Image-building op het internet: houd greep op je digitale identiteit

Colofon

Image-building op het internet: houd greep op je digitale identiteit is geschreven in opdracht van SURFdirect, de DIgitale Rechten Expertise Community van SURF.

SURFdirect
PO Box 2290
NL-3500 GG Utrecht
T + 31 30 234 66 00
F + 31 30 233 29 60

info@surf.nl
www.surf.nl/surfdirect

Auteurs
Tina van der Linden - *Universiteit Utrecht*
Tijmen Wisman - *zelfstandig privacy-adviseur*

Redactie
Evelijn Jeunink - *SURFnet*

Eindredactie
Annemiek van der Kuil - *SURFfoundation*

SURF is de ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek (www.surf.nl).
Deze publicatie is digitaal beschikbaar via de website van SURFfoundation:
www.surffoundation.nl/publicaties

Maart 2010
ISBN *9789078887096*

Inhoudsopgave

1 Inleiding

Imago is het beeld dat anderen van een persoon hebben. Imago is de basis waarop mensen met elkaar omgaan: het bepaalt of iemand met respect of met argwaan wordt bekeken, of iemand wel of niet wordt uitgenodigd of gevraagd voor iets. Logisch dus dat het belangrijk is om zorgvuldig met je imago om te gaan.

In het dagelijks leven betekent dat onder meer: aandacht besteden aan uiterlijk, en dat zal voor verschillende gelegenheden (een promotiefeest of deelname aan een sportevenement) anders zijn. De modewereld en de cosmetica-industrie varen er wel bij.

Maar ook in het hoger onderwijs is het noodzakelijk bewust te zijn van imago. Een belangrijk deel van iemands imago als wetenschapper of professional (in spe) wordt tegenwoordig bepaald door wat er over hem of haar op het internet te vinden is. Sollicitanten worden op het internet opgezocht.[1] Als bij een onderwerp in de pers een deskundige nodig is, wordt die vaak via internet gevonden. En hoe cool (of niet) medestudenten zijn wordt voor een deel bepaald door hoeveel vrienden ze hebben op Hyves en wie dat zijn. En als er over iemand helemaal niets op het internet te vinden is, zegt dat ook wat. Het beeld dat van iemand naar voren komt op basis van gegevens (data, foto's, filmpjes, associaties) die op internet gevonden kunnen worden, noemen we hier zijn of haar digitale identiteit.

Net als het imago in de fysieke wereld, behoeft ook de digitale identiteit zorg en aandacht. Daarom heeft SURFdirect, de Digitale Rechten Expertise Community van SURF, een studie laten uitvoeren hoe iemand, als student en als wetenschapper, op een verstandige manier om kan gaan met zijn of haar eigen digitale identiteit èn die van anderen.

Dit rapport begint dan ook met een hoofdstuk waarin wordt aangegeven waarom het zo belangrijk is dat iemand zelf kan bepalen wat anderen van hem of haar weten, ook als hij of zij “niets te verbergen” heeft. Daarna volgen concrete aanbevelingen voor image-building op het internet op bladzijde 8.

De onderbouwing van de aanbevelingen is te lezen in de hoofdstukken 4, 5 en 6.
De officiële regels worden in hoofdstuk 4 besproken: wat zeggen de Wet bescherming persoonsgegevens, en de ‘Richtsnoeren Publicatie van Persoonsgegevens op Internet’ van het College Bescherming Persoonsgegevens over de omgang met persoonsgegevens op internet?
In hoofdstuk 5 wordt de overstap gemaakt van theorie naar de praktijk van sociale netwerksites. De gebruiksvoorwaarden en het privacybeleid van Hyves, Facebook en LinkedIn worden onder de loep genomen.
In hoofdstuk 6 wordt besproken hoe online identiteitsmanagement vorm kan krijgen.
Tot slot bevat het rapport een lijst met aanbevolen literatuur.

[1] De nieuwe sollicitatiecode van de Nederlandse Vereniging voor Personeelsmanagement & organisatieontwikkeling (NVP) verbiedt googelen van een sollicitant zonder diens medeweten en toestemming, art. 5.1 De Sollicitatiecode is te vinden op www.nvp-plaza.nl/documents/doc/sollicitatiecode/sollicitatiecode-oktober-2009.pdf

2 Niets te verbergen?

Idealiter bepaalt iemand zelf wie wat over hem of haar weet of mag weten. Dit is het ideaal van **informationele zelfbeschikking**.[2] In het begin van de jaren tachtig heeft het Duitse Constitutionele Hof hier een uitspraak over gedaan waarin het achterliggende belang van dit recht binnen een democratie wordt benadrukt. Het Hof stelde: 'Iedereen die er niet zeker van kan zijn dat gegevens over maatschappelijk afwijkend gedrag voor langere tijd worden geregistreerd en kunnen worden gebruikt op een manier waarvan hij niets weet, zal proberen om dat gedrag niet te vertonen. Dat is in strijd met de elementaire functie van zelfbeschikking in een democratische samenleving waarin de burgers de mogelijkheid moeten hebben om deel te nemen aan het maatschappelijke en politieke leven zonder risico te lopen op een voor hem ondoorzichtige manier te worden geregistreerd.'[3]

Als Achilles een Hyve had gehad waarop hij (of iemand anders) had verteld hoe zijn moeder hem aan zijn hiel had gedoopt in de Styx, dan was zijn zwakke punt al een stuk eerder ontdekt en was de Trojaanse oorlog wellicht anders verlopen. Informatie vormt de basis voor kennis, kennis is macht, en macht kan worden misbruikt.

Contacten leggen èn onderhouden impliceert wetenswaardigheden over jezelf vertellen, dat geldt zowel in de fysieke wereld als op internet. Anders dan in de fysieke wereld worden die wetenswaardigheden op internet gemakkelijker uit hun context gehaald èn ze kunnen gemakkelijker terechtkomen bij mensen voor wie die informatie niet bedoeld was. Bovendien 'vergeet' het internet niets en kan allang achterhaalde informatie tot in lengte van dagen te vinden zijn. Zo kan een imago van iemand ontstaan dat onjuist, eenzijdig of onvolledig is. Zelfs als de gegevens op zich kloppen, zijn ze wellicht niet relevant – maar dragen wel bij aan een imago. Hierdoor is het moeilijk voor iemand om zich vrij van vooroordelen in het maatschappelijk verkeer te begeven. Voorbeelden van gegevens die bepaalde vooroordelen oproepen: als iemand aan sport doet, is dat dan paardrijden, skaten, of biljarten? Iemand houdt van muziek: speel hij harp of is hij een rapper?

Een paar voorbeelden van hoe het mis kan gaan:

- Dat iemand één keer heel dronken is geworden maakt hem of haar nog geen alcoholist. Maar als hier een filmpje van gemaakt is dat een eigen leven is gaan leiden op internet, dan kan dat idee desondanks ontstaan. En het kan zijn dat het alleen maar erger wordt door pogingen om het filmpje van internet af te krijgen.[4]
- Iemand snapt maar niet waarom zij nooit wordt uitgenodigd voor een sollicitatiegesprek, totdat zij er achterkomt dat een naamgenoot actief is op een rechts-radicaal forum.

Kortom: ook als iemand niets te verbergen heeft, betekent dat nog niet dat hij of zo ook alles wat er over hem of haar te weten valt met iedereen wil delen. Zonder paternalistisch te willen zijn: dat kun je niet willen.

Wat kan er verder misgaan? Iemand kan slachtoffer worden van identiteitsfraude: iemand doet zich voor als iemand anders. Het kan ook zijn dat er geld van een rekening verdwijnt, of dat 'vrienden' boos op iemand zijn om iets dat hij weliswaar niet gezegd heeft – maar hoe bewijst hij dat? Op internetsoa.nl is een aantal vervelende 'overdraagbare ziekten' te vinden. Daarnaast zijn er verschijnselen als internetpesten, ware digitale hetzes of haatcampagnes.

---

[2] A.F. Westin, Privacy and Freedom, New York 1967, p. 7

[3] BVerfG 15 december 1983, (*Volkszählung*), *BVerfG 65, 1.*

[4] Zie bijvoorbeeld de dronken studente en het filmpje op GeenStijl: Voorzieningenrechter Amsterdam 11 september 2009 (GeenStijl / majesteit), vonnis te zien op www.boek9.nl/www.delex-backoffice.nl/uploads/file/Boek9%20/Boek%209%20Uitspraken/Auteursrecht/Rb%20ASD%20studente%20-%20geenstijl.pdf.

Van ieder van ons zijn gegevens opgenomen in heel veel verschillende bestanden. Vaak weet iemand zelf niet, wie wat over hem of haar weet. Zeker als bestanden gecombineerd worden (bijvoorbeeld: surfgedrag zoals bijgehouden door een cookie, met aankoopgegevens aan de hand van een klantenkaart) dan kan uit die informatie een bepaald beeld naar voren komen, een profiel. Zo'n profiel kan gaan werken als een geautomatiseerd vooroordeel: omdat iemand in een bepaald profiel zit, worden die overige kenmerken die bij dat profiel horen, ook aan hem of haar toegedicht. Iemand krijgt bijvoorbeeld bepaalde aanbiedingen wel of juist niet, of afhankelijk van postcode kan wel of niet iets op krediet besteld worden. Dit zogenaamde 'verrijken' van klantgegevens voor marketingdoeleinden is een vak apart, waar geld mee verdiend wordt.[5]

Dat is op zichzelf niet slecht of verwerpelijk, zolang degene op wie die gegevens betrekking hebben, zich ervan bewust is dát het gebeurt en er toestemming voor gegeven heeft. Zonder die toestemming kun je al gauw denken aan begrippen als manipulatie, surveillance society, en een heleboel kleine zusjes van 'Big Brother' die op ondoorzichtige wijze van alles en nog wat van iemand (denken te) weten en hem of haar op basis van die informatie op een bepaalde manier behandelen. Het is daarom belangrijk om een begrip te krijgen van de verschillende risico's die zijn verbonden aan het plaatsen van persoonlijke informatie op internet. Zodat men zelf kan bepalen wie wat over hem of haar weet: informationele zelfbeschikking.

[5] Zie bijvoorbeeld www.crmpapers.nl, of Google eens op een term als "datamining" of "verrijking klantgegevens".

3 Aanbevelingen voor image-building op het internet

Algemeen

- Denk na over hoe je jezelf wilt presenteren. Wat mag iedereen altijd over jou weten?
- Check regelmatig wat er over jou op internet te vinden is. Niet alleen Google, maar ook bijvoorbeeld wieowie. Controleer of het beeld dat op basis van die informatie van jou naar voren komt ook het beeld is dat je van jezelf wilt laten zien. Overweeg of je actie wilt ondernemen als er iets opstaat wat je eraf wilt hebben (zie het 'notice-and-take-down' verzoek in bijlage 1).
- Maak een mooie, professioneel ogende, eigen website met alles waar je trots op bent. Geef alleen je zakelijke contactinformatie (liefst nog via een contactformulier om spam te voorkomen). Zorg voor een goede URL, en zet die standaard onder je e-mailberichten, op je visitekaartje, etc. Link zelf op je site naar sites die voor vakgenoten interessant zijn. Informeer bij je eigen instelling hoe je dit het beste kunt aanpakken.
- Maak publicaties waar je trots op bent zoveel mogelijk online (als pdf) beschikbaar. Check wel even of het auteursrechtelijk kan (en vraag evt. mede-auteurs om toestemming). Raadpleeg de website **Auteursrechten in hoger onderwijs** (www.surf.nl/auteursrechten).
- Zorg dat je naam veel op internet genoemd wordt in verband met je vakgebied. Zorg dat er veel naar je eigen pagina gelinkt wordt.
- Als je een naamgenoot hebt: zorg dat onmiskenbaar duidelijk is dat jij niet die naamgenoot bent.

Sociale netwerksites

- Denk na over hoe je jezelf wilt presenteren. Wat mag iedereen altijd over jou weten? Wat voor beeld wil je van jezelf schetsen? Denk na welke sociale netwerksite(s) je wilt gebruiken: algemene en/of netwerksites op je vakgebied? Valt de sociale netwerksite die je op het oog hebt onder de bescherming van de Wbp?
- Plaats zelf alleen informatie die **iedereen, altijd** over jou mag weten.
- Mocht je toch informatie (bv. foto's) alleen aan je vrienden willen laten zien, zet ze dan bij voorkeur niet op een sociale netwerksite. Maak dan gebruik van sites waarbij je mensen persoonlijk via de e-mail moet uitnodigen om ze toegang tot jouw gegevens te geven.
- Wees alert op contacten die aanbiedingen doen of om gegevens vragen.
- Let op auteursrechtinbreuk. Raadpleeg de website **Auteursrechten in hoger onderwijs** (www.surf.nl/auteursrechten).
- Plaats foto's waar anderen herkenbaar op staan alleen mét hun toestemming.
- Wees terughoudend met het publiceren van persoonlijke gegevens van anderen.
- Hanteer zelf ook een goede 'notice-and-take-down' procedure, d.w.z. als iemand bezwaar maakt, haal het er dan meteen af.

Technisch

- Zorg voor up-to-date software, en in ieder geval een firewall (en zet 'm aan!) en virusscanner. Zie www.surfnet.nl/nl/Thema/cybersafe
- Check de URL van een website voordat je persoonlijke gegevens invult en helemaal voordat je iets betaalt.
- Open nooit zomaar bestanden.
- Log altijd uit als je bij de computer weggaat.
- Draai periodiek anti-spyware software.

4 De regels

Het recht biedt een aantal handvatten om greep te houden op wat er over personen bekend is, in juridische termen: persoonsgegevens.

In de eerste plaats is de Wet bescherming persoonsgegevens (Wbp) hiervoor van belang. Hiervoor heeft het College bescherming persoonsgegevens (CBP) zogenaamde 'Richtsnoeren Publicatie van Persoonsgegevens op Internet' opgesteld. Deze richtsnoeren beogen duidelijkheid te bieden met betrekking tot de vraag of het publiceren van persoonsgegevens van anderen op het internet is toegestaan, en zo ja, aan welke voorwaarden voldaan moet worden. Daarnaast zijn er ook relevante regels te vinden in de Telecommunicatiewet en de Auteurswet.

In dit hoofdstuk wordt eerst de omgang met persoonsgegevens uiteengezet aan de hand van de Wbp met behulp van de Richtsnoeren. Daarna komt de overige regelgeving aan bod, zover deze relevant is voor het omgaan met persoonsgegevens.

4.1 De Wbp en de Richtsnoeren Publicatie van Persoonsgegevens op Internet

Het centrale begrip in de Wbp is **persoonsgegeven**. Dit is: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd "*een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit*." De vraag is nu natuurlijk hoe deze definitie moet worden gezien in het licht van gegevens die op het internet worden gezet. Daarnaast is het belangrijk of de gegevens informatie over een persoon bevatten. "*In veel gevallen, zoals bij feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen, zal dit uit de aard van de gegevens voortvloeien. In andere gevallen zal mede aandacht moeten worden besteed aan de context waarin het gegeven wordt vastgelegd en gebruikt. Als gegevens medebepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, moeten die gegevens als persoonsgegevens worden aangemerkt. Het (maatschappelijk) gebruik dat van gegevens wordt gemaakt is dus medebepalend voor de beantwoording van de vraag of sprake is van een persoonsgegeven*."[6] Laten we het erop houden dat alles wat, vanuit een bepaald perspectief, interessant is om van iemand te weten, een persoonsgegeven is. Ook foto's, filmpjes en geluidsopnamen van herkenbare personen zijn volgens de Richtsnoeren persoonsgegevens.[7]

Art. 16 Wbp introduceert het begrip **bijzondere persoonsgegevens**. Dit zijn persoonsgegevens die gaan over: iemands godsdienst of levensovertuiging, ras, politieke gezindheid, seksuele leven, lidmaatschap van een vakvereniging – en strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (bv. een veroordeling voor stalking).[8] Dergelijke gegevens mogen helemaal niet op internet gepubliceerd worden, tenzij de betrokkene uitdrukkelijke toestemming heeft gegeven, of de betreffende informatie duidelijk zelf openbaar heeft gemaakt. Ook identificatienummers, zoals een burgerservicenummer, mogen niet op internet worden gepubliceerd.

---

[6] Memorie van Toelichting bij de Wbp, Kamerstukken II, nr. 25 892, nr. 3, blz. 46.

[7] Richtsnoeren p. 15 onder 8.2: "Herkenbaar is daarbij breder dan direct identificeerbaar. Zelfs als het gezicht van een betrokkene wordt gemaskeerd, bijvoorbeeld met een zwart blakje, kan een foto een persoonsgegeven zijn. Dat is bijvoorbeeld het geval bij publicatie van camerabeelden van vermeende winkeldieven. Er bestaat een kans dat de betrokkenen herkend worden door hun vrienden, bekenden of buren, op grond van hun uiterlijk, kapsel en kleding."

[8] Zie bijvoorbeeld Rechtbank Breda 30 oktober 2009 (belaging via Hyves), LJN BK1696.

De wet regelt het verwerken van persoonsgegevens. Het begrip '**verwerken'** omvat werkelijk alles wat met gegevens gedaan kan worden: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen.[9]

Voor zover iemand alleen zijn of haar eigen gegevens publiceert, is er juridisch gezien (nog) niets aan de hand. Er is wel het risico dat anderen met die gegevens aan de haal gaan, en op dat moment is er juridisch natuurlijk wèl iets aan de hand, maar daarover later meer.

Het kan ook zijn dat iemand, misschien zonder erbij stil te staan, gegevens van anderen op internet zet. Bijvoorbeeld door een foto te uploaden waar ook anderen op staan, of door de deelnemerslijst van een conferentie op een site te zetten. Op dat moment ben hij of zij **verantwoordelijke** in de zin van de wet[10] en moet hij of zij zich aan de regels houden, die hierna kort besproken zullen worden. Wellicht publiceren anderen, op eenzelfde manier, wetenswaardigheden over hem of haar. In dat geval is hij of zij **betrokkene** in de zin van de wet[11] en heeft hij of zij bepaalde rechten.

De Wbp is niet van toepassing op activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden.[12] Dat kan ook het geval zijn op internet, maar volgens de richtsnoeren moet de toegang dan wel effectief beperkt zijn tot het eigen huishouden, familieleden en/of kennissen, bijvoorbeeld door middel van een wachtwoord. Of gegevens die op een sociale netwerksite gezet worden, die alleen toegankelijk zijn voor 'vrienden' hier ook onder vallen is onduidelijk en zal onder meer afhangen van het aantal 'vrienden' en de mate van beveiliging.[13] De Wbp is alleen van toepassing als de verantwoordelijke een vestiging in Nederland heeft.[14]

Wat betreft de plichten van de verantwoordelijke stelt de wet dat persoonsgegevens in overeenstemming met de wet èn op behoorlijke en zorgvuldige wijze verwerkt worden[15] en dat ze voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld worden.[16] Dat is mooi, maar het zegt nog niet zo veel.

Wat wel veel zegt is de bepaling van art. 8, die aangeeft wanneer persoonsgegevens mogen worden verwerkt. In dit verband zijn met name van belang:

- sub a: indien *de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend*. Gegevens van anderen mogen best gepubliceerd, als er maar sprake is van ondubbelzinnige toestemming, dat wil zeggen: elke twijfel of de betrokkene zijn toestemming heeft gegeven dient te zijn uitgesloten.[17] Die ondubbelzinnige toestemming kan ook blijken uit het gedrag van de betrokkene, zoals poseren voor een foto als bekend is dat die foto op een website gepubliceerd gaat worden. Kinderen onder de 16 kunnen zelf geen rechtsgeldige toestemming geven, maar hebben toestemming van hun wettelijke vertegenwoordiger nodig.[18]
- sub b: indien *de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst*. Bijvoorbeeld: aanmelding bij een sociale netwerksite impliceert dat er persoonsgegevens verwerkt moeten worden, dat is het hele doel van gebruik van een sociale

[9] Art. 1 sub b Wbp.

[10] Art. 1 sub d Wbp: je stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast.

[11] Art. 1 sub f Wbp: jij bent degene op wie een persoonsgegevens betrekking heeft.

[12] Art. 2 lid 2 sub a Wbp.

[13] Zie bv. Rechtbank Almelo 15 oktober 2009 (kind op Hyves), LJN BK0555.

[14] Art. 4 Wbp. Facebook, bijvoorbeeld, heeft geen vestiging in Nederland en valt derhalve niet onder de Wbp.

[15] Art. 6 Wbp.

[16] Art. 7 Wbp.

[17] Art. 1 sub i Wbp, Tekst & Commentaar p. 448.

[18] Art. 5 Wbp.

netwerksite. In zo'n geval is verwerking van persoonsgegevens noodzakelijk voor de uitvoering van de overeenkomst. De vraag is natuurlijk hoever die noodzakelijke verwerking dan strekt: verstrekken van persoonsgegevens aan andere partijen zal zonder aparte toestemming niet onder deze grond geschaard kunnen worden.

- sub f: indien *de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert*. Dit is een lastige grond voor verwerking, want het betekent dat de verantwoordelijke belangen tegen elkaar af moet wegen.[19]

Deze bepalingen moeten in verband gelezen worden met art. 9 Wbp, dat verbiedt om persoonsgegevens verder te verwerken op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Zoals bijvoorbeeld de verkoop van persoonsgegevens aan derden voor marketingdoeleinden, terwijl ze zijn verkregen voor wetenschappelijk onderzoek.

Omdat gegevens alleen voor een bepaald doel verzameld mogen worden, is het van belang dat de betrokkene weet, op het moment van verkrijging van die gegevens, wie de verantwoordelijke is, en wat de doeleinden van de verwerking zijn. De verantwoordelijke moet dus de betrokkene hiervan op de hoogte brengen.[20]

De betrokkene krijgt van de Wbp een aantal rechten – die overigens niet van toepassing zijn bij een publicatie voor uitsluitend journalistieke, literaire of artistieke doeleinden.[21] Zo mag een ieder vragen of een verantwoordelijke gegevens van hem of haar verwerkt (en moet een verantwoordelijke daarop antwoorden).[22] Hij of zij kan vervolgens de verantwoordelijke *verzoeken deze gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.*[23] De verantwoordelijke hoeft niet aan zo'n verzoek te voldoen, maar een weigering moet wel *met redenen omkleed zijn*,[24] zodat de betrokkene kan beoordelen of het zinvol is om na een weigering verdere juridische stappen te ondernemen. In bijlage 1 is een voorbeeld van zo'n zogenaamd 'notice-and-take-down' verzoek opgenomen.

En voor zover persoonsgegevens gebruikt worden in verband met *de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen* – zeg maar: spam, kan de betrokkene te allen tijde kosteloos bezwaar maken, waarna deze verwerking terstond beëindigd moet worden ('opt-out'). Helaas is de Wbp alleen van toepassing als de verantwoordelijke een vestiging in Nederland heeft[25] en de ervaring leert dat de meeste spam uit onbekende buitenlanden komt.

De Richtsnoeren zijn bedoeld als leidraad voor mensen en organisaties die persoonsgegevens van anderen op internet publiceren, om gemakkelijker te kunnen beoordelen of die publicatie in overeenstemming is met de Wbp. Voorin de Richtsnoeren is een stroomschema[26] opgenomen aan de hand waarvan gemakkelijk is na te gaan of de voorgenomen publicatie in overeenstemming is met de Wbp of niet (en zo niet, waarom niet). En als het wel mag, aan welke eisen voldaan moet worden.

---

[19] Onder omstandigheden kan het zelfs onrechtmatig zijn om iemands identificerende informatie níet aan een derde te verstrekken: Hoge Raad 25 november 2005 (Pessers/Lycos), LJN AU4019.

[20] Art.33 en 34 Wbp.

[21] Art. 3 Wbp. De hiervoor genoemde verplichtingen van de verantwoordelijke gelden wèl.

[22] Art. 35 Wbp.

[23] Art. 36 Wbp.

[24] Art. 36 lid 2 Wbp.

[25] Art. 4 lid 1 Wbp.

[26] www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf

Dus: als iemand (verantwoordelijke) gegevens van anderen (betrokkenen) op zijn of haar Hyve of website wil zetten, moet hij of zij die anderen daarvan op de hoogte brengen en om toestemming vragen. En als iemand bezwaar maakt tegen vermelding (of bijvoorbeeld tegen het feit dat hij/zij herkenbaar op een foto staat) dan is het verstandig om die vermelding eraf te halen, tenzij er een hele goede reden is om dat niet te doen. Bijvoorbeeld als de publicatie als journalistiek, artistiek of literair gekwalificeerd zou kunnen worden. Het vreemde is, dat de invulling van deze begrippen (journalistiek, artistiek of literair) vrij onduidelijk is: veel Hyves-pagina's zouden met een beetje goede wil best voor kunst of journalistiek door kunnen gaan.

Men doet er verstandig aan om periodiek te checken wat er over hem of haar op het internet te vinden is, via een algemene zoekmachine (Google) of via een zogenaamde 'verticale' zoekmachine (wieowie). Voor zover hij of zij bezwaar heeft tegen een vermelding kan een gemotiveerd 'notice-and-take-down' verzoek (zie bijlage 1) ingediend worden bij de betreffende verantwoordelijke.

Als persoonsgegevens in strijd met de Wbp worden verwerkt, kun een klacht ingediend worden bij het Cbp.[27] Handelen in strijd met de Wbp levert ook een zogenaamde onrechtmatige daad op, zodat de betreffende verantwoordelijke voor de rechter gedaagd zou kunnen dagen om een verbod tot verwerking en eventueel een schadevergoeding te eisen. In de praktijk komt dit heel weinig voor.[28]

Kortom: de Wbp, zoals uitgewerkt in de Richtsnoeren, biedt een betrokkene in theorie een behoorlijke zeggenschap over zijn of haar persoonsgegevens. In de praktijk wordt de verwerking van persoonsgegevens op internet vaak gebaseerd op toestemming (art. 8 sub a Wbp), of op het feit dat het nodig is voor de uitvoering van de overeenkomst (art. 8 sub b Wbp). De betrokkene heeft dan eigenlijk zelf die zeggenschap uit handen gegeven.
Eenmaal verleende toestemming (art. 8 sub a Wbp) kan weliswaar ingetrokken worden, met als gevolg dat de gegevensverwerking waarvoor toestemming was gegeven beëindigd moet worden, maar als de betreffende gegevens al in andere handen terecht zijn gekomen is het kwaad al geschied en dat is vaak niet terug te draaien. Verder geldt de Wbp, als gezegd, alleen voor zover de verantwoordelijke een vestiging in Nederland heeft.

4.2 Portretrecht

De regeling van het portretrecht, opgenomen in de Auteurswet, lijkt in tegenspraak met de regeling in de Wbp. In de Auteurswet gaat het, de naam zegt het al, om het auteursrecht van de maker van een portret (bijvoorbeeld een schilder of een fotograaf). Daarbij kent de Auteurswet dan ook nog een recht toe aan degene die afgebeeld is: het portretrecht.

De Auteurswet maakt onderscheid tussen portretten die in opdracht van de geportretteerde gemaakt zijn en portretten die zonder opdracht van de geportretteerde gemaakt zijn.
Met betrekking tot portretten in opdracht gemaakt, geldt dat de auteursrechthebbende die alleen openbaar mag maken met toestemming van de geportretteerde.[29] Dus: als iemand gevraagd wordt om een foto van een vrouw te maken, dan mag die foto alleen met toestemming van die vrouw op een website gezet worden.

Voor portretten zonder opdracht gemaakt geldt, dat *openbaarmaking daarvan door dengene, wien het auteursrecht daarop toekomt, niet geoorloofd* [is], *voor zoover een redelijk belang van den geportretteerde of, na zijn overlijden, van een zijner nabestaanden zich tegen de openbaarmaking verzet*.[30] Opnieuw een belangenafweging dus. De wetgever heeft hier wellicht een situatie voor

[27] Zie hierover "Uw klacht en het Cbp", te vinden op www.mijnprivacy.nl/Vraag/Rechten/rechtensamengevat/klachtencbp/Pages/klacht.aspx.
[28] Jurisprudentie over de Wbp is verzameld in de Uitsprakenbundel Wet bescherming persoonsgegevens, uitgegeven door de Sdu in 2009.
[29] En tot 10 jaar na het overlijden van de geportretteerde is toestemming van de nabestaanden nodig, art. 20 lid 1 Aw.
[30] Art. 21 Aw.

ogen gehad waarin bijvoorbeeld een foto van een markt gemaakt wordt, waarop onvermijdelijk een aantal toevallige passanten staan. Als die geen redelijk belang hebben om zich tegen publicatie te verzetten, dan mag die foto gewoon ge-upload worden. Zo'n redelijk belang kan in een aantal omstandigheden zitten: bijvoorbeeld het zijn van een bekende Nederlander met een zogenaamde 'verzilverbare populariteit',[31] of in de context van bijvoorbeeld een naaktstrand of een 'kinky' party.[32] Portretrecht biedt over het algemeen weinig mogelijkheden om bezwaar te maken tegen publicatie van een portret.

Echter, omdat een herkenbaar portret óók gekwalificeerd wordt als een persoonsgegeven in de zin van de Wbp is het verstandig om zoveel mogelijk om toestemming voor publicatie te vragen en om aan een verzoek tot verwijdering meteen gehoor te geven.

4.3 Telecommunicatiewet

Het hier relevante onderwerp dat in de Telecommunicatiewet (hierna: Tw.) behandeld wordt is **spam**: *elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden*.[33] Heel kort: spam mag alleen met voorafgaande toestemming van de ontvanger (opt-in), behalve als het gaat om bestaande klanten, en het gaat om communicatie *met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens* (opt-out).

Harvesten van elektronische e-mailadressen op het internet, en die vervolgens platspammen met aanbiedingen van diverse artikelen of diensten, is dus uit den boze – maar de vraag is wat er, met het recht in de hand, tegen gedaan zou kunnen worden. Zeker als de afzender onduidelijk is. In ieder geval kan een klacht ingediend worden bij de Opta.[34] Verder geldt, uiteraard, dat men nooit, maar dan ook nooit in moet gaan op spam. Als immers maar een klein percentage van de gespamden reageert, is spam al rendabel. En natuurlijk moet men niet het eigen, maar ook niet andermans e-mailadres, op een website zetten.

[31] Hoge Raad 19 januari 1979 (Schaep met de Vijf Pooten), NJ NJ 1979, 383, m.nt Wichers Hoeth, zie ook Arnoud Engelfriet, Het verzilverbare portretrecht, 18 maart 2008, op http://blog.iusmentis.com/2008/03/18/het-verzilverbare-portretrecht/.

[32] Rb. Amsterdam 18 januari 1996 (Wasteland-party), LJN BA2473.

[33] Art. 11.7 lid 1 Tw.

[34] Zie www.spamklacht.nl.

5 Sociale netwerksites

Sociale netwerksites zijn bij uitstek geschikt om je digitale identiteit uit te dragen èn zorgvuldig te beheren. In dit hoofdstuk wordt een drietal sociale netwerksites besproken, die door de doelgroep van dit rapport (wetenschappers en studenten) veel gebruikt worden: Hyves, Facebook en LinkedIn.[35]

Bij aanmelding bij een sociale netwerksite moet over het algemeen **gebruiksinformatie** opgegeven worden: identificerende informatie, een gebruiksnaam en een e-mailadres. Dit komt niet noodzakelijkerwijs in het profiel te staan dat voor iedereen zichtbaar is, maar vervult de functie van accountinformatie, waarmee men bij de betreffende site is aangemeld. Gekoppeld aan de identificerende informatie kan de betreffende site **gegevens over iemand verzamelen**, bijvoorbeeld iemands surfgedrag, en die gegevens, met toestemming van betrokkene, commercieel exploiteren.
Eenmaal aangemeld kan een homepage of een profiel aangemaakt worden, waarop eigen gegevens, **profielinformatie**, aan de rest van de wereld (al dan niet onderverdeeld in categorieën van bijvoorbeeld 'vrienden' of 'contacten') bekend maakt kunnen worden. In de profielinformatie kan ook informatie over 'vrienden' verwerkt zijn, bijvoorbeeld dat twee mensen samen een artikel aan het schrijven zijn. Ook kan profielinformatie bestaan uit content (filmpjes, foto's, liedjes) die onder het regime van het **auteursrecht** valt.

Per sociale netwerksite zal achtereenvolgens besproken worden hoe die sociale netwerksite met de verschillende hierboven genoemde soorten informatie omgaat. De laatste paragraaf van dit hoofdstuk gaat kort in op de informatie die door anderen over iemand op een sociale netwerksite gepubliceerd kan worden. Het hoofdstuk wordt afgesloten met conclusies.
Het hoofdstuk wordt afgesloten met conclusies en een schema waarin de belangrijkste aspecten per sociale netwerksite samengevat worden.

5.1 Hyves

Samenvatting Hyves

Gebruiksinformatie
- Omvat: voornaam, achternaam, e-mailadres, geboortedatum en een gebruikersnaam;
- Gebruiker geeft toestemming om gebruiksinformatie door te geven naar de Verenigde Staten of andere landen buiten Europa.

Profielinformatie
- Foto en gebruiksnaam zijn voor iedereen zichtbaar;
- Overige gegevens: in te stellen wie wat mag zien; mogelijkheid van schotten tussen verschillende groepen; blocklist mogelijk;
- Indien achternaam zichtbaar voor iedereen, dan ook voor zoekmachine.

Informatie die over iemand verzameld wordt
- Omvat: IP-adres, type browser, de pagina's die bezocht worden en cookies;
- Opt-out mogelijkheid voor cookies;
- Cookies worden gebruikt om advertenties toe te snijden op gebruiker.

Doorgeven van persoonsgegevens
➤ Worden allen aan derden verstrekt op basis van wettelijke verplichting.

[35] Er zijn uiteraard vele anders sociale netwerksites (MySpace, Schoolbank, Academia.eu, Orkut, Friendster om maar een paar te noemen) en ook andere toepassingen met sociale netwerk-eigenschappen (Flickr, YouTube, Twitter). Er zijn ook sociale netwerksites die zich specifiek op een bepaald onderwerp of een bepaalde beroepsgroep richten (bv. Legal360 voor juristen). Zie http://en.wikipedia.org/wiki/List_of_social_networking_websites voor een (niet uitputtend) overzicht.

Auteursrecht

- Hyves verkrijgt vergaande rechten met betrekking tot ge-upload materiaal.

Disclaimer

- Aansprakelijkheid van Hyves wordt zoveel mogelijk uitgesloten.

Hyves valt onder de Wbp, omdat Hyves in Nederland gevestigd is.

- **Gebruiksinformatie**

Gebruiksinformatie die opgegeven moet worden om een Hyves-account aan te maken omvat: voornaam, achternaam, e-mailadres, geboortedatum en een gebruikersnaam. In de gebruiksvoorwaarden vraagt Hyves om deze informatie juist, compleet en naar waarheid in te vullen, maar het is voor Hyves uiteraard niet controleerbaar of dit ook daadwerkelijk gebeurt. Dat geldt dus ook voor anderen: het is niet gezegd dat iedereen is wie hij zegt dat hij is. De privacy policy van Hyves bepaalt: *"Om technische en operationele redenen kan het nodig zijn dat jouw (persoons)gegevens worden doorgegeven (naar servers van) aan ons gelieerde ondernemingen en/of Adverteerders in de Verenigde Staten of andere landen buiten Europa, waar de regelgeving op het gebied van de privacybescherming mogelijk niet eenzelfde bescherming biedt als in de Europese Unie. Hierbij stem je, voor zover nodig, er mee in dat jouw (persoons)gegevens naar de Verenigde Staten of andere landen buiten Europa kunnen worden doorgegeven."*[36] Met andere woorden: iemand geeft toestemming[37] op het moment dat hij of zij de privacy-policy accepteert (hetgeen hij of zij wel moet doen om een account aan te maken). Ook zal Hyves informatie aan derden verstrekken op basis van een wettelijke verplichting, zoals bijvoorbeeld de Wet Vorderen Gegevens Opsporingsdiensten.

- **Profielinformatie**

Men kan zelf bepalen welke gegevens voor wie toegankelijk zijn, zij het dat profielfoto en gebruiksnaam wel altijd voor iedereen zichtbaar zijn. Men kan ervoor kiezen om gegevens voor niemand, vrienden, vrienden van vrienden, Hyvers of iedereen zichtbaar te maken. In het geval een boodschap bij iemand achtergelaten, in het jargon van Hyves een 'krabbel', dan zal de zichtbaarheid van deze krabbel worden bepaald door de instellingen van de ontvanger. Er is echter geen garantie dat 'vrienden' iemands informatie (nu of in de toekomst) niet verder verspreiden. Vrienden kunnen ingedeeld worden in groepen. Zo kunnen bijvoorbeeld schotten opgeworpen worden waardoor een werkgever bijvoorbeeld niet de foto's kan zien, die 'vrienden' wel kunnen zien. Het is ook mogelijk om bepaalde Hyvers op een *blocklist* te zetten. Voorts is het belangrijk om te weten dat als de zichtbaarheid van de achternaam ingesteld wordt op 'iedereen' het account ook vindbaar is in zoekmachines. De Privacy Policy van Hyves kan te allen tijde worden gewijzigd.

Om het bewustzijn rond het gebruik van een Hyves te verhogen was het Ministerie van Justitie een campagne begonnen, waarin Stanislav (een crimineel uit het Oostblok) een hoofdrol speelde. De campagne bestond uit een filmpje dat zich afspeelde in het hoofdkwartier van Stanislav, alwaar uit de printer, op de beeld- en projectieschermen en zelfs op een prikbord allerlei foto's verschenen van de Hyver die de link naar het filmpje toegestuurd had gekregen. Het filmpje eindigde met Stanislav en zijn 'gang' die zwaar bewapend erop uittrokken om eens een bezoekje aan Nederland te gaan brengen. Hoewel de campagne qua concept en vormgeving zeer geslaagd was, waren er wat kanttekeningen te plaatsen bij de uitvoering. Al snel bleek namelijk dat het filmpje ook gebruik maakte van foto's waarvan de toegang door de gebruiker was beperkt tot hemzelf of zijn vrienden. Dit betekent dat een derde partij toegang heeft gekregen tot gegevens waarvan de gebruiker duidelijk heeft aangegeven dat hij deze gegevens niet met derden wenst te delen. Ironisch genoeg is de derde ook nog het Ministerie van Justitie.[38]

---

[36] Dus niet om commerciële redenen – hetgeen dus toch een beperking inhoudt op het doorgeven van gegevens (namelijk uitsluitend om technische of operationele redenen).

[37] art. 8 sub a Wbp.

[38] Zie hierover: Erik van Roekel, Het einde van Stanislav: Hyves en Justitie over de campagne, 21 augustus 2009, te vinden op www.marketingfacts.nl/berichten/20090821_het_einde_van_Stanislav_Hyves_en_Justitie_over_de_campagne/.

➢ **Informatie die over iemand verzameld wordt**

Informatie die over iemand verzameld wordt door Hyves omvat zijn of haar IP-adres, het type browser dat gebruikt wordt, de pagina's die bezocht worden en 'cookies'. Hier moet dus rekening mee gehouden bij gebruik van een openbare computer of als iemand anders achter de eigen computer zit. Cookies kunnen worden gebruikt om te voorkomen dat de gebruiker een bepaalde advertentie te vaak ziet. Maar cookies kunnen ook worden gebruikt op bijvoorbeeld een nieuwswebsite om te zien welk nieuws iemand interesseert, oftewel om een gebruikersprofiel te maken. Men mag zelf bepalen of men wel of geen gebruik van cookies wilt maken. Met instemming van de gebruiker zal de informatie die onder andere middels cookies wordt verzameld worden gebruikt om Hyves aan te passen aan zijn of haar wensen en behoeften (speciaal op de gebruiker gerichte advertenties: "Zo proberen we bijvoorbeeld te voorkomen dat mannelijke Hyvers maandverbandreclame zien, en vrouwelijke Hyvers reclame voor scheermesjes. (Mannen die toch geïnteresseerd zijn in maandverband kunnen dat aangeven)."), voor communicatiedoeleinden, ter beveiliging en om geanonimiseerde statistische gegevens op te stellen.[39]

➢ **Auteursrecht**

Behalve tekst is het ook mogelijk om muziek, foto's en video's op Hyves te plaatsen. Hoe Hyves met deze content omgaat staat niet in de privacy policy, maar in de gebruiksvoorwaarden onder hoofdstuk 5 'Bestanden uploaden/licentie'. In beginsel behoudt de gebruiker de auteursrechten met betrekking tot de bestanden die op Hyves ter beschikking gesteld worden. In paragraaf 5.2 staat echter dat men door het beschikbaar stellen van deze bestanden instemt en erkent dat men hierdoor automatisch aan Hyves een kosteloze, onbezwaarde, wereldwijde, sublicentieerbare, niet-exclusieve licentie verleent om de bestanden, gegevens en/of materialen te gebruiken, te verveelvoudigen, te verspreiden en openbaar te maken in verband met de dienst van Hyves, maar ook voor marketing en promotie doeleinden in verband met de dienstverlening van Hyves. In concreto betekent dit dat een foto van een gebruiker in een bushokje in New York mag hangen ter promotie van Hyves.[40] Of dat liedje dat iemand had gemaakt en op haar profielpagina had gezet, kan zomaar op de televisie verschijnen. Hoe erg iemand dat vindt zal per persoon verschillen, maar als er bij de reclame wordt gezegd "voor mensen die normaal gesproken hun muziek niet aan de man kunnen brengen", dan is dat waarschijnlijk geen prettige ervaring. Deze licentie wordt overigens beëindigd zodra de bestanden verwijderd worden.
Verder is voorzichtigheid geboden bij het uploaden van materiaal dat men niet zelf gemaakt hebt. Zonder toestemming van de auteursrechthebbende wordt dan namelijk inbreuk op auteursrecht gepleegd. Als Hyves voor de rechter wordt gesleept door materiaal dat een gebruiker op Hyves heeft gezet, dan zal Hyves de kosten hiervoor op die gebruiker trachten te verhalen.

➢ **Disclaimer**

Uit de gebruikersvoorwaarden vloeit voort dat Hyves alle aansprakelijkheid, waarbij geen sprake is van opzet of bewuste roekeloosheid aan de kant van Hyves, uitsluit. Dat betekent dat n het geval van bijvoorbeeld reputatieschade of elke andere vorm van schade die iemand oploopt die direct, dan wel indirect wordt veroorzaakt door Hyves, Hyves die schade niet hoeft te vergoeden – tenzij Hyves er op uit zou zijn om iemands reputatie te beschadigen.

---

[39] In het vervolg van de privacy policy staat te lezen dat de persoonlijke informatie die wordt verzameld kan worden gebruikt om advertenties te personaliseren. Kennelijk valt dit voor Hyves onder de noemer "Hyves aanpassen aan de wensen en behoeften van de gebruiker", hetgeen enigszins vreemd is gezien het feit dat het niet mogelijk is voor de gebruiker om aan te geven dat hij geen behoefte heeft aan op maat gemaakte advertenties. Toch is het aannemelijk dat het uitschakelen van de cookies invloed zal hebben op de mate van personalisatie van de advertenties, ook al staat niet expliciet in de privacy policy dat Hyves ze hiervoor gebruikt.

[40] Hier zien we een vreemde inconsistentie, die veroorzaakt wordt door het feit dat het gaat om twee verschillende rechtsgebieden: privacy en auteursrecht. De gebruiker geeft hier in een (auteursrechtelijke) licentie toestemming om zijn of haar persoonsgegevens voor commerciële doeleinden te gebruiken.

5.2 Facebook

Samenvatting Facebook

Gebruiksinformatie
- Omvat: voornaam, achternaam, e-mailadres, geboortedatum;
- Gebruiker geeft toestemming voor verwerking in de VS;
- Facebook is aangesloten bij TRUSTe Privacy Program;
- Wordt aan derden verstrekt op basis van wettelijke verplichting.

Profielinformatie
- Per stukje profielinformatie in te stellen wie het mag zien (geldt alleen voor door gebruiker zelf verstrekte profielinformatie);
- News Feed and Wall, met informatie over laatste acties van gebruiker op Facebook;
- Deactivation en deletion zijn mogelijk, en ook voorziening in geval van overlijden van een gebruiker.

Informatie die over iemand verzameld wordt
- Omvat: IP-adres, type browser, en cookies;
- Mogelijkheid dat gegevens uit andere bronnen op internet over gebruiker verzameld worden (èn aan diens profiel toegevoegd worden!);
- cookies worden gebruikt om advertenties toe te snijden op gebruiker;
- 'web beacons' van derde partijen.

Doorgeven van persoonsgegevens
- informatie wordt gedeeld met derden, wanneer Facebook gelooft dat het delen
    - voldoende noodzakelijk is om een dienst aan te bieden,
    - juridisch noodzakelijk of
    - is toegestaan door de gebruiker.

Auteursrecht
- Facebook verkrijgt vergaande rechten met betrekking tot ge-upload materiaal.

Disclaimer
- Aansprakelijkheid van Facebook wordt zoveel mogelijk uitgesloten.

Facebook is een Amerikaans bedrijf zonder Nederlandse vestiging, dus de Wbp is niet van toepassing.

➢ **Gebruiksinformatie**

Ook Facebook vraagt bij registratie naar voornaam, achternaam, e-mailadres en geboortedatum. Na geboortedatum staat er een link met de vraag: "Why do I need to provide this?" Facebook vermeldt vervolgens dat het is bedoeld om authenticiteit aan te moedigen (waarbij niet geheel duidelijk is hoe dat dan zou werken) en om toegang tot content op de opgegeven leeftijd te kunnen afstemmen. Bij het aangaan van de overeenkomst met Facebook gaat de gebruiker ermee akkoord dat de gegevens naar de Verenigde Staten worden gestuurd en daar worden verwerkt. Het juridische regime van Amerika is dus van toepassing op de verwerking. Facebook is aangesloten bij het 'TRUSTe Privacy Program'. TRUSTe is een onafhankelijke organisatie wiens missie is om individuen en organisaties in staat te stellen om vertrouwelijke relaties aan te gaan, gebaseerd op respect voor de persoonlijke identiteit en voor informatie, door het behoorlijke gebruik van informatie te bevorderen (dit is letterlijk vertaald). Facebook is ook aangesloten bij de 'EU Safe Harbor Privacy Framework'. 'Safe Harbor' houdt in dat de bedrijven die zich hierbij hebben aangesloten zich aan de minimum eisen houden die de privacyrichtlijn van de EU van landen eist, wanneer er informatie vanuit de EU wordt overgedragen naar een land buiten de EU. Wanneer er klachten zijn ten aanzien van het beleid of de uitvoering hiervan door Facebook, wordt de

gebruiker erop gewezen dat eerst contact met Facebook te zoeken. Maar als men er niet uit komt dan stemt Facebook in dat TRUSTe het geschil zal beslechten.

- **Profielinformatie**

Facebook volgt naar eigen zeggen twee kernprincipes:

- *"You should have control over your personal information."*
- *"You should have access to the information others want to share."*

Uit het woord 'should' kan worden afgeleid dat het hier om een streven van Facebook gaat en geen garantie. Op de 'privacy help page' wordt uiteengezet hoe Facebook dit streven tracht te realiseren. Zo biedt Facebook de mogelijkheid per stukje profielinformatie uit te maken wie dit mag zien. Dit gaat zelfs zo ver dat je specifieke vrienden voor bepaalde gegevens kunt uitsluiten. Voorts is het mogelijk om in te stellen welke groepen mensen wat over de gebruiker kunnen vinden. Er is ook een 'News Feed and Wall' waarop informatie kan verschijnen over de laatste acties van de gebruiker op de site. Hierover heeft de gebruiker zelf controle, maar het wordt niet duidelijk uit de algemene voorwaarden of dit 'opt-in' of 'opt-out' is, hetgeen natuurlijk wel belangrijk is. Op het eerste gezicht lijkt het dus dat de gebruiker van Facebook goed in de gelegenheid wordt gesteld om de informatiestromen omtrent zijn of haar account te regelen. Dit gaat echter wel allemaal alleen maar om gegevens die iemand zelf bewust prijsgeeft en niet over de gegevens die Facebook over hem of haar verzamelt (zie hierna). Facebook kan ook haar Privacy Policy te allen tijde wijzigen.

Facebook geeft de mogelijkheid tot 'deactivation' of 'deletion'. De eerste mogelijkheid zorgt ervoor dat men onvindbaar wordt voor andere Facebook-gebruikers, maar dat Facebook de gegevens bewaart voor het geval dat de gebruiker het account zou willen heractiveren. De tweede mogelijkheid is een stuk definitiever en zal alle gegevens van het account verwijderen. Facebook wijst erop dat om technische redenen bepaalde gegevens, zoals foto's en berichten, achterblijven op de server, maar dat deze worden losgekoppeld van identificerend materiaal en ontoegankelijk worden gemaakt voor andere gebruikers. Dit is hoogstwaarschijnlijk niet het geval voor foto's die door anderen zijn overgenomen en voor foto's die voor zichzelf spreken. Facebook gaat ook in op de omstandigheid dat een gebruiker is overleden. Nabestaanden kunnen ervoor kiezen om een account open te houden of af te sluiten.

- **Informatie die over iemand verzameld wordt**

Browsertype en IP-adres worden opgeslagen. Daarnaast wordt er informatie verzameld met behulp van cookies. Deze cookies worden gebruikt om de gebruiker te herkennen. Maar er is meer, zie de één na laatste alinea van het hoofdstuk 'De informatie die we verzamelen' in de privacy policy. Hier staat namelijk dat Facebook ook informatie over de gebruiker kan verzamelen uit andere bronnen, waarvan vervolgens een niet-limitatieve opsomming wordt gegeven, 'zoals kranten, blogs, instant messaging diensten, en andere gebruikers van de Facebook dienst door het gebruik van diensten (bijv. foto tags), om je zo te voorzien van de meeste bruikbare informatie en een persoonlijke ervaring'. Het is alleen jammer dat de gebruiker niet in de gelegenheid wordt gesteld om het optimaliseren van deze persoonlijk ervaring uit te zetten, kortom de gebruiker heeft geen keuze.

Daarnaast gebruikt Facebook de profielinformatie om op maat gesneden advertenties aan te bieden terwijl de dienst wordt gebruikt. De aanbiedingen komen dan van derden en kunnen gerelateerd zijn aan bijvoorbeeld een film die als favoriet is bestempeld. Facebook doet dit zonder de identiteit van de gebruiker bekend te maken bij de derden, maar die is dan ook niet nodig voor het doen van een aanbieding.

Die reclame wordt onder andere ondersteund door cookies of zogeheten ´web beacons´, die externe adverteerders op de computer van de gebruiker plaatsen. Hiermee wordt getracht de doeltreffendheid van de advertenties in kaart te brengen en op basis hiervan de inhoud te veranderen. Waar dit in de praktijk op neerkomt is dat de gebruiker van een Facebook-account min of meer continue wordt gemonitord op zijn of haar voorkeuren en dit kan dus ook in zijn of haar profiel terechtkomen. Facebook geeft zelf ook aan dat informatie over het aantal klikken op advertenties ook aan Facebook kan worden doorgegeven. In de Engelse versie van de privacy policy wordt dit als volgt verwoord: "*We may ask advertisers to tell us how our users responded to*

the ads we showed them (and for comparison purposes, how other users who didn't see the ads acted on their site). This data sharing, commonly known as 'conversion tracking,' helps us measure our advertising effectiveness and improve the quality of the advertisements you see." Het is dus heel wel mogelijk dat Facebook bestanden bijhoudt van klikgrage en dus wellicht ook koopgrage gebruikers. Bij de Nederlandse vertaling geeft Facebook aan dat de externe adverteerders geen toegang hebben tot contactinformatie van de gebruiker en dat Facebook op haar beurt geen toegang heeft tot de cookies van deze adverteerders. Met het oog op wat er staat bij de Engelse versie is dit op zijn minst een vreemde mededeling. Hij suggereert dat informatie onderling delen door Facebook en adverteerders toch niet de bedoeling is. Maar gezien het feit dat Facebook op eigen initiatief wel informatie over de gebruiker kan verzamelen bij andere websites en ze informatie over de gebruiker mag delen als haar bedrijfsbelang daarmee wordt gediend, kunnen we er in ieder geval van uitgaan dat bij de behandeling van persoonlijke informatie Facebook haar winstbelang laat prevaleren boven het privacybelang van de gebruiker. Op internet is te vinden hoe in verschillende browsers cookies kunt verwijderen. Dan worden echter wel alle cookies van de computer verwijderd.

- **Gebruik van de verzamelde informatie**

De laatste alinea van het hoofdstuk 'Gebruik van informatie verzameld door Facebook' is de meest opvallende. Hierin staat dat Facebook de informatie die zij verzamelt bij derden (de blogs, instant messaging diensten, Facebook-platformontwikkelaars en dergelijke) kan gebruiken om toe te voegen aan het profiel van de gebruiker. Facebook geeft echter aan dat ze 'normaal gesproken' de gebruiker de mogelijkheid bieden om in zijn of haar privacyinstellingen aan te geven dat hij of zij niet wil dat dit gebeurt of om andere handelingen te verrichten waardoor de koppeling van deze informatie aan het profiel wordt beperkt. Uit de woorden 'normaal gesproken', kan worden afgeleid dat er ook uitzonderingen denkbaar zijn die het onmogelijk voor iemand maken om bepaalde informatie los te koppelen van zijn of haar profiel. Dit staat dus erg ver verwijderd van het ideaal van de informationele zelfbeschikking. Daarnaast biedt Facebook dus ook niet de mogelijkheid om haar eigen initiatief ten aanzien van informatieverzameling en het koppelen van die informatie aan het profiel van die gebruiker uit te schakelen.

Op Facebook worden verschillende platformtoepassingen aangeboden. Door gebruik te maken van deze toepassingen kan het zijn dat het platform toegang moet hebben tot de persoonlijke gegevens van die gebruiker. Deze platformontwikkelaars hebben allemaal een contract met Facebook ondertekend waarin ze moeten aangeven dat ze de privacyinstellingen van de gebruikers respecteren en waarin het verzamelen en gebruiken van persoonlijke gegevens 'aan banden wordt gelegd', zoals Facebook dit zelf formuleert. Facebook geeft zelf al aan dat, ondanks dit contract en technische voorzorgsmaatregelen, ze niet kan garanderen dat een platformontwikkelaar persoonsgegevens niet misbruikt. De toepassing van een ontwikkelaar kan gebruik maken van gegevens die zichtbaar zijn voor iedereen en openbare gegevens, zoals naam en profielfoto. Platformontwikkelaars kunnen daarnaast de gebruiker hún voorwaarden laten accepteren, waardoor ze meer rechten krijgen. Facebook doet geen onderzoek vooraf naar platformtoepassingen. Bij het gebruikmaken van dergelijke toepassingen is dus voorzichtigheid geboden. Een voorbeeld van een toepassing is 'Carpool' van Zimride. Op deze manier kan met medegebruikers van Facebook afgesproken worden om te carpoolen.

In het hoofdstuk 'Je informatie delen met derden' meldt Facebook dat er informatie wordt gedeeld met derden, wanneer Facebook 'gelooft' dat het delen 1) voldoende noodzakelijk is om een dienst aan te bieden, 2) juridisch noodzakelijk of 3) is toegestaan door de gebruiker. De formulering op zichzelf geeft Facebook alle ruimte om te doen en laten wat ze wil. Als Facebook immers gelooft dat het noodzakelijk is om gegevens te delen met derden, omdat dit voldoende noodzakelijk is om een dienst aan te bieden of omdat dit juridisch noodzakelijk is, dan is er dus al een grond voor een verwerking. Daarnaast maakt Facebook gebruik van derden die diensten voor haar verrichten, zoals het versturen van e-mails over Facebook-updates, het hosten van diensten bij een gedeelde faciliteit voor servers, het verwerken van betalingen voor diensten of producten en ga zo maar door. Facebook zegt dat de toegang tot persoonlijke informatie maar voor een beperkte tijd is en uitsluitend voor het uitvoeren van voornoemde zakelijke handelingen. Daarnaast implementeert Facebook, naar eigen zeggen, toereikende contractuele en technische beveiligingen om het gebruik van die informatie te beperken tot de door haar bepaalde doeleinden. Facebook kan worden

gedwongen om informatie vrij te geven bij een dagvaarding, verzoekschrift, een juridisch verzoek of naleving van een geldend recht. Maar daarnaast zegt Facebook ook letterlijk dat ze in de volgende omstandigheden informatie kan delen: "*als wij menen dat dit noodzakelijk is om de wet na te leven, onze belangen of eigendommen te beschermen, fraude te voorkomen of andere illegale activiteiten die zijn ontsprongen uit het gebruik van Facebook diensten of de naam Facebook, of om dreigend gevaar voor lichamelijk letsel af te wenden. Dit kan inhouden dat wij informatie delen met andere bedrijven, advocaten, bemiddelaars of overheidsorganen*." Met een dergelijke ruime formulering kan er altijd wel een reden worden gevonden om persoonlijke informatie te mogen delen. Facebook bepaalt immers zelf wanneer haar belangen moeten worden beschermd.

➢ **Auteursrecht**

In de 'Statement of Rights and Responsibilities' kan men vinden hoe Facebook omgaat met intellectuele eigendomsrechten ten aanzien van geschreven stukken, video's, foto's en muziek. *"For content that is covered by intellectual property rights, like photos and videos ('IP content'), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ('IP License'). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."* In concreto betekent dit dat Facebook alle gedeelde inhoud zoals liedjes, video's, foto's en blogs kan en mag gebruiken naar eigen goeddunken. Dit kan zo ver gaan dat er een foto van een gebruiker kan worden gebruikt in een reclame-campagne. Het is erg onwaarschijnlijk dat bepaalde inhoud die op deze manier populair wordt, verdwijnt als de gebruiker het verwijdert van zijn of haar account. Voorgaande ontwikkeling impliceert namelijk dat deze zeer waarschijnlijk ook zal komen te staan op andermans account, waardoor het onmogelijk wordt om het te laten verwijderen, ondanks dat natuurlijk wel altijd een 'notice-and-take-down' verzoek gedaan kan worden. Zoals iedereen weet kost het weinig moeite om digitale inhoud te verveelvoudigen. Dit alles betekent ook dat wanneer er een foto van iemand door iemand anders op Facebook wordt geplaatst, de afgebeelde persoon hier in de praktijk vrijwel machteloos tegenover staat.

➢ **Disclaimer**

Tenslotte wijst Facebook, terecht, op het feit dat geen enkele beveiligingsmaatregel 'ondoorbreekbaar' is en dat de gebruiker hier alert op dient te zijn: *"Je plaatst Gebruikers Inhoud (zoals omschreven in de Facebook Gebruikersvoorwaarden) op de Site op eigen risico. Alhoewel we je de privacy instellingen laten gebruiken om toegang tot je pagina's te beperken, wees er toch alert op dat geen enkele beveiligingsmaatregel perfect of ondoorbreekbaar is. We hebben geen controle over de handelingen van andere Gebruikers met wie jij wellicht pagina's en informatie deelt. Daarom kunnen wij niet garanderen dat Gebruikersinhoud die jij op de site plaatst, niet kan worden gelezen door onbevoegde personen. We zijn niet verantwoordelijk voor omzeiling van enige privacy instellingen of beveiligingsmaatregelen van deze Site. Je begrijpt en gaat ermee akkoord, dat zelfs na verwijdering, kopieën van Gebruikersinhoud zichtbaar kunnen blijven in gecachede en gearchiveerde pagina's of wanneer andere gebruikers Gebruikersinhoud hebben gekopieerd of opgeslagen."* Als een gebruiker iemand anders schade berokkent door middel van Facebook, dan moet hij of zij op basis van de 'Statement of Rights and Responsibilities' Facebook schadeloos stellen voor eventuele kosten (proceskosten, schadevergoedingen en dergelijke). Dit betekent dat als aan iemand schade wordt berokkend door middel van Facebook, het in theorie mogelijk is om dit op Facebook te verhalen.

Kortom: hoewel Facebook ongetwijfeld de beste intenties heeft voor wat betreft de privacy van haar gebruikers[41] is er geen garantie dat die privacy ook goed beschermd is. Facebook zelf exploiteert commercieel alle informatie die ze over haar gebruikers kan verkrijgen (het is tenslotte

[41] Maar daarover doen ook hele andere verhalen de ronde, zie bijvoorbeeld "The truth about Facebook" op www.youtube.com/watch?v=B37wW9CGWyY. Recentelijk is Facebook ook weer in opspraak gekomen omdat naam, foto, de woonplaats en de lijst met vrienden voortaan als openbaar toegankelijke informatie worden beschouwd: www.nu.nl/internet/2147618/privacybeschermers-klagen-facebook.html.

een gratis dienst en voor niets gaat de zon op). Voor wat betreft profielinformatie is men voor het gebruik daarvan afhankelijk van de integriteit van zijn 'vrienden' die toegang hebben gekregen tot die informatie. Alle reden dus om voorzichtig te zijn, Wat iemand over zichzelf bekend maakt, zou eigenlijk beperkt moeten zijn tot die informatie die iedereen, altijd over hem of haar mag weten. Het is ook geen slecht idee om de instellingen goed te bestuderen. Zelfs Mark Zuckerberg, CEO van Facebook, heeft hier volgens bronnen op internet moeite mee en daardoor per ongeluk privé-foto's van zichzelf in pyama met een teddybeer publiekelijk toegankelijk gemaakt.[42]

5.3 LinkedIn

Samenvatting LinkedIn

Gebruiksinformatie
- Omvat: naam, e-mailadres, land, postcode, korte samenvatting van professionele achtergrond en een password;
- LinkedIn is aangesloten bij TRUSTe Privacy Program.

Profielinformatie
- Optie om lijst met connections op 'invisible' te zetten.

Informatie die over iemand verzameld wordt
- Persistent cookies en session cookies;
- Cookies worden gebruikt om advertenties toe te snijden op gebruiker;
- 'Web beacons' van derde partijen.

Doorgeven van persoonsgegevens
- Alle informatie met uitzondering van naam kan doorgegeven worden aan derde partijen.

Auteursrecht
- LinkedIn verkrijgt vergaande rechten met betrekking tot ge-upload materiaal.

Disclaimer
- Aansprakelijkheid van LinkedIn wordt zoveel mogelijk uitgesloten.

LinkedIn is een Amerikaans bedrijf, met sinds januari 2010 een vestiging in Amsterdam. Dat betekent dat LinkedIn onder de werkingssfeer van de Wbp valt.

➢ **Gebruiksinformatie**
Om lid te worden van deze gemeenschap en voor LinkedIn om een gebruiker te identificeren, moet een gebruiker zijn of haar naam, e-mailadres, land, postcode, een korte samenvatting van zijn of haar professionele achtergrond en een password geven. Op LinkedIn is ook het 'TRUSTe Privacy Program' van toepassing en hiervoor gelden dus dezelfde voorwaarden als voor Facebook.

➢ **Profielinformatie**
Evenals Facebook blijkt LinkedIn, volgens haar privacy policy, bepaalde principes te hebben met betrekking tot de privacy van hun gebruikers. Dit zijn de volgende:
"We do not rent or sell your personally identifiable information to third parties for marketing purposes."
"We do not share your contact information with another User without your consent."
"Any personally identifiable information that you provide will be secured with industry standard protocols and technology."

In de 'profile section' bestaat de mogelijkheid om aanvullende informatie over zichzelf te verstrekken, zoals vaardigheden, werkervaring en netwerkdoelstellingen. Hierna wordt vermeld dat alle informatie die niet persoonlijk identificeerbaar is op dezelfde manier en in dezelfde mate kan

[42] http://de-gevaren-op-facebook.blogspot.com/

worden gebruikt zoals 'hieronder' beschreven. Hierbij moeten we voornamelijk denken aan advertenties. Door de informatie niet persoonlijk identificeerbaar te maken, meent LinkedIn problemen met betrekking tot persoonsgegevens van gebruikers te kunnen omzeilen. Maar dit, zoals al werd vermeld bij Facebook, ligt niet zo gemakkelijk. Immers zal de manier waarop iemand wordt benaderd door adverteerders afhangen van de informatie die over hem of haar bekend is. Het eerste principe van LinkedIn, dat ze geen persoonlijke informatie verhuren of verkopen aan derden voor marketingdoeleinden, geldt dus kennelijk alleen ten aanzien van de naam. Want als iemand een IT-manager is uit Doorn, dan kan deze informatie wel worden gebruikt voor marketingdoeleinden. Uit de privacy policy is echter op te maken dat er de mogelijkheid is om het delen van deze informatie uit te zetten, de zogenaamde 'opt-out'. Hierdoor loopt de gebruiker wel voordelen mis, zoals advertenties ontvangen die op zijn of haar interesses zijn gericht, aldus de policy. Informatie over wie door een gebruiker uitgenodigd wordt, wordt discreet behandeld en is alleen voor die gebruiker inzichtelijk.

Het is mogelijk om de persoonlijke informatie die iemand aan LinkedIn heeft verstrekt, te veranderen. Let wel, het kan zijn dat er nog enige tijd een back-up van de oude informatie wordt bewaard. Het is ook mogelijk om het account te beëindigen. De persoonlijke informatie zal dan worden verwijderd uit de publieke database. LinkedIn kan overgedragen informatie vasthouden om fraude of eventueel misbruik in de toekomst tegen te gaan, voor legitieme zakelijke doeleinden, herstel van de account of wanneer de wet dit vereist. Dit kan betekenen dat de informatie nog enige jaren op de servers zal staan. Echter: de privacy policy kan te allen tijde worden aangepast. Of dit ook voor bovengenoemde principes geldt is onduidelijk. Belangrijke veranderingen ten aanzien van de omgang met persoonlijke informatie worden op de website gezet of per e-mail bekend gemaakt. Wanneer de gebruiker na een dergelijke melding doorgaat met het gebruik van LinkedIn, geef hij of zij volgens LinkedIn aan dat hij of zij hiermee instemt. Er wordt ook duidelijk gesteld dat men bereid moet zijn bepaalde persoonlijke informatie te leveren, die (volgens de policy) nodig is om profijt te hebben van de LinkedIn website. Als iemand hier twijfels over heeft, of bij het feit dat deze informatie op de site wordt geplaatst of anderszins wordt gebruikt op een manier zoals beschreven in de privacy policy of de 'user agreement', zou hij of zij geen lid moeten worden van de LinkedIn gemeenschap, aldus LinkedIn.

Bij LinkedIn kan men ervoor kiezen om de lijst met connections wel of niet voor iedereen zichtbaar te laten zijn. Het risico van het laten zien van de connections is dat een kwaadwillende derde met één van hen contact kan zoeken en daarbij de naam van de betreffende gebruiker als introductie kan gebruiken. Een goede reden dus om de connections op 'invisible' te zetten.

➢ **Informatie die LinkedIn over iemand verzamelt**

Ook LinkedIn maakt gebruik van cookies. De eerste cookie die in de policy wordt vermeld is de 'persistent' cookie, een veelbelovende naam. Deze cookie zorgt ervoor dat de gebruiker de volgende keer dat hij of zij de website bezoekt wordt herkend.[43] Bij een eigen computer is dit erg handig, bij een openbare computer erg vervelend. Uitloggen betekent bij een volgend bezoek eerst weer inloggen, dus bij openbare computers is dit ten zeerste aan te raden. Daarnaast zijn er 'session' cookies die worden gebruikt om één specifiek bezoek aan de website te identificeren.

In de policy is te lezen dat de cookies worden gebruikt om de kwaliteit van de service te verbeteren, door gebruikers voorkeuren en trends op te slaan. LinkedIn kan derde partijen toestaan om een unieke cookie op de computer van de gebruiker te plaatsen. Informatie die aan derden wordt verstrekt door middel van deze cookie zal niet persoonlijk identificeerbaar zijn, maar geeft alleen informatie over iemands marktsegment, geografische locatie, beroep, professionele en educatieve achtergrond, allemaal ter verbetering van zijn of haar gebruikerservaring. Deze paragraaf geeft te denken over de voorgenoemde mogelijkheid tot 'opt-out'. Immers als de gebruiker heeft aangegeven geen informatie te willen delen met derden, maar deze cookie desalniettemin wordt toegestaan, dan lijkt dat met elkaar in tegenspraak. Echter, met een cookie kan wel informatie over de gebruiker verzameld worden, maar die informatie is dan niet aan zijn of

[43] Let wel: Deze cookie staat dus los van het antwoord op de vraag of de gebruiker wil dat de browser het wachtwoord opslaat.

haar naam te koppelen. Deze alinea van de privacy policy wordt afgesloten met de melding dat, wanneer de settings van de browser geen cookies accepteert of ervoor is gekozen om alle cookies te weigeren, de dienst van LinkedIn wellicht niet te gebruiken is.

'Ad networks' is de naam die LinkedIn geeft aan derden in de vorm van andere bedrijven die advertenties verzorgen voor de gebruikers. LinkedIn bedient zich, evenals Facebook, ook van de eerdergenoemde 'web beacons'. Deze zorgen dat de 'ad networks' geanonimiseerde, geaggregeerde, gecontroleerde en onderzochte gegevens ontvangen, zodat de gebruiker advertenties ontvangt die bij hem of haar passen. Er wordt echter bij vermeld dat het hier ook kan gaan om advertenties die verschijnen bij het bezoeken van andere websites! Met andere woorden, het eerste principe van LinkedIn heeft dus echt alleen betrekking op de naam, maar voor het overige wordt er getracht om een zo volledig mogelijk profiel van de gebruiker te maken en op basis hiervan de advertenties, die hij of zij bij zijn of haar overig internetgebruik ontvangt, aan te passen. Bovendien is het voor deze bedrijven mogelijk om hun eigen cookies op de computer van de gebruiker te plaatsen, aan te passen of te bekijken, omdat de browser om deze advertenties en 'web beacons' moet vragen bij de server van het 'ad network'. Wederom is het wel mogelijk om deze plaatsing van 'web beacons' en cookies uit te schakelen. Dit moet de gebruiker dan echter wel zelf zo instellen.

Bij LinkedIn heeft men de mogelijkheid om de eigen gegevens in te zien, te corrigeren en/of te verwijderen. Als de informatie aangepast wordt, kan het zijn dat er een kopie van de originele informatie door LinkedIn wordt bewaard. Wie gebruik wil maken van dit recht moet mailen naar *privacy@linkedin.com* of door anderszins contact op te nemen met het bedrijf zelf.

- **Het gebruik van de informatie die over iemand wordt verzameld**

LinkedIn onderhoudt contact met haar gebruikers door middel van e-mail en notities op de websites. Het is niet mogelijk om communicatie omtrent het functioneren van het account uit te schakelen. Informatie die wordt verstuurd met promotionele doeleinden kan wel worden uitgeschakeld. LinkedIn heeft ook betaalde services die door middel van een creditcard moeten worden betaald. Om deze betaling af te handelen wordt de informatie omtrent de persoon verwerkt zover dat hiervoor noodzakelijk is. Bij 'account and settings' kan ook ingesteld worden hoeveel persoonlijke informatie publiekelijk wordt gemaakt. Dit is standaard ingesteld op 'full view', ofwel volledig, maar kan door de gebruiker worden aangepast. Het e-mailadres blijft echter standaard verborgen. Ook bij LinkedIn kan er gebruik worden gemaakt van services van andere organisaties, zoals platformapplicaties, welke worden aangeboden door een ondergroep van ontwikkelaars of door één van de 'partners' van LinkedIn. In dit laatste geval wordt de informatie van het profiel gedeeld met de partner, omdat deze door LinkedIn wordt vertrouwd. Hierdoor kunnen gecombineerde services worden aangeboden. Als iemand dus met LinkedIn in zee gaat, dan gaat hij of zij wat persoonlijke gegevens betreft ook in zee met hun partners, als hij of zij daarvoor kiest tenminste. LinkedIn zegt wel de partners grondig te onderzoeken. Voor de overige ontwikkelaars van platforms moet de gebruiker gewoon toestemming geven om gegevens te delen. Met deze ontwikkelaars zijn afspraken gemaakt ten aanzien van de opslag en het gebruik van informatie, maar LinkedIn kan niet garanderen dat deze ontwikkelaars zich hier ook aan houden. LinkedIn neemt dan ook geen verantwoordelijkheid voor de acties van de ontwikkelaars. Het is niet duidelijk of dit ook geldt ten aanzien van de ontwikkelaars die partner zijn. Dat zou betekenen dat de gebruiker de rekening krijgt voor het eventuele onterechte vertrouwen van LinkedIn in haar partners. Er wordt ook aangegeven dat bepaalde acties van een gebruiker door middel van de applicaties zichtbaar zullen zijn voor zijn of haar contacten. Dit kan natuurlijk heel vervelend zijn als de applicatie impliceert dat iemand naar ander werk zoekt en één van zijn of haar contacten een collega is met wie hij of zij deze informatie eigenlijk niet wilde delen.

Gebruikers kunnen ook worden benaderd voor onderzoek. Antwoorden op de gestelde vragen kunnen openbaar worden gemaakt. Het is dus verstandig van tevoren na te gaan of dit het geval is, zeker met betrekking tot onderzoeken waarin wellicht gevoelige informatie prijsgegeven wordt. In 'account and settings' kan aangegeven worden dat de gebruiker niet voor onderzoek wil worden benaderd.

Alle informatie die geopenbaard wordt in publiek chat-, forum- en blogverkeer kan worden gelezen, gebruikt of verzameld door andere gebruikers van deze diensten, maar ook door platform ontwikkelaars en andere derden en kan worden gebruikt om ongevraagde boodschappen te versturen, met andere woorden spammen, zo staat in de volgende paragraaf te lezen. Het is niet duidelijk of dit ook geldt voor een forum van bijvoorbeeld vijf deelnemers, dat verder gesloten is. Laten we aannemen van niet. Het is desondanks opmerkelijk dat spam wordt verstuurd basis van het deelnemen aan een forum. Vermoedelijk gaat het hier om gevallen waarin de gebruiker wel de contactinformatie die daarvoor nodig is zelf plaatst.

LinkedIn geeft aan dat, wanneer de wet ze hiertoe verplicht, ze persoonlijke informatie over een gebruiker zullen overdragen. Dit doen ze alleen als ze er 'goed vertrouwen' in hebben dat ze zich moeten schikken naar het bevel van de gerechtelijke instantie, maar ook om hun eigen rechten uit te oefenen en/of te verdedigen.

LinkedIn geeft aan dat bij een reorganisatie of verkoop van onderdelen van LinkedIn de persoonlijke informatie ook kan worden overgedragen aan de derde partij die dit onderdeel overneemt.

Tenslotte geeft LinkedIn aan dat ze alle persoonlijke informatie goed beveiligen. Ze plaatsen hier echter wel een kanttekening bij het gebruik van e-mail, 'instant messaging' en andere soortgelijke manieren van communicatie met andere gebruikers over het LinkedIn-netwerk, omdat deze niet is versleuteld en daarom wordt men nadrukkelijk verzocht om geen vertrouwelijke informatie via deze kanalen te versturen. Het is verstandig dit advies ter harte te nemen.

- **Auteursrecht**

De gebruikersovereenkomst is van toepassing op alle informatie die een gebruiker op LinkedIn zet. Op al die informatie, variërend van concepten, ideeën, technieken of welke andere data dan ook, wordt een non-exclusief, onherroepelijk, wereldwijd, eeuwigdurend, ongelimiteerd toewijsbaar, 'sublicentieerbaar', onbezwaard recht aan LinkedIn toegekend om dit te kopiëren, er een afgeleide van te maken, verbeteren, verspreiden, verwijderen, publiceren, vasthouden, toevoegen of om het op welke denkbare, eventueel toekomstige manier te commercialiseren. Om het kort samen te vatten, door iets op LinkedIn te zetten, worden al de exclusieve rechten met betrekking tot dat werk overgedragen aan LinkedIn. De gebruiker garandeert daarbij dat deze informatie nauwkeurig, niet vertrouwelijk en niet in strijd is met eventuele, al dan niet contractuele, afspraken met derden. Als deze informatie wel vertrouwelijk is en er vindt een rechtszaak plaats, dan moet de gebruiker volgens de gebruiksovereenkomst LinkedIn schadeloos stellen.

- **Disclaimer**

Ook LinkedIn sluit aansprakelijkheid zoveel mogelijk uit. Er wordt nadrukkelijk gewezen op het feit dat *"LinkedIn does not have any obligation to verify the identity of the persons subscribing to its services, nor does it have any obligation to monitor the use of its services by other users of the community; therefore, LinkedIn declines all liability for identity theft or any other misuse of your identity or information."* Maar, evenals Facebook, stelt ze dat de gebruiker haar schadeloos stelt wanneer hij of zij schade veroorzaakt door zich niet te houden aan de gebruikersovereenkomst.

5.4 Gegevens die anderen over iemand op een sociale netwerksite genereren

Het is mogelijk dat er buiten een persoon om gegevens die hem of haar betreffen op een sociale netwerksite terecht komen. Dit kan op verschillende manieren.

Ten eerste is het mogelijk dat er bestanden, waar de betrokken persoon al dan niet aan heeft meegewerkt, op een sociale netwerksite komen. Het is haast een onvermijdelijke gevolg van de digitale revolutie en de gemakkelijke reproduceerbaarheid die hier onlosmakelijk mee verbonden is, dat bestanden overal snel en makkelijk worden verspreid. Nu zal dit zeker niet met ieder bestand gebeuren, maar het is mogelijk dat een bestand een eigen leven gaat leiden. De kans

hierop is het grootst als mensen een reden hebben om een dergelijk bestand te verspreiden, het moet een bepaalde vorm van nieuwswaarde hebben. Een goed voorstelbare reden hiervoor is dat het betreffende bestand heel grappig is. Op deze manier kan beeldmateriaal waaraan de betrokken persoon niet perse heeft meegewerkt, laat staan toestemming voor verspreiding heeft gegeven, zomaar de hele wereld rond gaan. Hiervan zijn al talloze voorbeelden.

Een tweede manier waarop informatie buiten de gebruiker om op een sociale netwerksite kan belanden is door middel van roddels. 'Krabbels' op Hyves kunnen gevoelige informatie bevatten over een persoon en hier is helaas weinig aan te doen. Als het echt de perken te buiten gaat en deze persoon er achter komt dan is het echter wel mogelijk om hier protest tegen aan te tekenen. Ook is het mogelijk dat er op een sociale netwerksite een haatcampagne op touw wordt gezet tegen een persoon, een goed voorbeeld hiervan is de anti-joranhyve. Het is in theorie wel mogelijk om de aanstichter van zo'n campagne juridisch aan te pakken, maar of het slachtoffer daar veel mee opschiet is de vraag. Het kwaad is dan immers al geschied en een rechtszaak leidt alleen maar tot meer publiciteit.

Een derde manier en misschien wel de meest kwalijke en voor de hand liggende van allen is dat er een account bij een sociale netwerksite kan worden aangemaakt, waarbij gebruik wordt gemaakt van andermans identiteit. Dit kan een foto, naam of een combinatie van beide zijn. Ook hierbij geldt dat er bezwaar kan worden gemaakt bij de sociale netwerksite tegen het feit dat dit gebeurt, maar de persoon wiens identiteit wordt gebruikt moet hier natuurlijk wel eerst achter komen.

5.5 Conclusie sociale netwerksites

Sociale netwerksites lijken bij uitstek geschikt om een digitale identiteit, een reputatie online, vorm te geven. Dat zijn ze ook. Sociale netwerksites brengen iemands 'netwerk' in kaart (voor de persoon zelf en voor anderen), bieden de gebruiker allerlei mogelijkheden (bijvoorbeeld om mensen op de hoogte houden van interessante ontwikkelingen en om zelf op de hoogte te blijven) om zijn of haar digitale ego te pimpen en uit te dragen. Maar er zijn wel een paar kanttekeningen te maken.

Sociale netwerksites zijn over het algemeen gratis.[44] Toch zijn de aanbieders van sociale netwerksites commerciële bedrijven, dus het geld moet wel ergens vandaan komen. Van advertenties dus en die zijn effectiever naarmate ze meer aansluiten bij interesses van degene die ze te zien krijgt. En dus zijn persoonlijke gegevens interessant, ze zijn namelijk commercieel te exploiteren.

De privacy-statements of -policies van sociale netwerksites beginnen met heel mooie uitgangspunten, maar verderop blijkt vaak dat ze eigenlijk juist het commerciële gebruik van persoonsgegevens faciliteren. De drie hier besproken sociale netwerksites, Hyves, Facebook en LinkedIn, laten zich niet goed in een rangorde zetten voor wat betreft de omgang met persoonsgegevens, de regels zijn daarvoor te ingewikkeld en ondoorzichtig geformuleerd.

In het algemeen worden algemene voorwaarden en privacy statements niet of alleen heel vluchtig gelezen – maar een gebruiker moet er wel mee akkoord gaan om de sociale netwerksite te kunnen gebruiken. En door ermee akkoord te gaan geeft hij of zij toestemming voor commerciële exploitatie van zijn of haar persoonsgegevens – iets waar men zich wel van bewust moet zijn. En bij applicaties die door derden worden aangeboden op een sociale netwerksite is de omgang met persoonsgegevens nog onduidelijker.

[44] Al is er ook altijd wel een betaalde variant die meer mogelijkheden biedt.

Waar men ook op bedacht moet zijn is misbruik van gegevens door 'vrienden' of contacten. Of misbruik door wie dan ook, van de gegevens (bv. naam, profielfoto en contacten) die voor iedereen zichtbaar zijn. Wees dus selectief in het accepteren van vrienden of contacten[45], schoon regelmatig de lijst met 'vrienden' op ('ontvrienden' heet dat) en in het uiterste geval kan natuurlijk altijd een account opgezegd[46] worden en kan (eventueel) opnieuw met een schone lei begonnen worden.

Tenslotte is er geen duidelijkheid over de beveiliging van gegevens, zoals de maatregelen tegen verlies, diefstal of oneigenlijk gebruik. In exoneratieclausules en disclaimers wordt alle aansprakelijkheid van de hand gewezen.

Kortom: Het is verstandig om alleen persoonlijke gegevens te publiceren die de hele wereld tot in lengte van dagen mag weten. En omdat dat niet altijd te overzien is, is het beter om terughoudend te zijn met het vermelden van sappige details.

5.6 Vergelijkingstabel sociale netwerksites

	Hyves	**Facebook**	**LinkedIn**
Valt onder Wbp	Ja	nee	ja
Verwerkt informatie met toestemming in Algemene Voorwaarden of privacy policy	Ja	ja	ja
Mogelijkheid om schotten aan te brengen in profielinformatie	Ja	ja	nee, alleen lijst met connections is onzichtbaar te maken
Toesnijden van advertenties door middel van cookies	ja, met opt-out	ja, met opt-out	ja
'Web beacons' van derde partijen	Nee	ja	ja
Verzamelt zelfstandig informatie over gebruiker uit andere bronnen	Nee	ja	nee
Auteursrecht	vergaande licentie	vergaande licentie	vergaande licentie
Disclaimer	zoveel mogelijk aansprakelijkheid uitgesloten	zoveel mogelijk aansprakelijkheid uitgesloten	zoveel mogelijk aansprakelijkheid uitgesloten

[45] Idealiter zou via een ander kanaal gecheckt moet worden of die ander ook werkelijk is wie hij of zij zegt dat hij of zij is.

[46] Of zelfs een tool gebruiken om iemands hele digitale identiteit om zeep te helpen: de Web 2.0 Suicide Machine op http://suicidemachine.org/; Facebook was, na verluid, "not amused": www.security.nl/artikel/31997/1/Facebook_verbiedt_digitale_zelfmoord.html.

6 Online identiteitsmanagement

Online identiteitsmanagement omvat een tweetal aspecten: het opbouwen van een online identiteit en ook het managen, het beschermen en onderhouden ervan. Op beide aspecten wordt in dit hoofdstuk ingegaan.

6.1 Opbouw online identiteit

Bepaal imago
Uitgangspunt van identiteitsmanagement (zowel online als offline) is dat iemand een duidelijk beeld heeft van hoe hij of zij zichzelf wil presenteren. Welk beeld wil iemand dat mensen van hem of haar hebben? Daar worden kleding, gedrag en kapsel op afgestemd. En ook wat er op internet over iemand te vinden is moet daarop gericht zijn. Heel in het algemeen geldt dat alleen online gezet zou moeten worden datgene wat iedereen, tot in de lengte van dagen, over die persoon mag weten.

Natuurlijk kan dat beeld in verschillend contexten anders zijn – dat kan in real life en dat kan op internet ook. Indien nodig moeten er dan wel schotten tussen die contexten zijn: een geweldige reputatie in de game-wereld draagt niet noodzakelijkerwijs in positieve zin bij aan iemands professionele imago.

Dus: wat voor beeld wil iemand over zichzelf schetsen, in welke contexten? Het gaat hier verder alleen over het imago als wetenschapper of professional (in spe). Het is belangrijk om ervoor te zorgen dat andere persoonlijke informatie op internet, die niet positief bijdraagt aan dat imago niet in verband gebracht kan worden met de professionele online identiteit (dus: door een goede 'nickname' te gebruiken). In zekere zin komt dat dus neer op: een dubbelleven leiden. In het echte leven wordt ook niet alles wat er over iemand te weten valt aan iedereen verteld. Dat zou online ook niet moeten gebeuren.

Website
Een wetenschapper doet er goed aan een mooie, goed gevulde eigen website te hebben, bij voorkeur in de huisstijl van de instelling waar hij of zij aan verbonden is. Als iemand een naamgenoot heeft, kan dat een goede reden zijn om een foto online te zetten. Alles waar een wetenschapper trots op is kan op die websites: publicaties (liefst 'open access' beschikbaar),[47] lezingen, conferenties,etc. Zorg voor veel en interessante content, en leg links naar sites die voor vakgenoten interessant zijn, dat is goed voor het bezoekersaantal van de site. Met een tellertje kan het aantal bezoekers van de site in de gaten gehouden worden en soms valt ook te zien via welke provider bezoekers binnenkomen.

Als elke publicatie en bij elke link opnieuw de naam van de auteur vermeld wordt is dat goed voor diens pagerank[48] als in de zoekmachine op de naam van die auteur gezocht wordt. Veel links naar een professionele website, en het feit dat iemands naam vaak op internet te vinden is, zijn ook goed voor zijn of haar online reputatie en pagerank. Geef alleen zakelijke contactinformatie (liefst

[47] Of eigen publicaties ook zelf gepubliceerd mogen worden hangt af van de afspraak met de uitgever. Voor boeken geldt vaak dat het auteursrecht overgedragen is (er is dan een contract, een onderhandse akte getekend), in dat geval mag een tekst niet zonder meer opnieuw door de auteur zelf gepubliceerd worden door 'm op een website te zetten. Bij tijdschriftartikelen geldt dat vaak niet: als er niets getekend is, is er geen auteursrecht overgedragen maar hooguit een licentie gegeven voor eenmalige publicatie. Eigen tekst mag in dat geval wel zelf nog een keer gepubliceerd worden door 'm op een website te zetten – maar misschien niet in de opmaak die voor het tijdschrift is gebruikt (op die opmaak kan namelijk ook weer auteursrecht zitten). Het verstandigst is om zelf een pdf van het oorspronkelijke manuscript te maken, met uiteraard vermelding waar het gepubliceerd is, en die als downloadable bestand op de site te zetten. Vraag wel eventuele mede-auteurs om toestemming.

[48] Je plaats in de lijst van zoekresultaten.

nog via een contactformulier om spam te voorkomen). Zorg voor een goede URL en zet die standaard onder e-mailberichten, op visitekaartjes, etc.

Weblog
Een uitstekende manier om een goede reputatie op internet op te bouwen is door het bijhouden van een weblog, waarin relevante ontwikkelingen op je vakgebied gesignaleerd worden en eventueel van commentaar en links voorzien worden. Een weblog dwingt de blogger zelf ook om zijn of haar vakgebied goed bij te houden. Het nadeel is ook meteen duidelijk: het kost veel tijd en werk.

Sociale netwerksites
Ook het gebruik van sociale netwerksites is een uitstekende manier om een online identiteit vorm te geven. Het profiel op zo'n site geeft vaak de mogelijkheid om naar een eigen website te linken. Ook op die sociale netwerksite kan alles gezet worden waar iemand trots op is en waarvan hij of zij zeker weet dat iedereen het altijd van hem of haar mag weten. Hoewel het bij sommige sociale netwerksites mogelijk is om schotten aan te brengen tussen de informatie die aan verschillende groepen bekend gemaakt wordt, doet men er goed aan daar niet al te veel op te vertrouwen. Echt vertrouwelijke informatie, of zaken (foto's, filmpjes, maar ook discutabele adviezen bijvoorbeeld) die tot problemen zouden kunnen leiden, kunnen misschien wel in de echte wereld met vrienden of collega's gedeeld, maar het is niet verstandig om die op internet te zetten.

Overige openbare informatie
Iedere keer als iemand onder zijn of haar eigen naam op een sociale netwerksite, forum, digitale petitie, datingsite, of andersoortig publiekelijk toegankelijke website informatie toevoegt, de mogelijkheid bestaat dat deze informatie voor de rest van zijn of haar leven voor iedereen vindbaar is. Daarom zou men bij het achterlaten van informatie in de digitale publieke ruimte, zich altijd moeten afvragen of het geen probleem is dat deze informatie voor altijd voor iedereen vindbaar is. Bijvoorbeeld: als iemand ooit op het forum van ouders online onder haar eigen naam haar hart lucht over het gedrag van haar dwarse peuter, dan moet ze er rekening mee houden dat iedereen voortaan van haar kan weten dat ze moeder is.

Het is wel goed voor iemands reputatie op internet, en voor zijn of haar vindbaarheid, om veel aan online discussies mee te doen, goede adviezen te geven en veel te linken naar de eigen site en eigen publicaties.

Als een wetenschapper te maken krijgt met pers, vakbladen, kranten, radioprogramma's etc., is het belangrijk om zich te realiseren dat dergelijk communicatie eigenlijk altijd ook op internet verschijnt. Ook hierbij is dezelfde vraag belangrijk: Wil ik dat deze informatie voor altijd, voor iedereen vindbaar is? Als iemand zelf iets opstuurt naar de opiniepagina van een krant en dit stuk wordt opgepikt door websiteredacteuren, dan kan het zomaar gebeuren dat dat stuk opeens verschijnt op tientallen websites.

6.2 Onderhoud online identiteit

Onderhoud van online identiteit wordt ook wel online reputatiemanagement genoemd. Het is een nieuwe tak van dienstverlening,[49] die zich vooralsnog vooral op bedrijven richt, maar ook voor wetenschappers en professionals (in spe) belangrijk is. Niet dat daar meteen een bedrijf voor ingeschakeld moet worden; een ieder kan prima zijn of haar online reputatie in de gaten houden.

In de eerste plaats door regelmatig te checken wat er over hem of haar op internet te vinden is. Bijvoorbeeld door de eigen naam in Google en www.wieowie.nl te zoeken, en door zich aan te melden bij Google-Alerts zodat hij of zij op de hoogte gehouden wordt als er iets nieuws met zijn of haar naam op internet verschijnt. Soms is het nuttig om op berichten te reageren, om de discussie aan te gaan, om zijn of haar mening te geven over zaken die in dat vakgebied belangrijk zijn.

[49] Google maar eens op "online reputatiemanagement" voor bedrijven die zich hiermee bezig houden.

Als er verwarring mogelijk is met naamgenoten, is het slim om in de eigen presentatie die verwarring zoveel mogelijk weg te nemen, bijvoorbeeld door een foto toe te voegen, of in extreme gevallen expliciet te vermelden dat het niet die ander betreft.

Ongewenste informatie
Wat te doen als iemand op informatie over zichzelf stuit die niet past bij het beeld dat hij of zij van zichzelf wilt laten zien?

Eerst moet vastgesteld worden of het om een rechtmatige of een onrechtmatige publicatie gaat. Een rechtmatige publicatie kan bijvoorbeeld een perspublicatie zijn. Als iets doorgaat voor 'journalistiek' (en dat is op internet al vrij snel het geval) dan is er niets aan te doen, tenzij het om apert onjuiste informatie gaat. In dat geval kan om een rectificatie gevraagd worden.
Een onrechtmatige publicatie is één die voor iemand (iemands reputatie) schadelijke gegevens bevat en die niet onder journalistiek valt. Bijvoorbeeld: een valse beschuldiging van een collega, een compromitterende foto, onthullingen die, al dan niet onjuist, hem of haar in een verkeerd daglicht stellen. Bij een onrechtmatige publicatie moet de betrokkene goed bij zichzelf te rade gaan of hij of zij echt wilt proberen om die van het internet af te krijgen. Het komt namelijk voor dat door de poging er wat aan te doen, een averechts effect bereikt wordt: meer mensen gaan het lezen, er komt meer aandacht voor (bijvoorbeeld ook in de pers) en zo wordt het alleen maar erger.[50]
Als iemand besluit om te proberen de publicatie over hem of haar van internet te verwijderen, dan kan hij of zij een 'notice-and-take-down' verzoek (zie bijlage 1) sturen naar degene die de informatie geplaatst heeft (de 'uploader'). Als die persoon niet te achterhalen is, niet reageert of het verzoek afwijst, kun hij of zij zich met hetzelfde verzoek wenden tot degene die feitelijk in staat is om de informatie te verwijderen, de forumbeheerder, de webhoster, de ISP. Afhankelijk van hoe formeel en juridisch-dreigend hij of zij het verzoek wilt formuleren, kan hij of zij die persoon erop wijzen dat hij zelf aansprakelijk is indien hij de informatie niet verwijdert (art. 6:196c lid 4 BW).

Als laatste kan de persoon die de informatie geplaatst heeft, dan wel degene die feitelijk in staat is om de informatie te verwijderen voor de rechter gesleept (gedagvaard) worden, met de eis dat de informatie verwijderd wordt en blijft. Als het gaat om smaad of laster (het bewust iemand in een kwaad daglicht plaatsen) kan ook nog aangifte bij de politie gedaan worden.

In alle gevallen (zowel bij rechtmatige als bij onrechtmatige informatie) kan Google, met onderbouwing van het verzoek, gevraagd worden om de betreffende vindplaats uit de pagerank te halen. Als iemand een gerechtvaardigd belang heeft, bestaat de kans dat Google zo'n verzoek honoreert.

Ongeoorloofde verstrekking
Stel dat iemand erachter komt dat, in strijd met de regels, persoonlijke informatie van hem of haar is doorgegeven of verkocht aan derden.

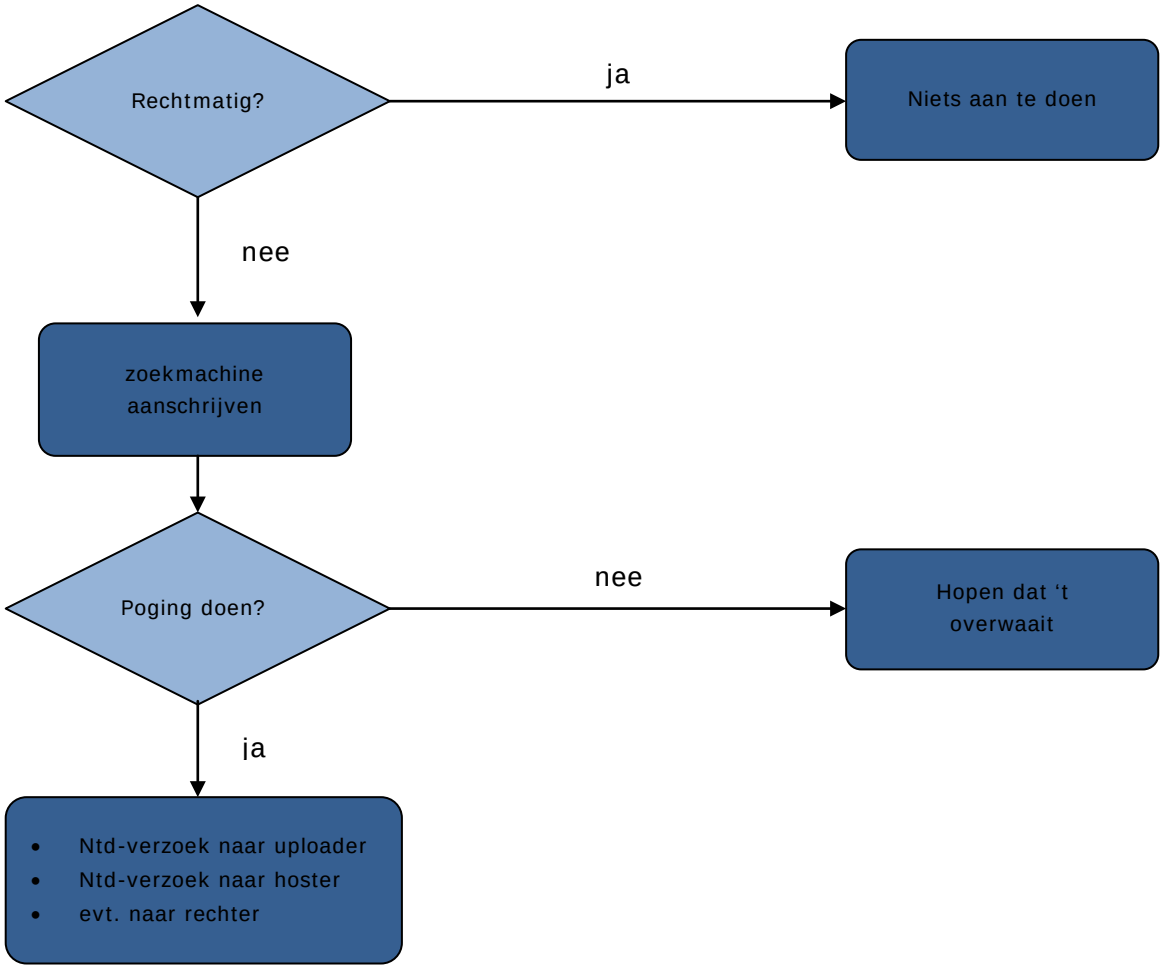
In theorie kan hij of zij dan, op basis van de Wbp, degene die zijn of haar gegevens in strijd met de regels verstrekt heeft, aansprakelijk stellen voor de schade die hij of zij hierdoor lijdt. Probleem is alleen dat die schade in het algemeen lastig of niet te bepalen zal zijn – en het kwaad is dan toch al geschied. Een nog veel groter probleem is dat in het algemeen niet bekend is waar die derde (die hem of haar bijvoorbeeld met ongewenste spam bestookt, of hem of haar niet uitnodigt voor een sollicitatiegesprek) zijn gegevens vandaan heeft. Sterker nog: vaak is men zich er niet eens van bewust dat men op een bepaalde manier behandeld of benaderd wordt, op basis van gegevens die men niet zelf aan die partij verstrekt heeft.

[50] Een extreem voorbeeld is dat van een Braziliaans fotomodel, dat met haar vriend in het openbaar aan het vrijen was, hetgeen gefilmd is en op YouTube werd gezet. Haar vruchteloze pogingen om het filmpje verwijderd te krijgen hebben er slechts toe geleid dat heel Brazilië het filmpje gezien heeft: Zie het bericht op nu.nl: www.nu.nl/internet/1132993/vrijend-braziliaans-model-verliest-zaak-tegen-youtube.html. Inmiddels is het filmpje overigens niet meer op YouTube te vinden.

Conclusie: in de praktijk staat men redelijk machteloos tegen ongeoorloofde verstrekking, tenzij er hard bewijs is dat persoonsgegevens zonder toestemming van de betrokkene en tegen de regels verstrekt zijn, èn die betrokkene daardoor aantoonbare schade lijdt.

Stroomschema ongewenste informatie

Wat iemand kan doen wanneer hij of zij op ongewenste informatie over zichzelf stuit, hangt af of die informatie wel of niet rechtmatig is verkregen:



Aanbevolen literatuur

- Daniel J. Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, San Diego Law Review, Vol. 44, p. 745, 2007, online beschikbaar op http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565&rec=1&srcabs=174508.
- Gedragscode Notice-and-take-down, online beschikbaar op www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf.
- NVP Sollicitatiecode, te vinden op www.nvp-plaza.nl/documents/doc/sollicitatiecode/sollicitatiecode-oktober-2009.pdf.
- College bescherming persoonsgegevens: 'Richtsnoeren Publicatie van Persoonsgegevens op Internet', online beschikbaar op www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf?refer=true&theme=purple.
- Mijn puber op Hyves, mijn kind online special, online beschikbaar op hwww.mijnkindonline.nl/uploads/mijn_puber_op_hyves1.pdf.

Websites

- www.wieowie.nl
- www.archive.org
- www.spamklacht.nl
- www.surfnet.nl/nl/Thema/cybersafe

Bijlage 1: Voorbeeld van een ‘notice-and-take-down’ verzoek

Denk goed na of het verstandig is een dergelijk verzoek te versturen en pas het qua toon en formulering aan aan de omstandigheden!

Geachte heer of mevrouw,

Op [deeplink] kwam ik het volgende bericht/de volgende informatie tegen: “[knip en plak de informatie die je verwijderd wilt hebben]”

Dit bericht/Deze informatie is onrechtmatig ten opzichte van mij, omdat [reden waarom het onrechtmatig is: het tast je aan in je eer en goede naam (aangeven waarom), het maakt inbreuk op je privacy, het maakt inbreuk op jouw auteursrecht]. Ik verzoek u daarom vriendelijk maar dringend/Ik vorder daarom dat u dit bericht/deze informatie meteen verwijdert en verwijderd houdt.
Indien u niet binnen twee dagen/op korte termijn aan mijn verzoek/eis voldoet, zal ik verdere stappen ondernemen.

Hoogachtend,

Naam, emailadres

N.B.
Het verdient aanbeveling om speciaal voor dit doel een apart webmail (Hotmail, Yahoo, Gmail) adres te gebruiken.
Het is te overwegen om dit verzoek meteen in kopie naar degene de sturen die de feitelijke macht heeft om de informatie te verwijderen (forumbeheerder, webhoster, ISP).