*Mr. drs. B. van der Sloot**

Wetenschappelijk artikel
De evaluatie van de Wet bescherming persoonsgegevens

205

Trefwoorden:
evaluatie Wbp, knelpunten

De Wet bescherming persoonsgegevens (Wbp) is één van de belangrijkste wetten ten aanzien van privacy in Nederland. Echter, al voor haar inwerkingtreding in 2001 is zij aan kritiek onderhevig en wordt zij op een aantal punten als inadequaat beschouwd. Niet alleen in de jurisprudentie en de wetenschappelijke literatuur zijn knelpunten opgeworpen, ook zijn de wet en de daarmee geïmplementeerde Europese Privacyrichtlijn meerdere malen aan een evaluatie onderworpen. In Nederland loopt dit evaluatieproces tot een einde nu het kabinet zijn plan van aanpak heeft gepresenteerd. Dit artikel beoogt een overzicht te geven van de belangrijkste knel- en discussiepunten die de afgelopen jaren de revue zijn gepasseerd en te beschouwen in hoeverre de kabinetsplannen hiervoor een oplossing aandienen.

1 Inleiding

De Wet bescherming persoonsgegevens is op 6 juli 2000 in het *Staatsblad* gepubliceerd en is in werking getreden op 1 september 2001.[1] De wet is grotendeels[2] de implementatie van de EU-Privacyrichtlijn.[3] De doelstelling van deze richtlijn is, naast het beschermen van het fundamentele recht op privacy, het realiseren van een interne markt binnen de Europese Unie, met een hoog en gelijkwaardig gegevensbeschermingsniveau in alle landen. De Nederlandse wetgever heeft deze richtlijn geïmplementeerd, daarbij rekening houdend met artikel 10 lid 2 en 3 Grondwet, waarin is vervat dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. Ook geeft de wet uitvoering aan het in artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) vervatte privacyrecht en aan het op artikel 8 EVRM steunende Verdrag van Straatsburg inzake gegevensbescherming.[4] Tot slot had de wetgever ten doel om het regime van de Wbp aan te laten sluiten op haar voorganger: de Wet persoonsregistraties (WPR).

Artikel 80 Wbp bepaalt dat de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties binnen vijf jaar na de inwerkingtreding van de wet aan de Staten-Generaal een verslag toezenden over de doeltreffendheid en de effecten van de wet in de praktijk. In 2007 verscheen het eerste rapport van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) waarin de Wbp werd geëvalueerd aan de hand van een literatuur- en jurisprudentieonderzoek.[5] In 2008 verscheen het tweede WODC-rapport waarin een praktijkanalyse was vervat.[6] Daarnaast zijn er tal van studies verschenen ten aanzien van gegevensbescherming en de Wbp zoals het rapport 'Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer'[7] van de Adviescommissie Veiligheid en persoonlijke levenssfeer, 'Niets te verbergen en toch bang'[8] in opdracht van het College bescherming

---

* **Bart van der Sloot is onderzoeker aan het Instituut voor Informatie Recht (IVIR) van de UvA. Hij doet onderzoek naar privacy in horizontale verhoudingen.**

1 *Kamerstukken II* 1997/98, 25 892, *Stb.* 2000, 302 en 2001, 337.
2 Zie voor enkele verschillen: C. Cuijpers, 'Verschillen tussen de Wbp en Richtlijn 95/46/EG en de invloed op de administratieve lasten- en regeldruk', juni 2006, <www.actal.nl/file/3776/>.
3 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
4 *Kamerstukken II* 1997/98, 25 892/3, p. 5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981. <http://conventions.coe.int/treaty/en/treaties/html/108.htm>.
5 *Kamerstukken II* 2006/07, 31 051/BLG11943 (verder: Eerste WODC-rapport). Zie daarover: J. Holvast, 'Eerste fase evaluatie Wet bescherming persoonsgegevens', *P&I* 2007-4.
6 *Kamerstukken II* 2006/07, 31 051/BLG19029 (verder: Tweede WODC-rapport). Zie daarover: H.B. Winter, 'De werking van de WBP in kaart gebracht: onbekend maakt onbemind', *RegelMaat* 2009-2. A.M. Klingenberg, 'Wat niet weet, wat niet deert: de evaluatie van de Wet bescherming persoonsgegevens', *P&I* 2009-2.
7 Adviescommissie Veiligheid en persoonlijke levenssfeer, 'Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer', januari 2009 (verder: Rapport Gewoon Doen), <www.veiligheidbegintbijvoorkomen.nl/images/Rapport%20commissie%20Brouwer-Korf_tcm62-164735.pdf>.
8 Regioplan Beleidsonderzoek, 'Niets te verbergen en toch bang: Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving', januari 2009, <www.cbpweb.nl/downloads_rapporten/rap_2009_niets_te_verbergen_en_toch_bang.pdf>.

persoonsgegevens (CBP), het rapport 'Data voor daadkracht'[9] van de Adviescommissie Informatiestromen Veiligheid en het onderzoek van TNS/NIPO 'Burgers en hun privacy'.[10]

Ook in de wetenschap staat de Wbp voortdurend ter discussie.[11] Zo verscheen vooruitlopend op de evaluatie van de Wbp in december 2005 het themanummer van *Privacy & Informatie* 'Evaluatie van de WBP',[12] maar ook daarna is deze wet een kernonderwerp in dit blad gebleven. Ook de parlementaire discussie ten aanzien van de Wbp staat niet stil. Zo is de wet reeds meer dan vijftien keer gewijzigd, zij het vaak op kleine punten,[13] en zijn er thans twee wetsvoorstellen aanhangig die beogen de Wbp te wijzigen.[14] Tot slot is ook op Europees niveau de Privacyrichtlijn al een aantal maal aan een uitgebreide evaluatie onderworpen[15] en heeft de Artikel 29 Werkgroep een flink aantal werkdocumenten gepubliceerd over deze regeling.[16]

Onlangs presenteerde het kabinet zijn plannen naar aanleiding van de evaluatie van de Wbp.[17] Daarin stonden vier punten centraal:

1. meer waarborgen bij de omgang met persoonsgegevens;
2. robuuster extern toezicht;
3. minder nadruk op procedures en controle vooraf;
4. het burgerperspectief.

Dit artikel beoogt een kort overzicht te geven van de belangrijkste knel- en discussiepunten die in de loop der jaren ten aanzien van de werking van de Wbp te berde zijn gebracht en te bezien in hoeverre de kabinetsplannen hier een adequate oplossing voor aandragen. Paragraaf 2 zal per subparagraaf een overzicht presenteren ten aanzien van respectievelijk de definities van de wet, de reikwijdte en excepties, de rechten van de betrokkenen, zelfregulering en toezicht en handhaving. Ook zal daarbij worden vermeld welke plannen het kabinet heeft gepresenteerd ten aanzien van deze knelpunten. Paragraaf 3 zal een samenvatting en conclusie bevatten.

Daarbij moet in ogenschouw worden genomen dat op Europees niveau de Privacyrichtlijn binnen afzienbare tijd aan een herziening zal worden onderworpen.[18] Onlangs is al het Telecom Package aangenomen, waarmee een aantal van de belangrijkste richtlijnen op telecomgebied werden gewijzigd en aangepast aan de tijd en de huidige stand van de techniek.[19] Onderdeel hiervan was de herziening van de e-Privacyrichtlijn[20] door de Richtlijn Burgerrechten,[21] waarover in de vorige editie van *P&I* een artikel is verschenen.[22] Daarnaast heeft ook commissaris Kroes een zeer ambitieuze Digitale Agenda doen

---

9 Rapport van de Adviescommissie Informatiestromen Veiligheid, 'Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse', april 2007, <www.google.nl/url?sa=t&source=web&cd=2&ved=0CB4QFjAB&url=http%3A%2F%2Fwww.rijksoverheid.nl%2Fbestanden%2Fdocumenten-en-publicaties%2Frapporten%2F2007%2F08%2F30%2Frapport-data-voor-daadkracht%2Fdatavoordaadkracht.pdf&ei=ZT5pTIOMFcyAOODB4LgF&usg=AFQjCNF-6eztgVaYgQJ7VaM4wYjR17ph3g>.

10 TNS/NIPO, 'Burgers en hun privacy. Opinie onder burgers', februari 2005, <www.cbpweb.nl/downloads_rapporten/rap_2004_privacy_burgers.pdf>.

11 Zie voor een meer algemene studie: D.W.F. Verkade, 'De nieuwe Nederlandse Wet bescherming persoonsgegevens: een bundeltje impressies', *Computerrecht* 2001-2, p. 56 e.v.

12 *P&I* 2005-6.

13 *Stb.* 2001, 180; *Stb.* 2001, 584; *Stb.* 2001, 581; *Stb.* 2001, 664; *Stb.* 2002, 148; *Stb.* 2002, 552; *Stb.* 2004, 119; *Stb.* 2004, 50; *Stb.* 2004, 215; *Stb.* 2004, 315; *Stb.* 2004, 306; *Stb.* 2004, 700; *Stb.* 2005, 282; *Stb.* 2005, 339; *Stb.* 2006, 24; *Stb.* 2006, 605; *Stb.* 2007, 300; *Stb.* 2008, 85; *Stb.* 2008, 100; *Stb.* 2009, 265; *Stb.* 2009, 8.

14 *Kamerstukken II* 2008/09, 31 734; *Kamerstukken II* 2008/09, 31 841.

15 Verslag van de Commissie, 'Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM 2003/265', Brussel, mei 2003 (verder: Eerste Commissie-rapport). Mededeling van de Commissie aan het Europees Parlement en de Raad, 'Over de follow-up van het Werkprogramma voor een betere toepassing van de Richtlijn gegevensbescherming. COM 2007/87', Brussel, juli 2007.

16 Art. 29 Werkgroep, 'Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU, (WP56)', Brussel, 30 mei 2002; Artikel 29 Werkgroep, 'Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995, (WP 114)', Brussel, 25 november 2005 (verder: Artikel 29 Werkgroep, WP 114, 2005); Artikel 29 Werkgroep, 'Advies 4/2007 over het begrip persoonsgegeven, (WP 136)', Brussel, 20 juni 2007 (verder: Artikel 29 Werkgroep, WP 136, 2007); Artikel 29 Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", (WP 169)', Brussel, 16 februari 2010 (verder: Artikel 29 Werkgroep, WP 169, 2010).

17 *Kamerstukken II* 2009/10, 31 051/5. Over deze plannen verscheen in *P&I* onlangs al het artikel van Anne-Wil Duthler: A.W. Duthler, 'Kabinetsplannen voor toekomst Privacybescherming', *P&I* 2010-2.

18 <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/63&format=HTML&aged=0&language=NL&guiLanguage=en> en <www.cbpweb.nl/Pages/med_20090529_privacyrichtlijn.aspx>.

19 Ten eerste vervangt Verordening 1211/2009 de European Regulators Group, die door de Commissie was geïnstalleerd om coöperatie en coördinatie tussen de nationale autoriteiten en de Commissie te bevorderen en een interne markt voor elektronische communicatienetwerken en diensten te creëren, door de Body of European Regulators for Electronic Communications (BEREC, <http://berec.europa.eu>). Hierdoor wordt de centralisatie van de bevoegdheden bevorderd, alhoewel veel van de macht in handen van de nationale autoriteiten blijft. Ten tweede wijzigt Richtlijn 2009/140/EG de Kaderrichtlijn (Richtlijn 2002/21/EG), de Toegangsrichtlijn (Richtlijn 2002/19/EG) en de Machtigingsrichtlijn (Richtlijn 2002/20/EG). Ten slotte wijzigt Richtlijn 2009/136/EG de Universele dienstrichtlijn (Richtlijn 2002/22/EG), de Verordening betreffende samenwerking met betrekking tot consumentenbescherming (Verordening EG nr. 2006/2004) en de e-Privacyrichtlijn.

20 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juni 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie) (*PbEG* 2002, L 201/37).

21 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (*PbEG* 2009, L 337/11).

22 B. van der Sloot & F. Zuiderveen Borgesius, 'De amendementen van de Richtlijn Burgerrechten op de e-Privacy Richtlijn', *P&I* 2010-4.

laten verschijnen.[23] De herziening van de Privacyrichtlijn op fundamenteel niveau lijkt een absolute noodzakelijkheid in het kader van deze ambities, mede gezien het feit dat de technische ontwikkelingen in razend tempo voortijlen en de digitale omgeving een steeds belangrijkere rol is gaan innemen in het dagelijks leven van de burger. Daarbij lijkt het aannemelijk dat het kabinet bewust een aantal zaken met betrekking tot de herziening van de Wbp voor zich uit heeft geschoven in afwachting van de Europese herziening. Dit heeft betrekking op de fundamentele uitgangspunten, definitie- en reikwijdtekwesties en de werking van de wet op Europees en internationaal niveau.

2 Knelpuntanalyse

2.1 *Definities*

De begrippen uit de Wbp kenmerken zich door hun brede en open karakter.[24] Dit blijkt onder andere uit artikel 6 dat bepaalt dat de verwerking van persoonsgegevens op een 'behoorlijke en zorgvuldige wijze' dient te geschieden, artikel 7 dat bepaalt dat persoonsgegevens voor 'gerechtvaardigde doeleinden' mogen worden verzameld en artikel 8 dat bepaalt dat de verwerking van persoonsgegevens mag plaatshebben als dit voor de 'behartiging van het gerechtvaardigde belang' van de verwerker noodzakelijk is. Voor deze open en abstracte normstelling is destijds gekozen opdat er zich geen witte plekken in de bescherming van persoonsgegevens zouden voordoen. Deze abstracte normen zouden dan per sector nadere invulling moeten krijgen.[25] Dit open karakter wordt in de praktijk echter vaak als belemmering ervaren, aangezien het rechtsonzekerheid meebrengt en omdat er kosten mee zijn gemoeid om deze onzekerheid te verhelpen, onder meer door het opstellen van codes en het daartoe aantrekken van deskundigen.[26] Toch is het onwaarschijnlijk dat er op dit punt een wijziging zal komen in de wet. Het kabinet wijt de problemen die in de praktijk worden ervaren aan de trage rechtsontwikkeling en hoopt dat de algemene normen na verloop van tijd alsnog een nadere en concretere invulling zullen krijgen, onder meer door jurisprudentie en het opstellen van sectorale gedragscodes.[27]

Ook wordt gewezen op de zeer ruime definities van 'persoonsgegeven',[28] dat in artikel 1 onder a wordt gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, en 'verwerking', dat in artikel 1 onder b wordt gedefinieerd als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het 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 van gegevens. Blijkens de memorie van toelichting op de Wbp vallen ook datamining en de uitvoering van bepaalde zoekopdrachten (queries) met behulp van daartoe geschreven programma's onder de reikwijdte van de Wbp.[29] De vraag die in de praktijk een steeds belangrijkere rol speelt, is echter of het maken van persoonsprofielen op basis van al dan niet geanonimiseerde persoonsgegevens ook onder de 'verwerking van persoonsgegevens' in de zin van de Wbp valt.[30] Deze vraag speelt bijvoorbeeld een steeds prominentere rol op het internet, waar aanbieders van zoekmachines op basis van zoekopdrachten klantenprofielen aanmaken die vervolgens worden gebruikt voor *behavioural advertising*,[31] het tonen van reclame op basis van het gemaakte persoonsprofiel.[32] De status van persoonsprofielen kwam ook in de veel besproken *Dexia*-zaak aan bod.[33] Daarin stond ter discussie of een klant een inzagerecht had ten aanzien van de op hem van toepassing verklaarde groepsprofielen. De Hoge Raad oordeelde dat persoonsprofielen inderdaad onder de reikwijdte van de Wbp vallen. Ook in de literatuur lijkt de algemene consensus dat als uitgangspunt heeft te gelden dat '[…] het genereren van groepsprofielen op grond van persoonsgegevens als een afzonderlijke finaliteit dient te [worden be-

23 Commissie, 'Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Een digitale agenda voor Europa (COM(2010)245 definitief)', Brussel, 19 mei 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:NL:HTML>.

24 E. Schreuders & H. Gardeniers, 'Materiële normen: de kloof tussen de juridische normen en de praktijk', *P&I* 2005-6.

25 *Kamerstukken II* 1997/98, 25 892/3, p. 11.

26 Tweede WODC-rapport, p. 94. Opvallend is dat veel van de bedrijven die dit niet als probleem ervaren vaak weinig met privacywetgeving in de weer zijn. Vandaar ook de titel van het rapport: 'Wat niet weet, wat niet deert'.

27 *Kamerstukken II* 2009/10, 31 051/5, p. 21.

28 Artikel 29 Werkgroep, WP 136, 2007. J.M.A. Berkvens, 'Persoonsgegevens, wat zijn dat?', *P&I* 2005-6.

29 *Kamerstukken II* 1997/98, 25 892/3, p. 52.

30 A. Cormack, 'Pseudonymous Identifiers and the Data Protection Directive (95/46/EC)', december 2008, <www.terena.org/activities/refeds/docs/PseudonymousIdentifiersv0.05.pdf>.

31 Art. 29 Werkgroep, 'Advies 2/2010 over online reclame op basis van surfgedrag ("behavioural advertising") (WP 171)', Brussel, 22 juni 2010.

32 College bescherming persoonsgegevens, 'Analyse surfgedrag Planet Internet', z2002-1146, mei 2004. College bescherming persoonsgegevens, 'verzoeker/bedrijf', z2004-0742, juni 2005. College bescherming persoonsgegevens, 'Ambtshalve onderzoek door CBP; bevindingen', z2001-1595, oktober 2002.

33 HR 29 juni 2007, nr. r06/045HR, *LJN* AZ4463 (*Dexia/X*). Hof 's-Hertogenbosch 16 januari 2006, nr. R200500692 I, *LJN* AV0011. HR 29 juni 2007, nr. R06/163HR, *LJN* BA3529 (*HBU/X*). P.J.A. de Hert, M. Hildebrandt, S. Gutwirth & R. Saelens, 'De WBP na de Dexia-uitspraken', *P&I* 2007-4. G-J. Zwenne, 'Nogmaals de WBP en de winstverdubbelaar', *Computerrecht* 2007-6. A.J E. van den Bergen, 'De Wet bescherming persoonsgegevens in de financiële procespraktijk', *Tijdschrift voor Financieel Recht* 2005-10. W.A.K. Rank & A.J. Haasjes, 'Misbruik van de Wbp in civiele procedures tegen financiële instellingen', *Tijdschrift voor Financieel Recht* 2005-12. E.J. Dommering: annotatie bij HR 29 juni 2007 (*Dexia*) en (*HBU*), *NJ* 2007, 51/52, nr. 638 en 639, p. 6483-6488. E. Hoving, 'De gevolgen van het Dexia-arrest voor de praktijk', *P&I* 2007-6.

schouwd] in de zin van de wet'.[34] Dit brengt mee dat het verwerken van persoonsgegevens, met name gevoelige persoonsgegevens als betreffende ras, geaardheid en medische informatie, ten behoeve van het maken van persoons- of groepsprofielen aan strenge voorwaarden is gebonden.[35] De meeste zoekmachines op het internet hebben dan ook het gebruik van gevoelige gegevens ten behoeve van *direct marketing* afgezworen.[36]

Daarnaast wordt er een probleem gesignaleerd ten aanzien van de op onderdelen verouderde terminologie die de Wbp bezigt.[37] Het uitgangspunt is dat de wet technologieneutraal moet zijn, blijkens overweging 27 van de Privacyrichtlijn, die leest dat de bescherming van personen zowel op automatische als op niet-automatische verwerking van toepassing is en dat de reikwijdte van deze bescherming niet afhankelijk mag zijn van de gebruikte technieken, omdat zulks ernstig gevaar voor ontduiking zou opleveren. Het probleem is echter dat de meeste basisbegrippen uit de richtlijn zijn ontwikkeld in de jaren zeventig van de vorige eeuw.[38] Dit brengt mee dat door nieuwe ontwikkelingen zoals het gebruik van bijvoorbeeld vingerafdrukken, biomedisch materiaal,[39] bodyscans,[40] digitale archieven[41] en radio frequency identification devices (RFID)[42] onduidelijkheid bestaat over de toepassing van de Wbp. Zo merkt Wisman op dat RFID-toepassingen op tal van punten strijdig kunnen zijn met de Wbp, maar dat omdat elke applicatie van RFID weer anders is, het vrijwel onmogelijk is om volledige duidelijkheid te verschaffen over de toepasbaarheid van de Wbp.[43] Een herziening van de wet op dit punt wordt dan ook algemeen voorgestaan.[44] Toch meent de regering dat deze technische ontwikkelingen in de praktijk niet tot grote privacyschendingen hebben geleid die aanleiding geven nieuwe wetgeving voor te stellen. Daarnaast is zij van mening dat de wet niet aan elke nieuwe technologie hoeft te worden aangepast. Wel geeft ze toe: 'Op langere termijn zal zich de noodzaak aandienen voor een meer fundamentele verandering van regelgeving. Verschijnselen als "*cloud computing*", maar ook RFID, leiden op den duur onvermijdelijk tot de noodzaak centrale begrippen uit de richtlijn en de Wbp als "persoonsgegeven" en "verantwoordelijke" opnieuw op hun bruikbaarheid voor de komende decennia te beoordelen.'[45] Daarbij zal aansluiting moeten worden gezocht bij een herziening van de Europese richtlijn.

Wellicht het belangrijkste definitieprobleem geldt ten aanzien van de in artikel 1 onder d respectievelijk e vermelde begrippen 'verantwoordelijke' en 'bewerker'.[46] De 'verantwoordelijke' voor de gegevensverwerking is de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De 'bewerker' is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. Dit onderscheid is van belang omdat op de verantwoordelijke tal van verplichtingen rusten die niet op de 'bewerker' van toepassing zijn. De belangrijkste zijn dat de verwerking zorgvuldig en met waarborgen omkleed moet geschieden en dat de verwerking op een in de wet genoemde grondslag moet stoelen. Artikel 8 vermeldt dat persoonsgegevens slechts mogen worden verwerkt indien de betrokkene zijn ondubbelzinnige toestemming heeft verleend, de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, om een wettelijke verplichting of publiekrechtelijke taak na te komen, ter vrijwaring van een vitaal belang van de betrokkene of ter behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Ook heeft hij wiens persoonsgegevens worden verwerkt ten aanzien van de verantwoordelijke het recht op inzage, correctie en verwijdering van de persoonsgegevens.

Het onderscheid tussen verantwoordelijke en bewerker is met name in de internetomgeving niet altijd evident. Zo is het ten aanzien van zogenoemde Web 2.0-applicaties als Youtube en Facebook bijvoorbeeld de vraag wie als verantwoordelijke voor de op de site verwerkte gegevens valt aan te merken: de website hoster of de gebrui-

34 P.J.A. de Hert, M. Hildebrandt, S. Gutwirth & R. Saelens, *P&I* 2007-4, p. 154.
35 Zie uitgebreider: E. Hoving, 'Modellering van persoonsgegevens en Groepsprofielen', *P&I* 2008-6.
36 Zie bijvoorbeeld: <www.google.nl/intl/nl/privacypolicy.html>.
37 J.P. van Schoonhoven, 'Scheiding der machten bij of krachtens de WBP', *P&I* 2006-5.
38 Artikel 29 Werkgroep, 'The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, (WP 168)', Brussel 1 december 2009, p. 11 (verder: Artikel 29 Werkgroep, WP 168, 2009).
39 E.R. Brouwer, 'Persoonsregistraties als grensbewaking: Europese ontwikkelingen inzake het gebruik van informatiesystemen en de toepassing van biometrie', *P&I* 2004-1.
40 College bescherming persoonsgegevens, 'Bodyscan', z2002-046324, mei 2002.
41 College bescherming persoonsgegevens, 'Privacyaspecten digitalisering cultureel erfgoed', z2006-00869, november 2006.
42 Artikel 29 Werkgroep, 'Working document on data protection issues related to RFID technology, (WP 105)', Brussel, 19 januari 2005. Artikel 29 Werkgroep, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, (WP 175)', Brussel, 13 juli 2010. Gerrit-Jan Zwenne & Bart Schermer, *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen*, 's-Gravenhage, 2005. S. Nas, 'Iedereen een chippie in zijn arm? RFID-labels en de wolk van gegevens', *P&I* 2005-3. W. Schreurs, 'Privacy en RFID-technologie', *P&I* 2005-5. T.H.A. Wisman, 'De RFID-golf in de detailhandel. Worden wij verplicht mee te surfen op het "internet van dingen"?', *P&I* 2008-4. P. Blok, 'De Wbp en RFID', in: G. Zwenne & B. Schermer, *Privacy en andere juridische aspecten van RFID. Unieke identificatie op afstand van producten en personen*, 's-Gravenhage, 2005.
43 T.H.A. Wisman, 'De RFID-golf in de detailhandel. Worden wij verplicht mee te surfen op het "internet van dingen"?', *P&I* 2008-4, p. 188.
44 Eerste WODC-rapport, p. 62-65.
45 *Kamerstukken II* 2009/10, 31 051/5, p. 22.
46 College bescherming persoonsgegevens, 'Begrip bewerker', z2002-0362, mei 2002. R. Wong, 'Social networking: a conceptual analysis of a data controller,' *Communications Law* 2009-5.

ker van de dienst. Om te bepalen wie de verantwoordelijke is, staat centraal wie het doel van en de middelen voor de gegevensverwerking vaststelt. In het geval waarin een gebruiker een video plaatst waarin ook andere personen herkenbaar in beeld komen kan enerzijds worden gesteld dat het Youtube is die de middelen voor de gegevensverwerking bepaalt en deze aanbiedt als een service op het internet. Zij organiseert en indexeert materiaal door middel van zoekalgoritmes en lijsten met meest bekeken video's. Anderzijds kan worden gesteld dat de gebruiker van Youtube dit platform heeft uitgekozen om zijn in de video vervatte gegevens te verwerken. Hij had hier ook van af kunnen zien of daartoe een ander platform kunnen kiezen. Enerzijds heeft Youtube een (afgeleid) financieel oogmerk met betrekking tot de gegevensverwerking. Anderzijds heeft de gebruiker van Youtube een doel met betrekking tot de gegevensverwerking, namelijk het openbaar maken van gedachten, informatie of meningen. Enerzijds is het ondoenlijk voor Youtube om alle filmpjes van te voren te controleren op de vraag of de verwerking onder één van de in de wet genoemde gevallen valt; anderzijds is het voor de gebruiker ondoenlijk om te voldoen aan een aantal verplichtingen die op de verantwoordelijke rusten, zoals de verplichting uit artikel 11 dat gegevens juist en nauwkeurig moeten zijn en artikel 13 dat bepaalt dat de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.[47] Hieruit blijkt dat het onderscheid tussen de bewerker en de daarvoor verantwoordelijke met name ten aanzien van Web 2.0-applicaties lang niet altijd helder is.[48] Een oplossing zou kunnen worden gevonden in het feit dat de verantwoordelijke ook tezamen met anderen het doel en de middelen voor de gegevensverwerking kan vaststellen. Er kan dan vanuit pragmatisch oogpunt per geval worden gezocht naar de meest wenselijke verdeling van verantwoordelijkheden.[49] Alhoewel op deze manier de juridische *idee-fixe*, dat voor iedere handeling een verantwoordelijke en voor elke geleden schade een aansprakelijke is, kan worden gehandhaafd, is het de vraag of deze interpretatie recht doet aan de oorspronkelijke logica van de bepaling en valt te betwijfelen of dergelijke ad-hocbeoordelingen de rechtszekerheid ten goede komen.

Tot slot staat de toestemming die de betrokkene kan geven voor de gegevensverwerking ter discussie.[50] De toestemming van de betrokkene wordt door artikel 1 onder i gedefinieerd als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. Artikel 8 onder a bepaalt verder dat deze toestemming ondubbelzinnig moet zijn en artikel 23 spreekt met betrekking tot bijzondere persoonsgegevens van uitdrukkelijke toestemming.[51] Deze toestemming komt in de praktijk onder druk te staan door het veelvuldig plaatsen van filmpjes op Youtube waarin derden zonder hun medeweten te zien zijn en het zonder toestemming taggen, het voorzien van meta-informatie, van foto's. Ook het feit dat veel internetfora niet strikt controleren op de naleving van de door artikel 5 vereiste toestemming van de wettelijke vertegenwoordiger ten aanzien van de verwerking van persoonsgegevens van kinderen die de leeftijd van zestien nog niet hebben bereikt doet daaraan afbreuk.[52] Echter, ook door nieuwe Europese regelgeving komt de toestemming met bijbehorende criteria onder druk te staan. De nieuwe regelgeving met betrekking tot cookies,[53] bestanden geplaatst door internetbedrijven om gegevens te verzamelen over een computergebruiker, stelt dat behoudens uitzonderingen de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig Richtlijn 95/46/EG, onder meer over de doeleinden van de verwerking. Overweging 66 bepaalt echter dat wanneer dit technisch mogelijk en doeltreffend is de toestemming van de gebruiker met verwerking kan worden uitgedrukt door gebruik te maken van de desbetreffende instellingen van een browser of een andere toepassing. Door de instellingen van de computer te beschouwen als afdoende om te voldoen aan de voorwaarden van een vrije, specifieke, geïnformeerde en ondubbelzinnige vorm van toestemming komen deze definities onder druk te staan.[54] De implementatie van deze richtlijn moet nog plaatsvinden en derhalve is het onzeker welke keuze het kabinet zal maken. Wel heeft het een consultatie uitgeschreven. Aanvankelijke leek het kabinet te kiezen voor een vorm van ondubbelzinnige toestemming, maar na de consul-

47 B. van der Sloot, 'De Leon & Vivi Down/Google', *Mediaforum* 2010-7/8.

48 Artikel 29 Werkgroep, WP 169, 2010. Artikel 29 Werkgroep, 'Advies 5/2009 over online sociale netwerken, (WP 163)', Brussel, 12 juni 2009. CBP, 'Richtsnoeren: publicatie van persoonsgegevens op internet', Den Haag, december 2007 (verder: CBP, Richtsnoer). J.M. van Essen, 'Richtsnoeren publicatie persoonsgegevens op internet, een brug te ver?', *P&I* 2008-2.

49 N. Helberger & J. van Hoboken, 'Little Brother is Tagging You – Legal and Policy Implications of Amateur Data Controllers', *Computer Law Review International* 2010-4, p. 101-109.

50 Zie ook de discussie rond het elektronisch patiëntendossier. J.P. de Jong, 'Toestemming onder druk', *RegelMaat* 2009-2.

51 Ook ten aanzien van wat als 'vrij', 'specifiek', 'geïnformeerd' en 'ondubbelzinnig' of 'uitdrukkelijk' moet worden beschouwd bestaat discussie. Dit zijn breed geformuleerde begrippen die op verschillende wijzen kunnen en worden geïnterpreteerd.

52 Eerste WOCD-rapport, paragraaf 4.3.4. CBP, 'Bijlage definitieve bevindingen onderzoek naar het door Diginus via de website www.zikle.nl verzamelen en verwerken van persoonsgegevens', z2007-01522, september 2008. Artikel 29 Werkgroep, 'Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), (WP 147)', Brussel, februari 2008.

53 De Richtlijn Burgerrechten amendeert de e-Privacyrichtlijn artikel 5.3.

54 F. Zuiderveen Borgesisus, 'De nieuwe cookie-regels. Alwetende bedrijven en onwetende internetgebruikers?', *nog te verschijnen.*

tatie lijkt het daarvan af te zien.[55] Daarnaast geeft het kabinet aan zich bewust te zijn van de problemen in de praktijk rond het toestemmingsvereiste ten aanzien van minderjarigen. Het kabinet probeert dit probleem aan te pakken door een grotere bewustwording te creëren, onder meer door middel van publiekscampagnes.[56]

2.2 *Reikwijdte en excepties*

Ten aanzien van de reikwijdte van de Wbp staat ten eerste het algemene karakter van de wet ter discussie. De wetgever heeft met betrekking tot de Wbp gekozen voor een zogenoemd 'omnibuskarakter', wat inhoudt dat de Wbp een algemene regeling is die van toepassing is op verwerking van persoonsgegevens, tenzij er een andere, sectorspecifieke regeling prevaleert.[57] Dit algemene karakter zou het voor zowel bedrijven als burgers makkelijker moeten maken hun rechten en plichten ten aanzien van gegevensverwerking respectievelijk te kennen, op te eisen en na te leven. Toch wordt er in de literatuur op gewezen dat dit algemene karakter van de wet, met haar bijbehorende algemene en open normen, juist vaagheid en rechtsonzekerheid meebrengt. Zo wijst Holvast vooruitlopend op de evaluatie van de Wbp erop dat het omnibuskarakter niet noodzakelijk is voor de bescherming van de privacy en dat er geen bewijs is '[…] dat voorafgaand aan de inwerkingtreding van de eerste omnibuswet in 1989 persoonsgegevens op grote schaal werden misbruikt en er is evenmin bewijs dat er op basis van de omnibuswetgeving vele misstanden zijn rechtgezet'.[58] Ook in de praktijk wordt deze algemene benadering als onpraktisch en onwenselijk ervaren omdat er bij veel voor gegevensverwerking verantwoordelijken onduidelijkheid bestaat over de precieze invulling van de algemene regels ten aanzien van hun specifieke situatie.[59] Toch lijkt de regering op dit punt geen verandering te willen brengen, omdat er volgens haar '[…] geen reëel alternatief bestaat voor het bestaande karakter van de Wbp'.[60]

Ook wordt met name door overheidsinstanties een probleem ervaren ten aanzien van de verwerking van bijzondere persoonsgegevens. Artikel 16 Wbp bepaalt dat de verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het 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, slechts onder strikte voorwaarden mag geschieden.[61] Artikel 17-24 geven specifieke regels met betrekking tot het in overeenstemming met de wet verwerken van bijzondere persoonsgegevens. De verwerking van strafrechtelijke gegevens door overheidsinstanties die hiertoe in het kader van hun taakuitoefening verplicht zijn, vormt het knelpunt.[62] Uitzonderingen op het verbod op de verwerking van strafrechtelijke gegevens zijn geformuleerd in artikel 22 en 23. Artikel 22 lid 4 onder c Wbp kent een open uitzondering voor die gevallen die niet in de Wbp zijn geregeld. In een aantal brieven heeft het CBP de minister verzocht ten aanzien van strafrechtelijke gegevens het systeem fijnmaziger in te vullen.[63] 'De afgelopen jaren is het CBP gebleken dat er meer dan wenselijk een beroep gedaan wordt op deze open uitzondering. Nader onderzoek is gewenst naar de mogelijkheid en wenselijkheid de uitzonderingen op het verbod van de verwerking van strafrechtelijke gegevens fijnmaziger in te vullen. Hierdoor zouden namelijk veel voorkomende en maatschappelijk geaccepteerde verwerkingen van deze gegevens die geen onaanvaardbare risico's met zich meebrengen voor de rechten en vrijheden van de betrokkenen niet langer vallen onder de uitzondering van het voorafgaand onderzoek door het CBP. Deze uitzondering is immers bedoeld voor niet voorziene gevallen.'[64] Deze bepaling wordt door een thans aanhangige wet zo aangevuld en uitgebreid dat de voorgenoemde gevallen worden verholpen.[65]

Ten aanzien van het toepassingsgebied van de Wbp is er met name discussie over de territoriale toepassing van de wet. Artikel 4 bepaalt dat de wet van toepassing is in twee gevallen:

1. als de verwerking van persoonsgegevens geschiedt in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland;
2. als de verwerking van persoonsgegevens geschiedt door of ten behoeve van een verantwoordelijke die

55 < www.internetconsultatie.nl/nrfimplementatie>. Zie: Voorstel van wet (consultatieversie d.d. 15 april 2010), <www.internetconsultatie.nl/nrfimplementatie/document/122>, memorie van toelichting (consultatieversie d.d. 15 april 2010), <www.internetconsultatie.nl/nrfimplementatie/document/123>. Consultatieverslag wetsvoorstel implementatie gewijzigd Europees regelgevend kader (NRF) in de Telecommunicatiewet, <www.internetconsultatie.nl/nrfimplementatie/document/167>.

56 *Kamerstukken II* 2009/10, 31 051/7, p. 21.

57 Om de onduidelijkheid tegen te gaan heeft het Ministerie van Justitie een handleiding geschreven. L.B. Sauerwein & J.J. Linnemann, 'Handleiding voor verwerkers van Persoonsgegevens. Wet bescherming persoonsgegevens', april 2002.

58 P.H. Blok, 'De waarde van de omnibuswet', *P&I* 2005-6.

59 Eerste WODC-rapport, p. 13.

60 *Kamerstukken II* 2009/10, 31 051/5, p. 21.

61 Zie ook: J. Holvast & P.R. Rodrigues, 'De gevoeligheid van bijzondere gegevens', *P&I* 2005-6.

62 Zie ook: Eerste WODC-rapport, p. 76. Zie ook: J.E.J. Prins, 'De veiligheid van privacy', *RegelMaat* 2009-2. F.K. Doornbos, 'De wolf in schaapskleren buiten de poort. Employment screening in het kader van AEO-certificering', *Tijdschrift Vervoer & Recht* 2008-5.

63 Zie ook: CBP, 'Brief aan Minister van Justitie', z2004-1086, december 2004 en CBP, 'Brief aan Minister van Justitie', z2004-1494, juli 2005. CBP, 'Actieplan voor een veilige stad', z2002-133521, november 2002. CBP, 'Zwarte lijsten en verwerking van strafrechtelijke gegevens', z2002-1135, november 2002. CBP, 'Fietsregister', z2004-0883, oktober 2004. CBP, 'Besluit inzake het verzoek tot het verlenen van ontheffing als bedoeld in artikel 23, eerste lid, onder e WBP', z2005-0668, juli 2005. CBP, 'Beslissing op bezwaar', z2007-01015, oktober 2007.

64 CBP, 'Brief aan Minister van Justitie', z2004-10867, december 2004, p. 4.

65 *Kamerstukken II* 2008/09, 31 841.

> geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.

Daarbij geldt dat het een verantwoordelijke als bedoeld in het tweede geval verboden is persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke. Uit de Europese evaluatie van de Privacyrichtlijn blijkt dat dit '[…] een van de bepalingen [was] die tijdens het beoordelingsproces het meest werd bekritiseerd. In de ingezonden bijdragen werd gepleit voor een op het land van herkomst gebaseerde bepaling zodat multinationale organisaties met één stel voorschriften in de gehele EU zouden kunnen opereren. Velen voerden ook aan dat het "gebruik van middelen" geen geschikt of werkbaar criterium is om te bepalen of de EU-wetgeving van toepassing is op voor de verwerking verantwoordelijken die buiten de EU zijn gevestigd.'[66]

De kritiek richt zich op beide gevallen waarin de Wbp van toepassing is.[67] Ten aanzien van de 'activiteiten van een vestiging van een verantwoordelijke in Nederland' is het lang niet altijd duidelijk wat als vestiging heeft te gelden, wat als activiteiten heeft te gelden en welk recht er van toepassing is in het geval een multinational vele verschillende vestigingen heeft.[68] Door vele betrokkenen wordt er dan ook voor gepleit om niet de vestiging van een multinational als leidend te beschouwen, maar de zogenoemde country-of-origin-regel toe te passen, wat inhoudt dat slechts de wetgeving van het land waar het moederbedrijf is gevestigd van toepassing is.[69] Dit zou zowel de bedrijven met minder regels belasten als de rechtszekerheid voor betrokkenen ten goede komen. Ook zouden daarmee de handhavingsproblemen verdwijnen, zoals de problemen ten aanzien een boetoplegging aan een multinational die in een land buiten de Europese Unie is gevestigd.[70]

Ten aanzien van het geval waarin 'gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden' bestaat evenzeer discussie. Zo is de verwerking door het gebruik van nieuwe technieken niet noodzakelijkerwijs meer gebonden aan één specifieke locatie. Door het gebruik van technieken als 'cloud computing',[71] waarbij de gebruikte software is verdeeld tussen meerdere computers op het internet en waarbij acties en applicaties worden gedeeld in een wolk van gegevens verspreid over het net, en het gebruik van 'grids', waarbij computers aan elkaar worden gekoppeld en samenwerken om zo grotere berekeningen en taken uit te kunnen voeren, is het allerminst evident op welke locatie de daadwerkelijke gegevensverwerking heeft plaatsgevonden.[72]

Tot slot zijn er ook knelpunten ten aanzien van het gegevensverkeer met landen buiten de Europese Unie dat door artikel 76-78 Wbp wordt geregeld.[73] Artikel 76 bepaalt dat persoonsgegevens slechts naar een land buiten de Europese Unie mogen worden doorgegeven indien dat land een passend beschermingsniveau waarborgt. Artikel 77 formuleert hierop uitzonderingen, grotendeels gelijkend aan die vermeld in artikel 8. Over deze bepaling is in de praktijk veel verwarring ontstaan.[74] 'Zo zijn er knelpunten rondom de interpretatie van de uitzonde-

66 Eerste Commissie-rapport, p. 19.

67 M.A.H. Fontein-Bijnsdorp, 'Enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens, art. 4.', *Computerrech*t 2008-6. E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008-3. M.B.J. Thijssen, 'De Wet bescherming persoonsgegevens in concernverband', *Computerrecht* 2002-2. H.H. de Vries, 'Grensoverschrijdende Gegevensbescherming', *P&I* 2005-6. G-J. Zwenne & G.C.J. Erents, 'Reikwijdte Wbp: enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp', *P&I* 2009-2.

68 Artikel 29 Werkgroep, WP 168, 2009, p. 9.

69 Eerste WODC-rapport, p. 31.

70 Zie bijvoorbeeld de bekende zaak: Tribunal de Grande Instance de Paris 11 augustus 2000. Yahoo! Inc. v. LICRA and UEJF, 433 F3d 1999 (9th Cir. 2006). Yahoo! Inc. v. LICRA and UEJF, 169 F Supp 2d 1181 (ND Cal. 2001). Yahoo! Inc. v. LICRA and UEJF, 169 F Supp 2d 1181 (ND Cal. 2001). Yahoo! Inc. v. LICRA and UEJF, 379 F 3d 1120 (9th Cir. 2004). Yahoo! Inc. v. LICRA and UEJF, 126 S.CT 2332 (Mem) (2006). Robert Corn-Reverem, 'Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?', Briefing Paper No. 71 (2002), Cato Institute, <www.cato.org/pubs/briefs/bp71.pdf>; Uta Kohl, 'Yahoo! – But No Hooray! For the International Online Community', *Australian Law yournal* 2001-75. Mathias Reiman, 'Introduction: The *Yahoo!* Case and Conflict of Laws in the Cyberage', *Michigan Journal of International Law* 2003-24. Horatia Muir Watt, 'Yahoo! Cyber-Collision of Cublures: Who Regulates?', *Michigan Journal of International Law* 2003-24. Molly van Jouweling, 'Enforcement of Foreign Judgements, the First Amendment, and Internet Speech: Notes for the Next Yahoo! V. Licra', *Michigan Journal of International Law* 2003-24. Mark Kightlinger, 'A Solution to the *Yahoo!* Problem? The EC E-Commerce Directive as a Model for International Cooperation on Internet Choice of Law', *Michigan Journal of International Law* 2003-24.

71 K. Sommer, 'Cloud computing: zegen, ramp of uitdaging?', *P&I* 2009-6. K.C. Sommer, 'Cloudcomputing en privacy, stof tot denken…' *P&I* 2010-1.

72 Zie hierover terloops: B. Schermer, 'Wat is RFID?', in: G-J. Zwenne & B. Schermers (red.), *Privacy en andere juridische aspecten van RFID*, Den Haag, 2005, p. 15-22.

73 S.H. Merkus, 'Toepassing van art. 76 en 77 lid 2 WBP', *P&I* 2004-1.

74 Artikel 29 Werkgroep, WP 56, 2002. Artikel 29 Werkgroep, WP 114, 2005. Artikel 29 Werkgroep, 'Advies 3/2009 over de ontwerpbeschikking van de Commissie inzake modelcontractbepalingen voor de doorgifte van persoonsgegevens naar in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van de voor de gegevensverwerking verantwoordelijke naar de verwerker), (WP 161)', Brussel, maart 2009. Artikel 29 Werkgroep, 'Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, (WP 172)', Brussel, 13 juli 2010. J.M.A. Berkvens, 'Het raadsel van 95/46/EG', *P&I* 2004-4. H.A.M. Fontein, 'Doorgiften naar derde landen: praktijkervaringen', *P&I* 2004-5. S. Artz, 'Derde modelcontract voor doorgifte naar derde landen goedgekeurd', *P&I* 2005-2. M.B.J. Thijssen, 'Grensoverschrijdend Gegevensbeschermingsrecht', *P&I* 2005-3.

ringsgronden, zelfregulering, het aanvragen van een vergunning, ook indien bijvoorbeeld gebruik wordt gemaakt van een modelcontract van de Europese Commissie, en de rechtsbescherming bij de vergunningprocedures.'[75] Het blijkt dat in de praktijk uitzonderingen nauwelijks worden toegekend, waardoor deze regeling een dode bepaling dreigt te worden. Het kabinet weidt weinig uit over het probleem van territoriale toepassing van de wet. Slechts kort verwijst zij naar de Europese regelgever die dit probleem zou moeten aanpakken.[76] Wel is er thans een wet aanhangig die een nieuw artikel toevoegt dat stelt dat onverminderd artikel 17-23 en 76-78 het verbod om bijzondere persoonsgegevens te verwerken niet van toepassing is voor zover deze verwerking (1) uitsluitend de doorgifte van deze gegevens naar de autoriteiten van een land buiten de Europese Unie betreft ten behoeve van een zwaarwegend algemeen belang; (2) de verantwoordelijke daartoe krachtens het recht van het desbetreffende land verplicht is; en (3) indien bij een bindend besluit van de Raad van de Europese Unie, van het Europees Parlement en de Raad gezamenlijk of van de Commissie van de Europese Gemeenschappen, dan wel bij verdrag, de doeleinden voor de verwerking van deze gegevens, rekening houdend met het zwaarwegend algemeen belang, zijn vastgesteld, alsmede passende waarborgen ter bescherming van de persoonlijke levenssfeer worden geboden.[77] Hiermee wordt vooral gereageerd op de Amerikaanse wens om passagiersgegevens van vliegtuigvluchten aan de autoriteiten te verstrekken.

Daarnaast zijn er een aantal onduidelijkheden ten aanzien van de excepties uit de Wbp. Artikel 2 lid 2 onder a verklaart de Wbp niet van toepassing op de verwerking van persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Dit wordt doorgaans de privé-exceptie genoemd. Ter discussie staat of de privé-exceptie ook voor activiteiten op het internet kan gelden, bijvoorbeeld ten aanzien van privécorrespondenties tussen vrienden, persoonlijke blogs of op socialenetwerksites als Facebook. Dit vraagstuk is beantwoord in het arrest *Lindqvist*, waarin het Europese Hof van Justitie oordeelde dat deze exceptie zo moet worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen volgens het Hof niet het geval is ten aanzien van de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt.[78] Deze uitspaak laat in het midden wat als een 'onbepaald aantal personen' heeft te gelden. De vraag die zich voordoet is of het beperken van de toegang tot bijvoorbeeld een Facebook-pagina tot vrienden voldoende is of dat er verdere waarborgen en maatregelen moeten worden getroffen om onder de privé-exceptie te vallen. De Artikel 29 Werkgroep geeft weinig meer verheldering als zij stelt dat in bepaalde omstandigheden het kan voorkomen dat de activiteiten van de gebruiker van een socialenetwerkdienst niet onder deze vrijstelling vallen en dat in bepaalde gevallen de gebruiker kan worden geacht bepaalde verantwoordelijkheden van een voor de verwerking verantwoordelijke op zich te hebben genomen.[79]

Hieraan gelieerd is het vraagstuk ten aanzien van de journalistieke exceptie. Artikel 3 lid 1 bepaalt dat delen van de Wbp niet van toepassing zijn op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden. De vraag is in hoeverre amateurjournalisten op het internet van deze exceptie gebruik kunnen maken. Het CBP stelt dat in het geval een internetpublicatie voldoet aan vier criteria, de journalistieke exceptie in ieder geval van toepassing is. Deze vier criteria zijn:

1. er heeft een objectieve informatieverzameling plaatsgevonden;
2. het publiceren van nieuws is een regelmatige bezigheid;
3. het nieuws heeft een maatschappelijke strekking;
4. er geldt het recht van repliek voor betrokkenen.

'Of een publicist betaald wordt voor zijn publicatie, is niet wezenlijk voor het bepalen van de reikwijdte van de journalistieke exceptie. Het is slechts aan weinigen gegeven om geld te verdienen met een (zelfstandige) publicatie op internet, terwijl met de publicatie wel een groot maatschappelijk belang gediend kan zijn.'[80] Of een internetpublicist onder de media-exceptie valt zal dan ook per geval moeten worden beoordeeld, rekening houdend met de omstandigheden van het geval. Ten aanzien van beide excepties bestaat dus onduidelijkheid over hun exacte toepassing in de digitale omgeving. Het kabinet zwijgt over de onduidelijkheden ten aanzien van beide excepties.

2.3 *Rechten van de betrokkenen*

Globaal vallen de rechten van betrokkenen in drie categorieën onder te verdelen. Ten eerste is er de uit het transparantiebeginsel van artikel 6 voortvloeiende[81] en in artikel 33 en 34 geregelde informatieverplichting. De verantwoordelijke moet vóór het moment van de verkrijging van de persoonsgegevens van de betrokkenen zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd mededelen, tenzij de betrokkene deze informatie reeds in zijn bezit heeft. In het geval

75 Eerste WODC-rapport, p. 115.
76 *Kamerstukken II* 2009/10, 31 051/5.
77 *Kamerstukken II* 2008/09, 31 734. Zie ook: CBP, 'Wijziging van de Wbp i.v.m. de PNR Overeenkomst 2007 tussen de EU en de VS', z2007-01530, februari 2008.
78 HvJ EG 6 november 2003, C-101/01, recital 47. Zie ook: HvJ EG 16 december 2008, C-73/07, nr. 44.
79 Artikel 29 Werkgroep, WP 163, 2009, p. 6.
80 CBP, Richtsnoer, p. 44. Zie ook Rb. 's-Hertogenbosch, kort geding 4 juli 2008, nr. 175262/ KG ZA 08-299. J.C. Kabel, 'De werkers van het woord verworden tot verwerkers', *NJB* 2008-35.
81 H.H. De Vries, 'Wet bescherming persoonsgegevens', in: P.C. Knol & G.J. Zwenne, *T&C Telecommunicatierecht*, Deventer, 2009, p. 604.

de persoonsgegevens worden verkregen via een andere weg, rust op de verantwoordelijke dezelfde verplichting, tenzij een dergelijke mededeling onmogelijk is, een onevenredige inspanning met zich brengt of indien de vastlegging of de verstrekking van de gegevens bij wet is voorgeschreven.[82] Ten tweede is er de in artikel 27-32 geregelde verplichting van de verantwoordelijke tot melding ten aanzien van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die voor de verwezenlijking van een doeleinde of van verscheidene samenhangende doeleinden bestemd is, alvorens met de verwerking wordt aangevangen. Deze verwerking moet worden gemeld bij het CBP of een functionaris voor de gegevensbescherming (FG).[83] Zowel het CBP als de FG houdt een register bij van de bij hen aangemelde gegevensverwerkingen. Er kan een voorafgaand onderzoek worden gestart in het geval van datakoppeling, het niet voldoen aan de informatieverplichting of het zonder vergunning verwerken van strafrechtelijke gegevens. Tot slot zijn in artikel 35-42 het inzagerecht, het aanvullings- en correctierecht en het verwijderings- en afschermingsrecht van de betrokkene vervat.[84]

Het belangrijkste euvel met betrekking tot de rechten van de betrokkenen lijkt de onbekendheid en de desinteresse die zowel bij verantwoordelijken als bij betrokkenen heerst.[85] Kolk & Verbruggen stellen bijvoorbeeld in hun artikel 'Het verborgen bestaan van de Wet bescherming persoonsgegevens' dat de wetgever met de Wbp een instrument heeft gecreëerd waarvan tot dan toe noch door advocaten, noch door rechters in de arbeidsrechtpraktijk veelvuldig gebruik werd gemaakt.[86] Ten aanzien van de informatieverplichting blijkt uit de praktijk dat veel bedrijven dergelijke informatievoorziening als overbodig of te kostbaar beschouwen en dat zij van het bestaan van deze plicht soms simpelweg geen weet hebben.[87] Ook ten aanzien van de meldingsplicht blijkt een behoorlijk gebrek aan bekendheid te bestaan bij betrokken organisaties.[88] Daarnaast bleek uit een steekproef dat slechts 69 procent van de ondervraagden een ontvangstbevestiging had ontvangen van het CBP na melding, dat geen enkele van de ondervraagden een inhoudelijke reactie had mogen ontvangen en dat bij geen enkele organisatie onderzoek was gedaan aan de hand van de gemelde verwerking.[89] J. Holvast concludeert dan ook in zijn artikel 'De aanmeldplicht, een overbodige bepaling?': 'Het beeld dat de meldingsplicht oproept stemt tot droefheid. Geconcludeerd kan worden dat amper aan de doelstellingen wordt voldaan. Zij leiden in meerderheid niet tot een vergroting van de doorzichtigheid en geven in geen geval een beschrijving van de feitelijke situatie. Uit dit laatste mag ook worden afgeleid dat de verheven doelstelling die het CBP heeft toegevoegd evenmin wordt gehaald. De administratieve lasten zijn aanzienlijk, terwijl het beroep op de vrijstellingen vaak ten onrechte heeft plaatsgevonden.'[90]

Tot slot blijkt uit de praktijk dat rechthebbenden nauwelijks gebruikmaken van hun recht op inzage, correctie en verwijdering. Uit de voorgenoemde steekproef bleek dat maar liefst 45 procent van de ondervraagde organisaties nooit een inzageverzoek had ontvangen, dat slechts 22 procent van de organisaties regelmatig een verzoek tot correctie of aanvulling van gegevens had ontvangen, dat de helft van de organisaties een dergelijk verzoek slechts zelden ontving en dat eenvijfde van de ondervraagde organisaties hier nimmer mee te maken had.[91] 'De zwaardere instrumenten zoals officiële klachten, bezwaar of verzet over privacyaspecten komen maar weinig voor, en ook geschilbeslechtingsprocedures bij de rechter, het CBP en geschillencommissies zijn een zeldzaamheid.'[92]

Het kabinet wil dit euvel voorkomen door ten eerste minder nadruk te leggen op de meldingsplicht, door middel van het toepassen van een ruimhartiger vrijstellingsbeleid.[93] Daarnaast wil het door middel van een grotere transparantie het privacybewustzijn onder burgers vergroten.[94] Het feit dat weinig burgers gebruikmaken van hun inzage- en correctierecht wijt het kabinet aan een gebrek aan kennis en transparantie. Pas als de burger daadwerkelijk weet voor welk doel zijn gegevens worden verwerkt, met welke andere gegevens die gegevens in verband worden gebracht en vervolgens aan anderen ter beschikking worden gesteld kan hij keuzes maken ten aanzien van deze gegevensverwerking.[95] Aan de formulering van de wettekst hoeft volgens het kabinet

82 Zie ook: Commissie van Beroep VPB 22 maart 2005, nr. 30516C01. CBP, 'Verplichtingen registratie hotelgasten', z2007-01131, november 2007.
83 Er is ten aanzien van deze verplichting een vrijstellingenbesluit van kracht. Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp). J.M. van Essen, 'Aanpassing van het Vrijstellingsbesluit', *P&I* 2005-2.
84 ABRvS 3 maart 2004, nr. 200304820/1, *LJN* AO4783. ABRvS 12 januari 2005, nr. 200402326/1, *LJN* AS2141. ABRvS 16 maart 2005, nr. 200406628/1, *LJN* AT0510.
85 Zie echter ook: K.P. Nagel, 'Privacy vanuit consumenten bezien', *P&I* 2005-6. Tweede WODC-rapport, p. 80-82.
86 D.J. Kolk & M. Verbruggen, 'Het verborgen bestaan van de Wet bescherming persoonsgegevens', *Arbeidsrecht* 2002-6/7, p. 32.
87 Zo bleek uit het onderzoek 'De naleving en beleving van de informatieplicht onder organisaties in Nederland: *Onderzoek onder huisartsen, onderwijsinstellingen en woningcorporaties*' dat slecht 35% van de huisartsen zichzelf redelijk tot goed op de hoogte van de Wbp vond. M. Tolboom & L. Mazor, *De naleving en beleving van de informatieplicht onder organisaties in Nederland: Onderzoek onder huisartsen, onderwijsinstellingen en woningcorporaties*, februari 2006, p. 4.
88 Tweede WODC-rapport, p. 72.
89 Tweede WODC-rapport, p. 77.
90 J. Holvast, 'De aanmeldplicht, een overbodige bepaling?', *P&I* 2005-6, p. 211.
91 Of de kabinetsvoorstellen hiertegen afdoende maatregelen treffen valt te bezien. *Kamerstukken II* 2009/10, 31 051/5, p. 23.
92 Tweede WODC-rapport, p. 82/83.
93 *Kamerstukken II* 2009/10, 31 051/5, p. 28-29.
94 *Kamerstukken II* 2009/10, 31 051/5, p. 13.
95 *Kamerstukken II* 2009/10, 31 051/5, p. 22.

niets te veranderen. Wel wil het kabinet het inzagerecht ondersteunen door een (facultatief) klachtrecht, welk niet noodzakelijkerwijs wettelijk geregeld hoeft te worden. 'De wet zou de totstandkoming van een dergelijk klachtrecht wel kunnen faciliteren, bijvoorbeeld door middel van een erkenningsregeling, gecombineerd met een vrijstelling van verplichtingen.'[96]

Een ander discussiepunt betreft de vraag naar de reikwijdte van het inzagerecht. Deze vraag speelde onder andere in de eerder aangehaalde *Dexia*-zaak. Een betrokkene eiste daar kopieën van de documenten waarin op hem betrekking hebbende persoonsgegevens waren verwerkt, inzage in de op hem van toepassing verklaarde persoonsprofielen en uitgeschreven transcripties van de telefoongesprekken die hij met de bank had gevoerd. De vraag rees of een samenvatting en overzicht van deze documenten afdoende was om aan de plicht te voldoen of dat er kopieën van alle documenten ter beschikking moesten worden gesteld. De Hoge Raad overwoog dat de verantwoordelijke bij de voldoening aan de door artikel 35 lid 2 Wbp op de verantwoordelijke gelegde verplichting om aan de betrokkene een volledig overzicht van de verwerkte persoonsgegevens te verschaffen niet kan volstaan met de verstrekking van globale informatie, maar dat alle relevante informatie over de betrokkene verschaft moet worden, hetgeen doorgaans zal moeten geschieden door het verstrekken van afschriften, kopieën en uittreksels.[97] Aangezien correctie op detailniveau plaatsvindt, moet het inzagerecht ruim worden opgevat. Het CBP stelt dat het overzien of gegevens feitelijk onjuist, onvolledig of niet ter zake dienend zijn voor het doel van de verwerking vereist zicht te hebben op zo veel mogelijk details van de verwerkte persoonsgegevens. Aangezien met het samenvatten van gegevens een belangrijk deel van de informatiewaarde verloren gaat, kan daar volgens het college in het algemeen niet mee volstaan worden.[98] Aangezien dit echter een enorme lastendruk meebrengt is over deze plicht in zowel de praktijk als in de wetenschappelijke literatuur veel discussie ontstaan.[99]

Tot slot woedt er een meer algemene discussie met betrekking tot de rechten van betrokkenen in de digitale omgeving. Steeds meer nadruk komt daar te liggen op het zogenoemde principe van 'consumer empowerment' en daaraan verwante begrippen als 'media literacy',[100] wat betrokkenen de middelen en capaciteiten verschaft om zelfstandige afwegingen te maken ten aanzien van gegevensverwerking, 'privacy by design',[101] dat betrokkenen invloed geeft op de mate van de op hen van toepassing zijnde gegevensbescherming, en 'commodified privacy', een steeds dominantere stroming onder privacyjuristen die stelt dat privacy een zelfbeschikkingsrecht is en dat er op persoonsgegevens een eigendomsrecht rust waardoor de privacybescherming plaatsvindt in het kader van het privaatrecht, waar principes als verantwoordelijkheid en contractsvrijheid het primaat hebben.[102] Door steeds meer privacydeskundigen worden hier echter vraagtekens bij geplaatst. Ten eerste wordt erop gewezen dat de contractsvrijheid in een privaatrechtelijk beschermingsmodel van privacy, altijd wordt beperkt door contractuele beperkingen die nietigheid bewerkstelligen, zoals bepalingen die tegen het in het maatschappelijk verkeer betamelijke indruisen. Daarnaast wordt erop gewezen dat 'media literacy' en 'privacy by design' vooral adequate beschermingsmethoden zijn voor hoogopgeleide volwassenen, terwijl kinderen, ouderen en lageropgeleiden simpelweg de zich in hoog tempo opvolgende technische mogelijkheden niet kunnen bijbenen.[103] Dit debat richt zich op de meest fundamentele keuze die de wetgever zal moeten maken ten aanzien van de Wbp. Kiest zij voor een bescherming van het zwakkere individu, met het gevaar paternalistisch te worden, of kiest zij ervoor om het individu meer vrijheid, meer autonomie en derhalve meer verantwoordelijkheid te geven? Voorlopig lijkt het kabinet zich te richten op

96 *Kamerstukken II* 2009/10, 31 051/5, p. 23.
97 HR, r.o. 3.4.
98 CBP, 'Onderzoek naar het recht op kennisneming Dexia Bank Nederland N.V.', z2003-16173, september 2004.
99 Berkvens stelt: 'Naar mijn mening is de uitleg die het College geeft aan art. 35 lid 2 WBP aanzienlijk ruimer dan uit de wet voortvloeit. De wet spreekt slechts over volledige overzichten van persoonsgegevens en niet over letterlijke kopieën van documenten of transscripties van gesprekken. De term "details" komt evenmin voor.' J.M.A. Berkvens, 'Inzage, inzicht of overzicht? Het aanzicht van artikel 35 WBP,' *P&I* 2005-3. Zie ook: E.J. Dommering, annotatie bij HR 29 juni 2007 (*Dexia*) en (*HBU*), *NJ* 2007, 51/52, nr. 638 en 639, p. 6483-6488.
100 Aanbeveling van de Commissie, 'Betreffende mediageletterdheid in de digitale omgeving voor een meer concurrerende audiovisuele en inhoudindustrie en een inclusieve kennismaatschappij, C 2009/6464,' Brussel, augustus 2009. Study on the Current Trends and Approaches To Media Literacy in Europa. Media Literacy Profile, <http://ec.europa.eu/culture/media/literacy/docs/studies/country/europe.pdf>. See also: Report on the Results of the Public Consultation on Media Literacy, <http://ec.europa.eu/avpolicy/media_literacy/docs/ report_on_ml_2007.pdf>, <www.epractice.eu/files/Study%20on%20Assessment%20Criteria%20for%20Media%20Literacy%20Levels%20-%20Final%20Report.pdf> en <www.euromedialiteracy.eu/>.
101 European Data Protection Supervisor, 'EDPS opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs', Brussel, maart 2010. European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy', Brussel, maart 2010. European Commission, 'Communication from the European Parliament, the council, The European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe. COM 2010/245', Brussel, mei 2010. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Privacy Enhancing Technologies. Witboek voor beslissers', december 2004.
102 Voor enkele belangrijke discussies omtrent 'commodified privacy': Paul Schwartz, 'Property, Privacy, and Personal Data', *Harvard Law Review* Vol. 117, No. 7. Jerry Kang, 'Information Privacy in Cyberspace Transactions', *Stanford Law Review* Vol. 50, No. 4. Pamela Samuelson, 'Privacy As Intellectual Property?', *Stanford Law Review* Vol. 52, No. 5. Zie ook recent nog: Egbert Dommering, 'Privacy als het zelfbeschikkingsrecht van de 21e eeuw', *Mediaforum* 2009-11/12.
103 Zie hierover al eerder: B. van der Sloot, 'De privacyverklaring als onderdeel van een wederkerige overeenkomst', *P&I* 2010-3.

deze laatste keuze, alhoewel het zich er niet expliciet over uitlaat.[104]

2.4 *Zelfregulering*

Er zijn twee vormen van zelfregulering opgenomen in de Wbp: gedragscodes en de aanstelling van een functionaris voor de gegevensbescherming.

Artikel 25 en 26 regelen dat hij die voornemens is een gedragscode vast te stellen, het CBP kan verzoeken te verklaren dat de daarin opgenomen regels, gelet op de bijzondere kenmerken van de sector waarin deze organisatie werkzaam is, een juiste uitwerking vormen van deze wet of van andere wettelijke bepalingen betreffende de verwerking van persoonsgegevens.[105] Door het opstellen van gedragscodes kunnen organisaties de algemene regels van de Wbp een sectorspecifieke invulling geven, waarmee de problemen ten aanzien van het omnibuskarakter van de wet kunnen komen te vervallen.[106] Toch blijkt dat dit instrument in de praktijk nauwelijks wordt gebruikt. Dit komt doordat de invloed en zeggenschap van het CBP op de code als te groot wordt ervaren; partijen vinden het CBP te weinig rekkelijk in de uitoefening van zijn goedkeuringsbevoegdheid. Bovendien is het opstellen van een dergelijke code een tijdrovend en kostbaar proces waar volgens veel organisaties weinig concrete voordelen tegenover staan.[107] Deze aversie tegen deze vorm van zelfregulering blijkt ook uit de frequentie waarmee dit instrument wordt gehanteerd. In 2007 waren er slechts negen gedragscodes opgesteld,[108] terwijl dit er thans slechts één meer is.[109]

Artikel 62-64 regelen de aanstelling van de functionaris voor de gegevensbescherming.[110] Hij ziet toe op de verwerking van persoonsgegevens. Het toezicht strekt zich uit tot de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd of door de verantwoordelijken die zijn aangesloten bij de organisatie die hem heeft benoemd. Indien op de verwerking een gedragscode van toepassing is, strekt het toezicht zich mede uit tot de naleving van deze code. De functionaris moet betrouwbaar zijn en over toereikende kennis beschikken, bovendien mag hij wat betreft de uitoefening van zijn functie geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die hem heeft benoemd. Ook mag hij geen nadeel van de uitoefening van zijn taak ondervinden. Deze functionaris krijgt zowel in de literatuur als in de praktijk een uitstekende waardering. Daarom is het des te opmerkelijker dat dit instrument slechts zelden wordt gebruikt; zo bleek in 2007 dat slechts 250 organisaties in Nederland een FG hadden aangesteld, wat gelijk was aan 0,3 promille van het toenmalige totaal aantal organisaties.[111] Daarnaast blijkt ook de onafhankelijkheid van de functionaris in de praktijk soms een probleem.[112] Zo geeft in een steekproef ondanks het wettelijke verbod bijna een kwart van de functionarissen aan verplicht te zijn aanwijzingen van zijn meerdere op te volgen.[113]

Het kabinet erkent zowel de waarde van zelfregulering als de problemen die ermee gemoeid zijn. Het geeft aan niet te ambiëren de samenleving het gebruik van gedragscodes of het aanstellen van FG's dwingend voor te schrijven. Zowel bedrijven als burgers moeten bij de wijze waarop zij invulling geven aan een gecompliceerde wet als de Wbp zo veel mogelijk vrijheid worden gegund. Het ziet meer in het door middel van wetgeving stimuleren van het gebruik van deze instrumenten. Hoe maakt zij niet duidelijk.[114]

2.5 *Handhaving en toezicht*

Ten eerste moet worden geconstateerd dat een niet gering aantal organisaties de Wbp niet strikt naleeft.[115] Dit is deels te wijten aan een gebrek aan bekendheid met de wet en aan onwetendheid over de precieze verplichtingen, maar vloeit soms ook voort uit laksheid en weigerachtigheid.[116] Daarnaast is een veel gehoord argument dat er vele administratieve lasten zijn gemoeid met de naleving van de wettelijke verplichtingen.[117] Dit laatste euvel wordt thans opgepakt met een wetsvoorstel,

---

104 *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 14.
105 Zie ook: CBP, 'Ambtshalve onderzoek: de bank', z2005-1028, maart 2006.
106 Zie ook overweging 61 van de Privacyrichtlijn.
107 Eerste WODC-rapport, p. 10/11.
108 Tweede WODC-rapport, p. 16.
109 <www.cbpweb.nl/Pages/ind_wetten_zelfr_gedr.aspx>.
110 Zie ook: J.C. Buitelaar & J. Borking, 'Invulling van de FG-functie bij een ministerie', *P&I* 2005-1. Z. Titulaer & F. Gimbrère, 'Zelfcontrole en zelfregulering: een wenkend perspectief (II)?', *P&I* 2005-1. P.G.C. Bunt, 'De functionaris voor de gegevensbescherming: een interne toezichthouder', *P&I* 2005-4. J. de Zeeuw, 'De toekomst van de functionaris voor de gegevensbescherming', *P&I* 2005-5. J.C. J. de Zeeuw & J.M. Titulaer-Meddens, 'De meldingsplicht en de FG', *P&I* 2006-5. L. Dubbeld, 'Functionarissen voor de gegevensbescherming: onzichtbare Privacybeschermers', *P&I* 2007-2. J. de Zeeuw, 'Het curriculum van de functionaris voor de Gegevensbescherming', *P&I* 2007-4. J.M. Titulaer-Meddens, 'Het toezichtbeleid van de functionaris voor de Gegevensbescherming', *P&I* 2007-6. J.M. Titulaer-Meddens, 'De overheids-FG en de FG in de zorgsector zijn ongerust over…', *P&I* 2008-2. F. Omidvary & J. de Zeeuw, 'Gevraagd: Een FG', *P&I* 2010-1.
111 Tweede WODC-rapport, p. 155.
112 Eerste WODC-rapport, p. 10-11 en p. 79-80.
113 Tweede WODC-rapport, p. 64. Daarnaast blijkt uit een gehouden enquête dat 16 procent van de ondervraagden het (zeer) oneens is met de stelling dat hij kan doen wat hij wil zonder anderen om toestemming te vragen. Tweede WODC-rapport, p. 98.
114 *Kamerstukken II* 2009/10, 31 051, nr. 5, p. 29.
115 S. Dekkers & G.H.J. Homburg, 'Private ondernemingen en handhaving van de WBP', *P&I* 2004-3.
116 Tweede WODC-rapport, p. 84-85.
117 Zie F. Kuitenbrouwer, 'Alarm over kosten WBP', *Computerrecht* 1999-4. Zie echter ten aanzien van de vergoeding van kosten ook artikel 39 en 40 Wbp. Besluit van 13 juni 2001 tot vaststelling van de vergoeding van de kosten als bedoeld in de artikelen 39 en 40 van de Wet bescherming persoonsgegevens (Besluit kostenvergoeding rechten betrokkene Wbp). CBP, 'Stichting Bureau Kredietregistratie', z2006-0052, juni 2008.

waarin wijzigingen van de Wbp zijn vervat in verband met de vermindering van administratieve lasten en nalevingskosten.[118] Uit de kabinetsplannen blijkt ook dat de regering de nalevingsproblemen wil verhelpen: 'Uit de eva-luatierapporten over de werking van de Wet bescherming persoonsgegevens (Wbp) blijkt een nalevingstekort. Het kabinet meent dat daarom de handhaving versterkt moet worden. Het kabinet zal de handhaving van de materiële normen van de Wbp door middel van het opleggen van bestuurlijke boetes wettelijk mogelijk maken.'[119]

Maar niet alleen bedrijven zijn debet aan de overschrijdingen van de wet, ook burgers dragen hieraan bij door het veelvuldig plaatsen van foto's, filmpjes en verhalen over anderen op sociale platformen op het internet. Tot slot heeft ook de overheid een negatieve invloed op de naleving van de Wbp. Eén van de belangrijkste fundamenten van de Wbp die in de praktijk onder druk komt te staan is de zogenoemde 'doelbinding'.[120] Artikel 9 bepaalt dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.[121] Doordat bedrijven de in databases opgeslagen persoonsgegevens gebruiken voor commerciële doeleinden en overheidsinstanties gebruikmaken van opgeslagen persoonsgegevens in het kader van strafrechtelijke opsporing en handhaving,[122] komt het principe van doelbinding in de praktijk steeds meer onder druk te staan. Dit fenomeen wordt doorgaans f*unction creep* genoemd.[123] Hieraan gelieerd zijn de problemen rond het aan elkaar koppelen van databases en het verzamelen van gegevens zonder direct vooropgezet doel of noodzaak. Het kabinet richt zich in zijn plannen met name tegen dit laatste probleem, door de nadruk te leggen op het principe van *select before you collect*. 'Nice to know' is daarbij geen afdoende reden, 'need to know' is een minimumvoorwaarde. Echter, dat strafrechtelijke opsporing en vervolging een uitzonderingsgrond op de doelbinding vormen, wordt expliciet benadrukt door de regering in de door haar opgestelde plannen.[124]

Daarnaast is er kritiek op de toezichtsfunctie van het CBP. Het CBP kan op verscheidene manieren zijn toezichtsfunctie uitoefenen, namelijk door een voorafgaand onderzoek in te stellen naar enkele specifieke typen verwerkingen (artikel 31 Wbp), door bemiddeling of advisering in geschillen (artikel 47 Wbp), door voorlichting te geven (artikel 51 Wbp) en door een ambtshalve of klachtonderzoek in te stellen (artikel 60 Wbp). De kritiek komt er voornamelijk op neer dat het CBP deze taak niet of nauwelijks uitvoert.[125] Ook geldt er kritiek op de relatief lange termijn van 24 weken met mogelijke verlenging die het CBP toekomt om de toestemming te geven voor gegevensverwerking.[126] Daarnaast wordt ook gemeend dat het CBP te weinig flexibel is in het goedkeuren van gedragscodes opgesteld om sectorspecifieke situaties te regelen.[127] Gutwirth & De Hert stellen tot slot: 'In Nederland treft ons dan de ogenschijnlijk drukke activiteit van het CBP rond controle door de werkgever van e-mails, maar de adviezen van het CBP worden door geen enkele arbeidsrechter gevolgd of gebruikt en in die adviezen wordt ten onrechte een onduidelijk antwoord gegeven op de essentiële vraag 'of een werkgever zonder enige individuele of collectieve kennisgeving e-mails mag controleren'.[128]

Tot slot is er kritiek op de handhavingsfunctie van het CBP. In hoofdstuk 10 staan de sancties genoemd die het CBP ten dienste staan: in paragraaf 1 is geregeld de bestuursdwang en in paragraaf 2 de bestuurlijke boeten die ten aanzien van overtredingen van formele vereisten kunnen worden opgelegd.[129] In paragraaf 3 staan de strafrechtelijke sancties vermeld. De bevoegdheden van het CBP werden destijds in het totstandkomingsproces van de Wbp al expliciet genoemd als één van de redenen om de Wbp aan een evaluatieonderzoek te onderwerpen.[130] De algemene consensus is dat deze bevoegdheden onvoldoende zijn. In 2006 gaf CBP-voorzitter Kohnstamm aan dat hij meer en ruimere bevoegdheden voor het CBP voorstond. Behalve ruimere bevoegdheden om boetes op te leggen aan organisaties die de wet overtreden, hoopte hij ook dat het CBP de bevoegdheid kreeg om wetten ter

118 *Kamerstukken II* 2008/09, 31 841.
119 *Kamerstukken II* 2009/10, 31 051/5, p. 2. Zie ook: C. Cuijpers, 'Kabinetstandpunt evaluatie Wbp – Boetebevoegdheid voor CBP op komst', *Computerrecht* 2010-1.
120 A. Holleman, 'Verantwoordelijkheid voor verenigbaar gebruik ex artikel 9 WBP', *P&I* 2004-4, p. 164-171. Rb. Amsterdam 12 februari 2004, *LJN* AO3649, nr. KG 04/65SR.
121 Daarbij speelt mee 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 de betrokkene, de wijze waarop de gegevens zijn verkregen en de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.
122 Zie bijvoorbeeld de discussie die speelde ten aanzien van het gebruik van gegevens die verzameld werden in het kader van de kilometerbeprijzing. *Kamerstukken II* 2009/10, 32 216. *Kamerstukken II* 2009/10, 31 051/5, p. 2.
123 J.Y. Dahl & A.R. Sætnan, '"It all happened so slowly". On controlling function creep in forensic DNA databases', *International Journal of Law, Crime and Justice*, 2009-37. G. Greenleaf, 'Function creep – Defined and still dangerous in Australia's revised ID Card Bill', *Computer law & security report* 2008-24. G. Greenleaf, '"Access all areas": Function creep guaranteed in Australia's ID Card Bill (No. 1)', *Computer law & security report* 2007-23. T. Thomas, 'The Sex Offender "Register": A Case Study in Function Creep', *The Howard Journal* 2008-47.
124 *Kamerstukken II* 2009/10, 31 051/5, p. 11-13. Rapport Gewoon Doen, p. 47.
125 Tweede WODC-rapport, p. 153.
126 Eerste WODC-rapport, p. 129.
127 Eerste WODC-rapport, p. 10-11.
128 P. de Hert & S. Gutwirth, 'Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek', in: E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn, 2004, p. 587-631.
129 F. Kuitenbrouwer, 'Amendementen WBP', *Computerrecht* 2000-2. Rb. 's-Hertogenbosch 18 januari 2005, nr. AWB 04/1196, *LJN* AT0462. Bestuurlijke boetes kunnen alleen ten aanzien van nieuwe verwerkingen worden opgelegd. ABRvS 21 september 2005, nr. 200504372/1, *LJN* AU2998. ABRvS 26 okober 2005, nr. 200502936/1, *LJN* AU4972.
130 *Kamerstukken II* 1998/99, 25 892/8, p. 31.

vernietiging voor te dragen bij de Hoge Raad of het Europees Hof van Justitie.[131] Daarnaast werd geopperd om alternatieve wijzen van handhaving toe te passen. Zo zou het publicatiebeleid kunnen worden uitgebreid en worden gebruikt voor een publieke schandpaal. Hierdoor zou handhaving kunnen geschieden door het principe van *naming and shaming*.[132]

Ook in de wetenschap wordt de handhaving van de Wbp als euvel beschouwd. Zo pleit Nouwt er in zijn artikel 'Tijd voor een nieuw punitief sluitstuk in de WBP?' voor om het misbruik van persoonsgegevens strafbaar te stellen, middels het strafrecht. Een uitgebreid punitief kader met bijbehorende sancties zouden wat hem betreft een oplossing kunnen bieden voor de handhavingsproblemen.[133] De regering onderkent de problemen ten aanzien van de toezichts- en handhavingsfunctie van het CBP. Zij wijt de problemen voornamelijk aan de vele taken van dit college, die naast toezicht en handhaving ook omvatten wetgevingsadvisering, voorlichting en advisering van betrokkenen. De oplossing ziet het kabinet in een verminderde nadruk op procedures en voorafgaande controle. Ook de adviesfunctie voor betrokkenen zal moeten worden ingeperkt. In de eerste plaats leidt volgens het kabinet een te intensieve uitoefening van de adviesfunctie tot potentiële conflicten met de handhavende rol, door de afbreuk aan de onbevooroordeeldheid. Daarnaast zijn er kosten mee gemoeid waardoor er minder financiële middelen overblijven om de handhavingstaak te vervullen. Door deze keuzes hoopt het kabinet een robuustere vorm van wetshandhaving te bewerkstelligen. Tot slot wordt de handhavingsfunctie ook versterkt door de uitbreiding van de boetebevoegdheden van het CBP.[134]

3 Conclusie

Er zijn in de loop der jaren tal van knel- en discussiepunten opgeworpen ten aanzien van de Wbp. Naar aanleiding van de evaluatie van deze wet heeft de regering onlangs haar plannen gepresenteerd om deze problemen te verhelpen.Ten aanzien van de open normen in de wet en haar omnibuskarakter brengt de regering geen wijzigingen aan. Zij ziet hiervoor geen reëel alternatief en hoopt dat jurisprudentie en sectorale gedragscodes zullen bijdragen aan de concretisering van de wettelijke bepalingen. In de klacht dat vele bepalingen achterhaald zijn door technologische ontwikkelingen ziet de regering geen acute aanleiding voor wijziging van de wet. In de praktijk doen zich ten aanzien hiervan volgens haar maar weinig problemen voor. Ook ten aanzien van de territoriale toepassing van de wet heeft het kabinet geen concrete plannen. Het verwijst slechts naar de Europese regelgever. Dit lijkt inderdaad voor de hand liggend, aangezien op dit punt overkoepelend Europees beleid wenselijk is. Tot slot heeft de regering geen plannen gepresenteerd ten aanzien van de toepassing van de in de wet vermelde excepties.

Ten aanzien van een groot aantal problemen zoekt het kabinet een niet-juridische oplossing. Zo zoekt het naar een oplossing voor de problemen rond het toestemmingsvereiste bij minderjarigen door in een publiekscampagne informatie hierover te verschaffen en wil het de uitoefening van de rechten van betrokkenen vergroten door meer nadruk te leggen op transparantie en bewustwording. Ook wil het kabinet het inzagerecht ondersteunen via een niet-wettelijk geregeld (facultatief) klachtrecht. De wet zou wel de totstandkoming van dat recht kunnen faciliteren, door middel van een erkenningsregeling, gecombineerd met een vrijstelling van verplichtingen. Ook ten aanzien van de problemen met betrekking tot zelfregulering kiest het kabinet voor een niet-juridische oplossing. Het kabinet geeft aan niet te ambiëren de samenleving het gebruik van gedragscodes of het aanstellen van FG's dwingend voor te schrijven. Het ziet meer in het door middel van wetgeving stimuleren van het gebruik van deze instrumenten.

Op een aantal terreinen kiest het kabinet wel voor een oplossing door middel van wetgeving. Zo zoekt het een oplossing voor de problemen die publiekrechtelijke organen ervaren met het verwerken van strafrechtelijke gegevens in een wijziging van de wet, evenals ten aanzien van vermindering van de administratieve lasten voor verantwoordelijken. Tot slot wil het kabinet de adviestaken van het CBP verminderen en staat het een wettelijke uitbreiding van de boetebevoegdheid van het college voor om zodoende een robuuster toezicht op de wet te bewerkstelligen.

De meer fundamentele knel- en discussiepunten met betrekking tot de open normen en het omnibuskarakter van de wet, de technologische bepaaldheid van de definities en de problemen ten aanzien van de reikwijdte en de excepties zullen op Europees niveau moeten worden besproken. Ook de evaluatie van de Privacyrichtlijn, waarvan de Wet bescherming persoonsgegevens een uitwerking is, loopt tegen haar einde. Naar verwachting wordt daarom binnen afzienbare tijd naast de onlangs herziene e-Privacyrichtlijn ook de Privacyrichtlijn gemoderniseerd. Het valt te hopen dat de Europese regelgever daarbij op een meer krachtdadige en doortastende wijze te werk gaat dan bij de herziening van de e-Privacyrichtlijn, waarbij hij regels heeft gesteld die op een aantal punten ronduit onduidelijk zijn en op andere punten reeds nu achterhaald lijken door technische ontwikkelingen.[135]

131 Eerste WODC-rapport, p. 84.
132 Eerste WODC-rapport, p. 86.
133 J. Nouwt, 'Tijd voor een nieuw punitief sluitstuk in de WBP?', *P&I* 2005-6.
134 *Kamerstukken II* 2009/10, 31 051/5, p. 24-27.
135 Zie daarover meer uitgebreid: B. van der Sloot & F.J. Zuiderveen Borgesius, *P&I* 2010-4.