

Van privacyparadox naar controlecontroverse

*Een antwoord op het privacydebat rond sociale netwerksites
in termen van de risicomaatschappij*

Suze Krijnen

*Universiteit Utrecht
Faculteit Geesteswetenschappen
Master Nieuwe Media & Digitale Cultuur
MA – Scriptie
9 juli 2010*

*Studentnummer: 0319597
Begeleider: Cris van der Hoek
Tweede lezer: Imar de Vries*

Inhoudsopgave

Abstract.....	4
Inleiding.....	5
Opzet.....	7
Verantwoording van het corpus.....	8
Sociale netwerksites en hun gebruikers.....	8
Privacy, privé en publiek	9
1. Het privacydebat: een vertooganalyse.....	10
1.1 Privé in publiek: een onderhandeling.....	10
1.2 Een kwestie van controle	11
1.3 Drie oplossingen.....	12
1.3.1 Bewustwording (I).....	14
1.3.2 Aanpassing van technologie (II).....	15
1.3.3 Sociale normen (III).....	17
1.4 Evaluatie van de oplossingen.....	19
2. Sociale netwerksites en de risicomaatschappij.....	21
2.1 Van rationaliteit naar reflexiviteit	21
2.2 Sociale risiconetwerken.....	22
2.3 Reflexieve netwerksites: ambivalente vooruitgang.....	24
2.4 Van privacyparadox naar controlecontroverse.....	25
3. De controlecontroverse als kosmopolitisch moment.....	26
3.1 Van ironie naar verlichting.....	26
3.2 De controlecontroverse als kosmopolitisch moment.....	27
3.3 Risico versus verwikkeling.....	28
3.4 Het privacydebat als netwerk.....	29
3.4.1 Sociale netwerksites als quasi-objecten.....	30
3.4.2 Gebruikers als quasi-subjecten.....	30
3.5 Naar een alledaags interpretatiekader.....	31
4. Interpretatie als alledaags wapen.....	32
4.1 Goffman en de kwetsbaarheid van sociale interactie.....	32
4.2 Situaties definiëren op sociale netwerksites.....	33
4.3 Anoniem versus kosmopolitisch publiek.....	34
5. Terug naar de praktijk: aanknopingspunten.....	36
5.1 Ironie en 'play'.....	36
5.2 Naar een ethiek van onnauwkeurigheid	37
5.3 'Social forgetfulness'.....	38
5.4 Een tragisch element.....	39
Conclusie: van controle naar interpretatie.....	40
Aanbevelingen en reflectie.....	41
Literatuur.....	42

Abstract

De theorie van de risicomaatschappij zoals uiteengezet door Ulrich Beck (1992) levert een relevante bijdrage aan het wetenschappelijke debat over sociale netwerksites en privacy. Dit debat is gericht op het in kaart brengen en bestrijden van risico's die de gebruikers van sociale netwerksites zelf creëren. Rationele, techno-wetenschappelijke strategieën om de controle over online gedeelde persoonlijke informatie te herwinnen leveren eerder minder dan meer controle op. Een alternatieve oplossing voor het probleem – aangescherpt van een 'privacyparadox' tot een 'controlecontroverse' – wordt op basis van de these van de risicomaatschappij, ondersteund door de sociologische perspectieven van Bruno Latour (2003) en Erving Goffman (1959), geformuleerd in termen van de interpretatie van persoonlijke informatie op sociale netwerksites door het publiek. Wanneer gebruikers van sociale netwerksites net als in face-to-face interactie kunnen vertrouwen op een loyaal en tactisch publiek, neemt de culturele perceptie van risico af. Een in Becks termen 'kosmopolitisch' interpretatiekader van online gedeelde persoonlijke informatie is zowel normatief – in de confrontatie met de 'ander' achter de schermen – als pragmatisch – in reactie op de ambivalente status van persoonlijke informatie op sociale netwerksites.

Inleiding

In 2006 sprak Susan B. Barnes voor het eerst van een 'privacyparadox' in relatie tot sociale netwerksites. Anno 2010 houdt het merkwaardige fenomeen, waarbij gebruikers in groten getale persoonlijke informatie online plaatsen en zich tegelijkertijd zorgen maken om de mogelijke gevolgen hiervan voor hun privacy, de gemoederen nog steeds bezig. Illustratief is de ontwikkeling van Facebook, wereldwijd één van de grootste sociale netwerksites. Sinds de introductie in september 2006 van de functie *News Feed*, dat gebruikers een overzicht toont van de activiteiten van andere gebruikers in hun netwerk, stuitte iedere wijziging die de site aanbracht op een storm aan kritiek – opmerkelijk genoeg zelfs in de vorm van anti-Facebook groepen *binnen* Facebook. Desondanks bleef het aantal actieve gebruikers stijgen tot meer dan 400 miljoen in februari 2010.¹

Populaire media richten hun pijlen met name op privacyschending via sociale netwerksites door bedrijven, waarbij niet zelden nogal lukrake vergelijkingen met *Big Brother* of *Brave New World* worden ingeroepen (bijvoorbeeld Thompson, 2008). Overheden die hun verantwoordelijkheid nemen waarschuwen met name voor identiteitsfraude en andere vormen van misbruik van online persoonsgegevens door criminelen (Ibrahim, 2008).² Een blik op de niet aflatende stroom gerapporteerde incidenten – van het verlies van een baan; zorgverzekering; ouderschapsregeling of relatie; tot stalken; chantage; vernedering; ruzie en pesten (boyd,³ 2010; De Souza & Dick, 2008) – wijst echter op het bepaald *alledaagse* karakter van het probleem.

Dit maakt de proliferatie van sociale netwerksites niet minder onrustbarend. Juist het gevaar uit onverwachte hoek, veroorzaakt door op het eerste gezicht onschuldige informatie, valt moeilijk te reguleren (Mooradian, 2009). Hoe gebruiksvriendelijk sociale netwerksites hun privacyinstellingen ook maken (cf. Zuckerberg, 2010), het valt te betwijfelen of gebruikers op voorhand kunnen bepalen wat zij wanneer met wie willen delen. Eenmaal online gedeelde informatie is in essentie de controle voorbij. Liever dan een positieve of negatieve ontwikkeling vormen sociale netwerksites daarmee voor alles een *onbekend* fenomeen. Met het oog op het *potentiële* leed dat het gebruik van sociale netwerksites veroorzaakt, wordt in het privacydebat

1 Bron: Bedrijfstijdlijn Facebook, via <http://www.facebook.com/press/info.php?timeline>.

2 Onderdeel van het overheidsinitiatief 'Nederland Veilig' vormt de voorlichtingscampagne over 'Veilig Internetten (heb je zelf in de hand)'. In het kader van deze campagne werden in 2009 en 2010 commercials gelanceerd die waarschuwen voor misbruik van online gedeelde persoonsgegevens door 'cybercriminelen'. De website VeiligInternetten.nl geeft tips voor de bescherming van persoonlijke gegevens op internet.

3 Sociale mediaonderzoeker danah boyd heeft haar naam bij wet laten vastleggen in kleine letters en wenst op deze wijze geciteerd te worden.

rond deze sites dan ook veelvuldig gesproken van 'risico's'. Sociale netwerksites zouden daarmee gevat kunnen worden in de woorden van de socioloog Ulrich Beck, die stelt dat "we do not know what it is we don't know – but from this dangers arise, which threaten mankind!" (2006: 329).

Beck stelt in zijn invloedrijke boek *Risk Society: Towards a New Modernity* (1992) dat de moderne samenleving een 'risicomaatschappij' is geworden, niet omdat er meer risico's zijn dan voorheen, maar omdat zij in toenemende mate bezig is met het bediscussiëren, controleren en voorkomen van risico's die zijzelf veroorzaakt. Die anticipatie op de mogelijk desastreuze effecten van complexe hedendaagse technologieën is problematisch, aangezien de ware dreiging nu juist uitgaat van de onbedoelde en onvoorziene neveneffecten van deze *unknown unknowns* (2006: 329). In het besef dat de uitoefening van controle in de technowetenschappelijke samenleving 'ironisch' genoemd kan worden, is de moderniteit volgens Beck 'reflexief' geworden (idem: 338).

Ondanks de alomtegenwoordigheid van de term risico in het academische debat over sociale netwerksites en privacy, is het theoretisch kader van de risicomaatschappij hier nog nauwelijks toegepast. Enkel de auteur Yasmin Ibrahim verwijst naar Beck in haar bespreking van sociale netwerksites als *complicit risk communities* (2008: 245), zonder echter in een door deze theorie gefundeerde oplossing te voorzien.⁴ Dit onderzoek veronderstelt dat de theorie van de risicomaatschappij een kritische bijdrage kan leveren aan het wetenschappelijke debat, met als doel het formuleren van een adequater antwoord op de 'privacyparadox'. Tegelijkertijd wordt daarmee een bijdrage geleverd aan de these van de risicomaatschappij. Deze werd door Beck uitgewerkt met betrekking tot de mondiale risico's van klimaatverandering, economische crises en terrorisme; de informatie- en communicatietechnologie wordt nog niet structureel als bron van risico geadresseerd.⁵ De centrale vraagstelling in dit onderzoek luidt:

Hoe kan het privacydebat rond sociale netwerksites begrepen en opgelost worden in termen van de risicomaatschappij?

4 Yasmin Ibrahim beschouwt sociale netwerksites als uitbreiding van het 'risicolandschap' in de manier waarop zij, in hun architectuur, risico tot de *structuur* van de sociale interactie zelf maken (2008: 251). Sonia Livingstone (2008) verwijst naar de socioloog Anthony Giddens, die zich in navolging van Beck met het perspectief van de risicomaatschappij bezighield, wanneer zij de praktijken op sociale netwerksites bespreekt in termen van 'een complexe relatie tussen kansen en risico's'.

5 Beck onderscheidt drie dimensies' van mondiale risico's, namelijk milieucrisis, risico's in de wereldeconomie, en terrorismedreiging. Een vierde dimensie wordt gevormd door biografische risico's, nauw verbonden met de dynamiek van individualisering. Deze biografische risico's laat hij echter expliciet buiten beschouwing (2009: 13).

Opzet

De beantwoording van de hoofdvraag is als volgt opgebouwd. Het onderzoek vangt aan met een vertooganalyse van het academische debat over sociale netwerksites en privacy. Hoe wordt het probleem gedefinieerd en waar worden oplossingen gezocht? Welke kanttekeningen worden bij die oplossingen geplaatst en welke opvattingen over de verhouding tussen technologie en samenleving liggen daaraan ten grondslag?

Dit vertoog wordt geanalyseerd met behulp van het theoretische instrumentarium van Ulrich Beck (2006; 2009). Welke invulling wordt in het debat gegeven aan de begrippen controle en risico? Hoe komen Becks ideeën over de moderniteit en de reflexieve moderniteit hierin naar voren? Kan aan de risico's van participatie in sociale netwerksites ook een 'verlichtende functie' toegeschreven worden in de vorm van het door Beck beschreven 'kosmopolitisch moment'?

Met behulp van het antropologische perspectief van de socioloog-filosoof Bruno Latour (2003) op de these van de risicomaatschappij wordt een brug geslagen van het universele perspectief van Beck naar het niveau van de individuele gebruikers van sociale netwerksites. Volgens Latour zijn hedendaagse technologieën niet complexer dan vroeger, maar worden ze nu pas als zodanig erkend. Welke implicaties heeft deze notie van continuïteit voor de interpretatie van (informatie op) sociale netwerksites?

Via Beck en Latour kan vervolgens een alternatieve oplossing voor het privacyprobleem geformuleerd worden op basis van vertrouwde strategieën om met alledaagse onzekerheden om te gaan. Daartoe wordt het dramaturgisch perspectief op sociale interactie van de socioloog Erving Goffman (1959) geraadpleegd. Kan de interactie op sociale netwerksites begrepen worden als een performance? In hoeverre ligt hier een mogelijkheid voor de totstandkoming van een 'kosmopolitisch publiek'?

Het kosmopolitische interpretatiekader voor online gedeelde persoonlijke informatie dat op basis van de behandelde theorieën geformuleerd kan worden vergt praktische vaardigheden in de omgang met sociale netwerksites. Bevat het huidige privacydebat aanwijzingen voor de ontwikkeling van dergelijke vaardigheden? Hoe kan het theoretische 'interpretatieargument' zodoende worden teruggekoppeld naar de problemen die zich in de praktijk voordoen?

Verantwoording van het corpus

Sinds 2005 is een groot aantal academische studies verschenen naar privacy in relatie tot sociale netwerksites (boyd, 2007). De vertooganalyse in dit onderzoek richt zich op het privacydebat over sociale netwerksites zoals sinds 2006 gevoerd in de sociale- en geesteswetenschappen (hierna te noemen: privacydebat). Artikelen met een sterk juridische of technische invalshoek zijn buiten beschouwing gelaten. Het corpus omvat vijftien wetenschappelijke artikelen en twee boeken. Hieronder bevinden zich vier etnografische studies, die voorzien in empirische gegevens. Daar veel van de geanalyseerde artikelen naar elkaar verwijzen kan gesproken worden van een debat.

De literatuur richt zich op diverse sociale netwerksites. De empirische studies behandelen de praktijken rondom specifieke sites, andere bronnen richten zich meer op sociale netwerksites in het algemeen. Facebook en MySpace zijn iets oververtegenwoordigd in verhouding tot andere (kleinere) sites. Het merendeel van de literatuur richt zich expliciet op het gebruik door sociale netwerksites door jongeren en studenten. Niet alle bronnen komen in de analyse evenredig aan bod. Dit komt doordat sommige van hen slechts ten dele op sociale netwerksites gericht zijn of zich grotendeels aansluiten bij eerder onderzoek.

De periode is afgebakend tot het debat zoals gevoerd werd tussen 2006 en 2010. In 2006 was Susan B. Barnes de eerste die de veelgeciteerde term 'privacyparadox' aanhaalde in relatie tot sociale netwerksites. Aangezien de geschiedenis van sociale netwerksites sinds hun ontstaan in het begin van de eenentwintigste eeuw gekenmerkt wordt door grote veranderingen (boyd & Ellison, 2007) zou het opnemen van oudere artikelen in het corpus leiden tot moeilijker vergelijkbare bevindingen. De periode is evenwel lang genoeg om eventuele historische ontwikkelingen te kunnen opmerken.

Sociale netwerksites en hun gebruikers

Sociale netwerksites kennen vele verschijningsvormen. In dit onderzoek verwijst de term naar alle sites die ten minste voldoen aan de drie gangbare kenmerken van een profielpagina; een lijst met virtueel gearticuleerde connecties of 'vrienden'; en een mogelijkheid berichten en reacties op profielen te plaatsen (boyd, 2007: 2). Daarbij wordt verondersteld dat sociale netwerksites voor veel gebruikers diepgeworteld zijn geraakt in de routines van het dagelijks leven (boyd, 2010). De toegenomen integratie van diverse vormen van online communicatie (bijvoorbeeld e-mail, *instant messaging*, bloggen, muziek luisteren, video's bekijken) alsook telefonische en zelfs face-to-face communicatie, maakt het zelfs niet langer zinvol te spreken van een onderscheid tussen het 'offline' en online sociale leven (Livingstone, 2008: 5).

Privacy, privé en publiek

Wanneer in dit onderzoek gesproken wordt van privacy, verwijst die term naar 'informatieele privacy'. Deze benadering van privacy is in de context van de ethiek van de informatietechnologie het relevantst (Shoemaker, 2010: 3). Informatieele privacy wordt gedefinieerd als de aanspraak van het individu om zelf te bepalen wanneer, hoe, en in welke mate anderen kunnen beschikken over informatie over hem- of haarzelf (Van der Ploeg & De Mul, 2000: 9).

Informatieele privacy kan betrekking hebben op verschillende vormen van informatie. Het is dit onderzoek in het bijzonder te doen om 'biografische persoonlijke informatie', oftewel alledaagse gegevens over individuen die vertellen wie zij zijn, wat zij doen en hebben gedaan, waar zij zijn geweest, etcetera. Onder deze informatie vallen tevens institutiespecifieke, bijvoorbeeld medische en financiële informatie alsook sociaal gevoelige informatie, die reputatie kan schaden zelfs al gaat het om praktijken die in het algemeen als normaal of acceptabel beschouwd worden. Biografische persoonlijke informatie is problematisch, ten eerste omdat zij in eerste instantie onschuldig en onschadelijk lijkt en ten tweede omdat zij niet gemakkelijk te reguleren valt (Mooradian, 2010: 166; 169).

Het publieke domein wordt in dit onderzoek opgevat als de publieke sfeer of openbaarheid, waarin informatie voor iedereen vrij toegankelijk is. Deze opvatting van het begrippenpaar publiek en privé onderscheidt zich van het traditionele 'privacydebat' in termen van het recht op privacy van de burger ten opzichte van de overheid (Martens et al., 2008: 34).⁶

⁶ Het traditionele privacydebat verwijst naar het spanningsveld tussen de filosofisch-ethische tendensen liberalisme en communitarisme in de moderne democratische staatsvorm. Waar de eerste het individuele belang vooropstelt, gaat het communitarisme uit van het collectieve belang, dat het controleren van individuen en eventueel ingrijpen in de privésfeer door een democratische overheid rechtvaardigt (Van der Ploeg & De Mul, 2000: 8).

1. Het privacydebat: een vertooganalyse

Dit hoofdstuk analyseert het academische privacydebat rond sociale netwerksites. Hoe wordt het probleem gedefinieerd en waar worden oplossingen gezocht? Welke kanttekeningen worden bij die oplossingen geplaatst en welke opvattingen over de verhouding tussen technologie en samenleving liggen daaraan ten grondslag?

1.1 Privé in publiek: een onderhandeling

Susan B. Barnes brengt in 2006 voor het eerst de term 'privacyparadox' in verband met sociale netwerksites. Zij interpreteert de volgens haar argeloze omgang van Amerikaanse tieners met sociale netwerksites als een discrepantie tussen denken en doen; hoewel de meeste gebruikers weten dat sociale netwerksites openbaar zijn, handelen zij alsof het een (semi-)privéruimte betreft. Sindsdien hebben diverse empirische en theoretische studies zich toegelegd op de ontrafeling van de schijnbare tegenstelling waarmee gebruikers persoonlijke informatie online plaatsen en zich tegelijkertijd zorgen maken om de mogelijke ongewenste consequenties hiervan voor hun privacy.⁷

De tegenstelling wordt in het debat opgeheven door privacy niet op te vatten als het tegenovergestelde van openbaarheid, maar als een 'onderhandeling' over ontsluiting en afsluiting van persoonlijke informatie. In die onderhandeling zouden gebruikers van sociale netwerksites wel degelijk bewust grenzen trekken tussen publiek en privé (Livingstone, 2008). Een hoge mate van afsluiting is daarbij niet noodzakelijk de meest wenselijke uitkomst (Tufekci, 2008). De Souza & Dick articuleren een 'kosten-baten analyse' waarin gebruikers bereid zijn concessies te doen aan hun privacy ten gunste van andere waarden (2008: 145). Motivaties die in de literatuur genoemd worden voor het ontsluiten of 'online delen' van persoonlijke informatie zijn, samengevat: zelfpresentatie, zelfexpressie, een gevoel van intimiteit, verbondenheid in een gemeenschap, het vindbaar zijn voor *peers*, *sociability*, het delen van culturele artefacten, nieuwe mensen leren kennen en flirten (Barnes, 2006; boyd, 2006; Preibusch et al., 2007; Ibrahim, 2008; Livingstone, 2008: 4).⁸ Openbaarheid vormt dus niet perse een bedreiging voor privacy. Het aan banden leggen van de praktijken op sociale netwerksites wordt dan ook zowel onwaarschijnlijk als onwenselijk bevonden (boyd, 2007: 5; De Souza & Dick, 2008: 155).

7 De term 'privacyparadox' gaat vooraf aan het debat over sociale netwerksites (zie bijvoorbeeld Van der Ploeg & De Mul, 2000: 5). In navolging van Barnes articuleren boyd & Ellison (2007), Livingstone (2008: 9) en Martens et al. (2008: 61) een 'paradox' in relatie tot sociale netwerksites en privacy. Andere auteurs verwijzen naar hetzelfde fenomeen met termen als *disconnection of discrepancy*.

8 Interessant op dit punt is de opmerking van Barnes (2006) en boyd (2007) dat (Amerikaanse) jongeren sociale netwerksites juist een relatief besloten hang- en ontmoetingsplek ervaren, omdat zij zich hier anders dan thuis, op school of op straat, ongestoord door autoriteiten wanen. Sociale netwerksites constitueren dus een ruimte die *tegelijkertijd* persoonlijk en publiek is (Rosenblum, 2007).

Het probleem is daarmee echter nog niet opgelost, zo stelt Livingstone (2008: 10). Er treedt immers nog steeds verontwaardiging op wanneer zich toch schade voordoet (De Souza & Dick, 2008: 143; Barnes, 2006: 4). Het werkelijke probleem wordt in het debat dan ook niet ontwaard in de ontsluiting van persoonlijke informatie *an sich*, maar in het gebrek aan *controle* van gebruikers over wie, wanneer en in welke mate toegang heeft tot hun persoonlijke informatie.⁹ Zoals Tufekci (2008) stelt: "Het gaat erom gezien te worden door wie men gezien wenst te worden, op de manier waarop men gezien wenst te worden."

1.2 Een kwestie van controle

Sociale mediaonderzoeker danah boyd (2007) biedt een overzicht van de eigenschappen van online informatie die controle ondermijnen, te weten *persistence* (permanente beschikbaarheid), *searchability* (eenvoudige doorzoekbaarheid), *replicability* (kopieerbaarheid en manipuleerbaarheid) en *invisible audiences* (het 'gemedieerde publiek' dat niet alleen onzichtbaar is maar zich ook nog eens in de toekomst kan bevinden). Tufekci (2008) voegt aan dit rijtje de eigenschap *cross-indexability* toe, oftewel de eenvoudige koppeling van online informatie uit verschillende, fysieke en virtuele plekken of contexten.¹⁰ Martens et al. merken bovendien op dat de eenmaal online geplaatste informatie vaak niet gemakkelijk te verwijderen valt (2008: 56).

Boyd noemt twee complicaties van deze eigenschappen voor de handhaving van controle over online gedeelde persoonlijke informatie. De eerste is het 'verlies van context'. Aangezien het onmogelijk is om iedereen – overal en op ieder moment – tegelijk toe te spreken, richten gebruikers van sociale netwerksites zich op een *imagined audience*, dat vaak niet overeenkomt met hun daadwerkelijke publiek. Een tweede complicatie voor het uitoefenen van controle vormt 'schaalvergroting'. Hoewel de meeste boodschappen op sociale netwerksites slechts door enkelingen worden gehoord, hebben gênante video's de neiging zich via de netwerktechnologie razendsnel te verspreiden. Onevenredige aandacht wordt bovendien gegenereerd wanneer een individu plotseling nieuwswaardig wordt, bijvoorbeeld door overlijden, misdaad of andere negatieve situaties.¹¹ Hiermee ontstaat een situatie die boyd omschrijft als *security through obscurity*. De door 'obscuriteit' gewaarborgde veiligheid is voorlopig en relatief; het online plaatsen van persoonlijke informatie heeft altijd *potentiële* consequenties.¹² De inherente mogelijkheid dat informatie op sociale netwerksites in de

9 Met uitzondering van Barnes (2006) en Rosenblum (2007).

10 Deze doorkruising van virtuele en fysieke ruimtes en contexten wordt versterkt door de tegenwoordig vaak aangeboden mogelijkheid profielen op verschillende sociale media, waaronder locatiegebaseerde media, aan elkaar te koppelen.

11 Recente Nederlandse voorbeelden zijn de moord op de twaalfjarige Milly uit Dordrecht en de negenjarige Ruben die als enige een vliegcrash in Tunesië overleefde (Dekker, 2010).

12 Ibrahim (2008) noemt sociale netwerksites 'rizomatische netwerken', daarmee verwijzend naar een concept van Gilles Deleuze en Félix Guattari. De consequenties van het handelen op sociale netwerksites kunnen opgevat worden als 'virtueel' in die zin dat zij enkel geactualiseerd hoeven te worden en daarmee altijd potentieel mogelijk zijn.

toekomst op ongewenste wijze gebruikt zal worden, wordt in het debat veelal gearticuleerd als een 'risico'.¹³

1.3 Drie oplossingen

In het wetenschappelijke debat worden diverse oplossingen voor het controleprobleem voorgesteld. Deze oplossingen kunnen worden onderverdeeld in drie categorieën, respectievelijk gericht op kennis of *bewustwording* bij gebruikers; op aanpassing van het technologische *systeem*; en op de ontwikkeling van *sociale normen*.¹⁴ De volgende paragrafen behandelen het debat over deze oplossingen zoals gevoerd in de geanalyseerde literatuur.

1.3.1 Bewustwording (I)

De oplossing die gebruikers bewust(er) wil maken van de risico's van participatie, veronderstelt dat meer kennis en inzicht leiden tot minder ontsluiting en meer afscherming van persoonlijke informatie. "Awareness is key to solving the solution", aldus Barnes (2006). Vooropgesteld geloven de meeste auteurs dat gebruikers, hoe jong ook (De Souza & Dick, 2008), min of meer bewuste afwegingen maken in wat zij wel en niet online plaatsen. Volgens een aantal van hen worden de risico's echter onderschat. Zo ontwaart Mooradian een *false sense of privacy* in het gebrek aan inzicht in de technologische architectuur en het businessmodel van sociale netwerksites (2009: 169). Tufekci (2008) observeert dat gebruikers hun gedrag weliswaar afstemmen op huidige zorgen, maar niet op toekomstige problemen.¹⁵ Boyd & Ellison (2007), Rosen (2007), Livingstone (2008) en De Souza & Dick (2008) wijzen erop dat 'vrienden' op sociale netwerksites niet hetzelfde zijn als echte vrienden, maar online wel als zodanig vertrouwd worden.¹⁶ Ibrahim (2008) ziet in de stimulering van bewustwording een belangrijke taak weggelegd voor de overheid.

Een eerste kanttekening bij de notie van bewustwording is de aanzienlijke mate van rationaliteit of autonomie die zij bij gebruikers veronderstelt. Met het oog op de sociale werkelijkheid wordt die rationaliteit door veel auteurs weliswaar aangehaald, maar tegelijkertijd gerelativeerd. Zo onderscheiden De Souza & Dick (2008: 145) alsook Ibrahim (2008: 247) groepsdruk en 'kuddegedrag' als sterke motivaties om persoonlijke informatie te delen. Livingstone merkt op dat gebruikers beperkt worden door de normen en praktijken in hun vriendengroep, waarvan zij niet uitgesloten willen worden (2008: 8; 12). Boyd (2007) en

13 In acht van de zeventien geanalyseerde bronnen wordt de term 'risico' gebruikt. Drie daarvan noemen de term in de titel.

14 Soms worden meerdere strategieën voorgesteld binnen één artikel.

15 Tufekci schrijft dit toe aan het overnemen van vertrouwde manieren van grensafbakening in de fysieke ruimte, zonder rekenschap te geven van het blijvende en doorzoekbare karakter van online informatie. Zij wijst echter ook op de neiging van de jeugd om 'in het moment' te leven

16 De Souza & Dick ondervonden dat jongeren vaak persoonlijke en gevoelige informatie delen met 'vrienden' die zij nauwelijks kennen. Livingstone ondervond dat gebruikers vaak persoonlijke informatie delen met honderden 'vrienden' die zij slechts terloops kennen en zich soms zelfs niet eens herinneren (2008: 10; 12).

Tufekci (2008) wijzen op de sociale druk om vriendschapsverzoeken te accepteren van ouders, collega's of andere personen ten opzichte waarvan het individu zich in een afhankelijke positie bevindt. Gebruikers hebben bovendien geen controle over wat er gebeurt op profielen van hun connecties, waarmee zij wel geassocieerd worden (Dwyer, Hiltz & Passerini, 2007; Boyd, 2010). Het in toenemende mate mobiele internet radicaliseert de afhankelijkheid van anderen bovendien doordat foto's gemaakt met een mobiele telefoon direct kunnen worden geüpload (Martens et al., 2008: 72).

Ook is niet altijd op voorhand duidelijk hoe onschuldig of omstrede persoonlijke informatie precies is. Tufekci (2008) wijst erop dat van gedeelde informatie zoals favoriete boeken, politieke voorkeur of favoriete quotes nog geen (negatieve) implicaties gerapporteerd zijn, omdat sociale netwerksites eenvoudigweg nog niet lang genoeg bestaan en het merendeel van de gebruikers nog geen verantwoordelijke maatschappelijke functies uitoefent.

In feite kan een al te 'bewuste' omgang met sociale netwerksites zelfs tot ongewenste consequenties leiden. Over dertig jaar zal het voor journalisten ongekend eenvoudig zijn om over willekeurige, al dan niet publieke personen compromitterende informatie te vinden. Dergelijke gegevens komen bovendien al boven water voordat een persoon überhaupt tot een hoge positie weet door te dringen; Tufekci voorspelt een 'filtering' in een vroeg stadium van de carrière, met drastische consequenties voor de eigenschappen van degenen die dit proces doorstaan. Dit negatieve aspect van bewustwording wordt door verschillende auteurs gearticuleerd als effect van permanente surveillance en internalisering van sociale normen in een 'decentraal panopticum', verwijzend naar de machtstheorie van Michel Foucault (Andrejevic, 2006; Barnes, 2006; Martens et al., 2008).

Rosenblum (2007) bepleit een zwakkere variant van 'bewustwording' in de vorm van *common sense*; een praktisch gereedschap dat individuen helpt stil te staan bij wat zij online plaatsen. Deze *common sense*-strategie biedt volgens hem echter eerder een intuïtieve richtlijn dan een concrete oplossing. Meer dan het ideaal van rationele bewustwording, houdt deze benadering voor ogen dat morele schade weliswaar beperkt kan worden, doch niet uitgesloten.

1.3.2 Aanpassing van technologie (II)

De oplossing in termen van technologie veronderstelt dat de huidige systemen gebruikers niet in staat stellen controle uit te oefenen op de manier waarop zij dat willen.¹⁷ Een eerste technologische argument pleit voor de ontwikkeling van flexibelere systemen. Boyd (2010) stelt dat differentiatie in de afscherming van verschillende soorten persoonlijke informatie makkelijker moet worden. Daarnaast zouden publieksgroepen makkelijker 'gesegregeerd' moeten kunnen worden. Jongeren houden er een graduele conceptie van vrienden op na, waarop de binaire classificatie in 'vrienden' versus 'de rest van de wereld' die sociale netwerksites hun gebruikers opleggen niet aansluit (Livingstone, 2008; Solove, 2007: 203). Terwijl mensen om uiteenlopende redenen online vriendschappen aangaan, hanteren sociale netwerksites slechts één brede categorie; Mooradian spreekt van 'ruwe tools' (2009: 173). Solove noemt de huidige opties 'sociologisch simplistisch' (2007: 202). Met betrekking tot de afhankelijkheid van vrienden die er andere opvattingen over privacy op nahouden, pleiten Preibusch et al. (2007) voor de ontwikkeling van flexibele 'privacytools' die rekenschap geven van de specifieke privacybehoeften in een netwerk.

Een tweede argument roept aanbieders van sociale netwerksites op impliciete normen in de door hen ontwikkelde technologie te incorporeren. Volgens Solove prefereert de architectuur van sociale netwerksites nu openheid boven privacy (2007: 200-201). Dit wil zeggen dat de standaardinstellingen zodanig zijn geprogrammeerd dat gebruikers geen controle hebben over wat zij op welke manier delen, totdat zij de instellingen expliciet wijzigen (Krishnamurthy & Willis, 2008; boyd, 2010). Sociale netwerksites wordt een rol toegeschreven in het stimuleren van meer of minder zichtbaarheid. Waar gebruikers van sites als Facebook en MySpace vaker geneigd zijn hun profielen af te schermen voor niet-vrienden, is het merendeel van de statusupdates op Twitter voor iedereen zichtbaar en doorzoekbaar (Ibrahim, 2008: 247; Xiao & Varenhorst, 2009: 29). De Souza & Dick identificeren bovendien een bescheiden morele sturing in de gebruikersinterface van sociale netwerksites, waarbij automatisch verschijnende *templates* de gebruiker stimuleren de gevraagde informatie op te geven (2008: 146).¹⁸ Verschillende auteurs benadrukken de morele opdracht van de bedrijven achter sociale netwerksites (Solove, 2007: 201; Krishnamurthy & Willis; 2008: 42; Xiao & Varenhorst, 2009: 32; boyd, 2010).¹⁹

17 Opmerkelijk genoeg heeft de academische literatuur nauwelijks aandacht voor de recentelijk op de markt verschenen software die op het probleem inspeelt. Alleen Martens et al. noemen kort 'gespecialiseerde bedrijven' die tegen betaling diensten aanbieden "om de online identiteit in de gaten te houden en/of op te poetsen. Ze nemen bijvoorbeeld contact op met sites die ongewenste informatie verspreiden en dringen erop aan die te verwijderen" (2008: 56). Hieruit kan worden geconcludeerd dat het privacydebat zoekt naar oplossingen *binnen* de sociale netwerktechnologie.

18 Een derde van de door de onderzoekers ondervraagde gebruikers van MySpace in de leeftijdscategorie van 12 tot 18 jaar gaf aan het eens te zijn met de stelling 'I posted the information because MySpace had a field for it'.

19 Martens et al. beschouwen het leggen van meer verantwoordelijkheid bij internetbedrijven als 'de Amerikaanse aanpak', waarvoor volgens hen ook in Europa steeds meer stemmen opgaan (2008: 59).

Een eerste kanttekening bij de technische oplossingen luidt dat de middelen om controle uit te oefenen te complex zijn. Het zou voor iedere gebruiker op eenvoudige wijze mogelijk moeten zijn de privacyinstellingen te begrijpen en aan te passen. Livingstone (2008: 12) en Mooradian (2009: 168) observeren dat gebruikers hun gebrek aan kennis en vaardigheden 'oplossen' door geavanceerde opties te negeren. Xiao & Varenhorst wijzen met betrekking tot Twitter op de effecten van systeemaanpassingen op de gebruikerservaring; zij veroorzaken irritaties, zijn gemakkelijk te negeren, of impliceren beperkingen zoals verminderde vindbaarheid door vrienden en het missen van *tweets* wegens beperkte bewaargeschiedenis (2009: 30).

Ten tweede wordt betwijfeld of de technologie de complexiteit van de werkelijkheid kan benaderen. Het differentiëren naar verschillende categorieën informatie en publieksgroepen impliceert het vastleggen van iets wat dynamisch is. Zo vallen mensen vaak in meer dan één categorie en kunnen vraagtekens geplaatst worden bij de morele wenselijkheid van labels als 'kneuzen'. Gebruikers zouden bovendien sociale druk kunnen ervaren bij het categoriseren van connecties.²⁰

De 'moralisering' van de technologie wordt bovendien geproblematiseerd door de commerciële leest waarop sociale netwerksites geschoeid zijn. Rosenblum (2007) en Ibrahim (2008) merken op dat de bedrijven achter sociale netwerksites geen belang hebben bij het instellen van toegangsbeperkingen; dit zou de open communicatie ondermijnen die nu juist de aantrekkingskracht – en het hoogst lucratieve potentieel²¹ – van deze sites vormt. De dreiging dat grote aantallen gebruikers hun profiel zullen opheffen is voor bedrijven als Facebook bovendien van weinig betekenis, aangezien dit volgens boyd (2010) geen optie is voor het merendeel van de (kern)gebruikers, die daadwerkelijk iets te verliezen hebben in wat een belangrijk deel van hun dagelijks leven is gaan uitmaken. Ten slotte wijzen De Souza & Dick (2008) op het gemak waarmee technologische regulering valt te omzeilen doordat de gegevens die gebruikers invullen, zoals leeftijd, moeilijk te verifiëren zijn.²²

20 De overwegingen in deze alinea zijn ontleend aan de presentatie 'Social Network Sites, Privacy and Publicity' die danah boyd gaf ter gelegenheid van een symposium van het Tilburg Institute for Law, Technology and Society (TILT), Universiteit van Tilburg, 7 april 2010.

21 Tijdens het symposium 'Social Network Sites, Privacy and Publicity', georganiseerd door het Tilburg Institute for Law & Technology (7 april 2010) kwam naar voren dat niet-commerciële sociale netwerksites in de praktijk niet erg levensvatbaar zijn.

22 MySpace hanteert bijvoorbeeld een leeftijdsgrens, waarbij profielen van gebruikers jonger dan 16 jaar standaard niet-openbaar zijn en meerderjarige gebruikers niet zomaar vrienden met hen kunnen worden. Aangezien de ingevulde leeftijd niet wordt geverifieerd wordt het systeem moeiteloos gemanipuleerd (De Souza & Dick, 2008).

1.3.3 Sociale normen (III)

Een derde oplossing veronderstelt een gebrek aan passende normen en waarden om de praktijken op sociale netwerksites in goede banen te leiden. Dat een heleboel persoonlijke informatie zichtbaar is geworden, wil immers nog niet zeggen dat de samenleving weet hoe zij hiermee moet omgaan; zij beschikt (nog) niet over de taal en de sociale normen die daarvoor nodig zijn (boyd, 2007). In plaats van morele oordelen te rationaliseren of uit te besteden aan technologische systemen, moet een maatschappelijk debat gevoerd worden over omgangsvormen in de nieuwe ruimtes die tegelijkertijd privé en publiek zijn (idem; Rosenblum, 2007).

Boyd (2007) ziet in sociale netwerksites niet per se een ondermijning van bestaande waarden en normen, maar juist een ruimte om hiermee te experimenteren, zoals publieke ruimten dat altijd geweest zijn.²³ Inderdaad wordt met de 'sociale textuur' van de netwerksites volop geëxperimenteerd. Dit zag boyd bijvoorbeeld gebeuren met het fenomeen van 'fakesters' – nepprofielen van veelal beroemde personen op MySpace. In dergelijke praktijken ontwikkelen zich in online omgevingen sociale normen en verwachtingen, bijvoorbeeld ten aanzien van het gebruik van echte naam of nickname. Ook Tufekci benadrukt de sturende rol van de intenties waarmee mensen sociale media gebruiken. Martens et al. doen in dit kader een oproep tot 'eigenlijkheid'; te midden van de totale zichtbaarheid ligt volgens hen de mogelijkheid om 'iets nieuws te beginnen': "Juist in zoverre het internet zich aan elke externe controle onttrekt, ontstaat de noodzaak dat wij *onszelf* in acht nemen" (2008: 31).

Om dit proces te bespoedigen doen de voorstanders van het normatieve debat een oproep aan ouders, docenten of meer in het algemeen 'opvoeders' om sociale netwerksites te omarmen in plaats van af te wijzen en daarbij te leren van de jongeren (De Souza & Dick, 2008; Ibrahim, 2008; boyd, 2007). Boyd (idem) en Tufekci (2008) benadrukken dat de ontwikkeling van sociale normen niet bestaat uit het opleggen van zwart-witte regels, maar uit een 'conversatie' en een 'dialog' over hoe 'de samenleving' wil omgaan met verschuivende grenzen. Er zijn geen goede antwoorden; enkel afwegingen en keuzes in normatieve vragen als: Welke informatie deel je wel en niet online? Wat is het verschil tussen offline en online vrienden? Is de aandacht die bepaalde foto's genereren de aandacht die je werkelijk wil? En wanneer spreek je op 'onverantwoordelijke' wijze over anderen (Solove, 2007: 135)?

Twee auteurs richten zich specifiek op de ontwikkeling van normen bij het publiek. Daniel Solove stelt een *grand normative experiment* voor waarin de maatschappij genoeg neemt met minder persoonlijke informatie (2007: 65-66). Daartoe zouden sociale netwerksites in de gebruiksvoorwaarden een 'belofte van vertrouwelijkheid' moeten opnemen; personen die de informatie op profielen van anderen bekijken moeten rekenschap geven van de voorkeuren van de eigenaar van die informatie (idem: 192). Ook bepleit hij dat werkgevers sollicitanten ervan op de hoogte stellen dat zij hen 'googlen', zodat deze personen ten minste een

²³ Boyd ontleent deze opvatting van de publieke ruimte aan de filosoof Hannah Arendt (1998).

weerwoord hebben (idem: 203). Tufekci (2008) borduurt voort op David Brins *The Transparent Society* (1999) in haar voorzichtige stelling dat toegenomen zichtbaarheid in combinatie met tijd en gewenning stigma's en taboes kan wegnemen, zoals bijvoorbeeld op homoseksualiteit.²⁴

Ook de oplossing op basis van sociale normen kent kanttekeningen. Solove erkent in zijn pleidooi voor een maatschappelijke waarde van vertrouwelijkheid zelf al dat dergelijke ethische codes moeilijk af te dwingen zijn. Ook boyd (2007) waarschuwt voor naïviteit in het argument dat 'niet alles mag wat technisch kan'; de hoge mate van anonimiteit die sociale netwerksites waarborgen ondermijnen immers juist gedrag op basis van normen en waarden. Barnes (2006), Andrejevic (2006)²⁵ en boyd (2007) wijzen in dit kader op het probleem van asymmetrische machtsverhoudingen; de *unwanted gaze* (Tufekci, 2008) vertegenwoordigt typisch personen met een machtspositie ten opzichte van het individu, zoals ouders, leraren, werkgevers, pedofielen, maar ook bepaalde leeftijdsgenoten.

24 Iets vergelijkbaars zag Tufekci (2008) gebeuren met betrekking tot de ontdekking van vroeger softdrugsgebruik bij Amerikaanse politici, dat inmiddels als een weinig opzienbarende jeugdzonde geaccepteerd wordt.

25 Barnes (2006) en Andrejevic (2007) verwijzen naar het concept van het panopticum zoals uiteengezet door Michel Foucault en vertalen dit naar een decentrale vorm van surveillance, waarin potentieel 'iedereen iedereen bekijkt'.

1.4 Evaluatie van de oplossingen

Het probleem wordt in het academische privacydebat veelal gedefinieerd in termen van controle van gebruikers over de toegang van anderen tot hun persoonlijke informatie. De oplossingen in termen van het stimuleren van bewustwording en aanpassen van technologie en/of standaardinstellingen suggereren dat persoonlijke informatie die online gedeeld wordt controleerbaar en beheersbaar is – in het eerste geval door gebruikers bewust te maken van het open karakter van de informatietechnologie, in het tweede geval door het open karakter van de informatietechnologie in te dammen volgens principes van de (eerder besloten) ongemedieerde interactie. De complexe, rationele aard van de oplossingen gaat voorbij aan de sociale en economische dynamiek waarmee de technologie verweven is.

De derde oplossing, in termen van de ontwikkeling van sociale normen om met de nieuwe situatie om te gaan, gaat juist uit van die sociale dynamiek. De problemen worden volgens de aanhangers van deze visie niet zozeer veroorzaakt door de technologie, maar door de mensen die haar op onverantwoorde wijze gebruiken. Twee auteurs articuleren, naast gebruikers of bedrijven, specifiek de normatieve rol van het publiek op sociale netwerksites. Hoe een moreel wenselijke omgang met online gedeelde persoonlijke informatie tot stand moet komen zonder formele regulering, die doorgaans problematisch wordt bevonden,²⁶ is onzeker. Het hier en daar doorklinkende vertrouwen in de uitkomst van het normatieve 'experiment' is nog weinig theoretisch onderbouwd.

Overigens is met het wijzen op de interne contradicties en beperkingen van de oplossingen in het huidige debat niet gezegd dat deze strategieën geen enkele waarde hebben. De bevordering van bewustwording (in de zin van *common sense*), aanpassing van de standaardinstellingen en een open conversatie kunnen vruchten afwerpen in met name de bescherming van minderjarigen²⁷ en andere kwetsbare groepen.²⁸ In de volgende hoofdstukken wordt echter gezocht naar een meer structurele en theoretisch onderbouwde oplossing voor de privacykwestie rond sociale netwerksites.

26 Danah boyd (2010) spreekt zich recentelijk wel nadrukkelijk uit voor regulering van bovenaf. Solove (2007) beschouwt formele (juridische) regulering als een oplossing in *laatste* instantie.

27 Regelmatig wordt in de literatuur een relatie met leeftijd gelegd (bijvoorbeeld Barnes, 2006; boyd, 2007; Livingstone, 2008; Ibrahim, 2008), waarbij zeer jonge gebruikers 'verantwoordelijker' gedrag vertonen naarmate zij ouder worden (De Souza & Dick, 2008: 152). Zo neemt volgens Tufekci (2008) de neiging om politieke voorkeur, 'burgerlijke staat', seksuele oriëntatie en telefoonnummer in te vullen af met het toenemen van leeftijd.

28 Ibrahim spreekt van 'uitbuiting van kwetsbare groepen' (2008: 246). Boyd (2010) benadrukt eveneens de hulp die minder technisch vaardige gebruikers nodig hebben, alsook gebruikers die het Engels niet machtig zijn. Ten slotte vormen vrouwen een relatief kwetsbare groepen, waarvan zij zich volgens Tufekci (2008) redelijk bewust zijn; de mannelijke studenten in haar onderzoek hebben significant vaker dan vrouwelijke studenten een openbaar profiel.

2. Sociale netwerksites en de risicomaatschappij

Dit hoofdstuk analyseert het privacydebat in termen van de risicomaatschappij van Ulrich Beck. In hoeverre kunnen de gegeven probleemdefinitie en voorgestelde oplossingen begrepen worden in termen van controle, risico, moderniteit en reflexiviteit? Welke alternatieve probleemstelling kan op basis daarvan geformuleerd worden?

2.1 Van rationaliteit naar reflexiviteit

De Duitse socioloog Ulrich Beck stelt in zijn boek *Risk Society: Towards a New Modernity* (1992) dat de moderne samenleving, gekenmerkt door complexe techno-wetenschappelijke ontwikkelingen, een 'risicomaatschappij' is geworden. Dit betekent niet dat er meer risico's zijn dan voorheen, maar dat de samenleving in toenemende mate bezig is met het bediscussiëren, controleren en voorkomen van risico's die zichzelf veroorzaakt (2006: 332). Deze 'gefabriceerde' onzekerheden worden niet overwonnen door meer kennis; zij zijn juist het resultaat van meer kennis. De risicomaatschappij moet dan ook niet gezien worden als de crisis, maar als de *overwinning* van het modernistische project; de 'radicalisering' van de moderniteit dwingt tot reflectie op de vooruitgang en haar onvoorziene en ongewenste neveneffecten. Hierin identificeert Beck een 'tweede' of 'reflexieve moderniteit' (2006: 336; 338).

Een risico moet worden onderscheiden van een ramp, in die zin dat risico bestaat in de anticipatie op een ramp: "Risks are always *future* events that *may* occur, that *threaten* us" (2009: 9). Risico's zijn daarmee volgens Beck niet 'echt', maar verkeren in een constante staat van virtualiteit (2006: 332).²⁹ Over hun aard bestaat onenigheid; risico betekent conflict, ambivalentie (2009: 48). In de risicomaatschappij worden risico's dan ook 'geënceneerd'. De 'enscenering van risico' verplicht tot preventief handelen (idem: 12-13).³⁰ Dit is problematisch, aangezien de ware dreiging nu juist uitgaat van de onbedoelde en onvoorziene neveneffecten van technologie en wetenschap; de door de mens zelf gecreëerde risico's en onzekerheden, waarop niet geanticipeerd kan worden. Beck duidt deze complexe techno-wetenschappelijke fenomenen – zoals bijvoorbeeld klimaatverandering of biotechnologie – aan als *unknown unknowns*: "We don't know what it is we don't know" (2006: 329).

De instrumenten die de instituties van de moderniteit – de overheid, de wetenschap, het bedrijfsleven en het militair apparaat – zijn geworteld in de moderne principes van

²⁹ Beck stelt het als volgt: "Risks are not 'real', they are 'becoming real'" (2006: 332).

³⁰ Beck benadrukt in zijn werk de politieke dimensie van de risicomaatschappij. Risico's worden 'geënceneerd'; zij weerspiegelen culturele percepties. Een risico kan door de één als urgent, dreigend en echt gevoeld worden, terwijl zij voor de ander verwaarloosbaar of onwerkelijk is. Hoe minder berekenbaar het risico, hoe meer gewicht culturele percepties van risico in de schaal leggen. De encenering van risico betekent niet dat risico's een illusie zijn of een sensationalistisch mediafenomeen. Het impliceert alleen dat risico geen objectief meetbare kwantiteit is. De realiteit van risico ligt juist in haar controversiële karakter; in haar diverse beoordelingen door groepen of 'risicoculturen' (2009: 12-13).

rationaliteit, beheersing en controle en daarmee niet in staat het onberekenbare te berekenen. Autoriteiten als politici en wetenschappers moeten dus beslissingen nemen op basis van tegenstrijdige visies of wat Beck een radicaal 'niet-weten' noemt. Daarmee maken zij deel uit van het probleem dat zij verondersteld zijn op te lossen; de gedwongen belofte van veiligheid en zekerheid kan daarom 'ironisch' genoemd worden (2006: 332; 336).

Met deze ondermijning van de positie van deskundigen, die zich immers niet langer, of ten minste niet meer dan 'leken', kunnen beroepen op de berekening van objectieve, rationele risico's (2009: 11-12), komt de verantwoordelijkheid te liggen bij de 'verantwoordelijke consument'. Tegelijkertijd blijft die consument afhankelijk van de definiërende macht van de 'expertsystemen' wiens oordeel zij niet kunnen, maar wel moeten vertrouwen. Beck spreekt van een 'tragische individualisering' (2006: 336).

2.2 Sociale risiconetwerken

Om na te gaan in hoeverre de risico's die worden toegeschreven aan het gebruik van sociale netwerksites gelden als de 'gefabriceerde risico's' die Beck beschrijft, kunnen zij worden getoetst aan de hand van drie eigenschappen waarmee Beck hen onderscheidt van traditionele catastrofes, namelijk delokalisatie, onberekenbaarheid en non-compenseerbaarheid (2006: 333-335).

Een eerste eigenschap van gefabriceerde, mondiale risico's is 'delokalisatie'. Dat wil zeggen dat causale verbanden tussen oorzaken en gevolgen zich niet beperken tot één geografische locatie, maar alomtegenwoordig zijn. Op temporeel niveau kent de participatie in sociale netwerksites inderdaad een *long latency period*; de negatieve effecten van het online plaatsen van persoonlijke informatie doen zich vaak pas op lange termijn voor – wanneer een persoon zich wellicht niet meer identificeert met vroegere uitspraken of bijvoorbeeld een publieke functie ambieert. In ruimtelijk opzicht is de informatie op sociale netwerksites in potentie voor iedereen ter wereld met een internetverbinding zichtbaar en doorzoekbaar. Hierbij moet overigens een kanttekening geplaatst worden bij de mate waarin sociale netwerksites *mondiale* risico's impliceren zoals Beck die beschrijft. Boyd & Ellison (2007) noemen sociale netwerksites een wereldwijd fenomeen. Hoewel deze sites via het internet voor iedereen toegankelijk zijn, observeren de auteurs dat zij in de praktijk veelal homogene gebruikersgroepen aantrekken. Die segregatie volgt onder meer de lijnen van nationaliteit, leeftijd en opleidingsniveau. Voorts wijzen de auteurs op de rol van taal- en cultuurverschillen in de ontwikkeling van een wereldwijde lappendeken van sociale netwerksites. De ontwikkeling van een 'mondiale sociale netwerksite' ligt om deze redenen niet voor de hand. Desalniettemin fungeren zoekmachines wel degelijk als zodanig, door met één zoekopdracht gegevens uit verschillende sociale netwerksites te doorzoeken en geïntegreerd te presenteren.

Een tweede eigenschap van de risico's die Beck beschrijft is onberekenbaarheid. Risico's zijn hypothetisch; over hun aard bestaat onzekerheid en conflict. Sociale netwerksites zijn een *unknown unknown* bij uitstek; nooit eerder was persoonlijke communicatie permanent en wereldwijd beschikbaar en de praktijken rond deze sites ontwikkelen zich snel. Wetenschappelijke experimenten zijn beperkt tot het bestuderen van motivaties, handelingen en incidenten die zich daadwerkelijk voordoen en die men in staat is te benoemen. De crux is nu juist dat incidenten plaatsvinden doordat ze niet geanticipeerd werden en in essentie onvoorzienbaar zijn (Beck, 2009: 47-48). Een voorbeeld van het anticiperen op de verkeerde, want meest voor de hand liggende risico's, is de veelgenoemde beperking van de zichtbaarheid van profielen tot 'alleen vrienden'. Deze vorm van bescherming veronachtzaamt de mogelijkheid van schade uit onverwachte hoek.³¹ Door minder zichtbare en daardoor minder anticipeerbare risico's op die manier 'obscur' te maken, worden deze risico's enkel acuter. Genoemde voorbeelden van onvoorzienbare en ongewenste bijproducten van de anticipatie op risico zijn vergaande zelfcensuur (Tufekci, 2008) en wat Boyd & Ellison (2007) aanmerken als 'sociale drama's'.

Ten slotte zijn Becks gefabriceerde risico's niet compenseerbaar. Wanneer complexe technologieën schade veroorzaken kan die schade vaak niet hersteld of gecompenseerd worden. Ook dit is van toepassing op sociale netwerksites. Door de exponentiële verspreiding van informatie via de netwerkstructuur van het internet is de keten die de schade veroorzaakt al snel niet meer herleidbaar en zijn pogingen de informatieverspreiding te stoppen, laat staan ongedaan te maken, vaak tevergeefs (Boyd, 2007). Daarom richt het wetenschappelijke privacydebat zich, gelijk de moderne instituties van de risicomaatschappij, op het voorkomen van risico's, zelfs wanneer de aard of het bestaan ervan onduidelijk is. Anderzijds valt immers ook niet vast te stellen dat sociale netwerksites op termijn *niet* schadelijk zullen zijn of *geen* ingrijpende transformaties teweeg zullen brengen (gehele paragraaf, tenzij anders vermeld: Beck, 2006: 333-335).

³¹ Een rekenvoorbeeld bij de privacyinstelling 'vrienden van vrienden', dat de indruk van vertrouwelijkheid wekt: Wanneer een individu 100 online vrienden heeft en ieder van die vrienden evenzo, is informatie op het profiel van dat individu voor $100 \times 100 = 10.000$ personen beschikbaar.

2.3 Reflexieve netwerksites: ambivalente vooruitgang

Het debat over de privacyparadox weerspiegelt de ambivalente verhouding tot technologische 'vooruitgang' die Beck kenmerkend acht voor de reflexieve moderniteit. Mark Zuckerberg, oprichter en directeur van Facebook, articuleert in een artikel in *The Washington Post* (24 mei 2010) een normatief communicatie-ideaal dat resoneert in een groot deel van de wetenschappelijke literatuur: "People want to share and stay connected with their friends and the people around them. If we give people control over what they share, they will want to share more. If people share more, the world will become more open and connected. And a world that's more open and connected is a better world." Dit communicatie-ideaal gaat vooraf aan de geschiedenis van sociale netwerksites, die niettemin verondersteld worden eerdere communicatietechnologieën weergaloos voorbij te streven in het benaderen ervan.

De ontwikkeling van communicatietechnologieën die openheid en verbondenheid voorstaan kan een modernistische oorsprong toegeschreven worden. Martens et al. schetsen een historische ontwikkeling die heeft geleid tot de huidige anonieme levenswijze in de moderne steden (2008: 34). Ontwikkelingen als de scheiding van het publieke (werk-) en privé-domein, de verlengde studietijd en de toename van het aantal alleenstaande huishoudens betekenden een breuk met de pre-moderne leefgemeenschap. De moderne mens moest op zoek naar nieuwe manieren om vertrouwen op te bouwen en uiting te geven aan identiteit en gemeenschapsgevoel (Nock, 1998). Het toenemende aantal geografisch sterk verspreide netwerken waarvan individuen deel uitmaken, vraagt om communicatiemiddelen die afrekenen met beperkingen van ruimte en tijd (Giddens, 1991: 47). In een artikel in de *New York Times* merkt Clive Thompson (2008) op dat sociologen zich lange tijd afgevraagd hebben hoe de mensheid zich zou aanpassen aan de anonimiteit van het leven in de stad – "a world of lonely people ripped from their social ties." De 'gemedieerde gemeenschap' die sociale netwerksites constitueren kan beschouwd worden als het technisch-rationele antwoord op die situatie.

In de proliferatie van sociale netwerksites ontstaan nu sociale transformaties die in het wetenschappelijke vertoog als 'onbekend' aangemerkt worden (bijvoorbeeld boyd, 2007). Deze onzekere 'bijproducten' zijn net als de neveneffecten van de moderniteit die Beck beschrijft onafwendbaar voor gebruikers in wiens leven sociale netwerksites dermate diep geïntegreerd zijn geraakt in hun sociale leven dat gesproken kan worden van afhankelijkheid van het systeem (boyd, 2010). Precies in de radicalisering van een modern communicatie-ideaal, waarbij zij in haar eigen vervolmaking onvoorziene en ongewenste effecten sorteert die de samenleving dwingen tot reflectie – tot uiting komend in de ongeruste en ambivalente reacties in zowel populair als wetenschappelijk discours – kunnen sociale netwerksites beschouwd worden als een manifestatie van de reflexieve moderniteit.

2.4 Van privacyparadox naar controlecontroverse

Nu het privacydebat rond sociale netwerksites geconceptualiseerd is in termen van de gefabriceerde risico's en de reflexieve moderniteit van Ulrich Beck, kan een alternatieve probleemdefinitie opgesteld worden. De privacyparadox ging uit van een discrepantie tussen wat gebruikers *denken* (het streven naar controle) en wat zij *doen* (het ondermijnen van controle). Het perspectief van de risicomaatschappij identificeert daarentegen de eigenlijke contradictie in het denken over controle zelf. Op vergelijkbare wijze als in technowetenschappelijke kwesties als bijvoorbeeld klimaatverandering, financiële markten en terrorisme, weerspiegelt het privacydebat rond sociale netwerksites een *ideaal* van controle dat in de zowel technisch als sociaal complexe *praktijk* ondermijnd wordt. Een adequatere probleemstelling kan daarom, liever dan als een privacyparadox, geformuleerd worden als een 'controlecontroverse': Hoe kan controle worden verkregen over via sociale netwerksites gedeelde persoonlijke informatie, wanneer die controle nu juist onmogelijk is?

3. De controlecontroverse als kosmopolitisch moment

Nu de probleemstelling in het privacydebat rond sociale netwerksites geherformuleerd is in termen die compatibel zijn met Becks these van de risicomaatschappij, rijst de vraag hoe deze 'controlecontroverse' opgelost kan worden. Kan aan de controlecontroverse een 'verlichtende functie' toegeschreven worden in de vorm van een 'kosmopolitisch moment'? Hoe kan dit 'moment' met de socioloog-filosoof Bruno Latour worden voorgesteld in de alledaagse context van het gebruik van sociale netwerksites?

3.1 Van ironie naar verlichting

Beck onderscheidt drie mogelijke reacties op de alomtegenwoordigheid van risico. Een typisch modernistische reactie is volgens hem de 'ontkenning' van controleverlies. Een in postmodern nihilisme tot uiting komend antwoord is 'apathie' of onverschilligheid. Beck treedt voorbij deze patstelling door een alternatieve reactie te verkennen, namelijk 'transformatie'. Deze reactie constitueert volgens hem het normatieve referentiekader van de risicomaatschappij (2009: 47). De mondiale risicomaatschappij heeft volgens Beck een 'verlichtende functie', omdat zij nieuwe voorwaarden schept voor gezamenlijk handelen. Hij licht dit idee toe met behulp van de filosoof Hannah Arendt (1998). Volgens Arendt schept de schok van een existentiële dreiging de mogelijkheid van een nieuw begin. De 'verwachting van het onverwachte' betekent immers dat het vanzelfsprekende niet langer voor vanzelfsprekend kan worden aangenomen. Van de ontwikkeling van iets nieuws en onbekends gaat een louterende werking uit, juist omdat ambivalente reacties ontstaan en daarmee een discussie op gang kan komen (2009: 48-9).

Beck beschrijft hoe de (anticipatie op) mondiale risico's in feite *iedereen* bedreigt. Overal ter wereld worden mensen met uiteenlopende sociaal-economische, politieke of culturele achtergronden abrupt en onvrijwillig met elkaar – met de voorheen uitgesloten 'ander' – geconfronteerd. Zij moeten betekenis verlenen aan hun leven in de uitwisseling met anderen in plaats van met mensen zoals zichzelf, of zij dit willen of niet (2009: 15; 56). Risico's zouden daarom afrekenen met typisch moderne grenzen en scheidingen en met denken in termen van 'wij versus zij' (2006: 331). De traumatische ervaring dat iedereen kwetsbaar is resulteert volgens Beck in het nemen van verantwoordelijkheid voor anderen, niet uit altruïsme maar met het oog op de handhaving van het zelf (2009: 57). Beck noemt dit het 'kosmopolitische moment'. Een dergelijk 'kosmopolitisme' is niet puur filosofisch en normatief, elitair en idealistisch – en daarmee geen *wishful thinking* – maar is de realiteit zelf geworden; zij overkomt de samenleving ongezien en onbedoeld 'door de achterdeur' (idem: 61; 66).

3.2 De controlecontroverse als kosmopolitisch moment

De gevonden parallellen met de risicomaatschappij doen vermoeden dat ook de 'controlecontroverse' over sociale netwerksites een verlichtende functie kent. Nu gaan de in het eerste hoofdstuk behandelde oplossingen in termen van bewustwording en aanpassing van het systeem een normatieve transformatie eerder uit de weg. Deze 'techno-wetenschappelijke' oplossingen blijven immers controle nastreven, waarmee Beck hen tot typisch moderne reacties zou rekenen.³² De derde oplossing, gezocht in de ontwikkeling van sociale normen, lijkt meer compatibel met de transformatie die Beck voorstaat.

Het relatief ontbreken van ruimtelijke en temporele afbakeningen op sociale netwerksites dwingt tot een confrontatie tussen jongeren, ouders, studenten, docenten, werknemers, werkgevers, overheden, bedrijven, vrienden en vijanden. Die confrontatie kan daadwerkelijk een nieuw begin betekenen,³³ wanneer zij aanleiding geeft tot gezamenlijke discussie over conflicterende waarden, in plaats van gedrag, beleid en systemen te modelleren naar een notie van 'controle' over een 'grens'. Het geanalyseerde privacydebat benadrukt dat in die maatschappelijke conversatie geen 'waarheid' bestaat; enkel overwegingen en keuzes. Dit komt overeen met Becks centrale argument, dat politieke actie niet het resultaat is van een 'universele consensus over waarden', die immers 'zelfs aan de eettafel' onmogelijk is, maar dat het geloof in de dreiging eenieder forceert in gezamenlijke actie (2009: 64). Verschillende betrokken partijen worden geacht van elkaar te leren; autoriteiten zoals opvoeders en wetenschappers – de 'deskundigen' – hebben evenveel in te brengen als actieve, vaak jongere gebruikers. De oproep aan opvoeders zelf ook te participeren in sociale netwerksites zorgt ervoor dat ook zij de 'oncontroleerbare kwetsbaarheid' (idem: 61) onder ogen zien die de basis vormt voor het kosmopolitische moment. Ook de in het debat gearticuleerde taboedoorbreking en emancipatie van minderheden als gevolg van zichtbaarheid kunnen gezien worden als manifestaties van het 'onvrijwillige' kosmopolitisme.

32 De door Beck onderscheiden postmoderne, apathische reactie lijkt het privacydebat over sociale netwerksites vreemd. Algemeen wordt aangenomen dat sprake is van een probleem en de relativering van dit probleem kan niet toegeschreven worden aan cynische gelijkstelling of verwerp van waarden.

33 Martens et al. articuleren zelfs letterlijk de mogelijkheid om te midden van de totale zichtbaarheid "iets nieuws te beginnen" en "onszelf in acht [te] nemen" (2008: 31).

3.3 Risico versus verwikkeling

Beck werkt zijn kosmopolitische moment uit op institutioneel niveau (2009).³⁴ Meer in het algemeen wordt de theorie van Beck een inherent 'universalisme' toegeschreven, dat weinig ruimte laat voor alledaagse 'onderhandelingen' over risico (Mythen, 2004: 8). De vraag hoe individuen in het dagelijks leven moeten omgaan met de alomtegenwoordigheid van risico, beantwoordt hij met een toevlucht in 'ironie' als het 'homeopathische, praktische, alledaagse tegengif tegen de risicomaatschappij' (2006: 345). Met het oog op sociale netwerksites kan een behulpzamer theoretisch kader gevonden worden in het antropologische perspectief op de these van Beck zoals geformuleerd door de Franse socioloog-filosoof Bruno Latour.³⁵

Volgens Latour zijn hedendaagse technologieën niet complexer dan vroeger, zoals Beck veronderstelt, maar worden ze nu pas als zodanig erkend. Daarmee introduceert de auteur een notie van continuïteit in de 'overgang' van moderniteit naar reflexieve moderniteit. Niet de wereld zou complexer geworden zijn; haar complexiteit wordt nu pas (h)erkend. De bewijslast voor de 're-moderniteit' komt daarmee te liggen op gegevens die aantonen dat de relatie is veranderd tussen 'wat de modernisten deden zonder dat zij het zeiden en waarvoor zij nu expliciet uitkomen', oftewel dat de collectieve *interpretatie* van technologie is veranderd (2003: 39).

Tot deze veronderstelling komt Latour door met terugwerkende kracht de praktijken van vroege modernistische wetenschappers te analyseren, die zoals ook Beck stelt in het teken stonden van beheersing van natuurlijke en sociale processen door middel van rationele beredenering en berekening. De modernisten waren uiterst bekwaam in het 'purificeren' van hun denken en handelen. Zo brachten zij scheidingen aan in de wetenschap, zoals die tussen object en subject, natuur en cultuur, alsook in maatschappelijke domeinen, zoals het onderscheid tussen een publiek- en privé-domein. Juist doordat de modernisten zichzelf zo puur en bevrijd voelden uit de ketens van het onverlichte verleden – Latour noemt dit *disentangled* – konden zij op ongekennd creatieve en efficiënte wijze alles op en buiten de aarde met elkaar verbinden. Alleen in de overtuiging dat wetenschap en samenleving twee gescheiden domeinen zijn, konden zij zo vergaand vervlochten raken als zij tegenwoordig zijn. Het vermogen 'met de rechterhand te negeren wat de linkerhand aan het doen is' ziet Latour als een ongekennde bron van vrijheid en creativiteit, die de modernisten zouden verliezen wanneer de ongewilde consequenties van hun handelen aan het licht zouden komen nog voor de oorzaken teweeg zijn gebracht (2003: 38-40).

34 Hoewel mondiale risico's de positie van de neoliberale staat ondermijnen, kan de staat aan hen ook nieuwe vormen van legitimatie ontleen. Beck pleit voor de ontwikkeling van een *cosmopolitan form of statehood* (2009: 66).

35 Het betreft een methodologisch commentaar getiteld 'Is Re-modernization Occurring – And If So, How to Prove It?' (2003). Latour bespreekt hierin de problematische toetsbaarheid van de these van Beck. Wanneer, zo vraagt hij zich af, zijn de neveneffecten van de moderniteit zo talrijk dat het moderne project onherkenbaar is getransformeerd? Hoe kan een modernist ervan overtuigd worden dat de 'eerste moderniteit' is geëindigd? De bewijslast ligt volgens Latour in de collectieve interpretatie, liever dan de substantiële verschuiving van technologische wetenschappelijke fenomenen.

De erkenning van barstjes in dit dichotome wereldbeeld is van relatief recente datum. Volgens Beck ontstond dit inzicht onder invloed van de complexiteit van de hedendaagse, techno-wetenschappelijke samenleving. Latour daarentegen veronderstelt dat de modernistische interpretatie van zichzelf nooit geheel adequaat haar eigen praktijk heeft beschreven. Volgens zijn actor-netwerktheorie was de mens altijd al diepgaand 'verwikkeld' in een 'netwerk', waaronder hij een 'labyrint van onverwachte associaties tussen heterogene elementen' verstaat – de volgende paragraaf gaat op dit concept nader in. 'Risico' houdt dan zoveel in als 'datgene dat afwijkt van het rechte pad van rede en controle'. Latour ontwaart in de moderne samenleving een discrepantie tussen zelf-representatie en praktijk, die hem uiteindelijk brengt tot de controversiële uitspraak dat 'wij nooit modern zijn geweest'. 'Re-modernisatie' zou betekenen dat mensen zich er nu wel van bewust zijn dat beheersing en bewustwording en daarmee controle over handelingen onmogelijk zijn; dat het bewustzijn is gerezen dat bewustzijn niet gelijkstaat aan volledige controle (idem: 36-37).

3.4 Het privacydebat als netwerk

Indien Latours theorie van toepassing is op sociale netwerksites, kan gesteld worden dat sociale interactie altijd al een onoverzichtelijk netwerk heeft betreft in plaats van recentelijk risicovol(ler) te zijn geworden. Hier zien we, net als Latour bij de modernisten observeerde, dat gebruikers met 'hun rechterhand' controle uitoefenen over de beschikbare informatie over henzelf in het (semi-)publieke domein, terwijl zij met 'hun linkerhand' die controle uit handen geven aan een onbekend, toekomstig publiek. Als ware modernisten zijn de gebruikers van sociale netwerksites in staat gebleken zodanig 'verwikkeld' te raken in een complex, heterogeen netwerk – sociale *netwerksites* vormen in die zin een letterlijke metafoor – *doordat* zij geloven in de scheiding tussen publiek en privé. Die discrepantie, of in termen van het geanalyseerde vertoog de 'paradox', heeft dan ook wel degelijk positieve aspecten – zij is in Latours termen 'functioneel' – die tot uiting komen in de uiteenlopende motivaties die in het debat worden onderscheiden voor het (online) delen van persoonlijke informatie (2003: 38-40). De volgende subparagrafen gaan na in hoeverre de praktijken op sociale netwerksites als een netwerk geconceptualiseerd kunnen worden bestaande uit heterogene 'quasi-objecten' en 'quasi-subjecten'.

3.4.1 Sociale netwerksites als quasi-objecten

Objecten en technologieën zijn voor Latour geen kale, objectieve feiten waarmee conflicten beslecht kunnen worden, maar complexe entiteiten die juridische of politieke, en dus sociale ordening nodig hebben. Hij spreekt daarom van 'quasi-objecten'. Wanneer sociale netwerksites hier als quasi-object geconceptualiseerd worden, wordt hun continuïteit met eerdere communicatiemiddelen benadrukt. Dit houdt geen ontkenning in van de eigenschappen van informatietechnologie die controle ondermijnen; sociale netwerksites constitueren wel degelijk een verschil met bijvoorbeeld telefonische-, e-mail- of face-to-face communicatie. Het gaat daarentegen om het inzicht in de manier waarop gebruikers met deze sites omgaan; niet als doorgrondbare objecten waarmee publiek, privé en semi-privé onderscheiden kunnen worden, maar als quasi-objecten waarop veranderende en conflicterende ideeën over die grenzen geprojecteerd worden. Communicatietechnologieën zijn constellaties die allerlei gebruikswijzen mogelijk maken, waarvan gebruikers er bepaalde oppakken en andere niet en op die manier de technologie mede betekenis geven. Sociale netwerksites kunnen op basis van deze opvatting van de verhouding tussen technologie en samenleving worden getransformeerd van een *unknown unknown* (in termen van Beck) tot een minder verontrustend 'quasi-object' (in termen van Latour).

3.4.2 Gebruikers als quasi-subjecten

Nu heeft de ontwikkeling van sociale netwerksites, zo kan worden geconcludeerd uit het levendige privacydebat, een punt bereikt waarop de fundamentele verwickeling *zichtbaar* wordt. Waar de grens tussen publiek en privé in de ontsluiting van persoonlijke informatie in de wetenschap al decennialang ter discussie gesteld wordt, worden nu 'gewone' gebruikers geconfronteerd met het trekken van een arbitraire grens bij iedere 'statusupdate' die zij plaatsen. Deze gebruikers of 'subjecten' staan in het risicovolle gebruik van sociale netwerksites op het punt 'quasi-subjecten' te worden, die gedwongen worden tot het inzicht dat het voorheen ervaren idee van controle relatief is. Het ontsluiten van persoonlijke informatie, wat mensen altijd al deden – gemedieerd en ongemedieerd – wordt reflexief. Zo bezien zijn het niet sociale netwerksites die de grens tussen publiek en privé ondermijnen, doordat de technologie complexer of ambivalenter zou zijn dan eerdere moderne communicatiemiddelen als e-mail of de telefoon, maar illustreren zij de contingentie van deze moderne tegenstelling.³⁶

36 Uit de relativisering van het onderscheid tussen publiek en privé volgt niet dat wij, naar analogie met Latour, 'nooit privé zijn geweest'. Dit vanwege het verschil tussen de cultureel, sociaal en historisch veranderlijke interpretatie van de grens tussen een publiek- en een privé-domein (Van der Ploeg & De Mul: 2000: 8) en de scheiding die het individu percipieert tussen zichzelf en de buitenwereld (Martens et al., 2008: 31; De Mul et al., 2001: 47-59). Zoals O'Hara et al. met het oog op het online delen van persoonlijke informatie vanuit pragmatisch perspectief concluderen: "The privacy argument is clearly real" (2008: 20).

3.5 Naar een alledaags interpretatiekader

Sociale netwerksites kunnen met Latour aldus beschouwd worden als een quasi-object dat in staat is mensen van hun quasi-subjectiviteit te doordringen.³⁷ Participatie op deze sites wordt daarmee een oefening in interpretatie; niet zozeer van de technologie, als wel van de manier waarop *mensen* die technologie gebruiken en betekenis geven aan de informatie die zij daarop plaatsen en aantreffen. De moderne mens moet daarom terug naar wat Latour (2001) *ordinary humanity* noemt. Het beslissingsmodel voor techno-wetenschappelijke kwesties is volgens dit antropologische perspectief niet anders dan dat waarmee besloten wordt over alledaagse onzekerheden, waarin men ook moet handelen zonder zeker te zijn van de gevolgen van dit handelen.³⁸ Alledaagse strategieën zijn in de door Beck en Latour geconceptualiseerde reflexieve moderniteit niet alleen even legitiem als de door 'deskundigen' gearticuleerde waarden en waarheden; ze geven er rekenschap van dat bewustwording en aanpassing van de technologie – of 'meer kennis' in de woorden van Beck – minder in plaats van meer controle oplevert.

37 Waar Latour veronderstelt dat 're-modernisatie' de status van objecten heeft veranderd, omdat de ambigue status van wetenschap en technologie tegenwoordig wordt erkend, laat de mens zich nog steeds leiden door het 'grote modernistische scenario.' Latour ziet vooralsnog geen duidelijke indicatie dat subjecten 'quasi-subjecten' zijn geworden. In de huidige praktijken op sociale netwerksites lijkt het er inderdaad op dat, terwijl zij informatie delen, gebruikers van sociale netwerksites een nieuwe samenleving produceren 'als een soort terzijde', net als Latours subjecten die 'enkel wetenschap bedrijven' (2003: 39; 45-6). Het 'quasi-subjectieve moment' is dus een hypothese.

38 Latour noemt als voorbeelden van alledaagse, onzekere beslissingsmomenten bijvoorbeeld het huwelijk, het krijgen van een kind, geld lenen, het planten van bomen (2001).

4. Interpretatie als alledaags wapen

Via Beck en Latour kan de controlecontroverse nu in het vertrouwde daglicht geplaatst worden van de interpretatie van technologie door 'gewone' gebruikers. Welke aanknopingspunten voor de omgang met sociale netwerksites biedt Erving Goffmans dramaturgische perspectief op face-to-face interactie? Op welke grenzen stuit deze vergelijking tussen gemedieerde en ongemedieerde interactie?

4.1 Goffman en de kwetsbaarheid van sociale interactie

In zijn boek *The Presentation of Self in Everyday Life* (1959) conceptualiseert de socioloog Erving Goffman sociale interactie als een 'performance'. Hij hanteert daarbij termen die afkomstig zijn uit de dramaturgie, zoals *front stage*, *backstage* en *impression management*. Waar deze termen in het privacydebat aangehaald worden met verwijzing naar de uitoefening van controle over de indrukken die het individu achterlaat op anderen (boyd & Ellison, 2007; Tufekci, 2008; Livingstone, 2008), beschrijft Goffman sociale interactie in feite als een in hoge mate onzekere en kwetsbare praktijk. Het hogere doel bestaat niet zozeer uit individuele zelfpresentatie, als wel uit de presentatie van een coherente 'definitie van de situatie'. Is die definitie onduidelijk of wordt zij verstoord, bijvoorbeeld wanneer een deelnemer 'discrepante rollen' vertolkt of anderszins 'destructieve informatie' aan het licht komt, dan worden rollen ongeloofwaardig en de gewekte indrukken zinloos. Een verstoring van de performance heeft volgens Goffman ernstige consequenties op verschillende niveaus. In eerste instantie wordt de interactie zelf ondermijnd; de situatie is ongedefinieerd, rollen worden onhoudbaar, deelnemers voelen zich ongemakkelijk en het minutieuze sociale systeem raakt ontregeld. Dit zet enerzijds de bredere sociale structuur onder druk, anderzijds wordt op individueel niveau de conceptie van het zelf als iemand die zich raad weet met sociale situaties en waar anderen van op aan kunnen in diskrediet gebracht (1959: 242-243).

Goffman benadrukt dan ook dat niet alleen de performer 'defensieve strategieën' toepast in samenwerking met zijn of haar 'team', maar dat ook het publiek er belang bij heeft zich loyaal en tactisch op te stellen.³⁹ Dit gebeurt in zogenaamde *protective practices*. Zo zullen mensen zich in een ruimte waarin zij niet zijn uitgenodigd de aanwezigen waarschuwen of zich ongeïnteresseerd en onbetrokken gedragen. Wanneer zich een ongemakkelijke situatie voordoet zal het publiek grote bereidheid tonen excuses te aanvaarden (idem: 141; 145; 229-230; 254-5).

³⁹ Als defensieve praktijken binnen het team van deelnemers in een sociale interactie onderscheidt Goffman dramaturgische loyaliteit, dramaturgische discipline en dramaturgische omzichtigheid. Loyaliteit bestaat erin hoge groepssolidariteit te ontwikkelen en/of regelmatig van publiek te wisselen. Discipline verwijst naar zelfcontrole, het onderdrukken van spontane gevoelens en bewaren van gepaste afstand. Dramaturgische omzichtigheid ten slotte veronderstelt een goede voorbereiding, door van tevoren te bepalen hoe een show het beste 'ge-staged' kan worden en een publiek kiezen dat zo min mogelijk problemen zal opleveren (1959: 212-219).

Van cruciaal belang is dat de deelnemers in een sociale interactie, om tot een definitie van de situatie te komen, op zoek gaan naar zoveel mogelijk aanwijzingen over wat hun 'medespelers' doen en denken. Omdat zij hierin noodzakelijkerwijs moeten afgaan op representaties, bestaat een inherente kans op 'misrepresentatie' (idem: 249-51). Goffman erkent dan ook dat 'incidenten' wel degelijk voorkomen. Het publiek vangt in zo'n geval een glimp op van wat er zich achter de schermen afspeelt (idem: 235). Hij stelt zelfs dat geen interactie mogelijk is *zonder* dat deelnemers een aanzienlijke kans lopen om in verlegenheid gebracht, of een kleine kans lopen om diep vernederd te raken door een verkeerde interpretatie. Sociale interactie was in dit opzicht altijd al een *gamble* (idem: 141; 243).⁴⁰

4.2 Situaties definiëren op sociale netwerksites

Op het eerste gezicht ondermijnen sociale netwerksites Goffmans theorie. Met het verlies van context – persoonlijke informatie wordt op deze sites anders dan in de ongemedieerde interactie die Goffman beschrijft niet afgebakend in ruimte en tijd – lijkt de mogelijkheid tot een gezamenlijke definitie van de situatie verloren. De vervlakking van context tot één onbegrensde sociale setting zorgt ervoor dat destructieve informatie op veel meer manieren aan het licht kan komen. Doordat gebruikers tegelijkertijd met een uiteenlopend publiek communiceren spelen zij bovendien continu discrepante rollen. In Goffmans ruimtelijke terminologie maken sociale netwerksites de 'coulissen' transparant waardoor allerlei taferelen die zich *backstage* afspelen zichtbaar worden.

In dit besef ligt echter wel degelijk de mogelijkheid de situatie te herdefiniëren. Sociale netwerksites maken het 'werk' dat het insceneren van sociale interactie (altijd al) kost zichtbaar en herinneren zodoende aan de inherente mogelijkheid dat tijdens de performance iets misgaat, door een falende performer of een falend publiek. Goffmans dramaturgische perspectief sluit in die zin aan bij het aan Beck en Latour ontleende idee dat interactie via sociale netwerksites niet risicovoller of meer 'verwikkeld' is dan ongemedieerde interactie, maar dat nu meer gereflecteerd wordt op de risico's. De nadruk in het privacydebat op controle bij de gebruiker – alsmede op de 'nieuwheid' van de technologie – veronachtzaamt dat zij altijd in grote mate afhankelijk geweest is van het publiek. Wanneer gebruikers van sociale netwerksites net als in de ongemedieerde interactie zouden kunnen rekenen op een tactisch publiek, vermindert niet alleen de perceptie van risico, maar neemt dit risico – als in de anticipatie op catastrofe – ook daadwerkelijk af.⁴¹

40 Overigens wijst Goffman erop dat zijn theorie zich beperkt tot de *Westerse* samenleving, omdat men hierin een *indoor* leven leidt: "We specialize in fixed settings, in keeping strangers out, and in giving the performer some privacy in which to prepare himself for the show. (...) If we are caught in a misrepresentation we feel deeply humiliated" (1959: 244).

41 In dit argument wordt een notie van vertrouwen bij de gebruiker verondersteld. Een fundament voor dit vertrouwen kan gevonden worden bij de socioloog Anthony Giddens (1991), die zich specifiek richt op de effecten van risicoperceptie op sociale interactie. Giddens veronderstelt een notie van 'basisvertrouwen' als 'interpretatief kader' voor risicovolle interacties. Hoewel iedere interactie in de toekomst (negatief) uitgebuit kan worden, gaat het individu ervan uit dat omstanders geen kwaad willen en doorgaans zelfs onverschillig staan

De controlecontroverse kan derhalve opgelost worden met de ontwikkeling van 'beschermende praktijken' à la Goffman bij het *publiek* van sociale netwerksites. Deze praktijken gaan niet uit van controle, maar van multi-interpretabele betekenissen en de kwetsbaarheid van de gebruikers/performers – net zoals in andere performatieve uitingen. Een op ongedimeerde interactie gebaseerd en op sociale netwerksites afgestemd interpretatiekader stelt dat ook gebruikers van sociale netwerksites indrukken (af)geven die zij passend achten voor de definitie van een *bepaalde* situatie, mogelijk afwijkend van de situatie waarin de indruk wordt ontvangen – bijvoorbeeld door een docent, werkgever of ex-partner. Wanneer een foto of uitspraak het publiek dan wel de 'performer' in een ongemakkelijke positie brengt, zal het publiek terughoudendheid moeten betrachten in het vellen van een oordeel. Het ligt immers voor de hand dat de betreffende informatie een andere definitie van de situatie voor ogen had. Overigens zouden gebruikers van sociale netwerksites – in Goffmans termen 'beginnende performers' die vatbaarder zijn voor gênante fouten – in dit opzicht op extra toegeeflijkheid moeten kunnen rekenen (1959: 231).

4.3 Anoniem versus kosmopolitisch publiek

Een probleem in de toepassing van Goffmans theorie op sociale netwerksites vormt de anonimiteit van het publiek.⁴² Het argument veronderstelt een welwillende houding bij het publiek om aanwijzingen te achterhalen en excuses te aanvaarden. Voor het anonieme publiek staat echter niet, zoals bij Goffman, de eigen positie als deelnemer aan de performance op het spel. Het publiek van sociale netwerksites wordt niet gemotiveerd door het verlangen een scène te voorkomen. Evenmin kan zij door het achterlaten van een innemende indruk zelf profiteren van de situatie. Hooguit gedraagt zij zich tactvol vanuit een onmiddellijke identificatie met de performer (1959: 231-2). Het publiek bevindt zich zodoende in een machtige positie.

Hier ligt evenwel de kans voor het kosmopolitische moment van Beck. Het loyale, tactische publiek zou in diens termen minder een normatief ideaal zijn dan een 'onvrijwillige' of 'geforceerde' realiteit. Nu veel informatie die voorheen zorgvuldig *backstage* werd gehouden zichtbaar wordt, zal het publiek verheugd doordrongen raken van het besef dat niet alle informatie voor iedereen bedoeld is, ook al staat die online, en vooral: dat het verbinden van consequenties aan die informatie vaak onredelijk is.

tegenover wat zij op een bepaald moment doet of zegt. Die onverschilligheid is met betrekking tot interacties in de openbare ruimte geconsolideerd in 'sociale codes' en 'beleefde onachtzaamheid' (idem: 128-9). Giddens spreekt van een *protective cocoon*, die voorkomt dat de anticipatie op alle potentiële gevaren die de sociale werkelijkheid impliceert individuen 'verlamt' (3). In hedendaagse 'abstracte expertsystemen', waaronder sociale netwerksites geschaard zouden kunnen worden, wordt vertrouwen volgens Giddens geïnstitutionaliseerd. In plaats van aanleiding tot cynisme ziet hij hierin ruimte voor de ontwikkeling van een zekere weerbaarheid of *empowerment* bij 'leken', in de vorm van het opnieuw toe-eigenen van alledaagse vaardigheden en kennis (133; 138).

⁴² Sommige sociale netwerksites bieden hun gebruikers, doorgaans tegen betaling, de mogelijkheid te zien wie hun profiel bezocht heeft. De zakelijke netwerksite LinkedIn is hiervan een voorbeeld. Het is echter wel mogelijk voor gebruikers hun zichtbaarheid (ook voor betalende gebruikers) uit te schakelen.

Dit is in Becks termen geen naïef idealisme maar een 'overlevingsstrategie'. Zoals in paragraaf 3.1 naar voren kwam zal de 'traumatische ervaring' van algemene kwetsbaarheid resulteren in het nemen van verantwoordelijkheid met het oog op de handhaving van het zelf (2009: 57). Wanneer het publiek deze nieuwe dramaturgische conventie – de confrontatie met de ander achter de schermen – weigert te accepteren, zal immers vroeg of laat het doek voor de performance op sociale netwerksites vallen. In de woorden van Goffman mag het publiek aan de ontdekking van andermans geheimen wellicht een 'agressief plezier' ontleen; in de gewaarwording van dit voyeurisme zal zij tegelijkertijd 'een les leren die haar uiteindelijk meer waard is' (1959: 235).

5. Terug naar de praktijk: aanknopingspunten

Dit laatste hoofdstuk vormt een terugkoppeling naar het privacydebat. De kosmopolitische interpretatie van persoonlijke informatie op sociale netwerksites vergt praktische vaardigheden in de omgang met deze sites.⁴³ Het reeds gevoerde debat biedt aanknopingspunten voor de ontwikkeling van een genuanceerd interpretatiekader, in termen van respectievelijk ironische of speelse; onjuiste of onvolledige; en verouderde of voorlopige informatie. Tot slot volgt een overweging voor als het toch misgaat.

5.1 Ironie en 'play'

De interpretatie van informatie op sociale netwerksites dient er allereerst rekening mee te houden dat niet alle persoonlijke informatie serieus is bedoeld. De toegenomen verstrengeling van online en offline praktijken heeft er niet alleen toe geleid dat op internet tegenwoordig 'iedereen weet dat je een hond bent' (Ibrahim, 2008),⁴⁴ maar impliceert ook dat speelse praktijken uit het dagelijks leven online verdergaan (Livingstone, 2008).⁴⁵ Zo signaleert Rosen een op internet ontstane 'mores' van 'persoonlijke grillen, spot en zelfspot, ironie, absurditeit, humor en bewuste misrepresentaties' (2007: 26). Ook boyd (2007), Tufekci (2008) en Livingstone (2008) identificeren bij jonge gebruikers speelse praktijken en 'trucs'. Voorbeelden zijn het opgeven van een nickname, een leeftijd van 99, een foto van een huisdier als profielfoto en het gebruik van de 'prikbord-' en reactiefunctie als decor voor rollenspellen en andere *joking content* (Livingstone: 7). Deze boodschappen zijn bedoeld voor een publiek dat ze begrijpt. Rosenblum (2007) waarschuwt echter dat het internet nauwelijks in staat is ironie en nuance vast te leggen. Valse en grappig bedoelde informatie kan dus (met name door buitenstaanders) gemakkelijk verkeerd geïnterpreteerd worden. Een geschikt interpretatiekader moet dus rekenschap geven van de mogelijk ironische of speelse intentie achter online gedeelde persoonlijke informatie.

43 Dit hoofdstuk leunt op de notie van 'mediawijsheid'. Hieronder wordt het vermogen verstaan van individuen om gemedieerde boodschappen in diverse contexten te analyseren, evalueren en zelf te creëren. Dit vermogen ligt niet uitsluitend bij de gebruiker, maar moet opgevat worden als een interactie tussen gebruiker en technologie. Een 'mediageletterde' omgang met de informatie op sociale netwerksites veronderstelt dus inzicht in zowel mediums specifieke eigenschappen als in de praktijken waarin mensen ze gebruiken (Livingstone, 2004).

44 De cartoon 'On the Internet, Nobody Knows You're a Dog' door Peter Steiner, gepubliceerd in *The New Yorker* in 1993 symboliseert de in de jaren negentig gangbare visie op het internet als een tekstgebaseerde ruimte waar geëxperimenteerd kan worden met identiteit, zoals bijvoorbeeld beschreven door Turkle (1995).

45 Het toenemende aandeel van foto's en video's in de informatie-uitwisseling via sociale netwerksites kan tegelijkertijd worden opgevat als een kans en als een bedreiging voor de interpretatie van ironische en speelse informatie. Enerzijds lijkt beeldmateriaal beter dan tekst in staat speelse boodschappen over te brengen, anderzijds wordt bij het kijken naar een filmpje wellicht minder ruimte voor interpretatie ervaren.

5.2 Naar een ethiek van onnauwkeurigheid

De implicaties van het spelen met de waarheid zijn breder dan de onder jongeren gangbare speelse praktijken. In het artikel 'Inaccuracy as a Privacy-Enhancing Tool' zet Gloria Fuster (2010)⁴⁶ de waarde uiteen van het opzettelijk opgeven van onnauwkeurige informatie voor de informationele autonomie van het individu – voor de vrijheid in openbare representatie en definitie van het zelf. Nauwkeurigheid is een fundamenteel principe van informationele privacy, wanneer zij individuen beschermt tegen onredelijke beslissingen. In antwoord op surveillance in de context van de ICT zijn echter strategieën van zelfbescherming ontstaan in praktijken van misrepresentatie, gedeeltelijke waarheden of de creatie van *clouds of inaccuracy*. Met betrekking tot sociale netwerksites bevestigen empirische studies dat ten minste een deel van de persoonlijke informatie op sociale netwerksites onjuist is, waarbij gebruikers onderscheid lijken te maken tussen door hen gepercipieerde categorieën van data. Fuster noemt dit 'creatieve benaderingen van *profiling*'.⁴⁷ Deze praktijken moeten niet begrepen worden als een oproep tot liegen, maar tot het besef dat individuen soms onvolledige of niet geheel kloppende informatie over zichzelf opgeven om op een voor hen wenselijke manier gebruik te kunnen (blijven) maken van een online dienst (idem: 88-91).

Dergelijke reflectie op de variabele kwaliteit van online gedeelde persoonlijke informatie ziet Fuster als een 'preventieve' strategie in de beperking van ongewenst gebruik van persoonlijke informatie. Uit de 'onderhandeling met het systeem' volgt immers dat informatie die wordt opgegeven voor een bepaald doel (waarvoor de nauwkeurigheid van die informatie irrelevant is) niet voor andere, ongerelateerde doelen gebruikt of geïnterpreteerd kan worden. Fuster noemt het respecteren van het 'recht' op de verspreiding van onnauwkeurige informatie een 'ethische keuze' die de samenleving moet maken, omdat uiteindelijk – net zoals in het kosmopolitische moment – de constructie van 'de ander' in het geding is (idem: 93)

46 Hoewel dit artikel zich deels richt op de bescherming van privacy op sociale netwerksites, is dit artikel niet opgenomen in de vertooganalyse van dit onderzoek vanwege de sterk afwijkende positie van Fuster in het debat.

47 Fuster noemt als voorbeeld de sociale netwerksite Last.fm, die door middel van software genaamd Scrobblen het luistergedrag van gebruikers in kaart brengt. Gebruikers hebben er om diverse redenen belang bij om selectief te 'scrobblen'. Ook wijst zij met betrekking tot locatiegebaseerde sociale media op de praktijk waarbij gebruikers handmatig hun locatie opgeven. Dit biedt de mogelijkheid hun locatie te verbergen of een andere plek op te geven dan waar zij zich daadwerkelijk bevinden (2010: 91).

5.3 'Social forgetfulness'

In het privacydebat wordt benadrukt dat de informatie die personen delen via sociale netwerksites opgeslagen wordt in een permanent beschikbaar persoonlijk archief. In de relatief jonge geschiedenis van sociale netwerksites kunnen echter wel degelijk aanwijzingen gevonden worden voor de ontwikkeling van 'digitale' context. Zo liet een 15-jarige respondent in de studie van Livingstone zijn profiel op de ene site achter om opnieuw te beginnen op een andere site, omdat het 'oude' profiel volgens hem ingebed was in een netwerk van "peer connections from which he felt he had moved on" (2008: 8). Boyd & Ellison (2007) beschrijven dynamische praktijken waarbij grote aantallen gebruikers bepaalde sociale netwerksites toe-eigenen of juist verlaten; hoewel de technologische kenmerken van deze sites vrij consistent zijn, ontwikkelen zich rondom de afzonderlijke sites verschillende 'culturen'. Gezien de jonge leeftijd van veel sociale netwerkgebruikers liggen grootschalige virtuele migraties in de toekomst voor de hand.

Deze aanwijzingen vergen een adequate interpretatie bij het publiek. Naarmate sociale netwerksites langer bestaan, zal die interpretatie rekenschap geven van het noodzakelijkerwijs achterblijven van ooit gedeelde persoonlijke informatie bij de realiteit.⁴⁸ Manders-Huits pleit (weliswaar met betrekking tot de interpretatie van persoonlijke informatie in *identity management*) voor een notie van *social forgetfulness*, oftewel de erkenning dat identiteit geen vaststaand gegeven is maar veranderlijk en dat individuen daarom een tweede kans verdienen (2010: 52). Langzamerhand ontstaat ruimte voor meer nuance. Zo is volgens Seeman (2009) de 'perfecte kandidaat' voor een baan tegenwoordig iemand wiens misstappen online staan en die van falen en nederigheid heeft geleerd. Jeff Jarvis gaat nog een stap verder met zijn *Doctrine of Mutual Humiliation*. Deze doctrine stelt dat een transparante samenleving waarin iedereen openheid betracht gepaard gaat met een wederzijdse vernedering, die zou leiden tot meer empathie en een grotere neiging om de fouten en misstappen van anderen, ook van publieke figuren, te vergeven. Persoonlijke informatie op sociale netwerksites zal volgens deze perspectieven in toenemende mate geïnterpreteerd worden als een verouderde of voorlopige versie – een 'beta' (2009: 232).⁴⁹

48 Sociale netwerksites vermelden over het algemeen automatisch data en/of tijdstip waarop content geplaatst werd.

49 Jarvis' boek *What Would Google Do?* waaraan deze passage gewijd is, werd niet opgenomen in de vertooganalyse omdat het een populair-wetenschappelijk werk betreft waarin verwijzingen naar wetenschappelijke literatuur ontbreken.

5.4 Een tragisch element

Tot slot moet het 'interpretatieargument' gewaardeerd worden als een theoretisch, preventief antwoord op de controlecontroverse. Waar zij de risicoperceptie kan verminderen sluit zij ongewenste consequenties niet uit en biedt zij in het geval zich toch persoonlijke schade voordoet geen compensatie. De kwestie past daarmee in een breder filosofisch perspectief, door Jos de Mul in zijn boek *De domesticatie van het noodlot* (2006) beschreven als het onvermogen van de hedendaagse cultuur om tragische incidenten een plaats te geven. De Griekse tragedie biedt volgens de filosoof een geschikter theoretisch kader om het conflict tussen botsende waarden – in het geval van sociale netwerksites tussen de 'vrijheid' om informatie af te sluiten en de 'noodzakelijkheid' om (sommige) informatie te ontsluiten – te interpreteren dan de fundamentele oppositie tussen privé en publiek. De moderne technologie, die enerzijds een ongehoorde verrijking biedt maar anderzijds ook een ongehoorde macht over ons uitoefent, noopt volgens De Mul tot de "wedergeboorte van het tragische wereldbeeld" (idem: 23).

Of zoals treffend uitgedrukt door de Amerikaanse toneelschrijver Arthur Miller: "Maybe all one can do is hope to end up with the right regrets."⁵⁰

50 De betrekking van dit citaat uit het toneelstuk *The Ride Down Mount Morgan* (1991) op het privacydebat rond sociale netwerksites is ontleend aan Swisher (2009).

Conclusie: van controle naar interpretatie

Dit onderzoek behandelt het privacydebat rond sociale netwerksites vanuit het perspectief van de risicomaatschappij van Ulrich Beck (1992). In het huidige vertoog wordt de 'privacyparadox' verklaard door de online ontsluiting van persoonlijke informatie op te vatten als een dynamische onderhandeling over de grens tussen publiek en privé. Het probleem wordt vervolgens geïdentificeerd in het verlies van controle over de eenmaal gedeelde persoonlijke informatie. Verschillende eigenschappen van de informatietechnologie ondermijnen deze controle fundamenteel, waardoor een onbedoeld publiek ongewenste consequenties aan de online informatie kan verbinden.

Oplossingen voor dit 'risico' worden in het debat gezocht in de stimulering van bewustwording bij gebruikers, de aanpassing van de technologie, en de ontwikkeling van informele sociale normen om met de nieuwe situatie om te gaan. De eerste twee kunnen in het perspectief van de risicomaatschappij beschouwd worden als typisch modern. Verondersteld wordt dat met meer kennis en nieuwe technologie controle herwonnen kan worden. In de sociale en economische werkelijkheid radicaliseert deze rationele benadering daarentegen het probleem, doordat zij anticipeert op wat vaak niet te anticiperen valt en in het proces onvoorziene en onbedoelde effecten produceert. Deze discrepantie tussen het ideaal van controle en de praktijk van complexiteit noopt tot een aanscherping van de probleemstelling tot een 'controlecontroverse'.

Als antwoord op de controlecontroverse komt de derde oplossing, in termen van sociale normen, in aanmerking. Zij kan gefundeerd worden in Becks theorie van het 'kosmopolitische moment'. In anticipatie op de onbekende dreiging die met participatie in sociale netwerksites gepaard gaat ligt een confrontatie met de 'ander'. De 'risicogemeenschap' op sociale netwerksites ontkomt niet aan een herevaluatie van de manier waarop zij met (informatie over) anderen omgaat. Met behulp van het antropologische perspectief van Bruno Latour (2003) wordt deze normatieve transformatie in een vertrouwder daglicht geplaatst. Sociale netwerksites maken de uiterst moderne scheidingen die individuen aanbrengen tussen sociale contexten en domeinen zichtbaar. Het kosmopolitische moment ligt in de interpretatie van die zichtbaarheid.

Die interpretatie is geen techno-wetenschappelijke, maar een alledaagse kwestie. Een kosmopolitisch interpretatiekader wordt daarom gebaseerd op Erving Goffmans theorie van face-to-face interactie (1959). Sociale interactie wordt daarin beschouwd als een kwetsbare performance, het slagen waarvan mede afhankelijk is van het publiek. Waar gebruikers van sociale netwerksites beperkte controle hebben over de circulatie van hun persoonlijke informatie in de openbare ruimte, kan het publiek een adequaat interpretatiekader ontwikkelen voor die informatie die in ongemedieerde interactie zorgvuldig *backstage* gehouden werd. Op

basis van het kosmopolitische moment wordt verondersteld dat het publiek op termijn niet anders kan. Het probleem van anonimiteit en asymmetrische machtsverhoudingen stelt aan dit element van de theorie van Beck evenwel een uitdaging.

Aanwijzingen dat zich in de praktijk wel degelijk een 'onvrijwillig' kosmopolitisch interpretatiekader ontwikkelt, worden gevonden in het reeds gevoerde privacydebat. In de marge van het vertoog wordt persoonlijke informatie op sociale netwerksites (onwillekeurig) als ambivalent begrepen. De ontwikkeling van praktische vaardigheden in de omgang met (informatie op) sociale netwerksites helpt bij de totstandkoming van een interpretatiekader dat rekenschap geeft van de speelse, opzettelijk onjuiste of onvolledige, verouderde of voorlopige status van online gedeelde informatie.

Aanbevelingen en reflectie

Het in dit onderzoek geformuleerde interpretatiekader vormt een eerste aanzet. In het licht van recente ontwikkelingen in *social networking*, zoals 'tag-bare' video's en locatiegebaseerde toepassingen, dient nader onderzocht te worden in hoeverre niet-tekstgebaseerde vormen van persoonlijke informatie openstaan voor flexibele interpretatie. Tevens kan onderzocht worden welke rol mediawijsheid speelt in de ontwikkeling van een kosmopolitisch interpretatiekader.

Voorts dient het interpretatieargument begrepen te worden als een theoretisch antwoord op het privacydebat. In de praktijk vormt het anonieme publiek een reëel obstakel. Dit ondergraaft echter geenszins de intentie van dit onderzoek, dat bij wijze van een gedachte-experiment een alternatief wil opperen voor de dominante interpretatie van de huidige praktijken op sociale netwerksites. Hoewel het kosmopolitische moment in de woorden van Beck 'door de achterdeur' zou moeten binnenvallen, kan het geen kwaad die deuren alvast van het slot te halen.

Overigens dient de oplossing voor het privacydebat in termen van interpretatie niet zonder meer opgevat te worden als een legitimatie van het gebruik van sociale netwerksites. Zo kunnen vraagtekens geplaatst worden bij de beperkingen die de 'epistemologie' van deze sites oplegt aan de vorm waarin persoonlijke informatie (online) beschikbaar is; het aanvinken van hokjes en invullen van voorgeprogrammeerde informatieelden structureert de manieren waarop mensen elkaar, maar ook zichzelf (kunnen) kennen. Als risico's met betrekking tot privacy momenteel het meest in het oog springen, dan is dat wellicht vanwege de publieke aantrekkingskracht van deze term. De waarde van een theoretisch kader dat culturele risicoperceptie benadrukt dient zich daarmee wederom aan.

Literatuur

- Andrejevic, M. (2006) 'The Discipline of Watching: Detection, Risk, and Lateral Surveillance', *Critical Studies in Media Communication* 25 (5): 391-407.
- Arendt, H. (1998) *The Human Condition*. Chicago: University of Chicago Press.
- Barnes, S. B. (2006) 'A Privacy Paradox: Social Networking in the United States', *First Monday* 11 (9).
- Beck, U. (1992) *The Risk Society: Towards A New Modernity*. Londen: Sage.
- , (2006) 'Living in the World Risk Society', *Economy and Society* 35 (3): 329-345.
- , (2009) *World at Risk*. Cambridge: Polity Press.
- boyd, d. (2007) 'Social Network Sites: Public, Private, or What?' *Knowledge Tree* 13.
http://kt.flexiblelearning.net.au/tkt2007/?page_id=28 [laatst bezocht op 30 juni 2010]
- , (2010) 'Quitting Facebook is Pointless; Challenging Them to Do Better is Not' [blogpost] 23 mei 2010. <http://www.zephorio.org/thoughts/archives/2010/05/23/quitting-facebook-is-pointless-challenging-them-to-do-better-is-not.html> [laatst bezocht op 30 juni 2010]
- boyd, d. & Ellison, N. B. (2007) 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer-Mediated Communication* 13 (1): 1-11.
- Brin, D. (1999) *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Perseus Books.
- Dekker, W. (2010) "'Digitale schandpaal is niet meer te stoppen'", *de Volkskrant*, 1 april 2010.
- Dwyer, C. Hiltz, S. R. & Passerini, K. (2007) 'Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace', Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, VS, 9-12 augustus 2007.
- Fuster, G. G. (2010) 'Inaccuracy as a Privacy-Enhancing Tool', *Ethics and Information Technology* 12: 87-95.
- Giddens, A. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Cambridge: Polity Press, 1991.
- Goffman, E. (1959) *The Presentation of Self in Everyday Life*. New York: Anchor Books.
- Ibrahim, Y. (2008) 'The New Risk Communities: Social Networking Sites and Risk', *MCP* 4 (2): 245-252.
- Krishnamurty, B. & Willis, C. E. (2008) 'Characterizing Privacy in Online Social Networks', *WOSN'08*, Seattle, Washington, 18 augustus 2008.
- Latour, B. (2001) 'What Rules of Method for the New Socio-Scientific Experiment?' [Darmstadt Colloquium lezing] 30 maart 2001. <http://www.bruno-latour.fr/poparticles/poparticle/p095.html> [laatst bezocht op 30 juni 2010]
- , (2003) 'Is Re-modernization Occurring – And if so, How to Prove it? A Commentary on Ulrich Beck', *Theory, Culture & Society: Explorations in Critical Social Science* 20 (2):

35-48.

- Livingstone, S. (2004) 'Media Literacy and the Challenge of New Information and Communication Technologies', *The Communication Review* 7: 3-14.
- , (2008) 'Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression', *New Media & Society* 10 (3): 393-411.
- Manders-Huits, N. (2010) 'Practical versus Moral Identities in Identity Management', *Ethics and Information Technology* 12: 43-55.
- Martens, B., Dierick, G. & Noot, W. (2008) *Ethiek en weerbaarheid in de informatiesamenleving*. Den Haag: Lannoo Campus.
- Mooradian, N. (2009) 'The Importance of Privacy Revisited', *Ethics and Information Technology* 11: 163-174.
- Mul, J. de. (2006) *De domesticatie van het noodlot. De wedergeboorte van de tragedie uit de geest van de technologie*. Kampen: Uitgeverij Klement/Pelckmans.
- Mul, J. de, Müller, E. & Nusselder, A. (2001) *ICT de baas? Informatietechnologie en menselijke autonomie*. Den Haag.
- Mythen, G. (2004) *Ulrich Beck: A Critical Introduction to the Risk Society*. Londen: Pluto Press.
- Nock, S. (1998) 'Too Much Privacy?' *Journal of Family Issues* 19 (1): 101-118.
- O'Hara, K., Tuffield, M. M. & Shadbolt, N. (2008) 'Lifelogging: Issues of Identity and Privacy with Memories for Life', *Identity and the Information Society Conference*, 28-30 mei 2008.
- Ploeg, I. van der, & Mul, J. de (2000) 'Internet en privacy'. *Onderzoeksinstituut Filosofie van de Informatie- en Communicatietechnologie (FICT)*.
- Preibusch, S., Hoser, B., Gürses, S. & Berendt, B. 'Ubiquitous Social Networks – Opportunities and Challenges for Privacy-Aware User Modelling', *Data Mining for User Modelling Workshop*, Korfu, Griekenland, juni 2007.
- Rosen, C. (2007) 'Virtual Friendship and the New Narcissism', *The New Atlantis: A Journal of Technology & Society* (zomer): 15-31.
- Rosenblum, D. (2007) 'What Anyone Can Know: The Privacy Risks of Social Networking Sites', *IEEE Security & Privacy* 5 (3): 40-49.
- Seeman, N. (2009) 'Privacy Has Lost its "Cool Factor"...' [online essay].
<http://www.longwoods.com/product.php?productid=20639> [laatst bezocht op 30 juni 2010]
- Shoemaker, D. W. (2010) 'Self-Exposure and Exposure of the Self: Informational Privacy and the Presentation of Identity', *Ethics and Information Technology* 12: 3-15.
- Solove, D. J. (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale Univeristy Press.

- Souza, Z. de & Dick, N. D. (2008) 'Information Disclosure on MySpace – The What, The Why and the Implications', *Pastoral Care in Education* 26 (3): 143-157.
- Swisher, K. (2009) "'You Have Zero Privacy Anyway. Get Over It" - That Goes Double on Social Networks' [blogpost] 16 februari 2009. <http://kara.allthingsd.com/20090216/you-have-zero-privacy-anyway-get-over-it-that-goes-double-on-social-networks> [laatst bezocht op 30 juni 2010]
- Thompson, C. (2008) 'Brave New World of Digital Intimacy', *The New York Times*, 7 september 2008. <http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html> [laatst bezocht op 30 juni 2010]
- Tufekci, Z. (2008) 'Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites', *Bulletin of Science, Technology and Society* 28 (1): 20-36.
- Turkle, S. (1995) *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schuster.
- Xiao, X. & Varenhorst, C. (2009) 'Stop the Tweet Show: Preventing Harm and Embarrassment to Twitter Users' [paper] 3 april 2009. <http://varenhorst.st/papers/tweetshow.pdf> [laatst bezocht op 30 juni 2010]
- Zuckerberg, M. (2010). 'From Facebook, answering privacy concerns with new settings', *The Washington Post*, 24 mei 2010. <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html> [laatst bezocht op 30 juni 2010]

Overige bronnen

'Social Network Sites, Privacy and Publicity'. Symposium met dr. danah boyd, Nine Ludwig (Hyves) en prof. dr. Ronald Leenes (TILT). Tilburg Institute for Law, Technology and Society (TILT), Universiteit van Tilburg, 7 april 2010.