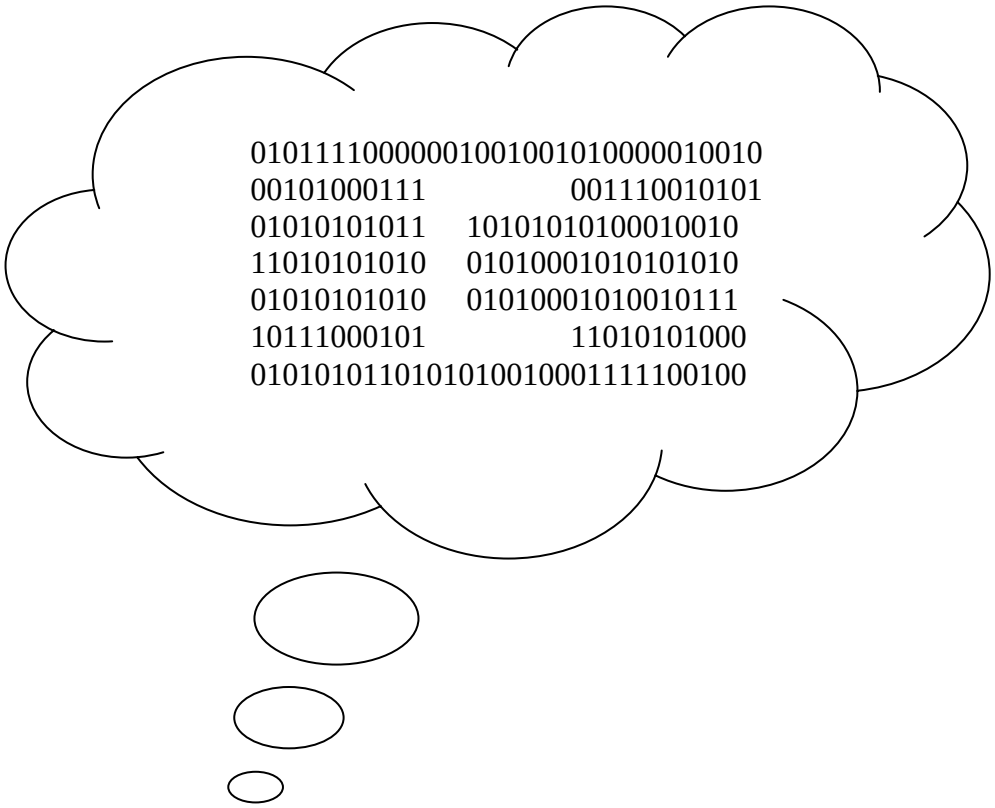
Macht en de cloud

De implicaties van de cloudtechnologie voor Deleuze's 'society of control'



Chantal van Elden

3837572

Marianne van den Boomen en Rick Dolphijn

Eindwerkstuk BA Communicatie- en Informatiewetenschappen

Jaar 4, blok 1

27 november 2014

Abstract

In deze scriptie heb ik onderzoek gedaan naar de staat van Deleuze's 'society of control' in het tijdperk van de cloud. In zijn naar de verbeelding sprekende tekst 'Postscript on the societies of control' (de Engelse vertaling van het origineel Franse 'Post-scriptum sur les sociétés de controle') beschrijft Deleuze de toestand van de westerse samenleving aan het einde van de 20ste eeuw, die hij de 'society of control' noemt, wat ik vertaald heb naar de 'controlemaatschappij' (deze vertaling zal verantwoord worden in hoofdstuk 0). In deze samenleving is de mens constant onderhevig aan toezicht en sturing, door middel van verschillende controlemechanismen. Zijn de controlemechanismen die Deleuze in 1992 signaleerde terug te zien de huidige maatschappij? Kan onze samenleving een volwaardige Deleuziaanse controlemaatschappij genoemd worden? Aan de hand van een objectanalyse van de cloudtechnologie – een technologie die een zeer belangrijke rol speelt in de moderne computertechnologie en derhalve zeer karakteristiek is voor onze huidige maatschappij, waarin informatie, diensten en digitaliteit centraal staan – heb ik getracht deze vragen te beantwoorden. Uit mijn analyse is gebleken dat de kenmerken van de cloudtechnologie zowel mogelijkheden bieden tot toezicht en sturing als mogelijkheden om deze uitoefeningen van macht te ondermijnen. De cloudtechnologie maakt het mogelijk om op grote schaal uiteenlopende voordelige en gebruiksvriendelijke computerdiensten aan te bieden. Cloudeigenaren en andere aanbieders van clouddiensten krijgen door de *input* van gebruikers enorme hoeveelheden informatie in handen – volgens Deleuze een belangrijke bron van macht. Daarnaast hebben cloudeigenaren ook vele mogelijkheden tot toezicht op individuen, en grote cloudeigenaren als Amazon hebben invloed op de markt – twee andere Deleuziaanse controlemechanismen. De kenmerken van de cloudtechnologie bieden tegelijkertijd ook mogelijkheden voor verzet tegen deze verschillende mechanismen. Dit verzet komt voornamelijk in de vorm van hackers, die zowel een gevaar vormen voor de systemen van de controlemaatschappij als voor de gebruikers van clouddiensten en andere internetdiensten. De machthebbers in de controlemaatschappij en de krachten van verzet werken met dezelfde digitale wapens. Complexe vormen van toezicht en sturing brengen even complexe vormen van verzet met zich mee, wat ertoe leidt dat de controlemaatschappij in het tijdperk van de cloud niet als een systeem van onbeperkt toezicht en constante sturing gezien kan worden. De analyse van de cloud legt een maatschappij bloot waarin de controlemechanismen die Deleuze beschrijft zeker aanwezig zijn, maar waarin ook al veel verzet plaatsvindt. De aard van dit verzet en de kenmerken van de instrumenten waarmee toezicht en sturing wordt uitgeoefend in het tijdperk van de cloud, hebben ertoe geleid dat de controlemaatschappij zich niet geheel ontwikkeld heeft zoals Deleuze voorzag.

Inhoudsopgave

“The coils of a serpent are even more complex than the burrows of a molehill.”
- Gilles Deleuze

“While it remains uncertain whether history has a purpose, it seems clear that development has a direction: things tend to move from lesser to greater complexity.”
- Mark C. Taylor

Macht en de cloud

De implicaties van de cloudtechnologie voor Deleuze’s ‘society of control’

0. Een verschuiving van systemen

Tweeëntwintig jaar geleden schreef de Franse filosoof Deleuze zijn ‘Postscript on the societies of control’, waarin hij het aanbreken van een nieuw soort samenleving inluidt, namelijk de ‘society of control’. In zijn tekst stelt Deleuze dat de systemen van de ‘society of control’ langzaam maar zeker de systemen van de ‘disciplinary society’ vervangen, zoals Foucault deze in het begin van de 20ste eeuw duidde en analyseerde (Deleuze 1992, 3). Deleuze vergelijkt de ‘disciplinary society’ met het gangenstelsel dat een mol bouwt: een keten van losse kamers die door donkere, nauwe gangen met elkaar verbonden zijn (ibid., 5). In de westerse wereld bewoog men zich in de ‘disciplinary society’ als in een door een mol geconstrueerde omgeving: van de ene door een gevestigd instituut gecontroleerde ruimte naar de volgende (van de familie naar de school en van de school naar de fabriek), door de duisternis vrijwel blind voor wat er in andere kamers gebeurt. In de ‘society of control’ – waarvan Deleuze het ontstaan beschrijft en de opkomst voorspelt – wordt de omgeving niet vormgegeven door een mol maar door een slang: een dier dat geen ruimtes bouwt maar over de vlakte kronkelt. De macht die in deze samenleving op de burger wordt uitgeoefend is net zo complex en flexibel als de bewegingen van een slang. Men leeft in een samenleving waarin geen op zichzelf staande instituten met eigen wetten en normen meer bestaan; een samenleving waarin groepen mensen

een verzameling codes zijn, transparantie centraal staat, marktwerking het voornaamste instrument van invloed op sociale systemen is, netwerken dichter en wijder verspreid zijn dan ooit, en toezicht en sturing altijd aanwezig zijn, zichtbaar en onzichtbaar (ibid., 4-6). In de 'society of control' kun je ook niet meer spreken van een individu – een term die volgens Deleuze staat voor een ondeelbare, enkelvoudige identiteit. Volgens Deleuze kun je enkel nog spreken van een 'dividual'; een deelbare identiteit die niet, zoals het individu, het taalkundige tegengestelde is van een massa of, in de praktijk van de disciplinesamenleving, een ongefragmenteerd onderdeel ervan, maar een identiteit waarvan de verschillende fragmenten onderdeel zijn van een veelvoud aan massa's, zoals datagroepen en doelgroepen (ibid., 5). Wie precies de macht heeft in deze samenleving van slangen en dividuen is niet specifiek van belang voor Deleuze. Hij stelt dat "there is no need to ask which is the toughest or most tolerable regime, for it's within each of them that liberating and enslaving forces confront one another" (ibid., 4). Het gaat Deleuze dus puur om een verschuiving van systemen, waarbij het ene systeem niet beter of slechter is dan het andere.

Bij het lezen van Deleuze's 'Postscript' kun je je afvragen: hoe staat het nu, meer dan twee decennia later, met de 'society of control'? Zijn de voorspellingen van Deleuze uitgekomen? Of hebben de veranderingen die hij signaleerde zich ontwikkeld op een manier die niet geheel past binnen de retoriek van 'Postscript on the societies of control'? Dit zijn vragen die centraal zullen staan in deze scriptie. Voor ik echter verder in kan gaan op deze vragen, de onderzoeksvragen die hieruit zullen volgen en de methode die ik zal gebruiken om deze onderzoeksvragen te beantwoorden, is het belangrijk om eerst dieper in te gaan op wat de 'society of control' precies inhoudt.

'Postscript' is een Engelse vertaling van een oorspronkelijk Franse tekst, waarin niet werd gesproken van 'the society of control' maar van 'la société de contrôle'. Letterlijk vertaald naar het Nederlands kan men spreken van 'de controlesamenleving', wat ook de vertaling is die ik vanaf nu in deze scriptie zal hanteren. Deze vertaling behoeft echter wel verdere uitleg, aangezien de term 'controle' in verschillende talen verschillende betekenissen heeft, en dus op verschillende manieren geïnterpreteerd kan worden. Het Franse 'contrôle' kan voor een inspectie of een test staan, maar ook voor het houden van toezicht of het hebben

van beheersing over iets (*Mijn woordenboek*). In het Engels daarentegen draait controle bijna altijd om beheersing: het hebben van een dominante invloed (*The free dictionary*). In het Nederlands staat de term net als in het Frans meestal voor het houden van een inspectie, maar iets 'onder controle hebben' betekent ook dat je de situatie in de hand hebt (*Encyclo*). Al deze verschillende definities geven nog geen echt houvast voor wat 'controle' precies betekent in de context van Deleuze's werk. Deleuze's concepten kunnen het best benaderd worden vanuit de tekst zelf; de specifieke betekenis van de termen die Deleuze gebruikt wordt duidelijk door de manier waarop hij deze termen inzet (Kleinherenbrink 2011, 6).

Deleuze beschrijft de 'society of control' als een "force" die opereert volgens verschillende "control mechanisms" (4). Deze mechanismen vormen samen een systeem van macht dat Deleuze voornamelijk beschrijft in abstracte termen als "ultra-rapid", "free-floating", "inseparable variations" en "a self-deforming cast" (Deleuze 1992, 4). Toch zijn er in de tekst ook drie concrete controlemechanismen te ontdekken: de werking van de markt, beheersing van de toegang tot informatie en de mogelijkheid om de positie van ieder element op elk moment op te vragen (ibid., 5-7). Het systeem van de controlemaatschappij draait dus zowel om sturing als om toezicht – twee uitoefeningen van macht. Controlemechanismen reguleren (bijvoorbeeld door marktwerking), geven dominante invloed over bepaalde middelen (zoals informatie en de toegang daartoe) en bieden mogelijkheden tot toezicht. Wanneer ik spreek over de controlemaatschappij, spreek ik dus niet enkel over een maatschappij van continu en onbeperkt toezicht, maar over een volledige 'société de contrôle', waarin de verschillende controlemechanismen in de maatschappij zowel sturing geven aan individuen als inzicht bieden in hun doen en laten.

1. De controlemaatschappij in het tijdperk van de cloud

Dit onderzoek zal zich richten op de staat van de controlemaatschappij in de huidige westerse samenleving. In het recente academische discours wordt vaak de term 'netwerksamenleving' gebruikt om naar de huidige samenleving te verwijzen. Een wetenschapper die grote invloed heeft gehad op de ontwikkeling van deze term is de

Spaanse socioloog Castells.[1] Volgens Castells is de netwerksamenleving een sociale structuur die het resultaat is van de interactie tussen een nieuw technologisch paradigma – dat van communicatie- en informatietechnologieën – en nieuwe manieren van sociale organisatie die gebaseerd zijn op netwerken. Macht, rijkdom en kennis is in deze samenleving sterk afhankelijk van de mogelijkheid om gebruik te kunnen maken van netwerktechnologieën (Castells 2005, 3).

Niet alleen het wetenschappelijke discours over de samenleving, maar ook de technologie in de samenleving heeft zich sinds 1992 verder ontwikkeld. Deleuze wees in zijn essay de computer aan als de meest karakteristieke en invloedrijke technologie in de controlesamenleving (Deleuze 1992, 6). Dit geldt zonder twijfel ook nu nog steeds, maar net zoals de bewegingen van een slang complexer zijn dan die van een mol, zijn ook de computertechnologieën van nu complexer dan die in de jaren ’90. Misschien wel de meest veelzeggende ontwikkeling binnen de computertechnologie is de opkomst van de *cloud*: een verzamelnaam voor datacentra waarmee via het internet contact gemaakt kan worden. Cloudconstructies worden steeds meer toegepast en moeten honderdduizenden servers verbinden. Het netwerkbedrijf Cisco Systems voorspelt dat in 2017 tweederde van al het dataverkeer vanuit de cloud plaats zal vinden en dat 76 procent van dit verkeer plaats zal vinden tussen technologische apparaten die een onderdeel zijn van een clouddatacentum (Lee 2014, 5). Opslagruimte in de cloud en toegang tot data die in de cloud opgeslagen liggen wordt aangeboden door bedrijven als Amazon (Amazon Web Services) en Microsoft (Azure). Deze bedrijven houden de cloud in stand (of beter gezegd: hun eigen cloud) en hebben macht over alle data die in de eigen cloud besloten liggen – ze kunnen deze data zowel inzien als verplaatsen en manipuleren.

De diensten die deze cloudeigenaren aanbieden hebben zowel voor andere bedrijven als voor consumenten vele praktische voordelen. Bedrijven kunnen in plaats van een eigen dure ICT-infrastructuur aan te schaffen en te onderhouden van de cloud gebruikmaken, en consumenten kunnen dankzij *streaming* diensten als Spotify en Netflix toegang krijgen tot talloze muziek- en videobestanden die zich in de cloud bevinden. Daarnaast kunnen consumenten ook eigen bestanden in de cloud opslaan via diensten als Google+, Dropbox en iCloud. Door informatie niet op een

[1] Overigens is Castells niet de eerste die de term ‘netwerksamenleving’ gebruikte; de term is in de academische wereld geïntroduceerd door Jan van Dijk in zijn boek *De netwerkmaatschappij* (1991).

eigen harde schijf of datacentrum op te slaan, geven gebruikers de macht over hun data uit handen. Dit is niet geheel zonder risico's, zoals de gehypete 'celebrity nude hack' in augustus 2014 liet zien. Hoewel het niet zeker is hoe de naaktfoto's van de beroemdheden precies zijn gelekt, heeft een hacker geclaimd de foto's uit Apple's iCloud gestolen te hebben (Coevert 2014). Het gebruik van clouddiensten zorgt dus voor een afname in macht over de eigen bestanden en gegevens voor gebruikers en een toename in macht over de data van gebruikers voor aanbieders van clouddiensten.

Aan de metafoor van een mol die gangenstelsels bouwt en een ingewikkeld kronkelende slang is een nieuwe metafoor toegevoegd, namelijk een enorme, dynamische wolk die boven de wereld zweeft. Wat kan deze wolk ons vertellen over de staat van de controlemaatschappij? Is de cloud een symptoom van de controlesamenleving, een instrument van macht dat past binnen het systeem dat Deleuze beschrijft? Of is de cloud een symptoom van een ander systeem: iets dat te groot, complex en ongrijpbaar is om te passen in een systeem van onbeperkt toezicht en constante sturing? In deze scriptie zal ik hier duidelijkheid in trachten te scheppen door te analyseren hoe het fenomeen van de cloud in verhouding staat tot de kenmerken van de 'society of control'. Op welke manieren biedt de cloud mogelijkheden tot toezicht en sturing? Zijn er ook manieren waarop het fenomeen afwijkt van het machtssysteem dat Deleuze beschrijft? Wat is de verhouding tussen de controlesamenleving en de netwerksamenleving in het tijdperk van de cloud? En is er nog verzet mogelijk?

Om deze vragen te beantwoorden zal ik een objectanalyse van de cloud uitvoeren. Dit roept al meteen een belangrijke vraag op – is de cloud wel een object? Zoals al eerder gezegd is de term 'cloud' een verzamelnaam voor een diversiteit aan datacentra waarmee via het internet contact gemaakt kan worden. In plaats van 'de cloud' is het dus correcter om te spreken van 'de cloudtechnologie' (de objecten en processen die een cloud tot gevolg hebben) of gewoon van een enkele cloud: een enkel datacentrum. Een cloud kan één gecentraliseerd, fysiek systeem van servers zijn maar ook een systeem dat bestaat uit meerdere autonome servers, die zowel fysiek als virtueel kunnen zijn (Hwang 2012, 7). De cloud is op geen enkele manier een eenduidig, enkelvoudig object; als fenomeen is het zowel fysiek als discursief, en als technologie is het zowel materieel als virtueel – er komt zowel hardware als

data aan te pas.[2] In deze scriptie zal ik dan ook onderscheid maken tussen de cloudtechnologie, een cloud en 'de cloud', waarbij ik een cloud zal beschouwen als een dienst die verleend wordt door cloudeigenaren; de cloudtechnologie als de hardware en computerprocessen die clouddiensten mogelijk maken; en 'de cloud' als een sociaal-cultureel fenomeen dat bestaat uit een interactie tussen de cloudtechnologie, de manier waarop mensen omgaan met deze technologie en de daarbij behorende diensten, en het discours. Het object dat ik ga analyseren is dan ook niet één object – ik zal zowel de cloudtechnologie analyseren als de verschillende clouddiensten die de technologie mogelijk maakt.

Volgens de Franse socioloog en filosoof Latour gaat technologie over een proces van verkenning van het 'zijn' te midden van alle andere dingen in de wereld (Latour en Venn 2002, 248). Een technologie zoals de cloud is niet slechts een gebruiksvoorwerp en staat ook niet op zichzelf; als ware het een levend wezen heeft het subjectieve relaties met de rest van de wereld en schenkt het gebruikers talloze bekende en onbekende mogelijkheden (ibid., 250).[3] De subjectiviteit en complexiteit van technologieën maakt dat we een technologie nooit helemaal onder controle kunnen hebben. Dit betekent dat we problemen met technologieën kunnen hebben, dat ons huidige gebruik van een technologie altijd in meer of mindere mate is afgedwaald van de oorspronkelijke intentie waarmee een technologie gecreëerd is en dat de manier waarop een technologie gebruikt kan worden invloed heeft op onze gebruiksintenties (ibid., 250-252). De manier waarop technologieën ons gebruik ervan beïnvloeden kan begrepen worden door middel van het concept *affordance*: de eigenschappen van een object die bepalen hoe het gebruikt kan worden (Norman in: Schaefer 2011, 19). Affordances zijn niet altijd zichtbaar; het zijn mogelijkheden voor handelingsrelaties tussen mensen en objecten, die soms wel en soms niet duidelijk aanwezig zijn (Norman 1999, 40). Bij een analyse van de affordances van objecten gaat het zowel om de fundamentele materiële aspecten van een object als

[2] Ik hanteer hier een Foucaultiaanse definitie van discours, namelijk een waarbij de term discours staat voor de betekenissen die gehecht worden aan dingen, die zowel geuit als geconstitueerd worden door middel van taal en de sociale realiteit zowel reflecteren als creëren. Doordat het discours het collectieve en persoonlijke bewustzijn beïnvloedt, en dus ook de discursieve en niet-discursieve acties van mensen, is de mogelijkheid om discours te kunnen beïnvloeden een vorm van macht (Jørgensen en Philips 2002, 12-13; Jäger en Maier 2009, 39).

[3] Dit betekent niet dat technologie een bewustzijn heeft maar dat het, net als een menselijk subject, niet enkel en alleen een passief object is. Een technologie heeft vanuit zichzelf een zekere invloed op de wereld.

de (doelbewuste) gevolgen van een menselijk ontwerp (Schaefer 2011, 19). In het kader van de cloud betekent dit dat het gebruik ervan zowel bepaald wordt door de kenmerken van de cloudtechnologie als door de manier waarop clouddiensten ingericht worden. Deze inrichting, het ontwerp van de dienst, heeft bepaalde affordances, ofwel bepaalde gebruikspotentiëlen, die voor de gebruiker wel of niet duidelijk zichtbaar kunnen zijn.

In deze scriptie zal ik de affordances van de cloudtechnologie en de daaruit voortvloeiende diensten analyseren. Ik zal allereerst kort de geschiedenis van de cloud doorlichten door te onderzoeken welke belangrijke menselijke en niet-menselijke invloeden de cloudtechnologie zoals wij deze nu kennen gevormd hebben. In het daaropvolgende hoofdstuk zal ik de affordances van de cloudtechnologie analyseren. In de eerste paragraaf van dit hoofdstuk zal ik de voornaamste fundamentele kenmerken van de cloudtechnologie in kaart brengen met behulp van bronnen uit de computerwetenschap. Vervolgens zal ik trachten te achterhalen hoe mensen de cloudtechnologie gebruiken, ofwel welke diensten er aangeboden worden en wat gebruikers wel en niet met deze diensten kunnen doen, door wetenschappelijke publicaties en de websites van aanbieders van clouddiensten te analyseren. Hierbij zal ik aandacht besteden aan de manier waarop de macht over de technologie verdeeld is. Tot slot zal ik de onderzoeksresultaten gebruiken om de cloud als technologie en sociaal-cultureel fenomeen te plaatsen in het kader van de netwerksamenleving en de controlesamenleving en uitspraken te kunnen doen over de implicaties van de cloud voor Deleuze's voorspellingen.

2. De geschiedenis van de cloudtechnologie

Technologieën hebben een geschiedenis die gevormd wordt door zowel de mogelijkheden van andere technologieën als mensen en hun acties en narratieven. De cloud is onderdeel van een geschiedenis waarin technologieën door de tijd heen steeds complexer, intelligenter en geavanceerder zijn geworden. De cloud is geen revolutionaire nieuwe fundamentele technologie zoals de *personal computer* (PC) of het *world wide web*, maar een gebruiksvriendelijke, efficiënte en voordelige toepassing van bestaande technologieën (Srinivasan 2014, 1).

Een computertechnologie die een voorwaarde is geweest voor de ontwikkeling van *cloud computing* (de computerprocessen die de cloudtechnologie vormen) is de *virtual machine* (in het Nederlands: virtuele machine): een computerprogramma dat computerhardware nabootst. Dankzij virtuele machines (die al sinds de jaren '60 bestaan) kunnen meerdere virtuele *servers* in één fysieke server ondergebracht worden, waardoor er meer opslagruimte beschikbaar is en meerdere applicaties onafhankelijk van elkaar in werking kunnen zijn, en ook probleemloos van de ene naar de andere server verplaatst kunnen worden (Hill et al. 2013, 70-72).[4] Virtuele machines zorgen er ook voor dat fysieke servers efficiënter gebruikt worden. Over het algemeen gebruiken servers slechts rond de 15 procent van hun totale capaciteit; met virtuele machines kan dit percentage veel hoger worden (ibid., 72). Virtuele machines zijn een cruciaal onderdeel van de cloudtechnologie omdat ze de mogelijkheid bieden van een externe infrastructuur die via het internet bereikt kan worden en krachtig genoeg is om duizenden gebruikers te kunnen hebben (Srinivasan 2014, 2).

Een andere belangrijke voorwaarde voor de ontwikkeling van cloud computing was de *low latency* van computertechnologieën: de beschikbaarheid van hogere bandbreedte (de hoeveelheid data die over een verbinding kan worden vervoerd), waardoor de reactietijd voor applicaties die op een ver verwijderde server draaien steeds lager kon worden (ibid., 2). Dankzij de toegenomen communicatiesnelheid van computers en de wijdverspreide beschikbaarheid van het internet konden computerprocessen steeds meer naar het internet verplaatst worden.

De ontwikkeling van de cloudtechnologie en de totstandkoming van het concept van 'de cloud' zoals we dit nu kennen is een proces waarbij vele actoren een rol gespeeld hebben, onder wie het bedrijf Amazon en Eric Schmidt, oud-CEO van Google. Amazon heeft enorme investeringen gedaan in het ontwikkelen van een gedecentraliseerde infrastructuur die computertaken van gebruikers over kan nemen en via het internet bereikt kan worden – een dienst waaraan zowel bedrijven als consumenten behoefte zouden hebben en die dus zeer winstgevend zou kunnen zijn (ibid., 2). Zo heeft het bedrijf grote invloed gehad op de technische ontwikkeling

[4] Een server is een computerprogramma dat kan corresponderen met *clients* (een programma dat toegang krijgt tot een dienst die mogelijk wordt gemaakt door een server). Zowel servers als clients bevinden zich op een computer. Met het woord 'server' wordt ook vaak bepaalde hardware bedoeld die het mogelijk maakt om softwareapplicaties beschikbaar te stellen.

van de cloud en de verschillende toepassingen van de technologie. Tegenwoordig is Amazon de grootste aanbieder van clouddiensten, en wel zo groot dat als de cloud van Amazon Web Services een computer was, deze vijf keer de capaciteit zou hebben van de veertien grootste concurrenten samen (Mims 2014).

Waar Amazon een grote rol gespeeld heeft bij de ontwikkeling van de cloudtechnologie, heeft Eric Schmidt een belangrijke rol gespeeld bij de popularisatie van de term ‘cloud’ toen hij tijdens de Search Engine Strategies Conference van 2006 het volgende over de cloudtechnologie zei:

> What's interesting [now] is that there is an emergent new model (…). I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it cloud computing – they should be in a ‘cloud’ somewhere. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – you can get access to the ‘cloud’ (Google Press Center 2014).

Schmidt typeert de cloud hier als een computermodel dat het mogelijk maakt om altijd en overal toegang te krijgen tot bepaalde data en diensten. Met zijn speech bracht Schmidt de mogelijkheden van de nieuwe opkomende technologie en de term waarmee deze technologie getypeerd kon worden onder de aandacht van de media en de informatie-industrie. De speech werd niet lang daarna gevolgd door de lancering van de eerste echte grote commerciële clouddienst: Amazons Elastic Compute Cloud, waarbij kleine bedrijven en consumenten een virtuele computer konden huren (Srinivasan 2014, 4).

Inmiddels is de cloudtechnologie geen opkomende technologie meer maar de belangrijkste technologische troef om de razendsnel groeiende vraag naar computerdiensten te kunnen opvangen (ibid., 14). De verwachting is dat in 2015 meer dan 2,5 miljard mensen met meer dan 10 miljoen verschillende apparaten toegang zullen hebben tot het internet, en dus ook tot de vele clouddiensten die via dit internet te bereiken zijn (ibid., 14). Om aan de verzoeken van al deze gebruikers te kunnen voldoen worden *resources* (fysieke en virtuele componenten zoals

documenten, netwerkaansluitingen, softwareapplicaties en geheugen, in het Nederlands: bronnen) in toenemende mate via het internet gedeeld (Hwang 2012, 5-6). Cloud computing is slechts een van de vele manieren om dit te doen – er bestaan ook andere netwerktechnologieën die het mogelijk maken om bronnen via het internet te delen, zoals *grid computing* en *peer-to-peer* (P2P) *computing* –, maar het is verreweg de meest succesvolle oplossing door de flexibiliteit van de virtuele servers waarvan cloud computing gebruik maakt en de servicegerichtheid van de technologie, waarbij gebruiksgemak en het beantwoorden van de verzoeken van gebruikers centraal staat.[5] [6]

Flexibiliteit en servicegerichtheid zijn slechts twee voorbeelden van de vele kenmerken van de cloudtechnologie. In het volgende hoofdstuk zal ik deze en andere kenmerken analyseren, alsmede de manier waarop mensen omgaan met de technologie.

3. De affordances van de cloudtechnologie

In dit hoofdstuk zal ik de affordances van de cloudtechnologie analyseren. Ik zal beginnen bij de belangrijkste fundamentele kenmerken van de technologie die ons gebruik ervan beïnvloeden. Vervolgens zal ik analyseren hoe mensen omgaan met de technologie, door te onderzoeken welke verschillende typen clouddiensten er aangeboden worden en welke beperkingen en mogelijkheden er aan de inrichting van deze diensten verbonden zijn.

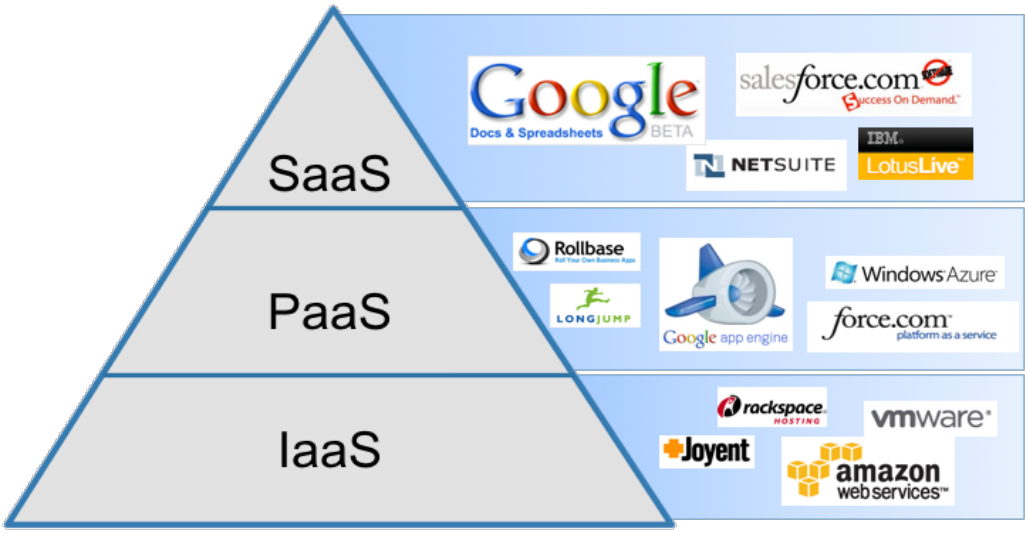
[5] Grid computing gaat om het verbinden en coördineren van meerdere (krachtige) servers in een zogenaamde *grid* om bronnen te kunnen delen voor een bepaald doel. PC's kunnen gebruikt worden om via het internet toegang te krijgen tot de grid. Binnen een grid kunnen complexe problemen heel snel worden opgelost. Nadelen van gridconstructies zijn de beperkte controle over alle hardware en het feit dat alle servers dezelfde software dienen te hebben (Kahanwal en Singh 2012, 185-186; Hill et al. 2013, 6-7; Hwang 2012, 30-31). Cloud computing en grid computing staan niet geheel los van elkaar – grid computing bestaat al langer dan cloud computing en heeft zo de cloudtechnologie beïnvloedt. Ook wordt de grens tussen cloud- en gridsystemen steeds minder scherp – de verschillende processen achter de technologieën kunnen gecombineerd worden (Villegas et al. 2010, 183; Hwang 2012, 40).

[6] P2P-constructies worden vooral gebruikt voor het delen van bestanden. Binnen een P2P-netwerk functioneert elke *node* (elk component van het netwerk) zowel als server als client; elke computer deelt en ontvangt bronnen. Binnen het netwerk is elk component gelijkwaardig en kan iedereen op elk moment besluiten het netwerk te verlaten. Een groot nadeel van P2P-constructies is de problematische complexiteit die het gevolg kan zijn van de verscheidenheid aan hard- en software van de verschillende componenten in het netwerk. Een ander probleem is het gebrek aan vertrouwen tussen de verschillende eigenaren van componenten (Kahanwal en Singh 2012, 184; Hwang 2012, 33-34). Ook P2P-constructies kunnen worden gecombineerd met cloud computing.

3.1 Fundamentele kenmerken

De term ‘cloud’ roept het beeld op van een virtuele wolk van informatie, iets dat ongrijpbaar, onmetelijk en in essentie volledig immaterieel is. Dit is echter slechts een gedeelte van de werkelijkheid – de hardware die nodig zijn om een cloud te creëren en in stand te houden zijn verre van immaterieel. Om een grote cloud in stand te houden zijn vaak wel duizenden fysieke servers nodig, die worden verzameld in enorme, dure industriële complexen die op grote stukken goedkope grond gebouwd worden (Hwang 2012, 25; Reading 2014, 7). Deze complexen worden ook wel *server farms* genoemd. Grote cloudeigenaren bezitten verschillende server farms, verspreid over allerlei landen. Deze verspreiding van servercomplexen is nodig vanwege de regelgeving van staten omtrent dataopslag, die stelt dat bepaalde soorten data de regio niet mogen verlaten (Srinivasan 2014, 84). Server farms kosten grote hoeveelheden materialen, energie, water, ruimte en onderhoud. Zo verbruikten server farms in 2009 al meer dan 1,5 procent van de totale hoeveelheid elektriciteit in de Verenigde Staten (Gandhi et al. 2009, 1). De wereldwijde uitgaven aan het draaiende houden van deze servers liggen naar schatting rond de 30 miljard dollar – een bedrag dat alleen maar zal stijgen (ibid., 1). Achter het ogenschijnlijk volledig virtuele fenomeen van de cloud ligt dus een uitgebreid materieel systeem dat veel onderhoud vergt en op verschillende niveaus invloed heeft op de omgeving, van de ruimte die het complex inneemt in een landschap tot de negatieve milieueffecten van de opwekking van de elektriciteit die de hardware verbruikt, en waaruit politieke, economische en sociale spanningen ontstaan (Reading 2014, 2).

Hoewel de cloudtechnologie afhankelijk is van fysieke materialen en processen, is cloud computing op zich een puur virtueel proces. De virtuele dimensie van de cloudtechnologie kan begrepen worden als de digitale structuur die het resultaat is van de processen die in en tussen de verschillende servers en de computers van gebruikers plaatsvinden. Deze structuur is op verschillende manieren schematisch te visualiseren, waarbij de details van het schema afhangen van de context waarin de technologie gebruikt wordt (Dihn et al. 2013, 1589). De meest voorkomende manier om cloud computing te visualiseren is de *layered architecture* (ibid., 1589) (zie afbeelding 1). Dit model onderscheidt drie ‘lagen’, drie types van



Afbeelding 1: Schematische visualisatie van de 'layered architecture'. Gevonden op: http://filiph.net/slides/idf-cloud/src/iaas-paas-saas.png

cloud computing, namelijk *infrastructure as a service* (IaaS), *platform as a service* (PaaS) en *software as a service* (SaaS). De eerste laag, IaaS, zijn de processen die het mogelijk maken om de infrastructuur van een cloud (opslagruimte, servers en netwerkonderdelen) aan te bieden aan derden. Het tweede type cloud computing, PaaS, gaat om het aanbieden van een omgeving voor het ontwikkelen, testen en in gebruik nemen van een applicatie (een computerprogramma). De derde laag, SaaS, zijn de processen die het mogelijk maken om gebruikers een softwareapplicatie aan te bieden (ibid., 1589-1590). Het is niet zo dat de drie lagen altijd in deze specifieke volgorde bovenop elkaar 'gebouwd' moeten worden; een softwareapplicatie kan direct aan een infrastructuur gekoppeld worden, zonder ook maar iets te maken te hebben met de PaaS-laag. Het is ook niet zo dat een clouddienst altijd maar van één proces gebruikt maakt; er bestaan diensten die gebruik maken van alle drie de verschillende cloud computing-processen en die dus van alle drie de lagen een onderdeel zijn (ibid., 1590).

De verschillende processen die samen de virtuele dimensie van de cloudtechnologie vormen, maken uiteenlopende diensten mogelijk. Al deze diensten worden gekenmerkt door een aantal basiseigenschappen, die als fundamentele kenmerken van de cloudtechnologie begrepen kunnen worden. De eerste eigenschap is *rapid elasticity*: de mogelijkheid om bronnen aan het netwerk te kunnen toevoegen en verwijderen, en vrijelijk bronnen binnen het netwerk te kunnen verplaatsen. Door de *elasticity* van de cloudtechnologie (in het Nederlands:

flexibiliteit) kan een cloud een toenemende of afnemende vraag naar een bepaalde bron opvangen, waardoor elke bron altijd voor iedere gebruiker beschikbaar is. Een cloud kan dus enorme hoeveelheden gebruikers tegelijkertijd hebben, ongeacht wat deze gebruikers precies willen doen (Fehling et al. 2014, 4-5). Naarmate het aantal gebruikers van een cloud stijgt, wordt de flexibiliteit van de cloud hoger. Hoe minder gebruikers een cloud heeft, hoe lastiger het dus wordt om aan de uiteenlopende en wisselende verzoeken van de verschillende gebruikers te voldoen (ibid., 60). Aanbieders van clouddiensten waarbij een hoge flexibiliteit wenselijk is, zullen omwille van de kwaliteit van de aangeboden dienst altijd zo veel mogelijk gebruikers willen hebben.

Twee andere fundamentele kenmerken van de cloudtechnologie zijn *on-demand self-service* (gebruikers kunnen diensten direct en op elk moment gebruiken) en *measured service* (data-uitwisseling kan transparant worden gemeten, waardoor een *pay-per-use model* mogelijk is waarbij je enkel betaalt voor wat je gebruikt) (Fehling et al. 2014, 3-4). Dit model is vooral van belang in de context van clouddiensten voor bedrijven, waarbij de ICT-structuur van een bedrijf als een dienst aangeboden kan worden. Dankzij de cloudtechnologie hoeven de ICT-kosten van bedrijven niet per se grote eenmalige investeringen te zijn, maar kunnen deze kosten ook relatief kleine dagelijkse uitgaven zijn die aan te passen zijn aan de specifieke en veranderlijke behoeften van een bedrijf (ibid., 4). Als het bedrijf groeit of krimpt, en bepaalde bronnen meer of juist minder nodig heeft, kan de ICT-structuur direct hieraan aangepast worden.

Een ander belangrijk kenmerk van de cloudtechnologie is afhankelijkheid van het internet. Het feit dat gebruikers enkel via het internet toegang tot een cloud kunnen krijgen, zorgt ervoor dat een goede internetverbinding een vereiste is om gebruik te kunnen maken van clouddiensten. Hieruit voortvloeiend is veiligheid geen inherent aspect van de cloudtechnologie. Het internet is voor iedereen met de juiste technologische middelen toegankelijk; dat datzelfde internet ook het toegangsmiddel tot een cloud is, maakt cloudomgevingen kwetsbaar voor cyberaanvallen (Hill et al. 2013, 26).

De fundamentele kenmerken van de cloudtechnologie passen in het paradigma van het zogenaamde *utility computing*. Deze term staat voor een computermodel waarbinnen bronnen als voorzieningen aan gebruikers aangeboden

worden (Kahanwal en Singh 2012, 185). In het utility computing-paradigma wordt het gebruiken van een computer (of beter gezegd: de bronnen waartoe mensen toegang krijgen door het gebruik van een computer) als een basisvoorziening beschouwd, zoals elektriciteit, gas en water. Het streven in dit paradigma is om bronnen steeds meer op basisvoorzieningen te laten lijken, waarbij de bronnen net als bijvoorbeeld kraanwater in principe nooit op raken of niet beschikbaar zijn, en de gebruiker nooit voor meer betaalt dan hij of zij ook daadwerkelijk gebruikt (Hill et al. 2013, 4). Cloud computing is een belangrijke stap geweest binnen dit paradigma omdat de technologie het mogelijk maakt om allerlei bronnen, van softwareapplicaties tot infrastructuur en opslagruimte, op ongekend grote schaal via het internet aan te bieden, waardoor taken die bedrijven en consumenten voorheen zelf uitvoerden, in diensten konden worden veranderd. Ook kennen deze diensten net als basisvoorzieningen een hoge betrouwbaarheid en bestaat er de mogelijk van een pay-per-use model.

De eigenschappen van de cloudtechnologie bieden mogelijkheden voor het ontwerpen en aanbieden van uiteenlopende diensten. De aanbieders van deze diensten kunnen cloudeigenaren zijn, maar ook bedrijven die gebruik maken van een cloud om een eigen dienst te lanceren. Cloudeigenaren bieden over het algemeen vier verschillende typen cloud aan: een privécloud, een openbare cloud, een *community* cloud en een hybride cloud. Deze verschillende typen onderscheiden zich van elkaar door het soort gebruiker dat toegang ertoe heeft en de mate waarin bronnen door de gebruikers gedeeld worden (Fehling et al. 2014, 60). Aan de verschillende typen cloud zijn uiteenlopende diensten gebonden. In de volgende paragraaf zal ik deze vier verschillende typen cloud analyseren en dieper ingaan op het ontwerp van een aantal concrete voorbeelden van clouddiensten.

3.2 Omgaan met clouddiensten: verschillende ontwerpen

Het eerste type cloud, de *private cloud* (in het Nederlands: privécloud), wordt voornamelijk gebruikt door grote bedrijven en instanties, die heel veel data hebben om te organiseren (Srinivasan 2014, 11). Gebruikers van een privécloud kennen een hoge mate van zeggenschap en verantwoordelijkheid over de infrastructuur van de cloud. Meestal is het zo dat de cloud onderdeel wordt van het eigen datacentrum van het bedrijf dat de cloud ‘huurt’, waardoor enkel de werknemers van het bedrijf

toegang hebben tot de cloud en het bedrijf zelf verantwoordelijk is voor zaken als beveiliging en organisatie. Het kan ook zo zijn dat het onderhoud van de privécloud wordt overgedragen aan een vertrouwde derde partij of de aanbieder van de clouddienst (ibid., 31). Een voorbeeld van een privécloud is de Rackspace Private Cloud, die wordt bestuurd met het softwareplatform OpenStack (een IaaS). Bij deze clouddienst kun je zelf kiezen waar de cloud zich bevindt, in een eigen datacentrum of in het centrum van Rackspace, en wordt het onderhoud door Rackspace geregeld. Rackspace promoot het systeem door de nadruk te leggen op de hoge mate van veiligheid en zeggenschap die een privécloud biedt, en het gemak en de efficiëntie die het verplaatsen van de ICT-infrastructuur van je bedrijf naar een cloud oplevert, waardoor bedrijven zich kunnen richten op hun “core-business”, ofwel hun kernactiviteiten (Rackspace 2014)

Het tweede type cloud, de *public cloud* (in het Nederlands: openbare cloud), is het meest populaire type cloud en wordt gedeeld door een veelvoud aan verschillende gebruikers (Srinivasan 2014, 29). De openbare cloud wordt gekenmerkt door een groot gebruiksgemak, waarbij de infrastructuur van de cloud en de beveiliging ervan de verantwoordelijkheid van de cloudeigenaar zijn (ibid., 30). Alle complexe taken worden hier dus van de gebruiker overgenomen. De meeste (gratis) softwareapplicaties waarvan consumenten gebruik maken zijn openbare clouddiensten, zoals bijvoorbeeld de opslagdienst Dropbox en e-maildiensten als Gmail en Hotmail. Naast consumenten gebruiken ook bedrijven de openbare cloud. Dit zijn vooral kleine en middelgrote bedrijven, omdat openbare clouddiensten goedkoper zijn dan privéclouddiensten en deze bedrijven over het algemeen minder kapitaalkrachtig zijn. Dankzij openbare clouddiensten kunnen kleine en middelgrote bedrijven op een voordelige manier toegang krijgen tot geavanceerde hard- en software waartoe ze zonder de cloudtechnologie geen toegang zouden hebben, omdat ze niet de kennis of middelen hebben om deze zelf aan te schaffen en te onderhouden of deze zelf te ontwikkelen (Marston et al. 2010, 182; Srinivasan 2014, 101-102). Ook grote bedrijven maken soms gebruik van diensten in een openbare cloud, bijvoorbeeld om back-ups van niet-gevoelige data te maken (Srinivasan 2014, 30).

Het derde type cloud dat door cloudeigenaren aangeboden wordt, de *community cloud*, is een openbare cloud die enkel toegankelijk is voor een

specifieke groep mensen, zoals organisaties binnen een bepaalde bedrijfstak, en waarvan de infrastructuur ook in handen ligt deze groep (Srinivasan 2014, 2-3). Het grote voordeel van dit type cloud is dat de verschillende leden van de groep die de cloud deelt gespecialiseerde applicaties in de cloud kunnen laten draaien (ibid., 35). Het is bij dit type cloud belangrijk dat de verschillende leden van de cloudgemeenschap dezelfde diensten nodig hebben en gedeelde belangen hebben wat betreft zaken als beveiliging (ibid., 11). Een interessant voorbeeld van een community cloud is de AWS GovCloud (US) Region, een samenwerking tussen Amazon en de regering van de Verenigde Staten. Deze cloud is de eerste cloudomgeving die voldoet aan de veiligheidseisen van het Amerikaanse ministerie van Defensie. Met deze cloud zal zeer gevoelige informatie gedeeld worden tussen overheidsinstanties (Amazon 2014).

Het laatste type cloud, de *hybrid cloud* (in het Nederlands: hybride cloud), is een combinatie van twee verschillende typen cloud (privé, openbaar of *community*). Vaak wordt in een hybride cloudconstructie een privécloud door middel van IaaS-processen gekoppeld aan een openbare cloud om bepaalde diensten aan consumenten te kunnen aanbieden (Srinivasan 2014, 34). Hierdoor kunnen bedrijven zowel profiteren van de mate van inspraak en veiligheid die een eigen infrastructuur biedt als van de kenmerken van een openbare cloud, die een grote flexibiliteit en zeer groot aantal gebruikers mogelijk maken (ibid., 34). Een voorbeeld van een bedrijf dat gebruik maakt van een hybride cloud is Spotify – een bedrijf dat consumenten software aanbiedt om online muziek mee af te spelen. Spotify heeft deze digitale omgeving gebouwd met behulp van de openbare cloud van Amazon Web Services en Apache Cloudstack, een open-source software die een IaaS-omgeving biedt om grote netwerken van virtuele machines te beheren (Resare en Van Alteren 2014). Zo kan Spotify een openbare clouddienst aanbieden aan consumenten via een eigen infrastructuur.

De cloudtechnologie kan dus op vele manieren gebruikt worden. De diensten die cloudeigenaren aanbieden, lopen uiteen van een gratis softwareapplicatie voor consumenten tot het beheren van (zeer gevoelige) informatie voor organisaties en overheden of het aanbieden van een omgeving aan bedrijven voor het ontwikkelen van een eigen applicatie. Deze bedrijven kunnen op hun beurt een eigen clouddienst aan consumenten aanbieden. Hierdoor kan een keten van bedrijven ontstaan die

elkaars diensten gebruiken om omzet te genereren. Aan de basis van deze keten ligt altijd een cloudeigenaar: het bedrijf dat een bepaald type cloud aanbiedt. Aan het eind van de keten bevindt zich de eindgebruiker, die toegang krijgt tot een vastgelegd systeem waarin door middel van een *interface* (het bedieningspaneel van een technologie) bepaalde verzoeken gedaan kunnen worden. In de volgende paragraaf zal ik de beperkingen en mogelijkheden van het ontwerp van clouddiensten voor de gebruiker analyseren.

3.3 Omgaan met clouddiensten: beperkingen en mogelijkheden

Het gebruik van clouddiensten kent vele voordelen. Zowel consumenten als bedrijven krijgen toegang tot een digitale omgeving die hen mogelijkheden biedt die ze buiten deze omgeving niet zouden hebben. De mate van zeggenschap die gebruikers binnen en over deze omgeving hebben, is zeer variabel. Zo hebben gebruikers van een privécloud veel invloed op de inrichting van het systeem en bestaat er vaak een hoge mate van eigen verantwoordelijkheid voor de beveiliging van hun data. Gebruikers van openbare softwareapplicaties zoals een e-mailsysteem hebben daarentegen veel minder mogelijkheden. Deze gebruikers kunnen het systeem niet inzien of bewerken; ze kunnen enkel de interface gebruiken. De mogelijkheden voor de gebruiker staan vast, evenals het beveiligingssysteem van de dienst. De gebruikers hebben enkel invloed op het daadwerkelijke invoeren van informatie in het systeem en eventueel over het wachtwoord van hun account. De eigenaar van de applicatie beheert alle data die in het systeem ingevoerd worden.

Hoe er binnen het systeem van een clouddienst precies om wordt gegaan met de data van gebruikers, wordt gespecificeerd in de gebruiksvoorwaarden van de dienst. Zo wordt in de voorwaarden van Dropbox, een clouddienst voor het online opslaan van documenten en het delen van deze documenten met andere Dropboxgebruikers, gezegd dat Dropbox persoonsinformatie als (e-mail)adressen, naam en telefoonnummer opslaat, en ook informatie verzamelt over de apparaten die gebruikt worden om toegang te krijgen tot Dropbox, zoals IP-adressen en de webpagina die bezocht is voor de webpagina van Dropbox. Deze informatie wordt volgens Dropbox niet verkocht maar wel gedeeld met vertrouwde partners (bedrijven waar Dropbox mee samenwerkt), en bepaalde informatie zoals naam en email is zichtbaar voor andere gebruikers. Dropbox is ook niet aansprakelijk bij

“enig verlies van gebruik, gebruiksgegevens, verlies van opdrachten of klanten of winstderving, ongeacht het juridische vermoeden van aansprakelijkheid” (Dropbox 2014). In februari 2014 is er een nieuwe clausule aan de gebruiksvoorwaarden van Dropbox toegevoegd waarin arbitrage, rechtspraak buiten de rechter om, verplicht gesteld wordt. Hierdoor worden grote collectieve rechtszaken tegen Dropbox in de Verenigde Staten onmogelijk. In veel Europese landen is verplichte arbitrage verboden, maar het feit dat Dropbox een Amerikaans bedrijf is dat al haar datacentra in de Verenigde Staten gevestigd heeft, maakt de regelgeving gecompliceerd (Koenis 2014). Dropbox heeft dus vele gebruikersgegevens in handen en heeft ook het recht om van deze informatie gebruik te maken, zonder aansprakelijk te zijn voor zaken als beveiligingslekken.

Dit voorbeeld illustreert de machtspositie van aanbieders van clouddiensten. Aanbieders hebben inzicht in allerlei persoonsinformatie en kunnen door hun internationale aanwezigheid binnen de mazen van de wet opereren. Voor gebruikers is het lastig te achterhalen hoe aanbieders precies omgaan met de informatie waartoe ze toegang hebben. Dit wordt nog lastiger als de exacte locatie waarop clouddiensten worden opgeslagen en uitgevoerd, onbekend is. In zo’n geval is het vrijwel onmogelijk om erachter te komen aan welke veiligheidsnormen precies moeten worden voldaan (Ouedraogo 2013, 5).

Machtsmisbruik van aanbieders van clouddiensten is een reële mogelijkheid. Sommige aanbieders zijn misschien niet trouw aan hun beloftes over privacywaarborging en verkopen vertrouwelijke data door aan derden (Dong et al. 2013, 152). Cloud computing is niet voor niets sterk gerelateerd aan ‘big data’.[7] Cloud computing biedt grote mogelijkheden voor het verzamelen, opslaan en verwerken van big data door de omvang en flexibiliteit van de datacentra, en genereert tegelijkertijd big data door de gegevens die gebruikers in cloudsystemen invoeren. Dit maakt van clouddiensten zowel een belangrijke bron van big data als

[7] Big data zijn datasets die te groot zijn om te worden verzameld, opgeslagen en verwerkt door traditionele hard- en software (Chen et al. 2014, 2). Het verzamelen van big data en het ontleden van deze ongestructureerde massa data door middel van geavanceerde algoritmen gebeurt in toenemende mate (ibid., 85). Het doel hiervan is het achterhalen van waardevolle informatie, zoals bijvoorbeeld informatie over het internetgedrag en de interesses van individuen, die gebruikt kan worden om internetgebruikers bloot te stellen aan gepersonaliseerde reclame. De opkomst van internetdiensten, waaronder ook clouddiensten, heeft voor een grote toename van big data gezorgd. Zo wordt er elke minuut maar liefst 72 uur aan film op YoutTube gezet en verwerkt Google elke maand honderden petabytes aan data (ibid., 2).

een instrument om ermee om te gaan. Daarnaast versterken de mogelijkheden van cloud computing voor het omgaan met big data de behoefte van bedrijven aan clouddiensten, waardoor de twee fenomenen elkaar in de hand werken (Chen et al. 2014, 12).

Een andere manier waarop aanbieders van clouddiensten hun machtspositie kunnen misbruiken is door een cyberaanval op hun systeem te maskeren met als doel het beschermen van de eigen reputatie (Dong et al. 2013, 152). Cyberaanvallen kunnen het imago van een aanbieder flink beschadigen. Dit kan goed geïllustreerd worden door de mediaophef die volgde op de 'celebrity nude hack', waarbij privéfoto's van honderden Amerikaanse beroemdheden dankzij een of meerdere hackers uitlekten. De foto's verschenen voor het eerst op *AnonIB*, een anoniem forum voor het delen van (al dan niet gestolen) pornografische afbeeldingen – en dan vooral afbeeldingen van beroemdheden (Sargent 2014; Cook 2014). De foto's werden daarna geplaatst op sites als 4Chan en Reddit – enorme webfora die elke dag miljoenen bezoekers hebben – begeleid door de claim dat de foto's uit de iCloud gestolen waren (Evans 2014). De hack werd algauw opgepikt door de media en mondde uit in een groot schandaal waarbij de reputatie van Apple een deuk opliep, ondanks het feit dat Apple beweert dat er niet in het iCloud-systeem is ingebroken (Li 2014).

De relatie tussen de hack en Apple's iCloud leidde in de media niet alleen tot vragen over de beveiliging van de iCloud, maar ook over de veiligheid van clouddiensten in het algemeen (Hijink 2014; Davey 2014). De kwetsbaarheid van clouddiensten voor aanvallen van hackers wordt als het grootste probleem van cloud computing gezien, zowel door academici als door consumenten en bedrijven (Chen, Paxson en Katz 2010, 3). Zowel de cloudtechnologie op zich als het ontwerp van clouddiensten heeft verschillende kenmerken die het systeem gevoelig maken voor aanvallen. Zo biedt het feit dat bij openbare softwareapplicaties meerdere mensen gebruik maken van een en dezelfde softwareapplicatie mogelijkheden voor aanvallen van medegebruikers (Ouedraogo 2013, 6). Een ander voorbeeld van een aspect van de cloudtechnologie dat beveiligingsrisico's met zich meebrengt, is het feit dat een cloud datacentrum gebouwd is als een netwerk van virtuele servers. Hierdoor is het mogelijk om vijandelijke virtuele machines aan het netwerk toe te voegen (Chen, Paxson en Katz 2010, 4).

Soms draagt het ontwerp van de beveiliging van clouddiensten zelfs bij aan de onveiligheid. Zo kan de mogelijkheid voor bepaalde gebruikers om van dataversleutelingmechanismen en anonieme communicatiekanalen gebruik te maken werken als een dekmantel voor criminelen, waardoor aanvallen minder snel opgemerkt worden en de daders moeilijker te traceren zijn (Ouedraogo 2013, 4). Daarnaast zorgt de complexiteit van cloudconstructies ervoor dat de beveiliging van zo'n constructie evenredig complex is (ibid., 6). Conventionele technieken om aanvallen te identificeren en verhelpen zijn dan ook vaak niet toereikend in de context van een cloudsysteem (Zinnedinne 2014, 4). Zo bemoeilijkt bijvoorbeeld de plaatsing van virtuele machines in verschillende geografische regio's de opsporing van cybercriminelen (Ouedraogo 2013, 4).

Een voorbeeld van een aanval die vaak tegen cloudsystemen ingezet wordt is een *side channel attack*, waarbij een bepaalde server vanuit een nabijgelegen server geobserveerd wordt om bepaalde patronen in activiteit te ontdekken, die informatie onthullen over de data in de server (Zinnedinne 2014, 6). Andere aanvallen die effectief tegen een cloud ingezet kunnen worden zijn *denial of service attacks*, waarbij er zoveel verzoeken naar een systeem verstuurd worden dat het systeem niet meer in staat is om te functioneren, en *authentication attacks*, waarbij accounts gekraakt en misbruikt worden, bijvoorbeeld door wachtwoorden te achterhalen (ibid., 6). Dit kan op vele manieren gebeuren, bijvoorbeeld door een computercode die wachtwoorden raadt of een *man-in-the-middle-attack*, waarbij informatie tussen twee communicerende systemen onderschept wordt. Een aanval op specifieke accounts is waarschijnlijk ook de methode van de hacker(s) van de 'celebrity nude hack' geweest (Arthur 2014a; Butcher 2014).

Natuurlijk kunnen deze aanvallen niet alleen tegen cloudsystemen ingezet worden. Man-in-the-middle-attacks bijvoorbeeld kunnen op verschillende niveaus via allerlei verschillende netwerken plaatsvinden, zoals openbare Wi-Fi netwerken en e-mailsystemen (Saltzman en Sharabani 2009). Hoewel de aanvallen die op cloudsystemen uitgevoerd kunnen worden dus op zichzelf niet uniek zijn, kunnen de gevolgen van de zwakke plekken in cloudconstructies echter bijzonder verstrekkend zijn. De grote schaal waarop cloudconstructies gebruikt worden en de enorme hoeveelheden persoonlijke, en soms zelfs zeer gevoelige informatie die in clouds opgeslagen worden, maken dat cyberaanvallen op een cloudsysteem voor ernstige

gevolgen kunnen zorgen. De infrastructuur van een cloud kan hackers ook toegang geven tot zeer krachtige computerbronnen waarmee ze extra schadelijke aanvallen kunnen uitvoeren, en doordat elke fysieke server is verbonden aan een veelvoud aan virtuele servers kunnen deze aanvallen ook nog eens op zeer grote schaal uitgevoerd worden (Zinnedinne 2014, 4; Ouedraogo 2013, 4).

De manier waarop clouddiensten ingericht worden biedt dus verscheidene mogelijkheden tot misbruik van het systeem, zowel van binnenuit (door cloudeigenaren of kwaadwillende gebruikers) als van buitenaf (door hackers). Gebruikers van een openbare softwareapplicatie kunnen zich niet of nauwelijks verdedigen tegen dit misbruik. Ze kunnen enkel handelen binnen de kaders van het systeem dat ze gebruiken, waarbij ze alleen invloed hebben op zaken als het wachtwoord van hun account. Het systeem dat gebruikt wordt werkt ook niet altijd zoals verwacht. Op het moment dat een gebruiker via de interface van een softwareapplicatie een bepaald verzoek doet, bestaat er geen garantie dat dit verzoek ook daadwerkelijk volledig uitgevoerd wordt. Als een gebruiker een bepaald bestand verwijdert, kan het zijn dat dit nog ergens in een server opgeslagen ligt, volledig buiten bereik. Sommige gedupeerden van de ‘celebrity nude hack’ hebben geclaimd dat ze bepaalde foto’s allang verwijderd hadden (Arthur 2014b). Daarnaast kan ook het wisselen van aanbieder lastig zijn. De inrichting van de clouddiensten kent een groot gebrek aan standaarden – verschillende aanbieders van diensten maken vaak gebruik van verschillende systemen, waardoor de data van gebruikers ‘vast’ kunnen komen te zitten in een bepaald systeem met een bepaalde gegevensindeling en het moeilijk kan zijn om de informatie over te plaatsen naar een ander systeem (Marston et al. 2010, 182).

De voor de gebruiker vaak vlekkeloze ervaring van clouddiensten, die draait om een onmiddellijke beantwoording van verzoeken en het altijd en via zoveel mogelijk apparaten beschikbaar zijn van een dienst, kan zorgen voor een onterecht gevoel van zekerheid en veiligheid (Chen, Paxson en Katz 2010, 5). Het utility computing-paradigma, waarbij computerdiensten steeds meer op basisvoorzieningen gaan lijken, gaat gepaard met een abstractie van de computerdiensten waar mensen gebruik van maken. De gebruiker ziet enkel de interface waarin verzoeken gedaan kunnen worden en resultaten worden gepresenteerd, zonder inzicht te hebben in of kennis te hebben van de complexe systemen die tussen verzoek en resultaat liggen

en kwetsbaarder zijn dan ze lijken. Hierdoor kan de gebruiker blind zijn voor de verschillende mogelijkheden tot misbruik die de cloudtechnologie biedt.

De analyse van de affordances van de cloudtechnologie heeft laten zien dat de kenmerken van de cloudtechnologie en de daaruit voortvloeiende clouddiensten hoofdzakelijk draaien om het aanbieden van bronnen als diensten. Dit maakt dat de technologie zowel de gebruikers als de aanbieders van clouddiensten vele positieve mogelijkheden biedt. Gebruikers krijgen toegang tot gebruiksvriendelijke systemen waar ze vele voordelen uit kunnen halen, van het streamen van muziek tot het opslaan van enorme hoeveelheden bedrijfsgegevens. Aanbieders van clouddiensten kunnen op zeer grote schaal uiteenlopende diensten aanbieden, al dan niet tegen betaling. Aanbieders krijgen ook inzicht in allerlei (persoonlijke) informatie die ze kunnen gebruiken om wist te genereren, ter aanvulling aan of ter compensatie van een gebrek aan een pay-per-use model. Aanbieders krijgen een zekere macht in handen door de *input* van gebruikers; ze krijgen inzicht in het gedrag en de interesses van gebruikers en kunnen, door hun invloed op interface van de dienst, de gebruikers sturen. Ook kunnen ze misbruik maken van de gegevens van gebruikers, bijvoorbeeld door deze te verkopen. Tegelijkertijd biedt de cloudtechnologie en het ontwerp van clouddiensten mogelijkheden voor misbruik door derden. De systemen van clouddiensten zijn vaak kwetsbaar voor aanvallen van hackers (die ook zelf gebruikers kunnen zijn). Hackers hebben de mogelijkheid om in te breken in de systemen en inzicht te krijgen in allerlei data, die ze voor uiteenlopende doeleinden kunnen gebruiken. Wat betekenen al deze gevolgen van de affordances van de cloudtechnologie voor de staat van de controlemaatschappij?

4. De cloud en de maatschappij

In dit hoofdstuk zal ik onderzoeken wat de implicaties zijn van de resultaten van de objectanalyse van de cloud voor de ‘society of control’. In de eerste paragraaf zal ik kort onderzoeken hoe de netwerksamenleving, de controlesamenleving en de cloud met elkaar in verhouding staan. In de tweede paragraaf zal ik de mogelijkheden en beperkingen van de cloudtechnologie en de inrichting van clouddiensten plaatsen in de context van de controlesamenleving, waarbij ik specifiek aandacht zal besteden aan de drie meest concrete voorbeelden van controlemechanismen die Deleuze

beschrijft, namelijk de werking van de markt, beheersing van de toegang tot informatie en de mogelijkheid om de positie van ieder element op elk moment op te vragen

4.1 Netwerken en macht

In de netwerkmaatschappij is informatie overal om ons heen, vluchtig en verstrekkend als een wolk, en zorgen digitale technologieën zoals de cloud voor verbondenheid en bereikbaarheid. De netwerkmaatschappij is net als een cloudsysteem (en alle andere netwerktechnologieën) georganiseerd als een netwerk, waarbij het netwerkaspect begrepen kan worden als een vorm van sociale organisatie: het patroon van relaties tussen mensen. Deze vorm van sociale organisatie is zeker niet nieuw, maar kon dankzij digitale technologieën naar een ongekend niveau getild worden, met meer en wijder verspreide mogelijkheden tot netwerkvorming, organisatie en controle (Castells 2005, 4).

De cloud is als sociaal-cultureel fenomeen een netwerk van virtuele en fysieke componenten, gebruikers en aanbieders, en discours en handelingen. Het gaat om relaties tussen mensen, die diensten aanbieden en van diensten gebruik maken, de manier waarop over de cloud en de bijbehorende voor- en nadelen gepraat wordt, en de manier waarop de affordances van de technologie in relatie staan met het gebruik ervan. De cloud is slechts een van de vele netwerktechnologieën in de netwerksamenleving en een van de vele instrumenten van sociale organisatie, maar de groeiende populariteit van clouddiensten en het bijbehorende utility computing-paradigma, gecombineerd met de kenmerken van de technologie, die grote mogelijkheden bieden voor het opvangen van de razendsnel groeiende vraag naar internetdiensten en big data, maken dat cloud computing een zeer belangrijke technologie is in de maatschappij en een betekenisvol instrument van macht.

Volgens Castells wordt macht in de netwerksamenleving uitgeoefend door en via netwerken (Castells 2011, 774). Ieder component in een netwerk heeft volgens Castells een zekere macht – een macht die actoren buiten het netwerk niet hebben, aangezien de macht voortkomt uit het bestaan van het netwerk en elk component bijdraagt aan dit netwerk (ibid., 774). De meest cruciale vorm van macht in de netwerksamenleving is volgens Castells ‘network-making power’: de macht om

netwerken te kunnen creëren en verbinden en de standaarden van een netwerk te kunnen bepalen (ibid., 776). De mogelijkheid om cloud computing te gebruiken om clouddiensten in te richten en in werking te stellen is een vorm van macht die Castells 'network-making power' zou noemen. Tegelijkertijd heeft de cloudtechnologie als object ook vanuit zichzelf een zeker vorm van macht, vanwege de fundamentele kenmerken van de technologie, die het gebruik ervan beïnvloeden.

Ook Deleuze beschrijft in 'Postscript' een systeem van macht, waarbij de macht voortkomt uit verschillende controlemechanismen. De cloudtechnologie, met haar mogelijkheden voor inzicht in en sturing van het gedrag van gebruikers, kan als instrument van macht als een onderdeel van deze mechanismen gezien worden. Hoe staan de mogelijkheden en beperkingen van de cloudtechnologie en de inrichting van clouddiensten precies in verhouding tot het systeem dat Deleuze beschrijft? Welke mogelijkheden biedt de technologie voor toezicht en sturing? En biedt de technologie ook mogelijkheden voor verzet?

4.2 Affordances en controlemechanismen

Volgens Deleuze bevindt de mens zich in de controlemaatschappij in een eindeloos netwerk waarbinnen men vrij kan bewegen, maar toch niet vrij is, en waarin men door verschillende controlemechanismen constant onderhevig is aan toezicht en sturing (Deleuze 1992, 6). Het systeem van de controlemaatschappij is flexibel, veranderlijk en werkt extreem snel, als een datadeeltje in cyberspace dat in minder dan een seconde van de ene kant van de wereld naar de andere kant vliegt. Het is een algemeen, alomvattend systeem van verschillende overlappende mechanismen, waaronder de werking van de markt, beheersing van de toegang tot informatie en de mogelijkheid om de positie van ieder element op elk moment op te vragen. Hoe verhouden de affordances van de cloudtechnologie zich tot deze drie controlemechanismen?

Bij een analyse van het eerste controlemechanisme kan Deleuze's neomarxistische insteek niet over het hoofd gezien worden. Zijn werk kent een zekere antikapitalistische dimensie (Patton 2002, 6). Deleuze ziet het kapitalisme als een politieke en economische coördinatie die ingebed is in het sociale en zichzelf steeds aanpast aan de situatie in de wereld (ibid., 7). Kapitalisme stuurt de ontwikkelingen en beperkingen in een maatschappij en heeft zo grote macht

(Deleuze 1990). Deze macht kan begrepen worden als de werking van de markt. Dit is een fluïde vorm van macht die alle aspecten van de maatschappij beïnvloedt door te bepalen wat wel en niet waarde heeft. Deleuze observeert in de controlesamenleving een verplaatsing van het zwaartepunt van het kapitalisme van het produceren van producten naar het aanbieden van diensten. De opkomst van clouddiensten past binnen deze verschuiving. Naar verwachting zal er in 2017 wereldwijd meer dan honderd miljard dollar aan openbare clouddiensten uitgegeven worden (IDC 2013). Cloud computing onderscheidt zich van andere netwerktechnologieën door de talloze mogelijkheden voor het aanbieden van verschillende diensten aan een enorm aantal gebruikers. Ook laat het de gebruikservaring van deze diensten steeds meer lijken op die van basisbehoeften, wat de vraag naar dergelijke diensten verder zal laten toenemen. Een basisbehoefte is ten slotte een behoefte die een fundament vormt voor een goed en gelukkig leven; het is iets waar ieder mens over zou moeten beschikken. Doordat computerdiensten steeds meer op basisbehoeften gaan lijken en ook als zodanig geformuleerd worden, zullen mensen deze diensten waarschijnlijk ook in toenemende mate als een basisbehoefte gaan beschouwen.

Ook het tweede controlemechanisme, beheersing van de toegang tot informatie, is terug te zien in de cloud. In de controlemaatschappij is informatie volgens Deleuze van cruciaal belang, en de mogelijkheid om de toegang ertoe te beheersen is een belangrijke bron van macht. De populariteit van big data illustreert de waarde van (digitale) informatie in de huidige westerse maatschappij en de macht die gepaard gaat met het in handen hebben van deze informatie. Het hebben van toegang tot big data en methoden om deze data om te zetten in waardevolle kennis, geeft bedrijven veel macht omdat ze deze informatie kunnen gebruiken om hun diensten aan te passen aan de behoeften van de gebruikers, of deze kunnen doorverkopen aan derden. Hierdoor kunnen ze meer omzet genereren en hun positie op de markt versterken – en vanuit deze positie kunnen ze weer beïnvloeden wat wel en niet waarde heeft. De cloudtechnologie met haar mogelijkheden voor het verzamelen, opslaan en verwerken van big data speelt hierbij een grote rol als instrument van macht voor cloudeigenaren en andere aanbieders van clouddiensten. Door clouddiensten aan te bieden waarin gebruikers potentieel waardevolle informatie kunnen invoeren, verkrijgen de aanbieders van deze diensten macht over

deze informatie en de toegang ertoe, die ze vervolgens voor eigen doeleinden kunnen gebruiken. Deze macht is echter niet absoluut – het gevaar van hackers bestaat altijd.

De manier waarop big data geproduceerd, verzameld en gebruikt wordt, doet ook sterk denken aan met Deleuze's beschrijving van de verschuiving van de mens als individu naar de mens als 'dividu'. In de huidige westerse samenleving worden veel zaken (gedeeltelijk) gedigitaliseerd – waaronder ook de menselijke identiteit. Mensen scheppen op verschillende platforms verschillende digitale identiteiten door bepaalde informatie (die waar of niet waar kan zijn) in het systeem in te voeren. Je naam, e-mailadres, de bands die je leuk vindt, de mensen aan wie je berichten, de verschillende afbeeldingen die je kiest om jou te representeren: allemaal zijn het fragmenten van onszelf die we via verschillende technologieën cyberspace in sturen, waarvan vele ergens in een cloud belanden. Verschillende fragmenten vormen verschillende identiteiten die een bepaalde betekenis hebben en onderdeel kunnen zijn van een veelvoud aan groepen – het klantenbestand van een bepaald (cloud)bedrijf, de vriendenlijst van een gebruiker van een (cloud)dienst, en onderdeel van de enorme massa data genaamd 'big data'. Als gebruiker van een clouddienst ben je een dividu en worden de verschillende fragmenten van de digitale informatie die jou representeert gebruikt om waardevolle kennis te creëren, waarbij het van het doel van het verzamelen van de informatie afhangt welke fragmenten gebruikt worden.

Het derde controlemechanisme dat Deleuze noemt, de mogelijkheid om de plaats van een component binnen een netwerk op te kunnen vragen, is relatief abstract en doet sterk denken aan de manier waarop het internet functioneert. Elk apparaat dat onderdeel is van een computernetwerk dat is aangesloten op het internet heeft een IP-adres: een numeriek label dat aangeeft hoe het apparaat bereikt kan worden. Dankzij dit label kan de plaats van een apparaat in het netwerk achterhaald worden. Een ander voorbeeld van een proces waarbij een component in een netwerk gelokaliseerd kan worden, is het opvragen van gps-informatie om achter de locatie van bijvoorbeeld een mobiele telefoon of het navigatiesysteem van een auto te komen. Al deze verschillende processen kunnen gezien worden als een onderdeel van één groot controlemechanisme, waarbij in theorie iedereen altijd wel door iemand gevonden kan worden.

De cloud speelt geen onderscheidende rol bij dit controlemechanisme – clouddiensten werken hier als elke andere internetdienst, waarbij de locatie van een apparaat gevonden kan worden aan de hand van het IP-adres. De mogelijkheden tot toezicht en sturing die cloud computing voortbrengt komen voornamelijk voort uit de diensten die ermee gegenereerd worden ('network-making power') en de informatie die door middel van het gebruik van deze diensten in cloudomgevingen belandt, en dus in de handen van cloudeigenaren. Uit 'network-making power' komt dus Deleuziaanze toezicht en sturing voort. De cloudeigenaren die de meeste 'network-making power' hebben en de grootste hoeveelheid data beheren zijn Amazon, Google, Microsoft en Salesforce, die samen meer dan 80 procent van alle clouddiensten bezitten (Srinivasan 2014, 85). Zij hebben grote invloed op de ontwikkeling van cloud computing en de markt van internetdiensten en big data, en hebben in theorie vele mogelijkheden tot toezicht en sturing, omdat ze vele diensten aanbieden en inzicht hebben in vele systemen. Aangezien het doel van een bedrijf in principe altijd het maken van winst is, zullen bedrijven die gebruik maken van deze mogelijkheden tot toezicht en sturing dit altijd doen vanuit het streven om meer winst te maken.

De aanbieders van clouddiensten zijn echter niet de enigen die macht hebben over cloudsystemen. De toegankelijkheid van het internetnetwerk waarmee alle clouddiensten verbonden zijn, maakt de systemen kwetsbaar voor aanvallen van derden. Deleuze wijst storingen, virussen en piraterij aan als de gevaren van de computertechnologie (Deleuze 1992, 6). Deze gevaren zijn een bedreiging voor de controlemaatschappij en kunnen gezien worden als nieuwe vormen van verzet (Deleuze 1990). Dit verzet is al in vele vormen bezig, van piraterij (waarbij mensen de dienstensector kunnen ondermijnen door bepaalde zaken die als een dienst verkrijgbaar zijn, vrijelijk voor elkaar beschikbaar te maken) tot zaken als de 'celebrity nude hack'. Castells stelt dat verzet tegen genetwerkte macht (macht die voortkomt uit het bestaan van een netwerk) altijd plaats vindt binnen datzelfde netwerk. Verzet tegen bestaande machtsverhoudingen werkt via dezelfde mechanismen als de machtshebbers gebruiken (Castells 2011, 778). Dit is ook terug te zien in de aanvallen op cloudsystemen. Hackers maken gebruik van de kenmerken van de cloudtechnologie en het ontwerp van clouddiensten om hun doelen te bereiken, waarbij ze richten op de zwakke punten in het systeem. Ze gebruiken

dezelfde computerprocessen die de cloudomgevingen vormen om in de omgeving in te breken en op een bepaalde manier schade aan te richten. Zo gebruiken hackers de middelen van cloudeigenaren tegen hen – en ook tegen de gebruikers.

Dit geldt natuurlijk niet alleen voor cloudsystemen. Elke (digitale) netwerktechnologie bevat mogelijkheden voor verzet en kent derhalve geen absolute macht. De analyse van de affordances van de cloudtechnologie laat zien dat de toekomst van digitale netwerktechnologieën, waarbinnen cloud computing een belangrijke rol zal spelen, evenzeer gekenmerkt wordt door mogelijkheden tot toezicht en sturing als door bedreigingen hiervoor. Complexere systemen zorgen voor een complexere beveiligingssituatie en evenredig complexe vormen van verzet. Wat betekent dit voor de staat van de controlemaatschappij? Kan de huidige maatschappij een volwaardige Deleuziaanse controlemaatschappij genoemd worden?

5. Society of (un)control

De cloud heeft vele kenmerken die het bestaan van de ‘society of control’ bevestigen, maar tegelijkertijd doen zich ook al vormen van verzet voor. Mijn analyse van de affordances van de cloudtechnologie heeft laten zien dat cyberspace het terrein is van strijdende machten – degenen die systemen beheersen en degenen die zich buiten deze systemen willen bewegen of deze willen ondermijnen – met de passieve eindgebruikers van computerdiensten in het midden, die weinig tot geen macht hebben over de systemen die ze gebruiken en niet de wil, kennis of mogelijkheid hebben om deze systemen te ondermijnen. De risico’s van utility computing (een trend die gepaard gaat met cloud computing) moeten hierbij niet onderschat worden, omdat dergelijke diensten passief gebruik van de computertechnologie aanmoedigen. Computerdiensten, of het nu clouddiensten zijn of niet, zijn geen risicoloze basisbehoeften.

De netwerksamenleving in het tijdperk van de cloud vertoont grote overeenkomsten met de controlemaatschappij. De macht die in de huidige westerse samenleving op individuen uitgeoefend wordt is complexer, flexibeler en minder zichtbaar dan ooit. Ook is het is heel lastig om los te breken uit het machtssysteem van de controlemaatschappij (of beter gezegd: de vele verschillende, overlappende

controlemechanismen waaruit dit systeem bestaat), aangezien digitale technologieën volledig geïntegreerd zijn in het dagelijkse leven en digitale informatie zich maar lastig laat verwijderen. De controlemechanismen kunnen wel elk moment door een aanval uit balans gebracht worden, waardoor een andere partij macht kan verkrijgen over bepaalde informatie, maar de rangen sluiten zich daarna direct weer en het mechanisme is weer hersteld, tot de volgende aanval. Sommige gebruikers verliezen misschien vertrouwen in een bepaalde computerdienst en stappen over naar andere, maar ook deze dienst is onderdeel van een controlemechanisme, en zo verandert er eigenlijk weinig.

Toch kunnen de controlemechanismen in het tijdperk van de cloud niet zonder meer onbeperkt genoemd worden. De digitale aard van technologieën als cloudsystemen maakt dat niemand volledige macht heeft over informatie die via het web bereikt kan worden, niet consumenten maar ook cloudeigenaren niet. Elke technologie moet altijd op zijn hoede zijn voor een aanval, die zichtbaar of onzichtbaar kan zijn. Deleuze erkent dat mogelijkheden voor verzet altijd een inherent aspect vormen van een systeem van macht (zonder verzet zou er nooit een verschuiving van systemen kunnen plaatsvinden), maar mijns inziens zijn de instrumenten van macht te kwetsbaar en het verzet te wijdverspreid, subtiel en succesvol om van de netwerkmaatschappij in het tijdperk van de cloud een echte, volwaardige controlemaatschappij te maken. De mens bevindt zich constant in een netwerk en de invloed van de markt en de mogelijkheid van toezicht zijn altijd aanwezig, maar de beheersing over informatie en de instrumenten van macht is gemakkelijk te breken. De bewerkelijkheid, complexiteit en kwetsbaarheid die voortvloeit uit de digitaliteit van instrumenten zoals cloudsystemen, maakt dat de ‘society of control’ in dit opzicht net zo goed de ‘society of uncontrol’ genoemd kan worden. Dit betekent niet dat de controlemaatschappij niet aanwezig is, maar dat deze in constant gevecht is met de krachten van het verzet, die beiden met dezelfde subtiele digitale wapens vechten. Mede dankzij de affordances van digitale technologieën zoals de cloud is de controlemaatschappij zoals Deleuze deze beschreef niet volledig tot bloei gekomen – in ieder geval nu nog niet.

Referenties

Amazon Web Services. 'AWS GovCloud (US) Region - Government Cloud Computing.' Bezocht op 22 oktober 2014. http://aws.amazon.com/govcloud-us/

Arthur, Charles. 2014a. 'Naked celebrity hack: Security experts focus on iCloud backup theory.' The Guardian, 1 september. http://www.theguardian.com/ technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence

Arthur, Charles. 2014b. 'Nude celebrity leak looks like phishing or email account hack.' *The Guardian,* 1 september. http://www.theguardian.com/technology/ 2014/sep/01/nude-celebrity-pictures-hack-jennifer-lawrence-rihanna

Butcher, Mike. 2014. 'Here's what we know so far about the celebrity photo hack.' *TechCrunch,* 1 september. http://techcrunch.com/2014/09/01/heres-what-we-know-so-far-about-the-celebrity-photo-hack/

Castells, Manuel. 2011. 'A network theory of power.' *International Journal of Communication* 5: 773-787.

Castells, Manuel. 2005. 'The network society: From knowledge to policy.' In *The network society: from knowledge to policy,* eds. Manuel Castells en Gustavo Cardosa, 3-22. Washington, DC: Johns Hopkins Center for Transatlantic Relations.

Chen, Min, Shiwen Mao, Yin Zhang, en Victor C. M. Leung. 2014. *Big data: Related Technologies, challenges and future prospects.* Springer.

Chen, Yanpei, Vern Paxson, en Randy H. Katz. 2010. 'What's new about cloud computing security?.' *University of California, Berkeley: Electrical Engineering and Computer Sciences,* 20 januari. http://www.eecs.berkeley. edu/ Pubs/TechRpts/2010/EECS-2010-5.html

Coevert, Annemarie. 2014. 'Privéfoto's beroemdheden online na hack.' *NRC,* 1 september. http://www.nrc.nl/nieuws/2014/09/01/privefotos-beroemdheden-online-na-hack/

Cook, James. 2014. 'The hackers behind the naked celebrity iCloud photo leak have regrouped, and they are not happy.' *Business Insider,* 2 oktober.

http://www.businessinsider.com/hackers-in-celebrity-icloud-photo-leak-are-back-on-anonib-2014-10

Davey, Gavin. 2014. ‘Jennifer Lawrence photo hack shows how privacy can float away.’ *The Guardian,* 3 september. http://www.theguardian.com/media-network/media-network-blog/2014/sep/03/celebrity-photo-hack-jennifer-lawrence- privacy-cloud

Deleuze, Gilles. 1990. ‘Control and becoming: Gilles Deleuze in conversation with Antonio Negri.’ *Futur Anterieur* 1.

Deleuze, Gilles. 1992. ‘Postscript on the societies of control’. October 59: 3-7.

Dinh, Hoang T., Choncho Lee, Dunsit Niyato, en Ping Wang. 2013. ‘A survey of mobile cloud computing: architecture, applications, and approaches’. *Wireless Communication and Mobile Computing* 13: 1587-1611.

Van Dijk, Johannes A. G. M. 1991. *De netwerkmaatschappij: Sociale aspecten van nieuwe media*. Bohn Stafleu Van Loghum.

Dong, Xin, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, en Minglu Li. 2013. ‘Archieving an effective, scalable and privacy-preserving data sharing service in cloud computing.’ *Computers & Security* 42: 151-164.

Dropbox. ‘Privacybeleid van Dropbox.’ Voor het laatst gewijzigd: 20 februari 2014. https://www.dropbox.com/privacy2014

Encyclo.nl. ‘Controle.’ Bezocht op 22 november 2014. http://www.encyclo.nl /zoek.php?woord=controle

Evans, Dayna. 2014. ‘J-Law, Kate Upton nudes leak: Web explodes over hacked celeb pics.’ *Gawker,* 31 augustus. http://gawker.com/internet-explodes-over-j-laws-alleged-hacked-nudes-1629093854

Fehling, Christoph, Frank Leymann, Ralph Retter, Walter Schupeck, en Peter Arbitter. 2014. *Cloud computing patterns: Fundamentals to design, build and manage cloud applications.* Springer.

Ghandi, Anhsul, Mor Harchol-Balter, Rajarshi Das, en Charles Lefurgy. 2009. ‘Optimal power allocation in server farms.’ *ACM SIGMETRICS Performance Evaluation Review* 37 (1): 157-168.

Google. 2006. ‘Conversation with Eric Schmidt hosted by Danny Sullivan.’ *Google Press Center,* 9 augustus. http://www.google.com/press/podium/ses2006. html

Hill, Richard, Laurie Hirsch, Peter Lake, en Siavash Moshiri. 2013. *Guide to cloud computing: Principles and practice*. Springer.

Hijink, Marc. ‘Baas in eigen cloud? Vergeet het maar.’ NRCQ, 3 september. http://www.nrcq.nl/2014/09/03/baas-in-eigen-cloud-vergeet-het-maar

Hwang, Kai, Geoffrey C. Fox, en Jack J. Dongarra. 2012. *Distributed and cloud computing: From parallel processing to the internet of things*. Elsevier.

ICD. 2013. ‘IDC forecasts worldwide public IT cloud services spending to reach nearly $108 billion by 2017 as focus shifts from savings to innovation.’ *IDC*, 3 september. http://www.idc.com/getdoc.jsp?containerId=prUS24298013

Jäger, Siegfried, en Florentine Maier. 2009. ‘Theoretical and methodological aspects of Foucauldian critical discourse analysis and dispositive analysis’. In: *Methods of critical discourse analysis,* eds. Ruth Wodak en Michael Meyer, 34-61. Londen: Sage Publications.

Jørgensen, Marianne W., en Louise J. Phillips. 2002. *Discourse analysis as theory and method*. London: Sage.

Kahanwal, Brijender, en Teijnder Pal Singh. 2012. 2012. ‘The distributed computing paradigms: P2P, grid, cluster, cloud, and jungle.’ *International Journal of Latest Research in Science and Technology* 2 (1): 183-187.

Kleinherenbrink, Arjen. 2011. ‘Subject to control: An essay on capitalism and subjectivity in the work of Gilles Deleuze.’ Radboud University Nijmegen. http://www.academia.edu/7016472/Subject_to_Control_-_An_Essay_on_Capitalism_and_Subjectivity_in_the_Work_of_Gilles_Deleuze

Koenis, Chris. 2014. ‘Nieuwe gebruiksvoorwaarden Dropbox zet rechter buitenspel.’ *Webwereld,* 21 februari. http://webwereld.nl/cloud/81446-nieuwe-gebruiksvoorwaarden-dropbox-zet-rechter-buitenspel

Latour, Bruno, en Couze Venn. 2002. ‘Morality and technology: The end of the means’. *Theory Culture Society* 19: 247-260.

Lee, Gary. 2014. *Cloud networking: Understanding cloud-based data center networks*. Burlington: Elsevier Science.

Li, Shirley. 2014. ‘Apple blames ‘targeted attack’, not iCloud, for celebrity photo hack.’ *The Wire,* 2 september. http://www.thewire.com/technology/2014/09/apple-finds-no-evidence-hackers-exploited-icloud-to-steal-celebrity-photos/379487/

Marston, Sean, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, en Anand Ghalsasi. 2010. ‘Cloud computing: The business perspective.’ *Decision Support Systems* 51: 177-189.

Mijn woordenboek. ‘Contrôle.’ Bezocht op 22 november 2014. http://www.mijnwoordenboek.nl/vertaal/FR/NL/contr%C3%B4le

Mims, Christopher. 2014. ‘Amazon and Google are in an epic battle to dominate the cloud—and Amazon may already have won.’ *Quartz*, 16 April. http://qz.com/196819/how-amazon-beat-google-attempt-to-dominate-the-cloud- before-it-even-got-started/

Norman, Donald. 1999. ‘Affordance, conventions and design.’ *Interactions* 6 (3):38-43.

Ouedraogo, Moussa, en Haralambos Mouratidis. 2013. ‘Selecting a cloud service provider in the age of cybercrime.’ *Computers & Security* 38: 3-13.

Patton, Paul. 2002. *Deleuze and the Political*. Routledge.

Rackspace. ‘Private Cloud: Powered by OpenStack.’ Bezocht op 22 oktober 2014. http://www.rackspace.nl/cloud/private

Reading, Anna. 2014. ‘Seeing red: A political economy of digital memory’. *Media, Culture & Society*. 1-13.

Resare, Noa, en Ramon van Alteren. ‘What we learned at Spotify, navigating the clouds.’ *Usenix.org.* Bezocht op 22 oktober 2014. https://www.usenix.org/ what-we- learned -spotify-navigating-clouds

Saltzman, Roi, en Adi Sharabani. 2009. *Active man in the middle attacks: a security advisory.* IBM. http://blog.watchfire.com/amitm.pdf

Sargent, Jordan. 2014. ‘Is this 4chan offshoot the ground zero for the leaked celebrity nudes?’ *Gawker*, 1 september. http://gawker.com/is-this-4chan-offshoot-the-ground- zero-for-the-leaked-c-1629190208

Schäfer, Mirko T. 2011. *Bastard culture: How user participation transforms cultural production.* Amsterdam: Amsterdam University Press.

Srinivasan, Srini. 2014. *Cloud computing basics.* Springer.

Taylor, Mark C. 2001. *The moment of complexity: Emerging network culture.* Chicago: The University of Chicago Press.

The free dictionary. ‘Control.’ Bezocht op 22 november 2014. http://www.thefreedictionary.com/control

Villegas, David, Ivan Rodero, Liana Fong, Norman Bobroff, Yanbin Liu, Manish Parashar, en S. Masoud Sadjadi. 2010. ‘The role of grid computing technologies in cloud computing.’ In *Handbook of cloud computing*, eds. Borko Furht en Armando Escalante, 183-218. Springer.

Zinnedinne, Mhamed. 2014. ‘Vulnerabilities and mitigation techniques toning the cloud: A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm flights.’ *Computers & Security* 48: 1-18.