, maart 2011.



datum 12 april 2011

ons kenmerk 147654.01U

blad 5

de regering op deze invulling van de afweging tussen privacy en veiligheid in het rapport van het Rathenau Instituut?

Wat is de algemene reactie van de regering op het WRR rapport 'iOverheid'? Herkent de regering het beeld dat de WRR schetst van een overheid (bestuurlijk en politiek), die denkt en handelt vanuit applicaties en technieken, maar de regie kwijt raakt over de informatiestromen die de technieken en toepassingen tot gevolg hebben? Is de regering het met de WRR eens dat de overheid verantwoordelijk is voor het stellen en bewaken van grenzen aan het gebruik van persoonsgegevens, zowel binnen als buiten de publieke sfeer, zo vragen de leden van de **Groen-Links**-fractie? Zo ja, kan de regering ingaan op deze grenzen en op welke wijze geeft de regering hieraan uitvoering?

Wat is het standpunt van de regering ten aanzien van het rapport en de aanbevelingen van het rapport van de Rekenkamer over open standaarden en open source software?

2. Toetsing

2.1 Toetsingskader

In de rapporten 'Gewoon doen' van de commissie Brouwer-Korf en 'iOverheid' van de WRR is een aantal beginselen geformuleerd als een richtinggevend kader of toetsingskader voor het optreden van de overheid. Deze beginselen dienen als handvaten bij de afweging tussen het beschermen van veiligheid en de persoonlijke levenssfeer van burgers enerzijds en de digitalisering van de samenleving anderzijds. Bij de leden van de **CDA**-fractie rijst de vraag hoe de regering deze kaders hanteert bij het voeren van beleid. Ten aanzien van het eerstgenoemde rapport is hieraan al aandacht besteed in een schriftelijk overleg⁹ van deze Kamer met de minister van Justitie, maar met betrekking tot het tweede rapport lijkt het thans het aangewezen moment om de reactie van de regering hierop te vernemen. Tevens speelt daarbij de vraag naar de samenhang tussen de benadering van de aanbevelingen van de commissie Brouwer-Korf en van hetgeen de WRR ons voorhoudt.

Het WRR rapport hanteert als flexibel toetsingskader de volgende zes beginselen: effectiviteit en efficiëntie (1), veiligheid (2), keuzevrijheid (3), privacy (4), transparantie (5) en *accountability* (6). De commissie Brouwer-Korf hanteert als richtinggevend kader de volgende principes: transparantie, tenzij (1); selecteer voor je verzamelt en houd het sober (2); indien nodig voor de veiligheid moet je delen (3); zorg voor de integriteit van gegevens, systemen en het handelen van gebruikers (4) zorg voor voorlichting en facilitering (5) en zorg voor naleving en intern toezicht (6). Kan de regering aan de leden van de **PvdA**-fractie aangeven op welke wijze beide kaders te hanteren zijn bij het bepalen en het toetsen van de rol van de overheid ten aanzien van de digitalisering van de samenleving?

Herkent de regering - uitgaande van het eerder genoemde toetsingskader van de WRR - de constatering dat tot nu toe een evenwichtige afweging van deze clusters ontbreekt en er geen expliciete en toetsbare publiekelijke verantwoording plaatsvindt? Acht de regering het mogelijk dat het bij een dergelijke afweging en verantwoording, vaker evident zou worden in welke situaties en op welke momenten er sprake is van ongefundeerd politiek bestuurlijk optimisme over ICT mogelijkheden, al dan niet in combinatie met 'spill over', doelverruiming en -vervuiling?

⁹ Kamerstukken I 2009/10, 31 051, A.



datum 12 april 2011

ons kenmerk 147654.01U

blad 6

Het rapport 'Check In/Check uit' van het Rathenau Instituut geeft een overzicht van de digitalisering van de openbare ruimte. Het rapport geeft voor identiteitsbeheer in het net vier clusters met bijbehorende ontwerpprincipes:

1. Gebruik van persoonsgegevens: waarborg anonimiteit, laat burgers mee profiteren, stimuleer toegankelijkheid overheidsinformatie;
2. Beheer van persoonsgegevens: institutioneel beheer, gebruik hackers, verhoog controle burger over eigen digitale identiteit;
3. Ontwerp van IT systemen: identiteiten gescheiden en herroepbaar, gebruik burgers, oude naast nieuwe systemen, niet te veel systeemdwang;
4. Gebruik persoonsgegevens voor opsporing: voorwaarden voor intrekken anonimiteit, kosten/baten opsporing versus doel, schending privacy.

Acht de regering de ontwerpprincipes hanteerbaar, zo vragen deze leden. Acht zij deze op onderdelen wellicht in hogere mate hanteerbaar dan het richtinggevend kader van de commissie Brouwer-Korf? Hoe kan dit ontwerp zich verhouden tot het richtinggevend kader van laatstgenoemde commissie?

In het kader van de behandeling van wetsvoorstel 30312 (Wet algemene bepalingen BSN) heeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties in een brief aan deze Kamer toegezegd te komen met een voorstel voor een overkoepelend beoordelingskader.¹⁰ Wat is de stand van zaken met betrekking tot deze toezegging en hoe gaat de regering doel en middel beter bewaken? De toezegging¹¹ staat sindsdien als nog niet uitgevoerd geregistreerd bij de Eerste Kamer, zo constateren de leden van de **SP**-fractie. De vaste commissie voor BZK/AZ van de Eerste Kamer schreef de staatssecretaris van BZK op 28 september 2010 een herinnering hieromtrent. Een antwoord daarop is nog uitgebleven.

Welke criteria zijn volgens de regering te destilleren uit het Marper-arrest van het EHRM voor het gebruik en de opslag van persoonsgegevens, zo vragen de leden van de **GroenLinks**-fractie.

2.2 Leidraad voor de wetgever

Bij de expertmeeting die de Eerste Kamer heeft gehouden op 20 maart 2008¹² is er door de woordvoerder van het CDA een overkoepelend beoordelingskader *voor de wetgever* geformuleerd teneinde nieuwe wetten af te stemmen op de Wbp. De aldaar genoemde beoordelingscriteria werden niet alleen Kamerbreed gesteund, maar kregen ook unaniem de instemming van de aanwezige deskundigen. Deze criteria zijn: noodzaak (en effectiviteit) (1), proportionaliteit (2), Privacy Impact Assessment (het vooraf duidelijk maken wat de risico's bij de uitvoering zijn) (3), controle en toezicht (4), een horizonbepaling (5). De voormalige minister van Justitie heeft destijds aangegeven deze criteria te zullen opnemen in een leidraad voor het afstemmen van wetgeving op de Wbp, met de aantekening dat de Eerste Kamer aan de desbetreffende punten bij de beoordeling van de haar voorgelegde wetsvoorstellen bijzondere aandacht pleegt te schenken.¹³ De leden van de **CDA**-fractie vragen hoever de minister van Veiligheid en Justitie nu is gevorderd met het opstellen van deze leidraad, en of deze criteria in de tussentijd al wor-

¹⁰ Kamerstukken I 2007/08, 30 312, K.

¹¹ Toezegging te vinden op www.eerstekamer.nl door te zoeken op 'T00285'.

¹² Kamerstukken I 2007/08, 31 200 VI, F.

¹³ Kamerstukken I 2007/08, 31 200 VI, F, p. 27.



datum 12 april 2011

ons kenmerk 147654.01U

blad 7

den gehanteerd. Daarbij vragen zij ook of op andere departementen thans reeds met deze aanpak wordt gewerkt. Deze leden willen meteen van de gelegenheid gebruik maken om ten aanzien van het vijfde criterium een correctie aan te brengen. De voormalige minister van Justitie zei tijdens genoemde expertbijeenkomst terecht, dat het beter is voor dit vijfde criterium een evaluatiebepaling te hanteren in plaats van een horizonbepaling. Met name met betrekking tot noodzakelijke implementatiewetgeving zou een horizonbepaling – hoewel op zich wenselijk – tot problemen kunnen leiden.

2.3 Privacy Impact Assessment (PIA)

De leden van de **CDA**-fractie vragen of het door het ministerie van Veiligheid en Justitie in overleg met het College bescherming persoonsgegevens en VNO-NCW ontworpen model voor de Privacy Impact Assessments - dat in de zomer van 2010 bedrijfsgeraad zou zijn - al wordt gehanteerd. In dit verband wijzen deze leden op het in juni 2010 verschenen proefschrift van dr. J.J.M. Borking, getiteld "Privacyrecht is code", waarin over het nut en de noodzaak van *Privacy Enhancing Technologies* behartigenswaardige opmerkingen worden gemaakt. Dergelijke technische toepassingen kunnen immers de belastende gevolgen van privacybeperkende maatregelen sterk reduceren.

Kan de regering aan de leden van de **PvdA**-fractie aangeven wat de vorderingen zijn met de praktijk van Privacy Impact Assessments? In welke situaties en in welke vorm worden deze toegepast? Wat is de reactie op de suggestie de PIA in verschillende stadia van een ICT ontwikkelingstraject toe te passen, onder andere ter voorkoming van *function creep*, oftewel doelvervuiling? Acht de regering een vorm denkbaar als 'social impact assessment', bijvoorbeeld onder verantwoordelijkheid van de Tweede Kamer? Of het creëren van meer openheid, bijvoorbeeld door het houden openbare audits voor het testen van systemen en ontwerpen van systemen? Is publieke betrokkenheid niet meer als instrument in te zetten ter voorkoming van de missers bij ICT projecten? Openheid over opdrachtverstrekking, reikwijdte, inhoud en resultaten van onderzoek naar en ontwikkeling van door de overheid gefinancierde systemen is dan toch wel een voorwaarde?

Vanuit het Cbp wordt gepleit voor *privacy by design* in de architectuur van nieuwe ICT producten, zodat al in de ontwerpfase elementen worden ingebouwd waardoor privacy effectief beschermd kan worden. Privacy Impact Assessments voor, tijdens en na de ontwikkeling van een groot ICT project zijn nodig om steeds het effect op de privacy te kunnen blijven bewaken, zo menen de leden van de **SP**-fractie. Toezicht in de ontwerpfase zou wettelijk verplicht moeten zijn, evenals verantwoording in de verschillende fasen van de uitvoering. Met behulp van zogenaamde gateway views kan men monitoren of het project volgens plan ontwikkeld wordt. Is de regering van plan hiervoor een wettelijke regeling te maken?

3. Toezicht

Het College bescherming persoonsgegevens maakt in een brief aan de Kamers van 6 december 2010 enige belangrijke opmerkingen over "de verantwoordelijkheid van de verantwoordelijke" voor de gegevensbescherming (de functionaris voor de gegevensbescherming als bedoeld in art.



datum 12 april 2011

ons kenmerk 147654.01U

blad 8

62 e.v. Wbp).¹⁴ Wil de regering op de in deze brief gemaakte opmerkingen ingaan? Het gaat om een functionaris, die is toegerust met de bevoegdheden van Titel 5.2 Awb en die in de opzet van de vigerende wetgeving een 'instituut' zou moeten zijn, zo stellen de leden van de **CDA**-fractie. Wordt aan deze verwachting voldaan?

Heeft de regering een visie op verbetering van de mogelijkheden tot handhaving bij overtredingen van de bepalingen tot bescherming van de persoonlijke levenssfeer, wanneer het een internationale casus betreft? Bijvoorbeeld kwesties waar hoofd- en bijkantoren in verschillende landen - al dan niet binnen de Europese Unie - een rol spelen, zo denken de leden van de **CDA**-fractie zich in. Wordt op Europees niveau een harmonisatie van *compliance rules* serieus nagestreefd, en worden hieromtrent ook stappen gezet in het rechtspersonenrecht?

De leden van de **SP**-fractie vragen de regering welke instantie toezicht houdt op grensoverschrijdend gegevensverkeer.

Kan in de opvatting van de regering niet worden voorzien in een *countervailing power* en in verbetering van de tot dusverre ontoereikende informatievoorziening aan het parlement, waar het specifieke expertise betreft zoals technische aspecten met grote beleidsmatige impact? Wat is de reactie van de regering als vanuit deze Kamer dringend zou worden aangedrongen op adequate voorzieningen voor het parlement opdat de wetgevende en controlerende taak in dergelijke specialistische aangelegenheden naar behoren kan worden vervuld? De leden van de **PvdA**-fractie willen ter illustratie verwijzen naar de drie expertmeetings in 2010 en 2011, die de Eerste Kamer nodig had voor een enigszins adequate informatievoorziening aan de Kamer over het EPD en uiteindelijk ook voor het onderhavige beleidsdebat.

3.1 Bevoegdheden Cbp

Een van de aanbevelingen van de commissie Brouwer-Korf betreft het scheppen van een robuuster extern toezicht op de gegevensbescherming. Wellicht ten overvloede vragen de leden van de **CDA**-fractie nog eens helder uiteen te zetten in hoeverre aan deze aanbeveling wordt voldaan. Daarbij geldt dat voor een adequaat toezicht een realistische pakkans een noodzakelijke voorwaarde is. Kan men van een realistische pakkans spreken? Zijn de sancties die aan het College bescherming persoonsgegevens zijn toegekend effectief? Verdient het aanbeveling het College bescherming persoonsgegevens zelf de bevoegdheid te geven om in ernstige gevallen een overtreding bij de rechter aan te brengen?

In het schriftelijk overleg over de kabinetsreactie op het rapport van de commissie Brouwer-Korf¹⁵ hebben de leden van de **PvdA**-fractie onder andere hun zorgen geuit over de uitholling van privacywaarborgen, door gebrek aan robuustheid van het toezicht in combinatie met achterblijvende bewustwording bij professionals en burgers. Dit mede naar aanleiding van signalen vanuit het Cbp. Kan de regering aangeven hoe de huidige stand van zaken is op deze twee aspecten?

¹⁴ Brief ter inzage gelegd bij de afdeling Inhoudelijke Ondersteuning.

¹⁵ Kamerstukken I 2009/10, 31 051, A.



datum 12 april 2011

ons kenmerk 147654.01U

blad 9

Het Cbp combineert taken die volgens de idee van de trias politica niet bij elkaar horen, zo stellen de leden van de **SP**-fractie. Het Cbp is namelijk toezichthouder en handhaver, is betrokken bij beleidsvorming en adviseert de regering over wetgeving. De woordvoerder van het Cbp gaf tijdens de expertmeeting zelf aan dat dit soms een ongemakkelijke positie is. Wie bewaakt het onderscheid tussen deze taken? In dit kader is de rol van het Cbp met betrekking tot de gang van zaken rondom het landelijk EPD opvallend.¹⁶ Deze instantie heeft ruim twee jaar - namelijk vanaf november 2008 - een onwettige situatie oogluikend gedoogd, namelijk dat zorgaanbieders zonder wettelijk grondslag patiëntgegevens aanmeldden en uitwisselden zonder vooraf gegeven toestemming van de patiënt. Nu het wetsvoorstel als ondeugdelijk en ondoelmatig van de hand is gewezen is het Cbp in een lastige positie gekomen, zo stellen deze leden. Wat is de mening van de regering hierover? De leden van de **PvdA**-fractie sluiten zich bij deze vragen en opmerkingen aan.

Het Cbp beoordeelt de effectiviteit van haar eigen mogelijkheden tot handhaving als niet erg sterk. De sancties zijn weinig afschrikwekkend en de transparantie is vaak ver te zoeken. Is de regering ook van mening dat het Cbp te weinig middelen en wettelijke mogelijkheden heeft om adequaat op te kunnen treden?

3.2 Voorstellen voor 'iPlatform' en 'iAutoriteit'

De leden van de **CDA**-fractie vragen de regering naar haar standpunt over de institutionele voorstellen van de WRR met betrekking tot een 'iPlatform' en een 'iAutoriteit'. De laatstgenoemde instelling krijgt de bevoegdheid de informatiemacht van personen of instellingen te controleren en na te gaan wie de knooppunten beheert, toegang krijgt en of de gebruikers en verwerkers zich uitsluitend op de toegestane doelen richten. Hoe zou een dergelijke autoriteit er uit moeten zien? Is het mogelijk een bestaande autoriteit met de bedoelde bevoegdheden te belasten?

Wat is de reactie van de regering op de voorstellen van de WRR inzake instituties als een permanente commissie voor de 'iOverheid', een 'iPlatform' en een 'iAutoriteit' met doorzettingmacht? De leden van de **PvdA**-fractie vragen in hoeverre – in de opvatting van de regering - de centrale positie van de Rijks Chief Information Officer, als onderdeel van de (bureaucratie van de) Rijksdienst, voldoende tegenwicht kan bieden bij de ondersteuning van deze instituties. Geeft deze opzet geen blijk van een traditionele 'top down' benadering met voorbijgaan aan de elders in het WRR rapport bepleite betrokkenheid van de samenleving, al dan niet via elektronische weg?

Vanuit de WRR wordt erop gewezen dat het in een digitale samenleving steeds meer gaat om het controleren van de informatiemacht, zo constateren de leden van de **SP**-fractie. Wie beheert de knooppunten? Wie heeft toegang tot gegevens, en met welk doel? Wie houdt het stapelen, koppelen en versmelten van alle databanken in toom? De WRR pleit voor een permanente commissie voor 'iOverheid' en een 'iAutoriteit' met doorzettingmacht. Wat vindt de regering van deze suggestie?

¹⁶ Aldus ook de brief van de minister van VWS d.d. 11 april 2011 aan het Cbp n.a.v. de brief van het Cbp d.d. 28 maart 2011 aan de voorzitter van de commissie VWS/JG van de Eerste Kamer; beide brieven zijn ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 141709.116.



datum 12 april 2011

ons kenmerk 147654.01U

blad 10

Wat is het standpunt van de regering ten aanzien van het voorstel voor een permanente commissie die de politieke en publieke alertheid voor de relevante ontwikkelingen stimuleert, en wat is haar standpunt ten aanzien van een zogenaamde 'iAutoriteit'? Hoe zou deze laatste functie zich moeten verhouden tot die van het College bescherming persoonsgegevens, zo vragen de leden van de **GroenLinks**-fractie.

4. Doelbinding

Uit het WRR rapport 'iOverheid' blijkt dat 'gewone' burgers in Nederland in vele honderden databases zijn opgenomen. Het gaat daarbij niet zonder meer om losse applicaties, zo constateren de leden van de **CDA**-fractie. Er is sprake van een gekoppelde, verketende en vernetwerkte wereld, aldus prof. dr. Prins tijdens de op 21 februari jl. in de Eerste Kamer gehouden expertmeeting. Al deze koppelingen en netwerken veroorzaken dat aan de doelbinding van de individuele systemen niet meer of niet voldoende de hand wordt of kan worden gehouden. Hoe zal dan de noodzakelijke afweging (kunnen) worden gemaakt om de doelbinding van de systemen, waarin gegevens van een burger met zijn toestemming zijn opgenomen, toch te realiseren? Welke procedures kunnen dan worden gevolgd?

De leden van de **CDA**-fractie vragen of het juist is dat de gegevens van de OV-chipkaart worden gebruikt als opsporingsmiddel? Hoe lang worden deze gegevens in dit verband bewaard?

Het richtinggevend kader in het rapport van de commissie Brouwer-Korf noemt geen nadere criteria voor de afweging tussen privacy en veiligheid, hetgeen door emeritus hoogleraar informatierecht prof. Dommering (UvA) als de bijl aan het beginsel van de doelbinding werd gekarakteriseerd. De leden van de **PvdA**-fractie lezen in het rapport 'Check in/Check uit' van het Rathenau Instituut het volgende: "Burgers hebben formeel gesproken inzicht in de bevoegdheden van opsporingsinstanties, oftewel onder welke voorwaarden hun recht op anonimiteit kan worden opgeheven. De overheid dient in alle gevallen duidelijk te maken in welke situaties en hoe opsporingsinstanties gebruik mogen maken van de informatie (...)." ¹⁷ Deelt de regering deze opvatting?

Het is belangrijk, zo stellen de leden van de **SP**-fractie, dat vooraf bestuurlijke keuzes door de overheid worden gemaakt over het doel van ICT projecten. Het doel moet nauw omschreven en afgebakend zijn. Wat moet het systeem eigenlijk doen, en biedt ICT daar de beste oplossing voor? Het doel en de middelen staan niet los van elkaar. Gegevens worden verzameld voor een specifiek doel en daar is een overkoepelend beoordelings- en afwegingskader voor nodig met afweging van de belangen van de verschillende *stakeholders*. Is de regering dat met deze leden eens? Hoe zorgt zij er voor dat dit op alle departementen een vanzelfsprekende praktijk is? En welke rol heeft de regering in deze ten aanzien van andere bestuurslagen?

Als doel en middel niet beter bewaakt worden is het risico *function creep*, waarbij een systeem wordt gebruikt voor andere doeleinden dan waarvoor het is ingericht. Deze leden zijn van mening dat de overheid zich bewust moet zijn van haar eigen kwetsbaarheid in grote ICT projecten. Is de regering ook van mening dat externe onafhankelijke audits door teams, die ook een

¹⁷ Rathenau Instituut, *Check in/ check uit: de digitalisering van de openbare ruimte*, mei 2010, p. 251.



datum 12 april 2011

ons kenmerk 147654.01U

blad 11

hoge mate van ICT deskundigheid in zich moeten bergen, belangrijk zijn? Beschikt de overheid zelf over voldoende kennis en inzicht in ICT systemen om de resultaten te kunnen beoordelen?

In het WRR rapport 'iOverheid' lezen de leden van de **GroenLinks**-fractie vele voorbeelden van *function creep*, het gebruik van data voor andere doelen dan waarvoor de data zijn opgevraagd en bewaard. Welk gebruik voor andere doelen acht de regering aanvaardbaar en welk niet meer? Welke voorwaarden dienen volgens de regering te worden gesteld bij het toelaten van *function creep*? Welke afweging maakt de regering hierbij tussen belangen als veiligheid, effectiviteit, privacy, keuzevrijheid en efficiëntie? Kan de regering hierbij ingaan op de afwegingen bij specifieke thema's als automatische nummerplaattherkenning, de VerwijsIndex Risicjongeren, het Schengen Informatie Systeem en het EPD?

5. Ondersteuning en rechten van burgers

5.1 Ondersteuning van burgers

Tekenend voor de schaal waarop digitalisering van de samenleving heeft plaatsgevonden, menen de leden van de **PvdA**-fractie, is een onderzoek van het Cbp naar de vraag in hoeveel databases mensen zitten. In genoemde expertmeeting wees de heer Kohnstamm, voorzitter van het Cbp, daarop. Dat onderzoek wijst uit dat een maatschappelijk weinig actieve persoon toch nog altijd in zo'n 250 databases zit en maatschappelijk actieve individuen in 1000, 1500 of zelfs meer. Prof. dr. Prins, lid van de WRR, wees er vervolgens op dat dit over meer gaat dan losse applicaties. Er is volgens haar een gekoppelde, verketende en vernetwerkte wereld ontstaan, waarin de burger bij één dossier wordt geconfronteerd met wel 100 organisaties, waar hij bij moet aankloppen als er iets niet klopt. Zij refereerde bovendien aan de constatering in het rapport Brouwer-Korf dat naast handhaving, advisering en voorlichting cruciaal zijn, onder andere over de interpretatie van essentiële criteria als doelbinding. Klopt de informatie van de heer Kohnstamm dat voor de advisering aan de 'professionals' in het kader van het rapport Brouwer-Korf, per 1 maart 2011 zegge en schrijve 3 fte's zijn vrijgemaakt? Kan de regering zich voorstellen dat niet alleen het Cbp dit uitermate teleurstellend vindt en een veel hogere benodigde arbeidsinzet inschat voor de ondersteuning van individuen en organisaties in deze materie? Kan de regering aangeven hoe een en ander zich verhoudt tot de ingeschatte risico's voor de burgers van de gedigitaliseerde samenleving? Wat is de regering voornemens hiertegen te ondernemen ter bescherming van haar burgers?

Ten aanzien van de controle van de burger over de eigen digitale identiteit noemt het rapport 'Check in/ Check uit' de privacycoach, die gebruikers helpt bij de onderhandeling met de aanbieder over het gebruik van persoonsgegevens en de beperking tot het overeengekomen gebruik. Ziet de regering mogelijkheden dergelijke vormen van ondersteuning te stimuleren en zo ja, op welke schaal?

De WRR stelt dat de overheid alert dient te zijn op de kwaliteit van de informatie (het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid) en de organisatorische inbedding van informatiestromen, zo menen de leden van de **PvdA**-fractie. Openheid en transparantie richting burgers is volgens de WRR nodig zodat zij inzicht hebben in wat over hen geregistreerd is, en er ondersteuning beschikbaar is indien correctie noodzakelijk blijkt. Deelt de regering deze opvatting? Zo ja, welke consequenties verbindt de regering daar dan aan? Wat is de reactie van de regering op de in de expertmeeting gesignaleerde 'fout percentages' in be-



datum 12 april 2011

ons kenmerk 147654.01U

blad 12

standen van onder andere de Belastingdienst? Deze foutieve registraties kunnen immers enorme overlast voor de individuele burger opleveren. Hoe beschermt en ondersteunt de overheid haar burgers hierin?

5.2 Rechten van burgers

De WRR spreekt over het belang van het recht om vergeten te worden en bepleit een radicale cultuuromslag met betrekking tot bewaren en archiveren, zo constateren de leden van **CDA**-fractie. Hoe staat de regering er tegen over wanneer deze leden voorstellen er *niet* mee te volstaan dit begrip eenvoudigweg te substantiëren door enerzijds de overheid een plicht op te leggen om - onder bepaalde voorwaarden en na een bepaald tijdsverloop - gegevens uit databases te verwijderen, en anderzijds in onderdelen van het privaatrecht (zoals het arbeidsrecht) op te nemen dat het verstrekken van bepaalde informatie kan worden geweigerd? Het voorstel betreft immers een cultuuromslag waarin de vrijheid van informatiegaring wordt beperkt.

Bij het cameratoezicht bevat de wettelijke regeling de mogelijkheid voor de burger de digitale identiteit te wissen, zo menen de leden van de **PvdA**-fractie. Deze optie wordt echter niet altijd geboden en niet iedere burger is zich van de optie bewust. Is de regering bereid proactiever op te treden in deze?

Hoe hanteert de overheid overigens het algemene recht van het individu om bepaalde incidenten na verloop van tijd achter zich te kunnen laten (het recht op vergeten) door opgeslagen informatie te verwijderen, zoals eveneens bepleit door de experts op 21 februari jl.?

De Staatscommissie-Thomassen constateert dat de overheid in toenemende mate een elektronische overheid is geworden.¹⁸ De aanbevelingen van de staatscommissie strekken er volgens de WRR toe de grondwetgever ter zake aan het werk te zetten, aangezien in het digitale tijdperk de betekenis van informatie (grond)rechten toeneemt. Dat is dé reden om de normativiteit van de Grondwet te versterken en de betekenis ervan voor de burger te vergroten, zo constateren de leden van de **PvdA**-fractie. Welke gevolgen verbindt de regering aan deze conclusies? Is een Grondwetswijziging in voorbereiding en zal de regering daarbij adequate voorzieningen treffen voor de handhaving van het informatierecht?

Wat verstaat de regering onder het recht om vergeten te worden? Is dat te organiseren, zo vragen de leden van de **SP**-fractie. Is het een verantwoordelijkheid van de overheid?

Met de inwerkingtreding in december 2009 van het Verdrag van Lissabon, is het Handvest van de grondrechten van de EU bindend geworden. Eén van de nieuwe elementen is - naast het recht op privacy dat al van veel ouder datum is - de uitdrukkelijke erkenning van het recht op bescherming van persoonsgegevens, zo constateren de leden van de **SP**-fractie. Op welke manier worden deze grondrechten in Nederlandse wetgeving geïmplementeerd?

6. Internationale aspecten

De Europese Commissie heeft over Europese ontwikkelingen met betrekking tot dataprotectie gemeld dat het bewaren van de gegevens, waartoe het Verdrag van Prüm de bevoegdheid

¹⁸ Eindrapport Staatscommissie Grondwet, 11 november 2010; *Kamerstukken II* 2010/11, 31 570, 17.



datum 12 april 2011

ons kenmerk 147654.01U

blad 13

geeft, in een centrale database gebeurt, zo menen de leden van de **CDA**-fractie. Vindt dit echt al plaats of is het een serieus streven van de Europese Commissie om tot een dergelijke opslag te komen? Wat zijn de overwegingen om tot een dergelijke wijze van opslag te komen?

In diverse krantenberichten (o.m. NRC Handelsblad 19 maart 2011) is aangegeven, dat de VS op grote schaal bankgegevens van Europese burgers hebben ingezien, en waarschijnlijk nog steeds inzien. Het is bekend dat door de SWIFT-organisatie maatregelen zijn genomen om de beschikbaarheid van gegevens van banktransacties die in Europa plaatsvinden, niet meer of slechts onder bepaalde voorwaarden door buitenlandse overheden te laten inzien. De leden van de **CDA**-fractie vernemen graag van de regering de gang van zaken betreffende deze aangelegenheid en hoe, gelet op de bestaande rechtshulpverdragen of op overeenkomsten van de regering met de VS, de stand van zaken thans is.

Kan de regering aan de leden van de **CDA**-fractie bevestigen dat er met betrekking tot het binnen de EU gebruikte Schengen Informatie Systeem grote verschillen bestaan tussen de signaleringen van de lidstaten en tussen de nationale interpretaties van wat wordt beschouwd als een 'bijzonder ernstig misdrijf'? Is het juist dat er in de diverse Schengen landen verschillende procedures bestaan voor een 'artikel 99 signalering' (personen die onopvallend of gericht gecontroleerd moeten worden)? Wat zijn de consequenties wanneer deze vragen bevestigend worden beantwoord?

Wat verwacht de regering van de herziening van de EU-privacyrichtlijn, die tegen de zomer wordt verwacht? Heeft de regering daarvoor een bepaalde doordachte insteek voor ogen? Is ze pro- of reactief in dezen? Het Cbp heeft op 6 december 2010 een brief aan de Kamers gezonden met het oog op de herziening van deze privacyrichtlijn.¹⁹ Graag zouden de leden van de **SP**-fractie op de hoogte gesteld worden van de inhoud van de reactie van de staatssecretaris op deze brief, die door de vaste Tweede Kamercommissie naar hem is doorgezonden.

7. Tot slot

In de diverse rapporten wordt de voortschrijdende digitalisering van gegevensbestanden gesignaleerd, zo constateren de leden van de **CDA**-fractie. Hierbij is de overheid direct betrokken voor zover de gegevens haar eigen informatiesystemen betreffen, dan wel wanneer het gaat om gegevens die aan de overheid dienen te worden verstrekt. De overheid kan echter ook indirect bij het beheer van digitale gegevens zijn betrokken wanneer het gaat om voornamelijk grote bestanden die door private organisaties, die een publieke functie hebben zoals banken en creditcard organisaties, worden beheerd. Acht de regering de huidige stand van de wetgeving voldoende om de veiligheid van de burger te waarborgen, niet alleen ten aanzien van de beveiliging van de systemen en de overdracht van de gegevens, maar ook ten aanzien van het gebruik door private rechtspersonen, die wanneer sprake is van onzorgvuldig gebruik of beheer (bijvoorbeeld datalekken), alleen ex post kunnen worden aangesproken? Voor de individuele burger is zo'n procedure achteraf buitengewoon belastend en de schade dikwijls onherstelbaar.

¹⁹ Brief ter inzage gelegd bij de afdeling Inhoudelijke Ondersteuning.



datum 12 april 2011

ons kenmerk 147654.01U

blad 14

Hoe kan de overheid interveniëren wanneer privaatrechtelijke rechtspersonen, die over grote databestanden beschikken, profielen van persoonsgegevens maken en die op de markt aanbieden? Is overheidsingrijpen mogelijk als private rechtspersonen gegevens laten lekken? Wat is de opvatting van de regering over een meldingsplicht bij datalekken (databreach), vragen de leden van de **CDA**-fractie.

Is de regering het eens met de constatering dat Google zoekopdrachten deel uitmaken van de verkeersgegevens van het betreffende informatieverzoek? Is de conclusie dat verkeersgegevens wel degelijk informatie kunnen verschaffen over de inhoud van de communicatie?

Klopt naar de mening van de regering de constatering van de WRR, bevestigd in genoemde expertmeeting door andere deelnemers, dat geloofwaardige evaluaties zeldzaam zijn, omdat – zo die al plaats vinden - die blijven steken in een discussie over de veiligheid van de technologie, dan wel de financiële debacles? Is de regering voornemens in de naaste toekomst meer aandacht te besteden aan adequate evaluaties, zo vragen de leden van de **PvdA**-fractie, te meer gezien de taakstelling van dit kabinet.

Veel aandacht werd er tijdens de expertmeeting besteed aan de kwaliteit van de informatie, zo merken de leden van de **SP**-fractie op. Gesteld werd dat de compleetheid en juistheid van de informatie lang niet altijd gegarandeerd kan worden. Bij de Belastingdienst wordt ervan uitgegaan dat 75% van de dossiers op orde is, wat overigens nog niet betekent dat die dossiers dan wel volledig kloppen. Des te grootschaliger een systeem des te groter het risico op onjuiste gegevens en op het vermenigvuldigen ervan. Ook zijn grootschalige systemen slechter te beveiligen en deze vormen daarmee een grotere bedreiging van de privacy. Is de regering dat met deze leden eens?

Is de regering zich bewust van het risico dat bij voor meer instanties toegankelijke databases, er geen enkele instantie is die de verantwoordelijkheid neemt voor signaleringen die vragen om actie, bijvoorbeeld in het eKD of de VerwijsIndex Risicjongeren? Indien dit het geval is, vragen de leden van de **GroenLinks**-fractie aan de regering hoe zij denkt dit risico weg te nemen?

De leden van de vaste commissies voor de JBZ-Raad, Justitie, OCW, VWS en BZK/AZ verzoeken de regering de reactie op deze brief op de kortst mogelijke termijn na de verschijningsdatum van de nota van de regering over gegevensbescherming - die verwacht wordt op 29 april 2011 - te zenden aan de Kamer, waarin verwijzing naar voornoemde nota een optie is. Een gelijklopende brief is tevens verzonden aan de ministers van BZK/AZ, OCW en VWS.

Namens de voorzitters van de vaste commissies voor de JBZ-Raad, OCW, VWS en BZK/AZ,
De voorzitter van de vaste commissie voor Justitie,

R.H. van de Beeten