# Bescherming persoonsgegevens 2.0

*A. Engelfriet*

**De recent verschenen Richtsnoeren Publicatie van persoonsgegevens op internet gaan niet goed samen met Web 2.0. Op dit nieuwe web staat sociale interactie tussen personen centraal en delen mensen massaal en vrijwillig hun persoonsgegevens met de hele wereld. Niet alleen namen en adresgegevens: ook mededelingen over een persoon zijn te kwalificeren als persoonsgegevens. En dergelijke mededelingen zijn aan de orde van de dag op sociale sites. De Richtsnoeren stellen strenge grenzen voor website-eigenaren, wat zich niet goed verhoudt met het bij Web 2.0 te verwachten niveau van privacy. De grootste knelpunten zitten bij de onderhoudsplicht en de beveiligingsplicht. De hier gestelde eisen zullen veel sociale sites, zoals forums, profielensites en weblogs, in de problemen brengen.**

## 1. Privacy, Web 2.0 en sociale sites

Op 11 december 2007 verschenen de *Richtsnoeren Publicatie van persoonsgegevens op internet* (hierna: de Richtsnoeren).[1] De Richtsnoeren geven aan hoe de Wet bescherming persoonsgegevens (Wbp) geldt voor website-eigenaren, forumbeheerders en andere internetters die persoonsgegevens verwerken.

Wbp en Richtsnoeren zien de internetter als consument: een passieve gebruiker van informatie, wiens persoonsgegevens hem door grote bedrijven worden ontfutseld en op een ondoorzichtige manier voor alle mogelijke doeleinden worden gebruikt. De Wbp is bedoeld om de consument te beschermen tegen misbruik in deze ongelijke situatie.[2]

De afgelopen jaren heeft zich op internet een kleine revolutie voorgedaan: Web 2.0. Dit is de verzamelnaam voor een nieuwe manier van omgaan met het World Wide Web. Websites zijn geen geïsoleerde silo's meer waarin een kleine, professionele redactie publiceert en de bezoeker braaf consumeert wat hem wordt aangeboden. Web 2.0 stelt sociale interactie tussen natuurlijke personen centraal.[3] Sites waarop dit gebeurt, heten dan ook *community sites* of in goed Nederlands *sociale sites.* Er zijn drie belangrijke soorten: discussieforums, weblogs en profielensites.[4] Deze worden uitgebreid besproken in het artikel van Van den Hoven van Genderen en Lodder in het vorige nummer.[5]

*Discussieforums* bieden de mogelijkheid om discussies te voeren, vaak rond een thema zoals computers, tuinieren, ziektes of persoonlijke problemen. Er is meestal weinig centrale sturing; binnen het thema leveren de deelnemers zelf de stellingen en reacties aan. Het grootste forum voor juristen is Rechtenforum.nl. Een variant op het forum is de *wiki:* de deelnemers schrijven (en bediscussiëren) gezamenlijk een artikel. Het bekendste voorbeeld is de 'vrije encyclopedie' Wikipedia.

Een *weblog* is een site waarbij artikelen chronologisch worden aangeboden, vaak in de vorm van een dagboek of serie columns. Lezers kunnen reageren en volautomatisch berichten in hun eigen blog verwerken.[6] Zo ontstaat een gemeenschap van gekoppelde blogs: de *blogosfeer.* Bekende blogs zijn Sargasso, Frankwatching, Dutch Cowboys en Geenstijl.

Op een *profielensite* of netwerksite presenteren mensen niet alleen zichzelf, zij kunnen hun profiel koppelen aan dat van vrienden of zakelijke relaties. Een dergelijk profiel bevat naam en contactgegevens, informatie over interesses, hobby's, werk en vaak ook foto's. De twee in Nederland bekendste profielensites zijn Hyves en LinkedIn. Netwerksites worden soms ook als een virtuele wereld vormgegeven, zoals bij Second Life en Habbo Hotel.

Hoe revolutionair dit Web 2.0 concept was, blijkt wel uit het feit dat U, de participerende consument, in 2006 door Time Magazine werd uitgeroepen tot persoon van het jaar.[7]

## 2. Persoonsgegevens op sociale sites

Bij sociale sites leveren de gebruikers, of liever gezegd de *deelnemers,* zelf de inhoud, in de vorm van discussies, reacties, informatie over zichzelf enzovoorts. Men bouwt een

1. *Stcrt.* 2007, 240, 11 december 2007.
2. J. Terstegge 'Privacy in the law', in: M. Petkovi en W. Jonker (red.), *Security, Privacy and Trust in Modern Data Management,* New York: Springer 2007, p. 18.
3. T. O'Reilly, 'What is Web 2.0', O'Reilly.com website 30 september 2005. www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.
4. D. Tapscott en A. D. Williams, *Wikinomics: How Mass Collaboration Changes Everything,* New York: Penguin, 2007, p. 14. Zie ook J. Kolbitsch en H. Maurer, 'The Transformation of the Web: How Emerging Communities Shape the Information we Consume', *Journal of Universal Computer Science,* vol. 12, no. 2 (2006), 187-213.
5. R. van den Hoven van Genderen en A.R. Lodder, 'Informatie leveren tegen elke prijs? Verkenning van het recht rond Web 2.0', *IR* 2008, 1, p. 4-8.
6. Zie ook E. Jacobs en W. Schreurs, 'U blogt toch ook?', *Ad Rem* 2005-5, p. 38-45. De auteur van dit artikel blogt dan ook op http://blog.iusmentis.com/.
7. *Time Magazine,* 'Person of the year: You'. 25 november 2006. http://www.time.com/time/magazine/article/0,9171,1569514,00.html.

Hyves-profiel, publiceert het CV in LinkedIn en discussieert mee op forums, wiki's en andere sociale sites. Het gemak waarmee mensen dit doen, vond stichting Bits of Freedom dusdanig schrikbarend dat men de *Big Brother Award* 2007 uitreikte aan diezelfde U.[8]
De Richtsnoeren bevatten strenge regels die bedoeld zijn om misbruik van persoonsgegevens op internet tegen te gaan. Sociale sites zijn echter ontworpen met als doel het publiceren en verspreiden van persoonsgegevens door de deelnemer zelf. In deze bijdrage zal ik laten zien dat deze twee uitgangspunten niet goed samengaan en dat de Richtsnoeren sociale sites dus eerder hinderen dan helpen.[9]
Daarbij moet worden opgemerkt dat de Wbp, en daarmee ook de Richtsnoeren, onverkort van toepassing zijn op sociale sites.[10] De uitzondering voor huishoudelijk gebruik (art. 2 lid 1 Wbp) gaat zelden op voor websites.[11] Alleen sites die toegang bieden tot een kleine en duidelijk afgebakende groep personen, en deze toegang ook nog eens adequaat afschermen voor derden, kunnen zich op deze uitzondering beroepen.[12] Dit is bij sociale sites zelden het geval. Het is juist de bedoeling dat iedereen lid kan worden van de gemeenschap. Sociale sites zijn ook meestal niet bezig met journalistieke uitingen.[13] Deze uitzonderingen laat ik dan ook verder buiten beschouwing.

## 3. Herleidbaar tot natuurlijke persoon

Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1(a) Wbp). Dit begrip wordt zeer breed uitgelegd.[14] Naast namen en nummers van personen vallen er bijvoorbeeld ook informatie over personen onder ('Peter heeft diabetes'). Gegevens over personen kunnen ook *subjectief* zijn: meningen en oordelen over een herkenbare persoon zijn ook persoonsgegevens.[15] De vorm waarin de informatie beschikbaar is, is niet relevant. Een profiel op bijvoorbeeld Hyves of LinkedIn is dus evident een verzameling persoonsgegevens. Maar ook een *mededeling over* een deelnemer is een persoonsgegeven. En dergelijke mededelingen zijn aan de orde van de dag op sociale sites: denk aan complimentjes bij iemands profiel, kritische reacties op een forumbericht of een persoonlijke aanval op een weblog. Of, heel eenvoudig, de naam van degene die een bericht plaatst.
Gegevens zijn persoonsgegevens als de identiteit van de persoon er redelijkerwijs, zonder onevenredige inspanning, mee kan worden vastgesteld.[16] Op internet wordt vaak gebruik gemaakt van pseudoniemen. Deze zijn hooguit herleidbaar tot het e-mailadres waarmee, of tot het IP-adres vanaf waar het pseudoniem is aangevraagd (geregistreerd). Voor verdere identificatie is medewerking van de internetaanbieder van de persoon in kwestie nodig. Dit is geen onevenredige inspanning, aldus het CBP.[17] Ook profielen en bijdragen onder pseudoniem zijn dus persoonsgegevens. Zelfs wijzigingen in Wikipedia zijn al snel persoonsgegevens. De 'vrije encyclopedie' publiceert het pseudoniem of het IP-adres van de maker van de wijziging in een voor iedereen zichtbare plek. De bijdragen is via deze publicatie te traceren naar de persoon die deze geplaatst heeft.
Zogeheten *bijzondere* persoonsgegevens zijn gegevens over ras, godsdienst, gezondheid, politieke of seksuele voorkeur (art. 16 Wbp). Hiervoor geldt een strenger regime. Op internet is dit vooral van belang bij foto's en ander beeldmateriaal.[18] Maar ook bij registratie van gebruikers wordt wel eens gevraagd naar zulke gegevens – denk aan een *dating*site of een profielensite zoals Gay.nl.

## 4. Privacyverwachting bij sociale sites

Persoonlijke levenssfeer, privacy, houdt niet op bij de voordeur.[19] Privacy geldt ook bij internetgebruik, zo blijkt uit rechtsoverweging 41 van het *Copland*-arrest van het EHRM.[20] Men mag dus enige mate van privacy verwachten bij uitlatingen op internet. Het gemak waarmee mensen persoonsgegevens over zichzelf delen, zou verklaard kunnen worden uit een verwachting dat deze gegevens binnen de groep van deelnemers aan de site blijft. Wie iets over zichzelf onthult op zijn Hyves-profiel of in een bijdrage op een discussieforum verwacht dat niet op een sollicitatiegesprek terug te horen. De vraag is wel of die verwachting onder alle omstandigheden *redelijk* is.
De Wbp geeft immers uitvoering aan (o.a.) art. 8 EVRM.[21] Uit de jurisprudentie van het EHRM blijkt dat dit artikel een *reasonable expectation of privacy* met zich meebrengt.[22] Zoals Dommering het in zijn noot bij *Copland* formuleert: wat mag men in de gegeven omstandigheden, gelet op de

8. 'U bent de winnaar van de Big Brother Awards 2007', persbericht stichting Bits of Freedom, 21 september 2007. http://www.bigbrotherawards.nl/.
9. Zie ook T. van Ringelestijn en P. Olsthoorn, 'Privacyregels versus web 2.0; een achterhaalde strijd?', *Netkwesties* 148, 29 december 2006. www.netkwesties.nl/editie148/artikel2.html.
10. Richtsnoeren p. 7-8. Vgl. P. Blok, 'De waarde van de omnibuswet', *Privacy & Informatie* 2005, p. 246-252.
11. HvJ EG 6 november 2003, zaak C-101/01, *Jur.* 2003, p. I-12971 (Lindqvist). Zie ook G-J. Zwenne, 'Bodil Lindqvist - Noot bij Europees Hof van Justitie 6 november 2003', *JAVI* 2004, 2, p. 66-69.
12. Richtsnoeren p. 12-13.
13. Richtsnoeren p. 43. Dit vooral vanwege het criterium of sprake is van 'iets van maatschappelijke strekking aan de orde te stellen'. Dit zal bij een discussieforum of netwerksite over het algemeen niet het geval zijn.
14. G-J. Zwenne et al., *Eerste fase evaluatie Wet bescherming persoonsgegevens*, WODC-rapport december 2007, p. 61.
15. *Advies 4/2007 over het begrip persoonsgegeven* (WP 136), Artikel 29-Werkgroep, 20 juni 2007, p. 6-9.
16. Overweging 26 van Richtlijn 95/46/EG.
17. Richtsnoeren p. 11.
18. Richtsnoeren p. 16.
19. HR 1 juli 1988, *NJ* 1988, 1000 (Vondelpark).
20. EHRM 3 april 2007, *NJ* 2007, 617 (Copland) m.nt. EJD.
21. *Kamerstukken II* 1997/98, 25 443, nr. 3, p. 8 (MvT).
22. EHRM 26 juni 1997, *NJ* 1998, 506, m.nt. PJB (Halford) en het *Copland*-arrest (zie noot 21). Zie ook P. de Hert en A. Hoefmans, 'Het arrest Copland in het kader van de verdieping van de Europese rechtspraak op het gebied van privacybescherming', *European Human Rights Cases* 13 juni 2007, vol. 8, nr. 6, p. 664-674.

heersende maatschappelijke opvattingen verwachten aan privacy, en welke verwachtingen behoren daarbij gehonoreerd te worden?[23]
De aard van sociale sites zal de doorslag moeten geven bij de beantwoording van deze vraag. Het bijzondere hier is immers dat de deelnemer zelf de informatie kiest die hij bloot wil geven, en die zelf ook nog eens publiceert. Hij bericht op zijn eigen weblog, en weet dat zijn berichten door anderen opgepikt, becommentarieerd en doorgeplaatst zullen worden. Hij plaatst bijdragen op forums en wiki's, of vermeldt dingen over zichzelf in zijn Hyves-profiel. De deelnemer lijkt dan weinig privacy te willen, en zou daarom ook niet veel privacy moeten verwachten.[24]
Wie zelf publiceert op een website, moet weten dat een potentieel groot publiek daar kennis van kan nemen. Het is dan niet redelijk om te verwachten dat verspreiding van deze informatie controleerbaar blijft. Door op internet zelf informatie te onthullen, stelt men zichzelf bloot aan het risico dat deze informatie elders opduikt en aanvaardt men de kans dat men daardoor schade zou kunnen lijden.[25] Het te verwachten niveau van privacy zal bij sociale sites dus laag zijn.[26]

## 5. Rechtvaardigingsgrond voor verwerking

De Wbp biedt geen lichter of zwaarder regime afhankelijk van het te verwachten niveau van privacy bij een verwerking van persoonsgegevens. Hoe publiek of privé de gegevens ook zijn, wie ze op internet publiceert, moet zich aan dezelfde strenge regels houden.
De belangrijkste regel is dat de beheerder van een sociale site een rechtvaardigingsgrond nodig heeft voor de verwerking (art. 8 Wbp). De Richtsnoeren presenteren toestemming als de hoofdregel, en andere grondslagen als uitzonderingen.[27] Bij sites waar natuurlijke personen hun zelfgemaakte foto's kunnen publiceren moet die toestemming ook nog eens van alle geportretteerden verkregen worden. Ondubbelzinnige toestemming wordt in de praktijk bij dergelijke sites zelden gevraagd. Als dit al gebeurt, dan is het als onderdeel van de algemene voorwaarden voor het gebruik van de sites.[28] Dit is eenvoudig te verklaren. Toestemming vragen is veel werk, en bovendien vaak een wassen neus: mensen lezen zulke juridische verzoeken toch zelden.[29]
Als er geen toestemming van de betrokkene is, moet de verantwoordelijke een aantoonbare noodzaak kunnen noemen. In de praktijk zal zich dit vertalen naar uitvoering van een overeenkomst (art. 8(b) Wbp). Om deel te nemen aan een sociale site is namelijk vrijwel altijd registratie vereist. Bij deze registratie kan acceptatie van een gebruiksreglement worden geëist waarin geregeld is wat de site met de persoonsgegevens mag doen.

Een bijzonder geval betreft toestemming door minderjarigen. Art. 5 lid 1 Wbp stelt expliciet dat bij betrokkenen onder de zestien jaar toestemming van hun wettelijke vertegenwoordiger nodig is. Een door de minderjarige zelf gegeven toestemming is nietig. De bewijslast ligt bij de verantwoordelijke.[30] Er is geen regime voor veronderstelde toestemming analoog aan art. 1:234 lid 3 BW.[31] Deze regel zal grote problemen op gaan leveren voor veel sites, nu meer dan 90 procent van alle jongeren regelmatig online bezig is en 58% vaak gebruik maakt van sociale sites.[32]
Onder omstandigheden zou ook het 'gerechtvaardigd eigen belang' (art. 8 sub f Wbp) een rol kunnen spelen, bijvoorbeeld bij bestrijding van vandalisme of computercriminaliteit (hackpogingen). Zo kan een site de IP-adressen bijhouden van de plaatsers van bijdragen, om indien nodig computers vanaf waar vandalisme wordt gepleegd, te kunnen blokkeren. Het gebruik van een IP-adres voor een blokkade of signalering naar de beheerders in het kader van vandalismebestrijding lijkt gerechtvaardigd. Sommige sociale sites, zoals encyclopedie Wikipedia, gaan verder en publiceren de IP-adressen van anonieme deelnemers, zodat iedereen kan zien wat deze deelnemers doen.[33] De vraag is echter of deze publicatie *noodzakelijk* is.[34] De maatregel riekt naar *naming and shaming*: persoonsgegevens worden getoond om vandalen af te schrikken of te kijk te zetten. Dat is meestal niet toegestaan.[35] Bovendien speelt het probleem dat veel

23. *Supra* noot 21.
24. Zie ook P. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (diss. Tilburg), Den Haag: Boom Juridische uitgevers 2002, p. 52.
25. Rb. Amsterdam 10 juli 1996, *LJN* BA2473 (Wasteland-party), r.o. 12.
26. Vgl. Blok 2002 (*supra* noot 25), p. 106-107, die zich terecht afvraagt of nu werkelijk elke publicatie van een persoonsgegeven als een privacy-probleem behandeld moet worden. Het recht op goede naam zou in veel gevallen een beter passende kapstok moeten bieden bij ongewenste (her)publicatie van persoonsgegevens op sociale sites.
27. Richtsnoeren p. 21.
28. Het is overigens niet voldoende om deze toestemming in algemene voorwaarden op te eisen. Een expliciete *opt-in* is nodig. Vgl. R. van Esch en P. Blok, 'Privacy en elektronische handel via internet', in: J. Berkvens en J. Prins (red.), *Privacyregulering in theorie en praktijk* (Recht en Praktijk 75), Deventer: Kluwer 2007, p. 221.
29. P. Shabayee, 'Informed Consent on the Semantic Web - Issues for Interaction and Interface Designers', *3rd International Semantic Web User Interaction Workshop* (2006). swui.semanticweb.org/swui06/papers/Shabajee/Shabajee.pdf, p. 11.
30. Richtsnoeren p. 21. Zo ook J. Nouwt, *Privacy voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet* (ITeR reeks 73), Den Haag: Sdu Uitgevers 2005, p. 90.
31. J. Nouwt, 'Kinderen, internet en privacy', *Privacy & Informatie* 6, 2003, p. 59-64.
32. A.P. Schouten, *Adolescents' online self-disclosure and self-presentation* (diss. Amsterdam UvA), Amsterdam: The Amsterdam School of Communications Research ASCoR 2007, ISBN 9789079213016, p. 9.
33. http://wikimediafoundation.org/wiki/Privacy_policy.
34. Richtsnoeren p. 23.
35. Richtsnoeren p. 23-24. Zie ook Rb. Amsterdam 26 augustus 2004, *LJN* AQ7877, waar sprake was van onrechtmatige publicatie van bijzondere persoonsgegevens (een foto) van een mogelijke winkeldief.

van de gebruikte IP-adressen slechts tijdelijk door één specifieke persoon gebruikt worden. Waarschuwingen en toegangsblokkades worden aan het IP-adres gekoppeld. Latere gebruikers van dat IP-adres kunnen dan mogelijk ten onrechte worden beschuldigd van vandalisme op Wikipedia. Wie immers dan de bijdragen die vanaf dat IP-adres zijn gedaan, natrekt, zal ook de waarschuwingen zien en de verwijzingen naar vandalisme. Dat het feitelijk een andere gebruiker van dat IP-adres was, is nergens aan te zien.

## 6. Informatieplicht

De verantwoordelijke moet de betrokkenen informeren over het doel van de verwerking (art. 33 Wbp). De gebruikelijke manier om de gebruiker te informeren, is publicatie van een privacyverklaring.[36] Deze is meestal niet prominent aanwezig, maar dat past bij het te verwachten lage niveau van privacy. Een verwerking die de deelnemer redelijkerwijs niet mag verwachten, kan niet via een privacyverklaring worden weggenomen.[37] Bovendien zou een dergelijke bepaling in strijd zijn met de eis van het welbepaalde doel van de verwerking (art. 7 Wbp).

Hoe ver de verantwoordelijke moet gaan met informeren, hangt af van wat redelijkerwijs mag worden verwacht.[38] Voor sociale sites mag weinig privacy worden verwacht; de privacyverklaring zou dan ook alleen bijzondere verwerkingen hoeven te vermelden. Dat een reactie in een discussie zal worden gepubliceerd, ligt zo voor de hand dat dat niet gemeld hoeft te worden. Dat een gebruikersprofiel wordt doorgegeven aan adverteerders, is geen automatisme en moet daarom expliciet worden vermeld.

De Richtsnoeren geven in hun model-privacyverklaring echter een zeer uitgebreide opsomming van informatie die moet worden gemeld.[39] Hoewel het melden van triviale verwerkingen op zich geen kwaad kan, bestaat het gevaar dat men daardoor de uitzonderlijke verwerkingen over het hoofd ziet.

Iets lastiger is de eis voor de verantwoordelijke om zijn identiteit te vermelden (art. 33 lid 2 Wbp). Beheerders van sociale sites hebben ook een eigen privacy-belang om hun identiteitsgegevens niet te publiceren. Zeker nu veel sociale sites door privépersonen worden beheerd. De Richtsnoeren stellen als compromis voor dat in dit geval het publiceren van een in Nederland uitgegeven e-mailadres voldoende is.[40] Dit lijkt een goede afweging. Zeker nu dankzij HR Lycos/Pessers[41] de andere informatie via een gerechtelijke procedure te achterhalen is, mocht daar aanleiding voor zijn.

## 7. Aanmeldingsplicht

Verwerkingen van persoonsgegevens moeten in principe worden aangemeld bij het CBP (art. 27 lid 1 Wbp). De Richtsnoeren noemen deze plicht zelf al niet goed passend bij sociale sites.[42] Als ieder weblog of forum haar ledenbestand – laat staan elke discussie onder een bericht op een weblog– zou aanmelden, zou een volstrekt onwerkbare situatie ontstaan. Het CBP werkt dan ook aan een vrijstelling voor internetpublicaties, die zal gelden voor 'persoonlijke, niet-commerciële verwerkingen die voor privédoeleinden zijn opgezet'.[43]

Het is echter nog maar de vraag of deze bruikbaar zal zijn bij sociale sites. Veel sociale sites maken gebruik van advertenties, al was het maar om de kosten te dekken. Is dat nog persoonlijke, niet-commerciële verwerking? Verder zou deze vrijstelling alleen gelden als alle persoonsgegevens afgeschermd worden tegen verwerking door zoekmachines. En dat is, zoals ik hieronder zal betogen, onaanvaardbaar voor sociale sites.

## 8. Onderhoudsplicht voor gegevens

De verantwoordelijke heeft ook een zorgplicht voor de juistheid van de persoonsgegevens (art. 11 Wbp). Dit hoeft voor sociale sites geen probleem te zijn, omdat de meeste persoonsgegevens immers door de deelnemer zelf worden ingevoerd. In andere gevallen is de betrokkene wiens persoonsgegevens worden verwerkt vaak ook deelnemer, zodat hij zelf kan signaleren dat er onjuiste dingen worden gezegd. Via art. 36 Wbp kan hij deze laten corrigeren.

Uit deze zorgplicht leidt het CBP echter af dat beheerders van sociale sites een plicht tot monitoren en *preventief* screenen van bijdragen hebben: 'verantwoordelijken dienen ervoor te zorgen dat bijdragen alleen gepubliceerd kunnen worden op tijdstippen dat er moderatie aanwezig is'.[44] Dit is volstrekt niet passend voor sociale sites. Moderatie (toezicht) is niet nodig wanneer mensen zelf hun eigen persoonsgegevens publiceren. Natuurlijk kunnen mensen andermans persoonsgegevens zonder toestemming (her)publiceren, maar dat is een uitzonderlijke situatie. Het voorkómen daarvan behoort het normale gebruik van de site niet in de weg te zitten.

## 9. Verwijderen van persoonsgegevens

Persoonsgegevens mogen verder niet langer worden bewaard dan strikt nodig, en in ieder geval niet nadat een gegeven toestemming wordt ingetrokken (art. 5 Wbp). Dit zou voor registratiegegevens, profielen en dergelijke geen probleem moeten zijn.

Deze eis past minder goed wanneer het gaat om persoonsgegevens die nauw gekoppeld zijn aan andere persoonsgegevens, zoals bijdragen aan discussies of samen geschreven wikiteksten. Een bijdrage uit een discussie verwijderen kan de logica van de discussie verstoren. Voor wikiteksten is het

36. Richtsnoeren p. 23.
37. Blok 2002 (*supra* noot 25), p. 194; H. Kranenborg, *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie: over de openbaarheid van persoonsgegevens* (diss. Leiden), Deventer: Kluwer 2007, p. 121-123.
38. *Kamerstukken II* 1997/98, 25 443, nr. 3, p. 66 (MvT).
39. Richtsnoeren p. 27 en 62.
40. Richtsnoeren p. 26.
41. HR 25 november 2005, *LJN* AU4019.
42. Richtsnoeren p. 29.
43. Richtsnoeren p. 23.
44. Richtsnoeren p. 34.

overzicht met wie wat wijzigde erg waardevol. De Richtsnoeren stellen in de model-privacyverklaring dat discussieforums kunnen volstaan met het anonimiseren van de gegevens van de plaatser.[45]

## 10. Beveiliging tegen onrechtmatig hergebruik

Als laatste is er de plicht om persoonsgegevens te beveiligen tegen onrechtmatig hergebruik (art. 13 Wbp). Voor sociale sites betreft het hier vooral overname door zoekmachines. Een algemene regel lijkt te zijn dat zoekmachines onder geen voorwaarde toegang mogen krijgen tot persoonsgegevens.[46] Dit zou betekenen dat bijvoorbeeld een forumdiscussie niet doorzoekbaar mag zijn, omdat er immers namen van deelnemers, en afhankelijk van het onderwerp ook mededelingen over hun gezondheid, hobby's, seksuele voorkeuren of andere persoonsgebonden zaken staan.
Deze eis past totaal niet bij sociale sites. Sites die niet te vinden zijn met zoekmachines, bestaan simpelweg niet. Weliswaar kunnen zoekmachines onbedoelde koppelingen of herpublicaties van persoonsgegevens veroorzaken, maar men aanvaardt deze kans door zelf deze gegevens bloot te geven op een sociale site. Zeker nu er gespecialiseerde 'mensenzoekmachines' beschikbaar zijn, zoals Wieowie.nl dat gegevens over personen uit verschillende zoekmachines en sociale sites met elkaar koppelt.[47]
Daarnaast: als het de zoekmachines zijn die persoonsgegevens herpubliceren op onverantwoorde wijze, waarom moeten beheerders van websites dan extra maatregelen nemen? Het zouden juist de zoekmachines moeten zijn die veel terughoudender moeten zijn met het indexeren, koppelen en tonen van persoonlijke informatie.[48] Het CBP zou dus harder moeten optreden tegen Google in plaats van beheerders van sociale sites strenge regels op te leggen.[49]

## 11. Conclusie

De Wbp past niet goed bij internet.[50] En al helemaal niet bij sociale sites. Sociale sites zijn gericht op verwerkingen van door deelnemers zelf aangeleverde persoonsgegevens. Dat is van een heel andere aard dan een website die gegevens over iemands surfgedrag verzamelt. Een dergelijk verzamelen is ondoorzichtig en voor de betrokkene moeilijk te beïnvloeden, en daar is de Wbp tegen ontworpen.
Door de brede definities uit de Wbp is vrijwel elke bijdrage aan een sociale site een persoonsgegeven. Hierdoor zijn de verplichtingen uit Wbp en Richtsnoeren onverkort van toepassing op sociale sites. Dit wringt, nu het te verwachten niveau van privacy bij sociale sites laag mag zijn. Men publiceert immers vooral zelf persoonsgegevens en aanvaardt daarmee de kans dat de gegevens op onverwachte plekken opnieuw opduiken.

De grootste knelpunten zitten bij de onderhoudsplicht en de beveiligingsplicht. Volgens de Richtsnoeren vereisen deze preventief screenen van bijdragen en afsluiten van bijdragen voor zoekmachines. Dit regime is veel te streng en sluit volstrekt niet aan bij de privacyverwachting op sociale sites. Ook lijkt het niet echt de bedoeling dat elke sociale site of elk afzonderlijke bijdrage zich moet aanmelden bij het CBP. Informeren van gebruikers via een verplicht te aanvaarden privacyverklaring lost een deel van de problemen op. Maar als de Wbp zo gemakkelijk weggecontracteerd kan worden, en zo'n overeenkomst ook nog eens gesloten zal worden met een verplichte klik om mee te kunnen doen, wat is dan nog de waarde van deze Richtsnoeren?

45. Richtsnoeren p. 62.
46. Richtsnoeren p. 35. Zie ook R.C. Winkelhorst, 'Privacy en zoekmachines: vergezocht?', *Privacy & Informatie* 2005-4, p. 146-153.
47. *Over Wieowie.nl*, Groningen: Centroid Media BV 2007. http://www.wieowie.nl/over.html.
48. Winkelhorst 2005 (*supra* noot 46), p. 152.
49. De Artikel 29-werkgroep heeft hierover op 16 mei 2007 al een brief aan Google gestuurd. www.cbpweb.nl/documenten/pb_20070724_google.shtml. Laatst gecontroleerd 2007-12-23.
50. Zie ook Zwenne 2004 (*supra* noot 11), p. 67.