Van openbaarheid naar hergebruik van overheidsinformatie

Of een vaarwel aan het sociaal contract

Bart van der Sloot[1]

Al decennia kent Nederland wetgeving op het gebied van de openbaarheid van informatie. Deze regels hebben ten doel overheidsmacht transparant en democratische controle mogelijk te maken. Onlangs is nieuwe regelgeving aangenomen door de Eerste Kamer. De Wet hergebruik overheidsinformatie ziet tevens op openbaarheid van overheidsinformatie, maar kent een fundamenteel ander doel dan voorgaande wetgeving. Niet de democratie of de controle op de macht staat centraal, maar de commerciële exploitatie van overheidsinformatie door private ondernemingen. Dit brengt met zich dat de wetgeving een fundamenteel ander karakter krijgt, dat de overheid gegevens over burgers aan derden geeft zonder te weten waarvoor deze worden gebruikt en dat het sociaal contract tussen overheid en burger onder druk komt te staan.

1. Inleiding

Nederland kent al decennia wetgeving op het gebied van transparantie in de overheidssector.[2] Zo kent de Wet openbaarheid van bestuur (WOB) het uitgangspunt dat een bestuursorgaan bij de uitvoering van zijn taak informatie verstrekt, daarbij uitgaande van het algemeen belang van openbaarheid van informatie. Dergelijke wetgeving heeft ten doel transparantie in de overheidssector te bewerkstelligen om zo controle op de macht te faciliteren.[3] Door deze openbaarheid worden burgers en (onderzoeks)journalisten in staat gesteld beweringen van politici te staven, mogelijke misstanden aan het licht te brengen en besluitvormingsprocessen in kaart te brengen.[4] De kern van deze wetgeving is derhalve de transparantie van en democratisch controle op de macht.[5]

Onlangs is echter wezenlijk andere wetgeving aangenomen door het parlement: de Wet hergebruik overheidsinformatie (Who).[6] Het voorstel is op 9 juni 2015 met algemene stemmen aangenomen door de Tweede Kamer,[7] de Eerste Kamer heeft het voorstel op 23 juni 2015 als hamerstuk afgedaan[8] en de wet is in werking getreden op 18 juli 2015.[9] Deze wet vormt een implementatie van de herziening van de Europese Richtlijn hergebruik overheidsinformatie (Rho).[10] De oorspronkelijke richtlijn stamt uit 2003, de herziening uit 2013.[11] Dergelijke regelgeving kent een fundamenteel ander oogmerk dan democratische controle of transparantie van de macht. Het ziet op het faciliteren van de economische exploitatie van overheidsinformatie door private ondernemingen. De kerngedachte is dat de overheid grote hoeveelheden informatie bezit over onder meer burgers, gebouwen, wegen en het klimaat en deze nu 'slechts' gebruikt worden voor publie-

Auteur

1. Mr. drs. B. van der Sloot is onderzoeker aan het Instituut voor Informatierecht, Universiteit van Amsterdam.

Noten

2. Wet van 31 oktober 1991, houdende regelen betreffende de *Openbaarheid van bestuur*, *Stb.* 1991, 703.

3. *Kamerstukken II* 1986/87, 19859, 3.

4. Zie verder: E. Daalder, 'Handboek openbaarheid van bestuur', Den Haag: BJu 2014.

5. Zie verder: J.A. Hofman & J.A. van Schagen, Openbaarheid van bestuur, Nijmegen: Ars Aequi Libri 2003.

6. Wet hergebruik overheidsinformatie, *Stb.* 2015, 271.

7. *Kamerstukken II* 2014/15, 34123.

8. *Kamerstukken I* 2014/15, 34123, A.

9. Besluit van 6 juli 2015, 2015/299.

10. Richtlijn 2003/98/EG van 17 november 2003 inzake het hergebruik van overheidsinformatie.

11. Richtlijn 2013/37/EU van 26 juni 2013 tot wijziging van Richtlijn 2003/98/EG.

ke doeleinden, zoals belastingheffing, dijkversterking, migratiepolitiek en het bijhouden van huwelijksregisters. Dit terwijl deze gegevens ook gebruikt zouden kunnen worden voor economische exploitatie. In feite zit de overheid op een berg met goud, zo is de gedachte, zonder deze te benutten. Een rapport van de EU uit 2000 stelt bijvoorbeeld: 'Our central estimate for the value of PSI [Public Sector Information] is € 68 billion annually. This represents a substantial slice of total economic activity within the European economy.'[12]

In feite zit de overheid op een berg met goud, zo is de gedachte, zonder deze te benutten

De Richtlijn hergebruik overheidsinformatie gaat uit van dezelfde gedachte: 'Overheidsinformatie vormt een belangrijke grondstof voor digitale informatieproducten en -diensten en zal een nog belangrijkere hulpbron worden voor de ontwikkeling van draadloze informatiediensten. In dit verband is een ruime, grensoverschrijdende dekking eveneens van wezenlijk belang. Ruimere mogelijkheden voor het hergebruik van overheidsinformatie zullen Europese ondernemingen onder meer in staat stellen om de mogelijkheden ervan te benutten en bij te dragen tot economische groei en het scheppen van werkgelegenheid. De verschillen tussen de voorschriften en praktijken in de lidstaten ten aanzien van de exploitatie van overheidsinformatie zijn aanzienlijk, waardoor de volledige exploitatie van het economische potentieel van deze essentiële bron van informatie wordt belemmerd.'[13] Ook in Nederland is de verschuiving in de doelstelling waar te nemen. Terwijl de richtlijn uit 2003 nog werd geïmplementeerd door de WOB te amenderen[14] is er nu voor gekozen om naast de WOB een nieuwe wet aan te nemen. De memorie van toelichting bij de Wet hergebruik overheidsinformatie verklaart dat behalve raakvlakken tussen het openbaar maken van overheidsinformatie en het hergebruik van deze informatie, er ook wezenlijke verschillen zijn. 'Aan de Wob ligt immers het belang van actieve en passieve informatieverstrekking ter bevordering van het democratisch proces en de controle op de legitimiteit van overheidshandelen ten grondslag. Daar staat tegenover dat diezelfde overheidsinformatie een substantiële economische waarde vertegenwoordigt als deze wordt gebruikt als grondstof voor allerlei nieuwe producten. De regels voor hergebruik zijn dan ook gestoeld op hele andere uitgangspunten dan de klassieke Wob en zijn van economische of mededingingsrechtelijke aard.'[15]

De belangrijkste wijzigingen van de herzieningsrichtlijn uit 2013 ten opzichte van de oorspronkelijke richtlijn zijn dat 1. de reikwijdte van de richtlijn is uitgebreid naar archieven, musea en bibliotheken, 2. de keuzevrijheid om hergebruik al dan niet toe te staan vervalt, 3. er een maximum geldt voor de redelijke vergoeding die instellingen mogen vragen voor het voor hergebruik beschikbaar stellen van informatie en 4. instellingen een inspanningsverplichting hebben om de informatie in een open en machine-leesbaar formaat aan te bieden en gebruik te maken van open standaarden.[16] De Wet hergebruik overheids-informatie volgt de richtlijn in grote lijnen en kent een relatief eenvoudige structuur. Artikel 1 bevat begripsbepalingen en artikel 2 regelt het toepassingsbereik. Artikel 3 stelt dat een ieder een verzoek om hergebruik kan richten tot een met een publieke taak belaste instelling, waarbij hij vermeldt welke informatie hij wenst te hergebruiken. Belangrijk is dat de verzoeker bij zijn verzoek geen belang behoeft te stellen. De instelling kan een verzoek om hergebruik slechts afwijzen als een uitzondering genoemd in artikel 2 van toepassing is. Artikel 4 geeft aan hoe verzoeken in behandeling moeten worden genomen en artikel 5 stelt dat de voor hergebruik beschikbare informatie voor zover mogelijk langs elektronische weg, in een open en machinaal leesbaar formaat, samen met de metadata moet worden verstrekt. Artikel 6 gaat in op mogelijke voorwaarden, artikelen 7 en 8 op exclusieve rechten en tot slot specificeert artikel 9 ten aanzien van de tarifering dat ten hoogste de marginale kosten van vermenigvuldiging, verstrekking en verspreiding in rekening mogen worden gebracht. Belangrijk is dat in artikel 2 is vervat dat een van de uitzonderingen voor de toepasselijkheid van de Who is 'informatie die betrekking heeft op openbare
persoonsgegevens waarvan hergebruik onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.'[17]

Alhoewel de wet specifiek het recht op verzoek om overheidsinformatie voor hergebruik regelt, moet deze regeling worden bezien in het licht van de meer algemene tendens naar de 'open overheid'.[18] Zo heeft de Nederlandse staat de website https://data.overheid.nl/ opgericht waarop structureel grote datasets van de overheid worden gepubliceerd.[19] Dit gebeurt niet op verzoek, maar geschiedt actief, op initiatief van de overheid. Daags nadat de Wet hergebruik overheidsinformatie werd aangenomen meldde minister Plasterk van Binnenlandse Zaken dan ook dat hij vijfhonderd digitale mappen met informatie zou publiceren op deze site. Ook pleitte hij daarbij voor een 'cultuuromslag' bij de overheid. Er zou volgens hem vanaf nu moeten worden uitgegaan van het actief openbaar maken van overheidsinformatie, tenzij er zwaarwegende bezwaren zouden zijn.[20] De Who moet dus worden gezien als onderdeel van een bredere 'open data movement'. Gegeven de economische projectie die ten grondslag ligt aan de wetgeving omtrent het hergebruik van overheidsinformatie is de verwachting dat er in de toekomst steeds meer en rijkere datasets op open.overheid.nl zullen worden gepubliceerd. Uit de weinige datasets die nu op deze site zijn gepubliceerd, die voornamelijk betrekking hebben op zaken als het sirenegebruik in de gemeente Nijmegen, kabels en leidingen in Zeeland en wandelroutes in Utrecht west, zal deze economische groei hoe dan ook niet volgen.

De centrale vraag van dit artikel is of en hoe de actieve publicatie van overheidsbronnen en het op verzoek verstrekken van data voor hergebruik door derden is te verenigen met het recht op privacy en de bescherming van persoonsgegevens. Daaraan gekoppeld is de vraag welke maatschappelijke en sociale gevolgen het hergebruik van overheidsinformatie door private ondernemin-

gen voor commerciële exploitatie zal hebben. Par. 2 van dit stuk geeft aan waarom het recht op privacy en gegevensbescherming niet zelden in het geding zullen zijn bij het hergebruik van overheidsinformatie. Par. 3 en 4 geven aan met welke principes uit het gegevensbeschermingsrecht rekening moet worden gehouden bij het hergebruik van overheidsinformatie. Tot slot geeft par. 5 aan welke maatschappelijke en sociale gevolgen het hergebruik van overheidsinformatie kan hebben.

2. Persoonsgegevens en persoonlijke levenssfeer

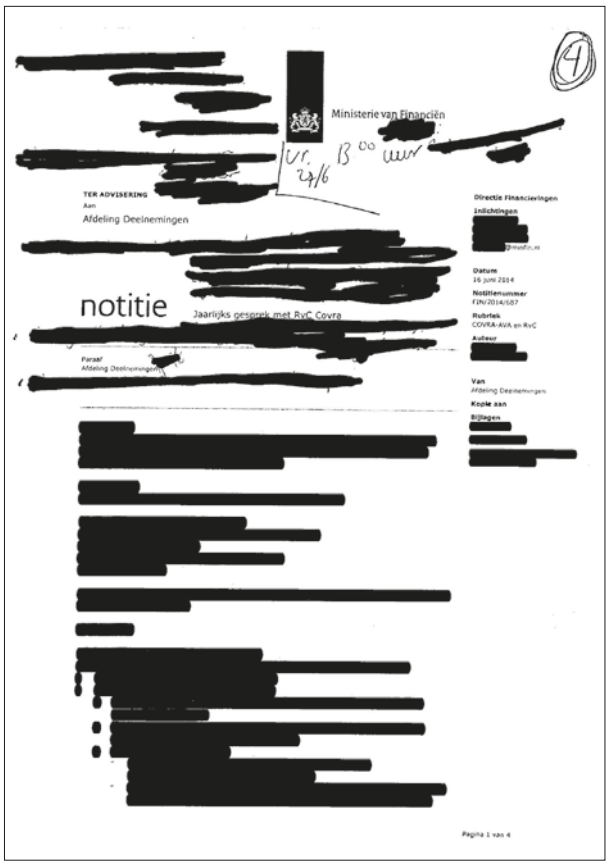
De eerste vraag die moet worden beantwoord is wanneer het recht op privacy en het recht op gegevensbescherming van toepassing zijn op het hergebruik van overheidsinformatie. Het recht op gegevensbescherming is van toepassing als er 'persoonsgegevens' worden 'verwerkt'. Van 'verwerking' is vrijwel altijd sprake, of het nu gaat om het verzamelen, opslaan, verwerken, openbaar maken, verwijderen of corrigeren van data.[21] Een 'persoonsgegeven' is 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[22] Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd middels de gegevens. Van een impact op de privacy of de persoonlijke levenssfeer van mensen is sprake als zij geraakt worden in hun wezenskenmerken, hun vrije handelen of de ontplooiing van hun persoonlijkheid. Beide definities zijn derhalve breed en hebben een zeer groot bereik. Bij persoonsgegevens gaat het bijvoorbeeld niet slechts om direct identificerende gegevens, zoals naam en adres, maar ook om indirect identificerende gegevens. De zin 'Die man daar bij de lantaarnpaal' kan als persoonsgegeven worden aangemerkt als die iemand in staat stelt de man te identificeren of te individualiseren, dat wil zeggen hem uit het grote publiek als individu te pikken.[23] Daarnaast gaat het ook om 'identificeerbare' gegevens, dat wil zeggen gegevens die op een bepaald moment nog niet identificerend zijn, maar dit wel kunnen worden als ze bijvoorbeeld worden gekoppeld aan andere data. Hierbij geldt de moeite die hiervoor moet worden gedaan als uitgangspunt – als er onredelijke moeite moet worden gedaan om een gegeven identificerend te maken dan valt het niet onder het begrip persoonsgegevens, als dit relatief eenvoudig kan geschieden wel.

Vaak worden documenten geanonimiseerd, om de toepassing van de gegevensbeschermingsregels te omzeilen. Geanonimiseerde gegevens vallen immers niet onder de reikwijdte van het recht op gegevensbescherming. Toch is de vraag of dit een succesvolle methode zal zijn bij het hergebruik van overheidsinformatie. Er zijn evident databases die niet op personen betrekking hebben, zoals de ligging van zeekabels of gegevens over het weer. Maar zelfs de ligging van gewone kabels kan al iets zeggen over personen: als een huis bijvoorbeeld geen aansluiting heeft op riolering, elektriciteit en water dan vertelt dit iets over de leefomstandigheden van de bewoners en wellicht hun financiële situatie. Daarbij komt dat, los van deze databases, verreweg de meeste data van de overheid betrekking hebben op mensen, op menselijke handelingen of gedragingen. Het probleem is dat het vaak onduidelijk is welke informatie in dergelijke databases als identificerend moet worden bestempeld en welke niet. Wil de overheid dit goed uitzoeken om te voorkomen dat direct identificerende gegevens worden gepubliceerd of verstrekt aan een hergebruiker, dan zal ze alle databases nauwkeurig moeten napluizen. Dit veronderstelt echter zulke sisyfusarbeid dat het de vraag is of het nog economisch rendabel is om het hergebruik van dergelijke overheidsinformatie na te streven.

Maar stel dat het lukt om een database volledig te ontdoen van direct identificerende gegevens, doordat bijvoorbeeld alle namen en adressen van personen zwart worden gemaakt, dan nog moet worden bedacht dat ook indirect identificerende persoonsgegevens onder de reikwijdte van het gegevensbeschermingsrecht vallen. Als in een document de naam en het adres van een persoon zijn verwijderd, maar uit de context desalniettemin blijkt wie het betreft, bijvoorbeeld 'minderjarige vrouw die een zeilreis om de wereld wil maken', dan zal dit ook als een persoonsgegeven hebben te gelden. Zeker in acht nemend de voortschrijdende techniek en de mogelijkheden om aan datamining te doen, zal het zeer moeilijk zijn om alle contextuele data te verwijderen, zodat een document volledig anoniem wordt. Als dit wel lukt dan is de vraag of er niet zoveel gegevens moeten worden verwijderd dat het overgebleven document van generlei waarde is. 'Data can be either useful or perfectly anonymous but never both', luidt een bekend adagium.[24] Het is bijvoorbeeld bekend dat veel WOB-verzoeken slechts leiden tot de vrijgave van documenten waarin veel informatie is weggelakt.[25]

Verreweg de meeste data van de overheid hebben betrekking op mensen, op menselijke handelingen of gedragingen

12. Europese Commissie, *Commercial Exploitation of Europe's Public Sector Information*, 20 september 2000, p. 6.
13. Rho, overweging 5-6.
14. Wet van 22 december 2005 tot wijziging van de Wet openbaarheid van bestuur en enige andere wetten in verband met de implementatie van Richtlijn 2003/98/EG, *Stb.* 2006, 25. *Kamerstukken II* 2004/05, 30188.
15. *Kamerstukken II* 2014/15, 34123, 3, p. 3.
16. *Kamerstukken II* 2014/15, 34123, 3, p. 2-3.
17. Art.2.1 sub g Who. Zie ook: art.1.4 Rho.
18. Zie ook: www.europeana.eu/portal/.
19. https://data.overheid.nl/.
20. www.radio1.nl/item/300975-Plasterk+wil+veel+overheidsdata+publiceren.html.
21. Art. 2 lid b Rbp.
22. Art. 2 lid a Rbp.
23. Article 29 Working Party (WP 29), 'Opinion 4/2007 on the concept of personal data', 01248/07/EN.
24. P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 2010, 57, p. 1704.
25. www.laka.org/nieuws/2015/wob-waarborgfonds-eindberging-in-problemen-3471/.



Zelfs als het lukt om een database volledig te anonimiseren en gegevens te de-identificeren, dan nog moet er rekening mee worden gehouden dat het omgekeerde proces vaak evenzogoed mogelijk zal zijn.[26] Zo blijkt uit onderzoek dat het zelfs bij zware anonimisering van zeer gevoelige medische gegevens het nog mogelijk is om zo'n 40% van de deelnemers aan een DNA-onderzoek te reïdentificeren.[27] Maar stel, het lukt de overheid toch om een volledig geanonimiseerde dataset te publiceren, die ook niet meer gedeanonimiseerd kan worden. Dan nog moet worden bedacht dat de gegevensbeschermingsregels ook van toepassing zijn op 'identificeerbare' gegevens, dat wil zeggen gegevens die op dit moment niet, maar in de toekomst wel, met relatief eenvoudige middelen, tot een identificerend gegeven kunnen worden gemaakt. Het zal, zeker met de voortschrijdende technische middelen, in toenemende mate eenvoudig zijn voor bedrijven om anonieme gegevens te koppelen aan data die al in hun bezit zijn, om zo identificerende persoonsgegevens te verkrijgen. Stel bijvoorbeeld dat de overheid een database publiceert over milieu- en omgevingsfactoren en dat daaruit blijkt dat een fabriek een bepaalde giftige stof heeft gelekt, waarbij de wijken in de omgeving zijn getroffen. Dit is op zich geen persoonlijke informatie, maar koppel dit aan het relatief publieke gegeven van iemands woonadres en er ontstaat een zeer gevoelig profiel, met informatie over mogelijke gezondheidsrisico's.[28] Ook hiermee moet rekening worden gehouden bij het vrijgegeven van overheidsinformatie.

Tot slot moet worden opgemerkt dat zelfs als een dergelijke koppeling niet mogelijk is, de anonieme gegevens toch kunnen worden gebruikt voor de beïnvloeding van personen en hun levenssfeer (ook al zijn de personen die worden geraakt niet direct geïdentificeerd). Vrijgegeven data over een groep of een categorie personen, bijvoorbeeld in het geval dat de overheid geaggregeerde of statistische gegevens openbaar maakt, kunnen immers worden gebruikt door instanties en bedrijven om beleid te formuleren en ten uitvoer te brengen die bepaalde groepen of categorieën privilegiëren, terwijl anderen juist worden beperkt in hun rechten of mogelijkheden. Dergelijke praktijken zullen dan weliswaar buiten het gegevensbeschermingsrecht vallen, maar desalniettemin binnen het recht op bescherming van de persoonlijke levenssfeer. Kortom, bij het hergebruik van overheidsinformatie moet er rekening mee worden gehouden dat als een dataset meer informatie bevat dan slechts de ligging van zeekabels en de wandelroutes in Utrecht west, het recht op privacy en gegevensbescherming al snel van toepassing zullen zijn. Dit betekent evenwel niet dat het publiceren van deze data verboden is, maar wel dat de materiële bepalingen van het gegevensbeschermingsrecht in acht moeten worden genomen.

3. Doel en doelbinding

Gegevensbeschermingsregels vereisen dat persoonsgegevens eerlijk en rechtmatig worden verwerkt.[29] Er zijn zes limitatieve gronden op basis waarvan de verwerking van persoonsgegevens kan worden gelegitimeerd, namelijk op grond van a. de toestemming van het datasubject, b. een contract met het datasubject, c. een wettelijke plicht om de gegevens te verwerken of indien de verwerking noodzakelijk is d. voor de vrijwaring van de vitale belangen van het datasubject, e. voor de naleving van een publieke taak of f. voor het verwezenlijken van een legitieme doel van de verwerker, waarbij bovendien geldt dat de belangen van de verwerker zwaarder moeten wegen dan die van het datasubject.[30] Er geldt een 'nee, tenzij' regime voor het verwerken van bijzondere persoonsgegevens, zoals die betreffende iemands ras, geloof of medische status.[31] Daarbij komt dat persoonsgegevens alleen mogen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[32] Tot slot geldt als regel dat persoonsgegevens 'vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden.'[33] Dit wordt ook wel het doelbindingsprincipe genoemd. Bij de afweging of een doel als 'onverenigbaar' heeft te gelden moet rekening worden gehouden met de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen, de aard van de betreffende gegevens, de gevolgen van de beoogde verwerking voor het datasubject, de wijze waarop de gegevens zijn verkregen en de mate waarin jegens het datasubject wordt voorzien in passende waarborgen.[34]

Bij de publicatie van stukken en databases door de overheid voor hergebruik door het bedrijfsleven speelt een aantal vragen. Ten eerste vereist het gegevensbeschermingsrecht dat de oorspronkelijke verantwoordelijke voor de gegevensverwerking duidelijk, helder en concreet specificeert voor welke doeleinden hij de gegevens verwerkt. De overheid is in dit geval de verantwoordelijke en het doel van de gegevensverwerking zal van geval tot geval verschillen, maar zal doorgaans betrekking hebben op publieke taken als fraudebestrijding, bevolkingsonderzoek en mobiliteitsbeleid. In ieder geval zal in het oorspronkelijke doel,

Zelfs bij zware anonimisering van zeer gevoelige medische gegevens is het nog mogelijk om zo'n 40% van de deelnemers aan een DNA-onderzoek te reïdentificeren

bijvoorbeeld de wettelijke taak- en doelstelling van de instanties, met daaraan gekoppeld de bevoegdheid om gegevens te verzamelen en te verwerken, niet zijn vervat de publicatie van gegevens ten behoeve van de economische exploitatie door private partijen. Dit werpt daarmee een vrij groot bezwaar op, aangezien de publicatie of het verstrekken van de gegevens als zodanig als een verwerking van persoonsgegevens heeft te gelden. Een oplossing kan mogelijk zijn om een dergelijk doel vervolgens wel op te nemen in de wettelijke taakstellingen van de diverse overheidsinstellingen. Toch volgt hieruit dat de gegevens die de overheid tot nu toe heeft verzameld niet mogen worden vrijgegeven, aangezien de tot nu toe verzamelde gegevens niet onder die nieuwe doelstelling vallen. Daarbij komt het punt dat deze nieuwe doelstelling helder en concreet moet zijn. De doelstelling 'publicatie van gegevens ten behoeve van economische exploitatie door derden' is echter op zichzelf vermoedelijk al te ruim om aan dit wettelijk vereiste te voldoen en dit punt geldt te meer als wordt meegewogen dat het onbekend is voor welke specifieke doelen de derden de gepubliceerde gegevens precies zullen gebruiken en wie die derden eigenlijk zijn.

Maar stel, de overheid neemt voortaan in haar doelstellingen op 'de publicatie van gegevens ten behoeve van ...' en dit wordt als voldoende specifiek en afgebakend gekwalificeerd, dan nog geldt dat zowel de overheid als de private onderneming een legitieme verwerkingsgrond zullen moeten hebben, de overheid voor de publicatie van gegevens en de hergebruiker voor het hergebruik. Wat betreft de publicatie van bijzondere persoonsgegevens moet worden opgemerkt dat dit vermoedelijk nimmer legitiem zal zijn onder het gegevensbeschermingsregime. Dat de publicatie van dergelijke gegevens bepaald niet illusoir is blijkt uit de praktijk in andere landen waarin open-overheidsprojecten reeds verder gevorderd zijn. Zo worden in Groot-Brittannië medische gegevens ter beschikking gesteld voor hergebruik voor wetenschappelijke en commerciële doeleinden.[35] Nog los van het vrijgeven van medische informatie moet worden opgemerkt dat veel beeldmateriaal bijzondere persoonsgegevens zal bevatten, als daarop bijvoorbeeld de huidskleur is te zien en derhalve het ras van een persoon valt te herleiden.[36]

Maar stel, de overheid weet te vermijden dat er bijzondere persoonsgegevens worden vrijgegeven, iets wat wederom een zeer nauwgezet en arbeidsintensief proces zal vergen, dan nog zal ze een legitieme verwerkingsgrond voor het publiceren van gewone persoonsgegevens moeten hebben. Echter, het zal doorgaans, refererend aan de zes eerder genoemde gronden, niet gebaseerd kunnen worden op a. de toestemming van het datasubject, b. een contract met het datasubject of c. de behartiging van de belangen van het datasubject. De publicatie zou kunnen worden gelegitimeerd door een beroep op d. een wettelijke plicht, maar de Who brengt zelf niet zo'n wettelijke plicht met zich, omdat daarin juist is vervat dat de gegevensbeschermingsregels voorrang hebben. De legitimatie op grond van e. het behartigen van een publieke taak zal niet opgaan, omdat het faciliteren van de economische exploitatie van informatie door private ondernemingen geen publieke taak is en f. de belangenafweging zal doorgaans geen soelaas bieden omdat het vrijgeven van overheidsinformatie enerzijds niet noodzakelijk is voor het behartigen van een publieke taak en anderzijds omdat de belangen van de burger in zake de bescherming van zijn fundamentele rechten en vrijheden doorgaans zullen prevaleren.[37] Dit geldt te meer voor de hergebruiker van de overheidsinformatie, die ook een legitieme verwerkingsgrond zal moeten hebben en wiens commerciële belangen doorgaans niet zullen opwegen tegen de belangen van het datasubject.

Maar zelfs als al deze hobbels zouden kunnen worden genomen, dan nog blijft er een laatste en wellicht meest fundamentele belemmering: het doelbindingsprincipe. Het hergebruik van informatie staat in principe diametraal tegenover het vereiste dat gegevens alleen mogen worden gebruikt voor het doel waarvoor zij zijn verzameld. Niet alleen gaat het bij het hergebruik van overheidsinformatie immers om een andere partij die de gegevens verwerkt, namelijk een private onderneming in plaats van de overheid, ook zal het doorgaans gaan om een volstrekt ander doel, namelijk een commercieel in plaats van een maatschappelijk doel. Wat als 'onverenigbaar' met het oorspronkelijke doel heeft te gelden is niet eenduidig te bepalen en zal van geval tot geval moeten worden beoordeeld, maar duidelijk is dat het hergebruik van overheidsinformatie door private ondernemingen voor economische exploitatie hier in principe buiten valt.[38]

26. M.R. Koot, *Measuring and predicting anonymity*, Amsterdam: Informatics Institute, UvA 2012.

27. A. Tanner, 'Harvard professor reidentifies anonymous volunteers in DNA study', *Forbes* 25 april 2013.

28. Custers et al. (eds.), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Heidelberg: Springer 2012.

29. Art. 6 lid 1 sub a Rbp.

30. Art. 7 Rbp.

31. Art. 8 Rbp.

32. Art. 6 lid 1 sub b Rbp.

33. Art. 6 lid 1 sub b Rbp.

34. Art. 9 Wbp.

35. www.england.nhs.uk/ourwork/tsd/care-data/; www.theguardian.com/society/2014/feb/21/nhs-25 plan-share-medical-data-save-lives; P. Carter, T.L. Graeme & M. Dixon-Woods, 'The Social Licence for Research: Why care.data Ran Into Trouble', *Journal of Medical Ethics* 2015, 41; Nuffield Council on Bioethics, The Collection, *Linking and Use of Data in Biomedical Research 29 and Health Care: Ethical Issues*, London: Nuffield Council on Bioethics 2015.

36. HR 23 maart 2010, 08/04524B.

37. WP 29, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', 844/14/EN.

38. WP 29, 'Opinion 03/2013 on purpose limitation', 00569/13/EN.

4. Controle en verantwoordelijkheid

Daarbij komt dat het uitgangspunt van het gegevensbeschermingsrecht is dat degene die de gegevens verzamelt en verwerkt ook verantwoordelijk is voor een eerlijk en rechtmatig gegevensverwerkingsproces.[39] Op hem rusten dan ook alle verantwoordelijkheden die in de regels zijn vervat, al kan er soms sprake zijn van een gezamenlijke verantwoordelijkheid.[40] Ten eerste veronderstelt het gegevensbeschermingsrecht dat gegevensverwerking veilig en vertrouwelijk moet geschieden.[41] Onbevoegde derden moeten dus uit worden gesloten van toegang tot deze gegevens en data moet worden beveiligd tegen onder meer verlies, vervalsing, niet-toegelaten verspreiding of toegang. Het principe van veilige en vertrouwelijke verwerking verhoudt zich fundamenteel slecht met actieve openbaarmaking en hergebruik van overheidsinformatie door derden, omdat er nu juist geen beveiliging mogelijk is tegen toegang door onbevoegde derden, er geen mogelijkheid is om vervalsing of misbruik van gegevens tegen te gaan, enz.[42]

Ten tweede ligt aan het gegevensbeschermingsrecht ten grondslag het principe van transparantie. Enerzijds heeft de verantwoordelijke de plicht om het datasubject te informeren over de identiteit van de voor de verwerking verantwoordelijke, de doeleinden waarvoor de gegevens zijn bestemd en de ontvangers van de gegevens,[43] anderzijds heeft het datasubject het recht om dergelijke informatie te verzoeken.[44] Ook dit principe lijkt zich slecht te verhouden met het ter beschikking stellen van overheidsinformatie aan derden omdat de overheid, zeker bij actieve openbaarmaking, niet weet aan wie zij gegevens verstrekt en derhalve het datasubject niet op de hoogte kan stellen van de doeleinden waarvoor de gegevens verder worden verwerkt en door wie. De hergebruikers weten op hun beurt vaak niet waar de informatie precies vandaan komt en op wie die betrekking heeft en zullen dus in de meeste gevallen niet in staat zijn om de datasubjecten van hun identiteit en de doeleinden van verwerking op de hoogte te stellen. Voor het datasubject zal het evenzo
lastig zijn om de hergebruikers op te sporen.

Stel, de economische prognose is wel realistisch, dan rijst de vraag wie dit economisch potentieel te gelde zal maken

Ten derde kent het gegevensbeschermingsrecht het zogenoemde dataminimalisatieprincipe,[45] waaruit volgt dat zo min mogelijk gegevens moeten worden verzameld, ze slechts mogen worden verwerkt in zoverre dit noodzakelijk is voor het bereiken van het doel en dat ze weer moeten worden verwijderd als ze niet langer noodzakelijk zijn voor het bereiken van dit doel. Het hergebruik van informatie is echter juist gestoeld op de gedachte dat gegevens niet slechts dienen voor het specifieke doel waarvoor ze zijn verzameld, maar dat ze daarna nog een tweede leven kunnen krijgen. Van het verwijderen van gegevens nadat ze hun doel hebben gediend zal dus geen sprake zijn en ook komt, zoals in de vorige paragraaf is besproken, het principe onder druk te staan dat er slechts gegevens mogen worden verzameld en verwerkt voor het specifieke, oorspronkelijke doel van de overheidsinstanties. Ten vierde en tot slot dient de verantwoordelijke voor de gegevensverwerking er zorg voor te dragen dat de gegevens up to date blijven en waar nodig worden gecorrigeerd, om zo de betrouwbaarheid van de data en de datasets te waarborgen.[46] Het is sterk de vraag hoe dit principe kan worden gehandhaafd bij het hergebruik van overheidsinformatie, omdat het geen zicht meer heeft op wie de gegevens heeft en of de bezitters van de gegevens zelf zorgdragen voor het updaten van de informatie.

5. Maatschappelijke en ethische vraagstukken

Naast deze juridische uitgangspunten zijn er echter ook maatschappelijke en ethische vragen gemoeid met het fenomeen van hergebruik van overheidsinformatie. Ten eerste moet worden opgemerkt dat het zeer twijfelachtig is of de prognoses wat betreft het economisch rendement op reële aannames is gebaseerd. Het bedrag van € 68 miljard, dat de overheidsinformatie in Europa jaarlijks aan omzet zou moeten generen, wordt door weinigen serieus genomen. In ieder geval valt de economische winst tot nu toe sterk tegen. In landen waar overheden al langer en sterker inzetten op open-overheidsprojecten en het her-gebruik van overheidsinformatie zijn er slechts weinig succesvolle nieuwe ondernemingen en bedrijfsactiviteiten aan te wijzen, afgezien van wat goedbedoelde start-ups wier winst nauwelijks in de buurt komt van de vele miljarden die het uitgangspunt van deze wetgeving vormen. In ogenschouw moet worden genomen dat de uit de wet voortvloeiende verplichtingen ook aanzienlijke kosten met zich mee zullen brengen. Een deel van de directe kosten kunnen wellicht op de hergebruiker worden verhaald, maar veel van de organisatorische en structurele kosten niet. Daarbij komt dat bij open overheidsprojecten de mogelijkheid om kosten terug te winnen vaak vervalt, omdat de data vrijelijk beschikbaar worden gesteld aan een ieder en dus ook weer kunnen worden doorgespeeld en verder verspreid door de verkrijgende partijen. Het is dan ook sterk de vraag of de bescheiden winst die de start ups generen wel opweegt tegen de structurele kosten voor de overheid.

Maar stel, de economische prognose is wel realistisch, dan rijst de vraag wie dit economisch potentieel te gelde zal maken. Ware dit de overheid geweest, dan zou het rendement ten goede komen aan de bevolking. Nu het private ondernemingen zijn, vloeit dit potentieel in principe naar particulieren. Dit is navrant omdat de winst grotendeels op basis van gegevens van en over burgers wordt gemaakt. Zelfs als de gegevens in geaggregeerde vorm worden vrijgegeven en dus niet als persoonsgegeven zijn aan te merken, dan nog is een geaggregeerde dataset of een groepsprofiel gebaseerd op en

afhankelijk van de persoonsgegevens die de overheid op last van dwang of boete verkrijgt van haar burgers. In andere rechtsgebieden, bijvoorbeeld in het portretrecht, gaat men er van uit dat bij de exploitatie van een beeld of gelijkenis van een persoon, de geëxploiteerde een deel van de winst moet kunnen opeisen of althans de exploitatie kan verbieden.[47] Voor een dergelijk uitgangspunt is hier echter niet gekozen. Daarnaast is de vraag wie er precies zou profiteren van het hergebruik. Als er inderdaad veel nieuwe business models en start ups zouden ontspruiten aan het hergebruik van overheidsinformatie, die nieuwe applicaties en diensten zouden aanbieden, dan zou dit wellicht een potentiële stimulans geven aan het maatschappelijke welzijn. Echter, de verwachting is dat het niet zozeer de onervaren start ups zonder technische infrastructuur en know how zullen zijn die zullen profiteren van de grote hoeveelheden openbaar gemaakte gegevens, maar de al bestaande technologiegiganten als Apple, Miscrosoft, Facebook en Google. Zij hebben immers al de capaciteiten, de kennis en de mankracht in huis om de beschikbaar gestelde informatie te verwerken en te integreren in hun al bestaande diensten. Daarbij komt dat het onzeker is of de eventuele winst die uit de overheidsinformatie is te putten wel in Europa, laat staan Nederland blijft, of dat het eerder naar Amerikaanse bedrijven zal vloeien.

Daarbij is het de vraag welke rol de overheid eigenlijk speelt. Thans geldt er een impliciete afspraak tussen de burger en de overheid. De burger staat zijn gegevens af aan de overheid en de overheid gebruikt deze gegevens om publieke taken en diensten te verrichten. Dit is een sociaal contract tussen de burger en de overheid. De burger is wettelijke verplicht deze gegevens af te staan, wat wordt gehandhaafd door boetes of door uitsluiting van bepaalde diensten als hij weigert.[48] Toch bestaat over deze plicht weinig controverse, omdat het voor eenieder duidelijk is dat de overheid deze gegevens nodig heeft voor het uitvoeren van haar taken. Door de Wet hergebruik overheidsinformatie ontstaat er echter een situatie waarin de overheid in feite als waterdrager van het bedrijfsleven fungeert. De burger is verplicht zijn gegevens af te staan aan de overheid, terwijl die ze vervolgens zonder toestemming aan private ondernemingen doorspeelt. Dit doorbreekt de impliciete afspraak en ondermijnt het sociaal contract tussen de burger en de overheid. Het idee achter het hergebruikproject is dat het zonde is dat de door de overheid verzamelde informatie 'slechts' wordt gebruikt voor de publieke doeleinden, terwijl de afspraak juist andersom is: de overheid mag deze gegevens slechts verzamelen en verwerken *omdat* ze nodig zijn voor de publieke taken.

Dit kan niet alleen het vertrouwen van de burger in de staat ondermijnen, maar ook de legitimiteit en het functioneren van specifieke instituten. Publieke instituten hebben draagvlak omdat zij een bepaalde publieke functie uitoefenen; als de data die zij beschikken structureel voor andere doelen worden gebruikt kan dit draagvlak afbrokkelen. Als voorbeeld kan dienen het archiefwezen,[49] dat vrij actief beleid voert ten aanzien van het digitaliseren en het openbaar maken van stukken en documenten.[50] In archiefstukken staan natuurlijk veel persoonsgegevens, het archief gaat immers over personen en hun verleden. Deze archieven zijn traditioneel toegankelijk voor eenieder, maar gezien de tijd en moeite die het kost om naar archieven toe te gaan en documenten te raadplegen, maken in de praktijk voornamelijk historici, journalisten en mensen die hun stamboom willen uitzoeken er gebruik van. De documenten zijn gezien hun format niet voor hergebruik geschikt, wel kunnen op basis van deze achtergronddocumenten wetenschappelijke analyses en journalistieke stukken worden geschreven. Kortom, de praktijk is grotendeels in lijn met de wettelijke doelstelling van archieven.[51] Als archieven op termijn steeds meer materiaal gaan digitaliseren en actief openbaar gaan maken dan zou hiermee een nieuw publiek, met nieuwe doeleinden worden aangeboord. Hiermee kan ook de legitimiteit van dit instituut onder druk komen te staan – burgers zullen minder snel instemmen met de opname van hun gegevens in archieven of verzoeken om al opgenomen gegevens te verwijderen als zij weten dat hun gegevens door bedrijven voor economische exploitatie kunnen worden gebruikt. Dat een dergelijke vrees bepaald niet illusoir is bleek onlangs toen het Hof van Justitie het recht om vergeten te worden omarmde.[52] Veel archieven zijn fel gekant tegen dit recht.[53] Ook in de zaak voor het HvJ EU ging het immers om een gedigitaliseerd archief. Google heeft sinds de uitspraak op 13 mei 2014 al bijna 300 000 verzoeken om vergeten te worden ontvangen.[54] Veel archieven vrezen dat burgers ook hun gegevens zullen laten verwijderen uit archieven, waardoor archieven op termijn incompleet en onvolledig zouden worden, een vrees die zeker realistisch lijkt als zij zouden weten dat hun persoonsgegevens en familiegeschiedenis worden gebruikt als bron voor bedrijfsactiviteiten. De open overheid-beweging en het hergebruik van overheidsinformatie voor commerciële exploitatie door private ondernemingen ondermijnt dus niet alleen de legitimiteit van instituten, ook hun functioneren kan hiermee onder druk komen te staan. •

39. Art. 6 lid a Rbp.

40. Art. 2 lid d Rbp.

41. Art. 16, 17 Rbp.

42. Zie verder: art. 25 Rbp.

43. Art. 10 Rbp.

44. Art. 12, 13 Rbp.

45. Art. 6 Rbp.

46. Art. 6 Rbp. Zie ook: art. 12 Rbp.

47. Zie verder: G.A.I. Schuijt & D. Visser, *Portretrecht voor iedereen*, Amsterdam: Mets & Schilt 2003.

48. Personen die bijvoorbeeld weigeren hun vingerafdruk af te staan, krijgen simpelweg geen paspoort.

49. De regering benadrukt dat erfgoedinstellingen veel waardevolle informatie voor hergebruik bezitten. *Kamerstukken II* 2014/15, 34123, 3, p. 5. Toch zijn onderwijs- en onderzoeksinstellingen en andere culturele instellingen dan bibliotheken en musea uitgezonderd van de Who; Art. 2.1 lid c-e Who; Het (her)gebruik van informatie uit archieven wordt in de archiefwet zelf geregeld.

50. Zie o.a. www.nationaalarchief.nl/digitaal-archiveren.

51. Wet van 28 april 1995, houdende vervanging van de Archiefwet 1962 (*Stb.* 1995, 313) en in verband daarmede wijziging van enige andere wetten.

52. HvJ EU 13 mei 3014, *(Google vs. Spain)*.

53. Zie o.a. www.kvan.nl/files/Activiteiten_KVAN_2015.pdf.

54. www.google.com/transparencyreport/removals/europeprivacy/.