Cloud Computing en Gegevensbescherming

Door C.M.C. Sjerps, afdeling Juridisch Adviseur[1]

1. Inleiding

Cloud computing, computeren via het internet, is 'hot'. Gegevensbescherming is eveneens een onderwerp dat de laatste tijd volop in de belangstelling staat. De vraag is hoe deze twee ontwikkelingen zich verhouden. Cloud computing is een domein dat nog volop in beweging is, en waar nog vele vragen open staan.

Aan de ene kant wordt cloud computing aangedragen als dé oplossing voor organisaties om grondig op ICT-uitgaven te kunnen bezuinigen.[2] Aan de andere kant deed Eurocommissaris Neelie Kroes een oproep voor strengere regels voor bescherming van data bij cloud computing.[3] Op dit moment wordt bij de rijksoverheid een beleidsmatige visie op cloud computing ontwikkeld. Het is de bedoeling is om uiteindelijk te komen tot een cloud voorziening voor de hele overheid. Aanleiding voor deze beleidsontwikkeling is de motie Van der Burg c.s. waarin de regering wordt verzocht om een visie op cloud computing, die de mogelijkheden voor de inrichting van de overheidscloud duidelijk omschrijft met bijbehorende voor- en nadelen.[4] Wat miste in de beleidsnotitie die hierover is geschreven, was een juridische analyse van cloud computing, vooral in relatie tot de Wet bescherming persoonsgegevens (Wbp). In dit artikel wordt een aanzet gedaan om het juridisch kader te schetsen.

---

[1] Graag wil ik John Morijn, Willem Pedroli en Peter Stolk bedanken voor hun hulp bij de totstandkoming van dit artikel.

[2] S van der Schaaf 'Bezuinigen met cloud computing?' http://www.it-executive.nl/blogs/blog/het_mes_in_de_overheidsuitgaven_denk_eens_aan_cloud_computing/, geraadpleegd op 3 maart 2011.

[3] C van Hoek 'Kroes wil strengere regels cloud computing' http://www.nu.nl/internet/2387902/kroes-wil-strengere-regels-cloud-computing.html, geraadpleegd op 26 november 2010.

[4] Motie van het lid Van der Burg c.s., 2009-2010, 26 643 (Informatie- en communicatietechnologie (ICT)), nr. 157.

Om de toegankelijkheid van deze analyse voor alle typen lezers te garanderen, geeft paragraaf 2 een introductie van het begrip cloud computing en worden kort de voor- en nadelen van cloud computing op een rij gezet. In paragraaf 3 worden de gevolgen van cloud computing voor de naleving van de Wbp onderzocht. Paragraaf 4 bevat een aantal meer beschouwende overwegingen ten aanzien van cloud computing. In de conclusie, paragraaf 5, wordt een korte samenvatting van de belangrijste bevindingen gegeven.

2. Cloud computing: wat is dat en welke juridische vragen roept het op?

> *"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. […] Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?" L. Ellison, CEO van Oracle*[5]

Cloud computing is computeren via het internet. De gegevens of programma's die je op je scherm ziet, worden verwerkt en opgeslagen op computers die zich ergens anders bevinden: in de 'cloud'. Aangezien er vele, zeer uitgebreide definities van cloud computing zijn is het handig om dit simpele idee als uitgangspunt te nemen bij het onderzoeken van cloud computing.[6] Omdat de term 'cloud computing' op veel verschillende ICT-situaties wordt toegepast en verhandelingen over cloud computing veel jargon bevatten, is het echter wel nodig om kort verschillende onderscheiden die op dit gebied gemaakt worden in deze paragraaf op een rij te zetten.

---

[5] D Farber 'Oracle's Ellison nails cloud computing' op http://news.cnet.com/8301-13953_3-10052188-80.html, geraadpleegd op 1 februari 2011; GA Fowler & B Worthen 'The internet industry is on a cloud – whatever that may mean' Wall Street Journal, http://online.wsj.com/article/SB123802623665542725.html, geraadpleegd op 1 februari 2011.

[6] Een voorbeeld van een ingewikkelde definitie afkomstig van het US National Institute of Standards and Technology is: "Cloud computing is […] a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Een mogelijke verklaring voor het wijdverbreide gebruik van de term 'cloud computing' kan gevonden worden in het feit dat toen ICT-bedrijf Salesforce de term ging gebruiken, de opbrengst van het bedrijf met 44% groeide.[7] Dit vormde een belangrijke inspiratiebron voor andere bedrijven in de ICT-branche om hetzelfde te doen. Cloud computing blaast nieuw leven in de gecentraliseerde servermarkten, omdat er hoge winsten worden behaald met verkoop en servicecontracten. Het geeft ook meer mogelijkheden voor bedrijven voor koppelverkoop,[8] ook wel vendor lock-in genoemd. Als de data van een organisatie eenmaal in een bepaald systeem zijn gezet, is het niet eenvoudig om naar een andere leverancier over te stappen die er een ander systeem op nahoudt. Tevens word je als afnemer vaak gedwongen om bepaalde software te kopen die alleen verenigbaar is met het systeem van je leverancier. Dit maakt het overstappen tussen leveranciers van clouddiensten moeilijk en vormt een bedreiging voor de mededinging op de markt. Hieraan zal in paragraaf 4 meer aandacht worden besteed.

Maar eerst terug naar de definitie van cloud computing: Cloud computing is een nieuwe manier van ICT-benodigdheden leveren. Het is geen nieuwe technologie.[9] Cloud computing maakt het mogelijk om ICT-services via het internet beschikbaar te stellen. Het gaat dan om ICT-services als het opslaan en verwerken van data en het leveren van software.

Kenmerken van cloud computing die verschillen van klassieke ICT-voorzieningen zijn:

- Het delen van ICT-middelen met meerdere gebruikers;
- Het gebruik en het bezit van ICT-middelen worden losgekoppeld. Het is mogelijk om ICT in te huren;
- De servercapaciteit is elastisch en kan zowel meteen worden opgeschaald als worden teruggebracht;

[7] Fowler en Worthen (n 5).

[8] J Cascio 'Dark Clouds', Open the Future blog, artikel geplaatst op 19 januari 2009, http://www.openthefuture.com/2009/01/dark_clouds.html, geraadpleegd op 15 februari 2011.

[9] D Catteddu & G Hogben 'Cloud computing – Benefits, risks and recommendations for information security' European Network and Information Security Agency (ENISA november 2009) p 4.

- Data worden niet meer opgeslagen op de eigen computer, maar op een externe harde schijf (van de leverancier).[10]

De meest genoemde voordelen van het gebruiken van cloud computing ten opzichte van het gebruiken van klassieke ICT-voorzieningen hangen hier direct mee samen. Deze voordelen zijn kostenbesparing op ICT-middelen, meer flexibiliteit en betere schaalbaarheid.

Er wordt doorgaans een onderscheid gemaakt tussen drie typen cloud computing:

- Software as a Service (SaaS): levert software, zoals Gmail, Facebook of Google Docs;
- Platform as a Service (PaaS): levert ICT-diensten op de platformlaag en/of het besturingssysteem voor onder andere toegangsbeheer of identiteitsbeheer. Een voorbeeld van PaaS is PayPal;
- Infrastructure as a Service (IaaS): levert technische infrastructuurcomponenten zoals opslag, geheugen en netwerk.[11]

Een ander onderscheid dat gemaakt wordt, is dat tussen een:

- *Public* of publieke cloud: een ICT-omgeving waar iedereen toegang toe zou kunnen krijgen;
- *Private* of exclusieve cloud: een ICT-omgeving die alleen beschikbaar is voor personen binnen een bepaald netwerk;
- *Partner* of *community* cloud: een clouddienst die beschikbaar wordt gesteld voor een beperkte, goed gedefinieerde groep afnemers;
- Hybride cloud: een ICT-omgeving die een combinatie is van meerdere cloudtypen.[12]

---

[10] 'Cloud computing voor de Nederlandse overheid – Eindrapport werkpakket 3' KPMG IT Advisory (oktober 2010) p 11.

[11] ibid p 14; Cloud computing wiki http://nl.wikipedia.org/wiki/Cloud_computing, geraadpleegd op 3 mei 2011.

[12] 'Cloud computing voor de Nederlandse overheid' (n 10) p 12, 13; 'Cloud computing – Benefits, risks and recommendations for information security' (n 9) p 15.

Bij het gebruik van een publieke cloud zijn de voordelen van cloud computing het grootst, omdat ICT-middelen dan zo veel mogelijk worden gedeeld tussen afnemers.[13] Hier tegenover staat dat de risico's bij het gebruik van een publieke cloud ook het hoogste zijn. In de cloudstrategie voor de overheid wordt er daarom voor gekozen om een hybride cloud te realiseren (de overheidscloud) die zal bestaan uit een intern en een extern exclusief gedeelte. De hybride cloud beoogt een middenweg te bewandelen, waarbij wel voldoende (schaal)voordelen worden behaald, maar tegelijkertijd de risico's van cloud computing worden ingeperkt. Deze hybride cloud moet diensten gaan leveren voor alle overheidsorganisaties.

De risico's wat betreft het interne en het externe gedeelte van de overheidscloud zijn verschillend. Het interne exclusieve gedeelte van de cloud verschilt niet wezenlijk van de bestaande ICT-omgeving. Maar in plaats van de situatie waarin overheidsorganisaties allemaal hun eigen servers hebben, worden servers tussen organisaties gedeeld en heeft men via het internet toegang tot deze servers. Het grootste risico dat hiermee gepaard gaat is dat het (publieke) internet onvoldoende beschikbaar is. Er bestaat ook een iets hoger risico op vendor lock-in. Dit komt doordat er minder leveranciers zijn van exclusieve cloudproducten dan van klassieke ICT.[14] Voor het externe exclusieve gedeelte[15] wordt een externe leverancier gekozen die aan de overheid clouddiensten gaat leveren. Dit houdt in dat een deel van het ICT-beheer uit handen wordt gegeven. Welke gevolgen dit kan hebben wordt in de volgende hoofdstukken nader onderzocht.

3. Cloud computing en gegevensbescherming

[13] 'Cloud computing voor de Nederlandse overheid' (n 10) p 12, 13.
[14] ibid p 20.
[15] Het woord 'exclusief' hoeft overigens niet te betekenen dat de leverancier geen andere klanten heeft. Het houdt in dat in bepaalde mate ICT-middelen alleen aan de overheid beschikbaar worden gesteld. De mate van exclusiviteit verschilt per leverancier. Er zal ook altijd sprake zijn van een bepaalde graad van overlap met andere gebruikers, bijvoorbeeld voor fysieke faciliteiten (serverruimte, koeling) en beheer. Het onderscheid tussen een externe exclusieve cloud en een publieke cloud is daarom niet altijd even scherp.

'Before building an infrastructure that enables manipulation and abuse, we should carefully research legal and technological possibilities to protect the positive and negative freedom of citizens'.[16]

In deze paragraaf zullen de juridische en beleidsmatige implicaties van de inzet van cloud computing in kaart worden gebracht.

De Kernbegrippen van de Wbp

De Wbp draait eigenlijk om drie begrippen: het begrip 'persoonsgegeven', het begrip 'verantwoordelijke' en het begrip 'verwerken'. Een persoonsgegeven is een gegeven dat herleidbaar is tot een levende, natuurlijke persoon.[17] De verantwoordelijke stelt het doel en de middelen voor de verwerking van persoonsgegevens vast.[18] Het begrip 'verwerken' is zeer ruim gedefinieerd en behoeft enige nadere toelichting.

Verwerken behelst elke handeling die met betrekking tot een persoonsgegeven verricht kan worden, met uitzondering van de 'enkelvoudige transmissie'.[19] Van verzamelen tot vernietigen, van raadplegen tot ter beschikking stellen, het valt allemaal onder de term verwerking. Deze veelomvattende definitie vindt zijn oorsprong in Europese regelgeving. Ter illustratie: in een recente uitspraak van het Europese Hof voor de Rechten van de Mens (EHRM) stelt het Hof dat '*the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*'.[20] Bij cloud computing is de vraag of iets een verwerking is niet altijd direct evident. Is de verzending van een bestand via het internet voor opslag in de cloud een verwerking of valt dit onder de uitzondering van

[16] M Hildebrandt & S Gutwirth 'Implications of profiling practices on democracy and rule of law' (FIDIS 5 september 2005) http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf, p 80.
[17] E Thole 'Privacy en cloud computing', http://217.114.90.55/Global/Publicaties/Privacy%20en%20cloud%20computing_Thole_Informatie%202010.pdf geraadpleegd op 10 februari 2010, p 28.
[18] Artikel 1, onder d, Wbp.
[19] Artikel 1, onder b, Wbp. De enkelvoudige transmissie van gegevens, behelst het zenden van gegevens van punt A naar punt B.
[20] EHRM 4 december 2008, appl. 30562/04, NJ 2009, 410.

de enkelvoudige transmissie? Kort gezegd valt het verzenden van een bestand via internet voor opslag niet, maar het opslaan van het gegeven zelf wél onder het begrip verwerken. Daarmee wordt de vraag wanneer er sprake is van een enkelvoudige transmissie al snel slechts van theoretisch belang. Immers, de enige reden om persoonsgegevens van A naar B te sturen is om er 'iets' mee te doen. Dat kan zijn raadplegen, wijzigen, verzamelen, vernietigen, enzovoort. Al deze handelingen vallen onder de definitie van verwerken zoals opgenomen in de Wbp en dus zal er aan de vereisten van de Wbp moeten worden voldaan. Het feit dat het verzenden van de gegevens van de cloud naar je beeldscherm is uitgezonderd, maakt in de praktijk daarom weinig verschil.

De relatie verantwoordelijke – bewerker

Zoals hierboven gesteld worden het doel van en de middelen voor de verwerking van persoonsgegevens vastgesteld door de verantwoordelijke voor de gegevensverwerking.[21] De verantwoordelijke bepaalt ook wie de daadwerkelijke verwerking van de persoonsgegevens gaat uitvoeren en aan welke eisen dit moet voldoen.[22] De uitvoerder van de verwerking wordt in de Wbp aangeduid met de term 'bewerker'.

Voor verwerkingen van gegevens die bij de rijksoverheid berusten, is de desbetreffende minister 'de verantwoordelijke' voor alle verwerkingen van informatie van zijn eigen departement. Dit geldt voor de huidige ICT-situatie, maar ook bij een overgang naar een externe exclusieve cloud. Bij een externe exclusieve cloud stelt de cloud provider de middelen voor de gegevensverwerking aan de overheid beschikbaar en biedt deze aan als een service, toegankelijk via het internet. Of de cloud provider alleen bewerker, of óók verantwoordelijke is hangt af van de vraag in hoeverre de cloud provider zich opstelt als een neutrale intermediair. Dit sluit aan bij de opinie van de Artikel 29 Werkgroep, het onafhankelijke adviesorgaan van Europese privacytoezichthouders, dat *hosting providers* bewerker zijn ten

[21] Artikel 1, onder d, Wbp.
[22] Artikel 1, onder e, Wbp.

aanzien van de gegevens die hun klanten plaatsen op hun site, maar als verantwoordelijke vallen aan te merken ten aanzien van de persoonsgegevens van hun klanten die zij opslaan en verwerken.[23] Deze opinie kan analoog worden toegepast op cloud providers. Als de gegevens in de cloud bijvoorbeeld zouden worden doorverkocht aan andere bedrijven, dan heeft de cloud provider zelf, naast het doel van de overheid, óók een doel voor de gegevensverwerking. In dat geval moet de cloud provider zelf ook voldoen aan de verplichtingen uit de toepasselijke privacyregelgeving.[24] Dat leidt er bij eventuele schendingen van privacyregelgeving toe dat de cloud provider aansprakelijk gehouden kan worden voor deze schendingen.[25]

Hoewel het bijna te voor de hand liggend lijkt dat het natuurlijk niet de bedoeling is dat de cloud provider overheidsgegevens aan bedrijven verkoopt, is het erg belangrijk dat hier zeer goede afspraken over worden gemaakt met de cloud provider. Een bedrijf als Google haalt immers zijn winst uit het bundelen van informatie over individuele gebruikers, om dit vervolgens door te verkopen aan bedrijven die deze informatie gebruiken voor hun marketingstrategieën.[26] Contractueel zal moeten worden vastgelegd dat dit soort handelingen niet zullen worden verricht ten aanzien van gegevens die zich in de externe overheidscloud bevinden.

Het territorialiteitsvraagstuk

Bij gebruik van een externe cloud is het belangrijk om extra aandacht te besteden aan de vraag waar de verantwoordelijke en de bewerker in juridische zin zijn

[23] 'De Leon & Vivi Down/Google' met noot van B van der Sloot, Jurisprudentie nr. 23 in Mediaforum 2010-7/8 p 265-266.
[24] Thole (n 17) p 30.
[25] HvJ EG 23 maart 2010 zaken C-236-/08 t/m C-238/08, Google France http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=nl&num=79899676C19080237&doc=T&ouvert=T&seance=ARRET, geraadpleegd op 23 februari 2011, r.o. 114-115.
[26] J Valentino-Devries 'What they know about you' Wall Street Journal http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html?KEYWORDS=%22What+they+know%22, geraadpleegd op 3 maart 2010.

gevestigd.[27] Dit wordt ook wel het territorialiteitsvraagstuk genoemd. Volgens de Artikel 29 Werkgroep moeten verantwoordelijken in de toekomst weten waar verwerkingen plaatsvinden.[28] Afhankelijk van welke cloud provider (bewerker) wordt gekozen kan dit nog wel eens problemen opleveren, omdat niet alle cloud providers inzicht willen geven in de plaats waar hun datacenters zich bevinden. En zelfs als men wel weet waar deze zich bevinden, dan nog is het niet altijd evident op welke locatie de daadwerkelijke gegevensverwerking plaatsvindt.[29] In het geval van onduidelijkheid over de locatie van datacentra en/of de plaats van de gegevensverwerking bestaat er een reële kans op overtreding van de artikelen 76-78 van de Wbp, die het gegevensverkeer met landen buiten de Europese Unie regelen. Het kan dan immers voorkomen dat gegevens worden verwerkt in een datacentrum dat zich bevindt in een land dat geen passend beschermingsniveau waarborgt. Zo een overtreding komt voor rekening van de verantwoordelijke.

De kernbeginselen van de Wbp

De kern van het beschermingsmechanisme zoals het is neergelegd in de Wbp kan worden samengevat aan de hand van vier beginselen, namelijk het:

- Doelbindingsbeginsel: gegevens mogen alleen worden verwerkt voor een bepaald en gerechtvaardigd doel;
- Transparantiebeginsel: de persoon wiens gegevens worden verwerkt moet inzicht hebben in welke gegevens over haar worden verwerkt;
- Proportionaliteitsbeginsel: er mogen niet meer gegevens worden verwerkt dan voor een gerechtvaardigd doel nodig is;
- Kwaliteitsbeginsel: de kwaliteit van de gegevens moet zijn gewaarborgd en dit kan worden afgedwongen door diegene op wie de gegevens betrekking hebben.[30]

[27] Artikel 4 Wbp.
[28] Thole (n 17) p 31.
[29] 'De Leon & Vivi Down/Google' (n 23) p 266.
[30] EJ Dommering 'Recht op persoonsgegevens als zelfbeschikkingsrecht' in JEJ Prins (red.) '16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk' (Leiden 2010) Stichting NJCM-Boekerij (47) p 85-86.

Bij een overgang naar cloud computing komen al deze beginselen mogelijk in het geding. In een hybride cloud omgeving kan de controle op kwaliteit en verwerking van persoonsgegevens vrijwel onmogelijk worden gemaakt door de ondoorzichtigheid van de techniek, in combinatie met de complexiteit van de problematiek en de hoeveelheid data die door de overheid worden verwerkt.[31] Aan de andere kant is het niet zo dat er op dit moment een glashelder overzicht bestaat van welke gegevens door welk overheidsonderdeel worden verwerkt. Een herinrichting van het ICT-landschap zou dan ook kunnen worden aangegrepen om orde op zaken te stellen en een systeem te ontwerpen waarbij alle beginselen gewaarborgd worden. Dat kan in het kader van een overgang naar cloud computing, maar zo een doorlichting kan natuurlijk ook op zichzelf staan.

Privacy-by-design

Privacy-by-design is een principe dat door de Europese privacytoezichthouders wordt gepromoot. Het houdt in dat verantwoordelijken al in een zo vroeg mogelijk stadium moeten nadenken over de vraag hoe de vereisten van gegevensbescherming in het ontwerp van nieuwe technologieën geïncorporeerd kunnen worden.[32] Zaken waarover nagedacht moet worden zijn onder meer dat:

- Technologie dusdanig ontworpen wordt dat zo min mogelijk persoonsgegevens worden verwerkt;
- Een nieuw ICT-systeem de betrokkene effectieve middelen toekent om de verwerking van haar persoonsgegevens te controleren;
- Zowel de ontwerpers als degenen die een nieuw ICT-systeem gaan gebruiken ervoor moeten zorgen dat de betrokkene voldoende wordt geïnformeerd over de manier waarop het systeem functioneert;
- Het nieuwe systeem zodanig wordt ontworpen en beveiligd dat toegang tot de gegevens alleen mogelijk is voor daartoe bevoegde personen;

[31] Dommering (n 30) p 87.

[32] HR Kranenborg en LFM Verhey 'Wet bescherming persoonsgegevens in Europees perspectief' Kluwer (Deventer 2011) p 190.

- Het waarborgen van de kwaliteit van gegevens door technische middelen wordt ondersteund;
- Als er binnen het systeem gegevens verwerkt worden voor verschillende doeleinden (en die kans is groot binnen de overheid), gegarandeerd moet worden dat de verschillende verwerkingen op veilige wijze van elkaar gescheiden zijn.[33]

Dat dit meer is dan alleen een aanbeveling van de Europese privacytoezichthouders kan worden afgeleid uit de recente uitspraak van het Bundesverfassungsgericht met betrekking tot de Dataretentierichtlijn. Daarin bepaalt het Hof dat bij de *vormgeving* van de opslag en het gebruik van de gegevens rekening gehouden moet worden met het *bijzondere gewicht* van een dergelijke opslag. Er moet daarom aan strenge eisen worden voldaan ten aanzien van de beveiliging, het gebruik van de gegevens, de transparantie en de rechtsbescherming.[34] Ook in een brief aan de Tweede Kamer van de ministers van V&J en BZK werd privacy-by-design aangemerkt als "een goede manier om privacybescherming concreet vorm te geven in informatiesystemen waarin persoonsgegevens worden verwerkt".[35] In de brief wordt ook aangegeven dat de gedachte van privacy-by-design al langere tijd bekend is, maar in de praktijk nog geen grote toepassing vindt. Een overgang naar cloud computing vormt een unieke kans dit principe bij de herinrichting van de ICT-infrastructuur wél in de praktijk te brengen.

WRR rapport: iOverheid

Een bredere toepassing van het privacy-by-design principe zou een goede stap in de richting van verbeterde privacybescherming zijn. In het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat in het voorjaar 2011 is uitgebracht over de zogenaamde 'iOverheid', wordt echter betoogd dat men nog een

[33] ibid.

[34] WAM Steenbruggen 'Annotatie bij BVerfG 2 maart 2010 (Vorratsdatenspeicherung)', Tijdschrift voor Constitutioneel Recht, Jaargang 2 januari 2011, p 73.

[35] Brief aan de Tweede Kamer van de staatssecretaris van V&J en de minister van BZK over privacybeleid, 2010-2011, 32 761, nr. 1, p 12.

aantal stappen verder zou moeten gaan. Er wordt in het rapport beargumenteerd dat de overheid een iOverheid is geworden, gekenmerkt door informatiestromen en –netwerken, die niet alleen gericht is op dienstverlening, maar ook op controle en zorg.[36] Er 'heeft zich een praktijk ontwikkeld, waarin samenhangende informatiestromen het karakter van de overheid domineren. En daarmee bepalen deze informatiestromen de nieuwe mogelijkheden, maar ook de afhankelijkheden en de kwetsbaarheden voor zowel de overheid als haar burgers'.[37] De overgang naar cloud computing vormt een wezenlijk onderdeel van dit proces, aangezien de cloud de vernetwerking van informatie verder zal faciliteren. De overgang naar een iOverheid is een proces dat zich sluipenderwijs en zonder een overkoepelende maatschappelijke discussie heeft voltrokken. Juist daarin zit volgens de WRR het probleem. Het is essentieel dat de verdere ontwikkeling van de iOverheid plaatsvindt in een context waarin afwegingen worden geëxpliciteerd, toetsbaar zijn en waarbij publiekelijk verantwoording wordt afgelegd van gemaakte keuzes.[38] Als uitgangspunt moeten bij de besluitvorming verschillende beginselen, zoals efficiëntie, privacy en transparantie, expliciet tegen elkaar worden afgewogen.[39] Alleen door een open debat over de verdere ICT-ontwikkelingen bij de overheid kan ervoor worden gezorgd dat de kwaliteit van het beleid en de informatie kan worden gegarandeerd en dat burgers inzicht hebben in welke informatie over hen wordt vergaard.[40] Het is daarom zaak de voorgenomen plannen op het gebied van cloud computing langs de genoemde beginselen te leggen en hierover een maatschappelijke discussie te starten. Hoewel dat het proces om tot een overheidscloud te komen waarschijnlijk zal verlengen, zal een publieke discussie bijdragen aan een eindproduct waarin de kernbeginselen van de Wbp stevig verankerd zijn.

4. Strategische overwegingen ten aanzien van de cloud

[36] "iOverheid" Rapport van de Wetenschappelijk Raad voor het Regeringsbeleid, Amsterdam University Press (Amsterdam 2011) p 11.
[37] ibid p 11.
[38] ibid p 15.
[39] ibid p 15.
[40] ibid p 16.

'A resilient cloud is certainly possible, but would mean setting aside some of the cherished elements of the cloud vision'.[41]

Deze paragraaf kijkt verder dan alleen het juridische, om zo ook ruimte te geven aan andere overwegingen die een belangrijke rol in de discussie rondom cloud computing zouden moeten spelen.

Cloud computing als besparingsmogelijkheid?

Kostenbesparing wordt als een van de grootste voordelen van cloud computing genoemd. Het vormde ook een aanleiding voor het indienen van de motie-Van der Burg c.s.[42] Echter, er kunnen wel vraagtekens geplaatst worden bij de hoeveelheid geld die bij een overgang naar cloud computing bespaard kan worden. De overgang van ICT-voorzieningen, die per departement zijn georganiseerd, naar een overheidscloud is een vorm van schaalvergroting die zich ook op andere terreinen heeft voltrokken: denk aan de overgang van de departementale personeelsadministratie naar het interdepartementale P-Direkt. Deze schaalvergroting zou een besparing moeten opleveren op materieel en personeel en daarom veel efficiënter zijn. Echter, een deel van het geld dat wordt bespaard met de schaalvergroting, moet meteen weer in de organisatie worden geïnvesteerd. Er moet namelijk een zogenaamde tussenafdeling komen die als schakel fungeert tussen de cloud provider en de ambtenaar/gebruiker. Daarbij moet het geld dat bespaard wordt op eigen ICT-personeel, geïnvesteerd worden in het bekostigen van servicecontracten met de cloud provider.

Wellicht een nog belangrijkere overweging is dat volgens een recent onderzoek maar een heel klein deel van de ICT-informatie van de overheid geschikt is voor plaatsing in een cloud.[43] Zaken die niet voor plaatsing in een cloud in aanmerking komen, zijn:

- Zeer confidentiële data;

[41] Cascio (n 8).
[42] Motie van het lid Van der Burg (n 4).
[43] 'Cloud computing voor de Nederlandse overheid' (n 10) p 48.

- Grootschalige 'legacysystemen'. Dit zijn systemen die al lang binnen een organisatie gebruikt worden, geschreven zijn in 'oude' computertalen en daardoor moeilijk verenigbaar zijn met nieuwe programma's zoals die in een cloud te vinden zijn. Deze systemen vervullen wel een belangrijke rol binnen de organisatie en kunnen dus niet zomaar gemist of vervangen worden;
- Systemen die aan het begin van hun levenscyclus staan en waarvan de afschrijvingsperiode ruim is;
- Zeer complexe applicaties waar cloud computing op dit moment nog geen oplossingen voor biedt.[44]

Je houdt dan maar een klein gedeelte van de ICT over dat in aanmerking komt voor plaatsing in de cloud. Het effect van een eventuele schaalvergroting en de bijkomende kostenbesparing wordt daarmee, in ieder geval op de korte termijn, aanzienlijk beperkter.

Vendor lock-in

Het aanbod van cloud diensten is op dit moment nog maar beperkt. Ook het aantal programma's dat de overgang van data, applicaties of diensten van het ene naar het andere systeem kan faciliteren is beperkt. Dit houdt in dat als er eenmaal voor een cloudleverancier is gekozen, het heel moeilijk kan zijn om in de nabije toekomst naar een andere (goedkopere en/of betere) leverancier over te stappen.[45] Dit kan het tevens moeilijk maken om data van de cloud naar het eigen ICT-systeem te verhuizen.[46] Het fenomeen dat je, als je voor een leverancier kiest, ook aan die leverancier vastzit, wordt ook wel 'vendor lock-in' genoemd. EU-commissaris Neelie Kroes heeft hier tijdens het Open Forum Europe Summit 2010 in Brussel voor gewaarschuwd. Zij vindt dat vendor lock-in bij overheden een verspilling is van publieke gelden en pleit voor Europese richtlijnen voor aanbestedingen die overheden voor vendor lock-in moeten behoeden.[47]

[44] ibid p 41-44.
[45] 'Cloud computing & security' (n 11) p 41.
[46] ibid.
[47] ibid.

Hoewel hieruit niet direct de conclusie moet worden getrokken om maar helemaal niet te beginnen met cloud computing, zou dit wel een reden kunnen zijn om een overgang naar cloud computing uit te stellen. In ieder geval zou de overheid daarmee kunnen wachten totdat er meer open standaarden worden gebruikt door ICT-leveranciers en de producten van verschillende marktspelers de mogelijkheid bieden om van leverancier te switchen.

De kwetsbaarheid van een gecentraliseerd systeem

In de systeemtheorie[48] zijn enkele principes aangewezen die de voorwaarden voor een veerkrachtig systeem vormen. Met een veerkrachtig systeem wordt een systeem bedoeld dat tegen een stootje kan, een systeem dat je niet zomaar plat legt. De principes voor een veerkrachtig systeem zijn onder andere: decentralisatie, diversiteit, transparantie, samenwerking, flexibiliteit, openheid, vooruitzien en omkeerbaarheid.[49] Een veerkrachtige strategie is een strategie waarbij als uitgangspunt wordt genomen dat er gegarandeerd iets met het systeem fout zal gaan, maar dat de manier waarop het fout gaat niet precies voorspeld kan worden.[50] Een adequate strategie om hier mee om te gaan bereidt zich voor op deze onverwachte problemen, niet alleen qua tijdspanne, maar vooral ook wat betreft de omvang van het probleem.

Centralisatie is de kern van het cloud computing model. Dit betekent dat alles wat de centrale service raakt, zoals het falen van het netwerk, een effect heeft op iedereen die de service gebruikt.[51] Als gebruikers in dat geval niet hun eigen back-up systeem hebben, met documenten en programma's, betekent dit dat niemand meer iets kan doen. Hetzelfde geldt voor virussen die de cloud binnen dringen. De centralisatie van

[48] Systeemtheorie wiki, http://nl.wikipedia.org/wiki/Systeemtheorie, geraadpleegd op 15 maart 2010.
[49] Cascio (n 8).
[50] ibid.
[51] ibid.

de cloud is dus in het geval van een falen van het systeem een nachtmerrie.[52] En hoe groter de cloud, hoe meer mensen erdoor geraakt zullen zijn.

Een veerkrachtig cloud systeem zou eruit kunnen bestaan dat data en programma's op de cloud, maar ook op de individuele pc beschikbaar zijn. Als de cloud uitvalt heb je een back-up op je eigen computer, en als je computer het begeeft heb je een back-up in de cloud.[53] Dat is echter niet de ontwikkeling die de overheid op dit moment beoogt: in het beoogde systeem wordt deze wisselwerking tussen centrale en individuele opslag niet opgenomen. En dat maakt het systeem kwetsbaar. Hoe goed je de cloud ook beveiligt, er zullen zich op den duur problemen voordoen die zeer vele gebruikers zullen raken. Ook nu doen zich geregeld problemen voor met grote gecentraliseerde systemen: denk aan de urenlange storing met DigiD op 18 en 23 maart.[54] Wanneer dit ook gebeurt met de cloud, zal dat waarschijnlijk een negatief effect hebben op het draagvlak voor de cloud.

5. Conclusie

> *"Any intelligent fool can make things bigger and more complex [..]. It takes a touch of genius - and a lot of courage - to move in the opposite direction."*
> *Albert Einstein*[55]

Een overgang naar een zogenaamde overheidscloud is geen sinecure. Het is zaak voor de overheid om zo een overgang gedegen voor te bereiden en hier de tijd voor te nemen. Haast maken is niet nodig, want op de korte termijn is het kostenbesparende effect van een overgang naar de cloud immers gering. Ook bestaan er op dit moment nog niet veel cloud leveranciers. Het is daarom voordeliger om de markt eerst de tijd te geven om verder te groeien en pas daarna een cloud provider te kiezen, ook om het risico op vendor lock-in te verkleinen. In de

[52] ibid.
[53] ibid.
[54] 'Storing DigiD' http://www.telegraaf.nl/digitaal/6358180/__Storing_DigiD__.html, geraadpleegd op 27 april 2011.
[55] http://rescomp.stanford.edu/~cheshire/EinsteinQuotes.html, geraadpleegd op 20 oktober 2011.

tussentijd kunnen we ons buigen over de vraag hoe we een gecentraliseerd cloud systeem voldoende weerbaar kunnen maken, zodat bijvoorbeeld grootschalige uitval van het systeem wordt voorkomen.

Wanneer wordt besloten tot het opslaan van gegevens in een externe overheidscloud, dan zal er vanuit het perspectief van gegevensbescherming kritisch naar de cloud provider moeten worden gekeken en zullen er duidelijke afspraken met de provider moeten worden gemaakt. Het is van belang om vast te leggen dat de provider alleen als bewerker ten aanzien van de overheidsgegevens zal fungeren. Het is niet de bedoeling dat de provider zelf verwerkingen uitvoert ten aanzien van de in de cloud opgeslagen gegevens. Tevens moeten er afspraken worden gemaakt over de locatie van de servers, om te voorkomen dat gegevens worden verwerkt in landen waar geen passend beschermingsniveau voor persoonsgegevens bestaat.

Een overgang naar cloud computing brengt het risico met zich mee dat de kernbeginselen van de Wbp in het geding komen. Het is daarom zaak om het privacy-by-design principe toe te passen tijdens het ontwerp van het nieuwe systeem. Dit houdt in dat al in een zo vroeg mogelijk stadium wordt nagedacht over de vraag hoe de vereisten van gegevensbescherming in het ontwerp van de overheidscloud geïncorporeerd kunnen worden. De besluitvorming rondom het invoeren van de cloud zal in het publieke domein moeten plaatsvinden, waarbij expliciete afwegingen worden gemaakt over de efficiëntie van het systeem en de privacy van de burger. Beleidsmatige keuzes zullen gedegen moeten worden gemotiveerd. Het is belangrijk hier op gezette tijden richting het parlement en de burger over te communiceren. Gezien de aandacht die er op dit moment is voor privacy en ICT-projecten bij de overheid, denk aan het elektronisch patiëntendossier, kan stevige feedback vanuit de maatschappij worden verwacht. Dit is alleen maar positief. Het zal leiden tot een robuust beleidsplan en tot minder problemen bij de daadwerkelijke verwezenlijking van een overheidscloud waarin de kernbeginselen van de Wbp verankerd zijn.

Naschrift

Zoals is vermeld in de inleiding is dit artikel geschreven als reactie op een beleidsdocument over cloud computing. Dat document stamt uit het najaar van 2010 en toen had men voor ogen om een hybride overheidscloud te realiseren. Een aantal van de bovengenoemde nadelen van een externe cloud hebben er echter toe geleid dat de minister van BZK heeft besloten om een pas op de plaats te maken en op de korte termijn alleen een interne overheidscloud te verwezenlijken.[56] De strategie voor de interne overheidscloud zal verder worden doorontwikkeld en over de resultaten zal worden gerapporteerd in het bedrijfsvoering jaarverslag 2012.

[56] Brief van de minister van BZK aan de Tweede Kamer, 2010-2011, 26 643, nr. 179.