



Universiteit
Leiden
The Netherlands

Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie : over de openbaarheid van persoonsgegevens

Kranenborg, H.R.

Citation

Kranenborg, H. R. (2007, September 20). *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie : over de openbaarheid van persoonsgegevens*. Kluwer, Deventer. Retrieved from <https://hdl.handle.net/1887/12352>

Version: Corrected Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/12352>

Note: To cite this publication please use the final published version (if applicable).

8 | De afstemming van openbaarheids- en gegevensbeschermingswetgeving in de EU-lidstaten

8.1 INLEIDING

De confrontatie tussen het recht op toegang tot documenten en het recht op bescherming van persoonsgegevens is geen exclusieve Europese aangelegenheid. Ook de lidstaten hebben hiermee te maken, uiteraard indien zij beide rechten in de nationale rechtsorde erkennen.

In dit hoofdstuk wordt weergegeven of en hoe de lidstaten de mogelijke botsing tussen toegang tot documenten en bescherming van persoonsgegevens op elkaar hebben afgestemd. Het doel van dit hoofdstuk is een indruk te krijgen in hoeveel lidstaten aan de afstemming van beide regimes bij wet bijzonder aandacht is besteed en op welke wijze dat is vormgegeven. Het overzicht blijft beperkt tot de relevante *wetgeving*, omdat het voor het onderhavige onderzoek te ver zou voeren om van alle wetten te achterhalen hoe zij in de praktijk worden toegepast. Dit heeft tot gevolg dat sommige conclusies niet de bestaande nationale rechtspraak zullen reflecteren. In het geval er Engels- of Nederlandstalige literatuur voor handen was waarin op basis van een gedegen jurisprudentie- of praktijkanalyse conclusies zijn getrokken, komt de praktische toepassing van nationale wetgeving overigens wel ter sprake. Bij de bespreking van de Nederlandse wetgeving zijn daarnaast een aantal rechterlijke uitspraken betrokken.

In dit hoofdstuk krijgt een uitspraak van de Britse *Court of Appeal* in de zaak *Durant t. Financial Services Authority* apart aandacht. Hoewel deze uitspraak niet de relatie van toegang tot documenten en bescherming van persoonsgegevens betreft, is zij wel van belang voor dit onderzoek. De Engelse rechters morrelen aan de gangbare definitie van het begrip ‘persoonsgegevens’ en beperken daarmee de reikwijdte van de bescherming van persoonsgegevens zodanig dat het in hoofdstuk 4 beschreven onderscheid tussen privacy en bescherming van persoonsgegevens lijkt te vervallen.¹ Daardoor vallen bepaalde situaties buiten de gegevensbescherming en daarmee buiten de overlap van beide rechtsregimes. De uitspraak wordt in dit hoofdstuk behandeld omdat de zaak zich vooralsnog alleen in de Britse context afspeelt.

Hieronder volgt in § 8.2 een korte uiteenzetting over de invloed van de EG op de relevante nationale wetgeving. Daarna worden in § 8.3 de bevindin-

1 Zie ook § 5.2.1.

gen ten aanzien van de nationale wetgeving weergegeven. In § 8.4 ga ik in op de *Durant*-zaak.

8.2 DE INVLOED VAN DE EG OP NATIONALE WETGEVING OVER TOEGANG TOT DOCUMENTEN EN BESCHERMING VAN PERSOONSgegevens

8.2.1 Toegang tot documenten

Het reguleren van toegang tot documenten op nationaal niveau behoort niet tot de bevoegdheid van de EG of de EU.² Het in hoofdstuk 2 besproken artikel 255 EG-Verdrag creëert alleen een competentie ten aanzien van toegang tot documenten in handen van het Europees Parlement, de Raad en de Commissie.³ Het staat de lidstaten vrij om wel of geen regels te stellen ten aanzien van toegang tot overheidsinformatie.

De enige invloed die uitgaat van de Eurowob is, zoals eerder aangegeven, dat in artikel 5 is bepaald dat als een lidstaat om toegang wordt gevraagd tot een document dat afkomstig is van een instelling, deze instelling geraadpleegd moet worden om zodoende tot een besluit te komen dat het doel van de Eurowob niet in gevaar brengt.⁴ Als sprake is van een document dat afkomstig is van één van de instellingen en als dat document persoonsgegevens bevat, kan het Europese wettelijke kader ten aanzien van het raakvlak van toegang tot documenten en bescherming van persoonsgegevens ook op nationaal niveau een rol spelen.

8.2.2 Bescherming van persoonsgegevens

8.2.2.1 Richtlijn 95/46 harmoniseert nationale gegevensbescherming

De invloed van de EG op nationale gegevensbeschermingswetgeving is groot. Met richtlijn 95/46 wordt immers beoogd nationale regels over gegevensbescherming te harmoniseren om zodoende belemmeringen van de interne markt te voorkomen. De rechtsgrondslag voor de richtlijn is dan ook artikel 95 EG-Verdrag dat de EG de bevoegdheid geeft om regels te stellen om de werking van de interne markt te bewerkstelligen.⁵ In zijn jurisprudentie heeft het HvJ de relatie met de interne markt ruim uitgelegd. Zowel in *Rundfunk* als in *Lindqvist* werd aangevoerd dat er sprake was van een activiteit die buiten het reguleren van de interne markt viel en dat daardoor de richtlijn niet van

2 Dit is alleen anders ten aanzien van toegang tot milieu-informatie, zie § 1.9.

3 Zie § 2.4.2.1.

4 Zie § 2.4.8.

5 Zie hierover § 3.2.2.

toepassing was of anders ongeldig.⁶ In *Rundfunk* zou sprake zijn van een situatie die het grensoverschrijdende werknemersverkeer niet belemmerde: het publiceren van het inkomen van personen die bij bepaalde instanties werken zou er voor personen uit andere lidstaten niet aan in de weg staan om bij die instanties te gaan werken. In *Lindqvist* zou het geen economische activiteiten betreffen: mevrouw Lindqvist plaatste gegevens van haar collega-vrijwilligers bij de lokale kerk op een website. In beide zaken overwoog het HvJ dat voor een beroep op artikel 95 als rechtsgrondslag niet vereist is dat in elke situatie die valt onder een op deze grondslag gebaseerde handeling een daadwerkelijk verband bestaat met het vrije verkeer tussen lidstaten.⁷ Zou de toepasselijkheid van richtlijn 95/46 afhankelijk zijn van de vraag of de concrete situatie wel verband houdt met de interne markt, dan zouden de grenzen van de werkingssfeer van de richtlijn volgens het HvJ bijzonder onzeker en vaag worden.⁸ Het HvJ concludeerde vervolgens dat de richtlijn op beide zaken van toepassing was.

Het HvJ acht een link met de interne markt bij het verwerken van persoonsgegevens snel aanwezig, maar ziet ook toe op de beperking van de reikwijdte van de richtlijn zoals die is neergelegd in artikel 3 lid 2 van de richtlijn. Daarin staat dat de richtlijn niet van toepassing is op de verwerking van persoonsgegevens die plaatsvindt in het kader van activiteiten die buiten de reikwijdte van het Gemeenschapsrecht vallen, zoals activiteiten die tot de tweede en derde pijler van de Unie behoren. Dat hiermee daadwerkelijk een grens is getrokken, blijkt uit de uitspraak van het HvJ in de zogenaamde 'PNR-zaken'.⁹ In deze twee politiek gevoelige zaken uitte het Europees Parlement zijn onvrede over een overeenkomst van de EG met de VS op basis waarvan het Europese vliegmaatschappijen werd mogelijk gemaakt aan de Amerikaanse verplichting te voldoen om bepaalde passagiersgegevens aan Amerikaanse douaneautoriteiten te overhandigen of beschikbaar te stellen. De Amerikaanse maatregel was genomen na de aanslagen van 11 september 2001 als onderdeel van de strijd tegen terrorisme.¹⁰ Op basis van artikel 25 van richtlijn 95/46 had de Commissie een beslissing genomen over het gegevensbeschermingsniveau in de VS, waarna de Raad op basis van artikel 95 (in combinatie met artikel 300 EG-

6 Zie HvJ EG 20 mei 2003, *Österreichischer Rundfunk*, C-465/00, C-138/01 en C-139/01, *Jur.* 2003, p. I-4989, r.o. 36 en HvJ EG 6 november 2003, *Lindqvist*, C-101/01, *Jur.* 2003, p. I-12971, r.o. 30.

7 HvJ, *Rundfunk*, r.o. 41 en *Lindqvist*, r.o. 40.

8 HvJ, *Rundfunk*, r.o. 42 en *Lindqvist*, r.o. 41.

9 HvJ EG 30 mei 2006, *Parlement t. Raad en Commissie*, C-317/04 en C-318/04, *Jur.* 2006, p. I-4721. Zie over deze zaken uitgebreid H.R. Kranenborg, annotatie in *EHRC* 2006, p. 751-766 en M. Mendez, 'European Court of Justice: Passenger Name Record Agreement', *ECLRev.* 2007, p. 127-147.

10 Zie hierover uitgebreid H.R. Kranenborg, 'Een dilemma voor Europese vliegmaatschappijen: inbreuk maken op Amerikaans recht of inbreuk maken op Europees recht?', *NTER* 2003, p. 162-166 en E. Brouwer, 'Verstreking van passagiersgegevens ten behoeve van de grensbewaking: wie bewaakt de grenzen van de rechtsstraat?', *NJB* 2003, p. 1548-1553.

Verdrag) de overeenkomst sloot.¹¹ Het HvJ vernietigde zowel de Commissiebeslissing als het Raadsbesluit omdat het doel van de doorgifte terrorismebestrijding was en niet de bewerkstelling van de werking van de interne markt.¹²

Het HvJ houdt dus (terecht) vast aan de begrensde reikwijdte van richtlijn 95/46. De grens tussen verwerking in het kader van de eerste pijler en de tweede of derde pijler is alleen niet altijd even makkelijk te trekken. Dat blijkt al uit de PNR-zaken zelf. Het vergaren en opslaan van passagiersgegevens door vliegmaatschappijen viel binnen de reikwijdte van richtlijn 95/46, het doorgeven van diezelfde gegevens aan de VS viel erbuiten.

Mede door de ruime manier waarop het HvJ richtlijn 95/46 in de uitspraken in *Rundfunk* en *Lindqvist* toepast, wordt het nationale gegevensbeschermingsrecht voor een belangrijk deel bepaald door richtlijn 95/46. Alleen voor het verwerken van gegevens voor situaties die binnen de EU als tweede en derde pijler aangelegenheden worden beschouwd, is ruimte voor de lidstaten om het gegevensbeschermingsrecht anders in te richten dan richtlijn 95/46 voorschrijft.¹³ Overigens merkt het HvJ in *Lindqvist* op dat niets eraan in de weg staat om de draagwijdte van de nationale wettelijke regeling tot omzetting van de bepalingen van richtlijn 95/46 uit te breiden tot niet onder de werkingssfeer daarvan vallende gebieden.¹⁴ Uiteraard zijn de lidstaten ongeacht het beleidsterrein bij de verwerking van persoonsgegevens hoe dan ook gebonden aan de vereisten die voortvloeien uit artikel 8 EVRM en het Verdrag van Straatsburg.¹⁵

8.2.2.2 *Laat richtlijn 95/46 ruimte voor het openbaren van persoonsgegevens om redenen van transparantie?*

Net als in verordening 45/2001 is in richtlijn 95/46 over het openbaren van persoonsgegevens om transparantieredenen niets te vinden.¹⁶ Een verschil tussen beide regelingen is echter dat verordening 45/2001 direct de gegevensbeschermingsregels vaststelt voor de Europese instellingen, terwijl richtlijn 95/46 eerst nog een implementatie in nationaal recht vereist. Hieronder wordt besproken of de richtlijn de lidstaten ruimte laat om bij de implementatie ervan te voorzien in het openbaren van persoonsgegevens om redenen van transparantie.

In *Lindqvist* heeft het HvJ zich in het algemeen uitgesproken over de handelingsruimte die de lidstaten onder richtlijn 95/46 wordt gelaten. Op de

11 Zie over deze procedure § 3.4.2.1.

12 HvJ, *Parlement t. Raad en Commissie*, r.o. 55 en r.o. 68.

13 Tenzij er specifieke EU regelgeving bestaat.

14 HvJ, *Lindqvist*, r.o. 98.

15 Zie § 3.3.1.

16 Zie § 7.1 en § 7.3.

vraag van de Zweedse *Göta Hovrätt* of lidstaten een verdergaande bescherming van persoonsgegevens mogen bieden, met andere woorden, of de richtlijn een vorm van minimumharmonisatie betreft, antwoordde het HvJ dat dat niet het geval is.¹⁷ De richtlijn leidt tot een volledige harmonisatie van de nationale wetgeving. Het is immers juist het doel van de richtlijn om de verschillen tussen nationale gegevensbescherming die leiden tot een belemmering van de interne markt op te heffen.¹⁸ Het HvJ voegde eraan toe dat de richtlijn op bepaalde gebieden de lidstaten wel een zekere ruimte om te manoeuvreren toekent.¹⁹ Diezelfde ruimte maakt, aldus het HvJ in antwoord op een andere vraag van de Zweedse rechter, dat de richtlijn zélf niet in strijd is met het recht op vrijheid van meningsuiting uit artikel 10 EVRM.²⁰ Het is veeleer in het stadium van de concrete toepassing op nationaal niveau dat een juist evenwicht tussen de betrokken rechten en belangen moet worden gevonden.²¹ Grondrechten hebben daarbij een bijzonder belang:

Bijgevolg moeten de autoriteiten en de rechterlijke instanties van de lidstaten niet alleen hun nationaal recht conform richtlijn 95/46 uitleggen, maar moeten zij er ook op toezien dat zij zich niet baseren op een uitlegging daarvan die in conflict zou komen met de door de communautaire rechtsorde beschermde grondrechten of met de andere algemene beginselen van gemeenschapsrecht, zoals het evenredigheidsbeginsel.²²

In hoofdstuk 6 voerde ik aan dat het recht op toegang tot documenten beschouwd kan worden als een algemeen beginsel van Gemeenschapsrecht.²³ Dit recht, en de uitwerking daarvan, is echter alleen inroepbaar tegenover de Europese instellingen. Het recht op toegang tot documenten kent niet, zoals bij de vrijheid van meningsuiting, een nationaal equivalent dat volgt uit een ander bindend Europees- of internationaalrechtelijk instrument. Hoewel de instellingen, zoals aangegeven in hoofdstuk 7, bij de toepassing van verordening 45/2001 het recht op toegang tot documenten in acht moeten nemen, is dat niet per se het geval op nationaal niveau.²⁴ Gelet op de status van het recht op toegang tot documenten op het Europese niveau is het wel voorstelbaar dat de lidstaten, als zij een recht op toegang tot documenten erkennen, bij de toepassing van de nationale gegevensbeschermingswetgeving conflicten met het *nationale* recht op toegang tot documenten moeten en ook mogen voorkomen. In beginsel is er dan ook niets op tegen om in de nationale ge-

17 HvJ, *Lindqvist*, r.o. 96.

18 HvJ, *Lindqvist*, r.o. 95.

19 HvJ, *Lindqvist*, r.o. 97.

20 HvJ, *Lindqvist*, r.o. 90.

21 HvJ, *Lindqvist*, r.o. 85.

22 HvJ, *Lindqvist*, r.o. 87. Deze overweging kwam eerder ook ter sprake in § 7.3.4.

23 Zie § 6.3.1.

24 Zie § 7.3.4.

vensbeschermingswetgeving, anders dan in richtlijn 95/46, in algemene bevoordingen wél expliciet iets over de verhouding tot toegang tot documenten te bepalen.

Net als bij verordening 45/2001 kan bekeken worden welke bepalingen in richtlijn 95/46 de mogelijkheid bieden om toegang tot documenten te verlenen om transparantieredenen. Verordening 45/2001 zet de bepalingen van richtlijn 95/46 om, waardoor er veel overeenkomsten zijn met de analyse uit het vorige hoofdstuk. Daarom wordt volstaan met een aantal korte opmerkingen.

De toegangsverlening zou in de eerste plaats mogelijk kunnen zijn als er een wettelijke plicht aan ten grondslag ligt (artikel 7 sub c richtlijn 95/46). Deze zou in de nationale openbaarheidswetgeving gevonden kunnen worden. Deze wetgeving moet dan wel voldoende duidelijk zijn. Zoals aangegeven, voldoet de Eurovob daar momenteel niet aan.²⁵ In hoofdstuk 7 werd besproken dat het openbaren van gegevens op basis van een verzoek om toegang tot documenten (als secundaire vorm van verwerken met een nieuwe doelstelling) op gespannen voet kan staan met het doelbindingsbeginsel. Alleen als het openbaar maken een met het oorspronkelijke doel verenigbaar wijze van verwerken vormt, is openbaarmaking in overeenstemming met het beginsel.²⁶ Het doelbindingsbeginsel is in richtlijn 95/46 in dezelfde bevoordingen neergelegd als in verordening 45/2001. Bij de analyse van nationale wetgeving hieronder zal bekeken worden of aan de relatie tussen dit beginsel en het openbaren van gegevens als gevolg van de uitoefening van het recht op toegang tot documenten bijzonder aandacht is besteed. In tegenstelling tot verordening 45/2001 kent richtlijn 95/46 géén apart regime voor het openbaren van persoonsgegevens aan derden. Verwerking is mogelijk als dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de derde aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene niet prevaleren (artikel 7 sub f richtlijn 95/46). Anders dan artikel 8 van verordening 45/2001 staat dit artikel niet in de weg aan het openbaren van persoonsgegevens aan derden om redenen van transparantie.²⁷

Over het openbaren van persoonsgegevens om transparantieredenen is, zoals gezegd, niets bepaald in de richtlijn. Dit is wél het geval ten aanzien van de vrijheid van meningsuiting. In artikel 9 wordt de lidstaten de mogelijkheid gegeven om uitzonderingen op de bepalingen van richtlijn 95/46 te maken als de verwerking voor uitsluitend journalistieke of voor artistieke of literaire doeleinden is. Het recht op eerbiediging van de persoonlijke levenssfeer kan zodoende verzoend worden met de regels over de vrijheid van meningsuiting.

25 Zie § 7.3.2.

26 Zie § 7.3.3.

27 Zie de analyse in § 7.3.1.

8.3 DE AFSTEMMING VAN OPENBAARHEIDS- EN GEGEVENSBECHERMINGSWETGEVING IN DE EU-LIDSTATEN

8.3.1 Inleiding

In deze paragraaf wordt een overzicht gegeven van de afstemming van openbaarheids- en gegevensbeschermingswetgeving op nationaal niveau.²⁸ De 27 lidstaten van de EU hebben ter implementatie van richtlijn 95/46 allemaal een wet die de rechtmatige gegevensverwerking regelt. In afwezigheid van harmoniserende EG-regelgeving of andere (bindende) Europese of internationale rechtsinstrumenten is niet in alle lidstaten een wet te vinden waarin toegang tot overheidsinformatie is gereguleerd.²⁹ Een dergelijke wet ontbreekt in de drie kleinste lidstaten: Cyprus, Luxemburg en Malta. Ook in de gegevensbeschermingswetgeving van deze drie landen is niets over toegang tot persoonsgegevens om redenen van transparantie terug te vinden.³⁰ De wetgeving van Cyprus, Luxemburg en Malta blijft hieronder dan ook verder onbesproken.

Voordat de bevindingen worden weergegeven moet een opmerking over de status van beide rechten op nationaal niveau worden gemaakt. Zoals aangegeven in hoofdstuk 6 hebben zestien van de 26 lidstaten met een constitutie een constitutionele bepaling over toegang tot documenten.³¹ Twaalf van deze zestien landen kennen de burger een recht op toegang tot documenten toe, de overige vier leggen de overheid de verplichting op om informatie toegankelijk te maken.³² Door de toepasselijkheid van artikel 8 EVRM is de status van het recht op bescherming van persoonsgegevens, althans voorzover het binnen de privacyreikwijdte valt, in alle lidstaten de hoogste en nagenoeg gelijk. Omdat niet in alle landen aan het recht op toegang tot documenten (minstens) een constitutionele waarde wordt toegekend, is de gelijkwaardigheid tussen dit recht en het recht op bescherming van persoonsgegevens niet altijd een gegeven. De gelijkwaardigheid of ongelijkwaardigheid van de rechten

28 In de voetnoten wordt, m.u.v. van oorsprong Duits-, Frans- en Nederlandstalige titels, de Engelse vertaling van de oorspronkelijke titel van de betreffende wetgeving weergegeven. Een overzicht van de vindplaatsen van de genoemde wetten is in de besluitenlijst bij dit onderzoek opgenomen.

29 Zie voor een uitgebreid overzicht en beschrijving van de nationale en Europese openbaarheidswetgeving van vóór de uitbreiding van de EU met Bulgarije en Roemenië H.R. Kranenborg & W.J.M. Voermans, *Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation*, Groningen 2005, Europa Law Publishing.

30 Zie voor Cyprus: Law 138 (I) 2001 on The Processing of Personal Data (Protection of Individuals) van 2 mei 2003, voor Luxemburg: Loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel van 2 augustus 2002 en voor Malta: Data protection Act XXVI van 14 december 2001.

31 Zie § 6.3.1.2.

32 De twaalf landen met een constitutioneel recht op toegang tot documenten zijn: België, Bulgarije, Estland, Finland, Griekenland, Hongarije, Nederland, Polen, Portugal, Roemenië, Slovenië en Zweden. De vier landen die een constitutionele plicht kennen, zijn: Oostenrijk, Slowakije, Spanje en Tsjechië. Zie hierover uitgebreid Kranenborg & Voermans 2005.

vormt de achtergrond van de regulering van het raakvlak. Zoals betoogd in hoofdstuk 6 is de wetgever bij gelijkwaardigheid van beide (fundamentele) rechten aan bepaalde grenzen gebonden. Bij ongelijkwaardigheid hoeft daarvan geen sprake te zijn. Het kennen van de precieze verhouding tussen beide rechten is vooral van belang voor een oordeel over de wijze waarop beide regimes op elkaar zijn afgestemd, zoals in het vorige hoofdstuk ten aanzien van de Europese situatie is gebeurd. Het is echter niet de bedoeling om hieronder per land een normatief oordeel te vellen over de nationale regulering van het raakvlak. De status van en de verhouding tussen het recht op toegang tot documenten en het recht bescherming van persoonsgegevens blijven daarom in beginsel onbesproken.

8.3.2 Een overzicht van de afstemming van openbaarheids- en gegevensbeschermingswetgeving in de EU-lidstaten

– In *België* wordt toegang tot een bestuursdocument geweigerd als de openbaarmaking ervan afbreuk doet ‘aan de persoonlijke levenssfeer’, tenzij de betrokken persoon met de inzage heeft ingestemd.³³ De uitzondering kan als een absolute uitzonderingsgrond worden aangemerkt: stelt het overheidsorgaan vast dat openbaarmaking van een document afbreuk doet aan de persoonlijke levenssfeer dan weigert dit de toegang tot het document.³⁴

Volgens verschillende auteurs blijkt uit de praktijk dat de precieze invulling van het begrip ‘persoonlijke levenssfeer’ een knelpunt vormt.³⁵ De verwijzing is erg algemeen en geeft geen concrete of onbetwistbare omschrijving.³⁶ Volgens Voorhoof zijn de openbaarheidswetgeving en de gegevensbeschermingswetgeving onvoldoende op elkaar afgestemd.³⁷ De Hert geeft aan dat het onduidelijk is hoe het begrip ‘persoonlijke levenssfeer’ zich verhoudt tot het begrip ‘persoonsgegevens’ uit de gegevensbeschermingswetgeving.³⁸ Het is volgens De Hert niet mogelijk een eenduidig antwoord te geven op de vraag

33 Artikel 6 § 2 sub 1 Wet betreffende de openbaarheid van bestuur van 11 april 1994. Bij de bestudering van de Belgische wetgeving is alleen federale wetgeving in acht genomen.

34 Zie hierover P. de Hert, ‘De grondrechten en wetten m.b.t. openbaarheid van bestuursdocumenten en bescherming van persoonlijke levenssfeer. Analyse van de onderlinge relatie en commentaar bij het arrest Dewinter van de Raad van State’, *CDPK* 2001, p. 374-481, op p. 396 en F. Schram, *Tussen Openbaarheid en Privacy. Een verhaal in grijstinten*, Brussel 2006, Uitgeverij Politeia, § 3.2.4.

35 De Hert 2001, p. 399; D. Voorhoof, ‘Tien jaar openbaarheid van bestuur in België: het mag wel iets meer zijn’, in A.W. Hins & A.J. Nieuwenhuis, *Van ontvanger naar zender*, Amsterdam 2003, Otto Cramwinkel Uitgever, p. 389-406, op p. 401 en Schram 2006, p. 145.

36 De Hert 2001, p. 399, voetnoot 152. De Hert citeert J. Goorden, ‘De relatie openbaarheid-vertrouwelijkheid van gegevens’, in een congresbundel uit 1998, *Privacy*, Brussel, p. 228. Zie ook Schram 2006, p. 145.

37 Voorhoof 2003, p. 401.

38 De Hert 2001, p. 423.

wanneer de gegevensbeschermingswetgeving in openbaarheidkwesties ingeroepen kan worden.³⁹ In de praktijk blijken overheidsinstanties zich terughoudend op te stellen ten aanzien van openbaarmaking of slechts voorzichtig tot openbaarmaking over te gaan.⁴⁰

Opvallend is dat de Belgische wetgeving als speciale categorie bestuursdocumenten documenten 'van persoonlijke aard' kent.⁴¹ Dit zijn documenten die een beoordeling of een waardeoordeel bevatten van een met naam genoemd of gemakkelijk identificeerbaar natuurlijk persoon of de beschrijving van een gedrag waarvan het ruchtbaar maken aan die persoon kennelijk nadeel kan berokkenen. Toegang tot deze documenten is alleen mogelijk als de verzoeker een bijzonder belang heeft.⁴²

In de Belgische gegevensbeschermingswetgeving is (uiteraard) ook het doelbindingsbeginsel terug te vinden.⁴³ In afwijking van de formulering van dit beginsel in richtlijn 95/46, is nader bepaald hoe beoordeeld moet worden of verwerking als 'niet onverenigbaar' met de oorspronkelijke doeleinden moet worden beschouwd. Om te bepalen of daarvan sprake is moet rekening worden gehouden met de redelijke verwachtingen van de betrokkene en de toepasselijke wettelijke en reglementaire bepalingen.

– De *Bulgaarse* openbaarheidswet is vrij ondoorgrondelijk.⁴⁴ Het is niet eenvoudig om er uit af te leiden hoe met het openbaren van persoonsgegevens moet worden omgegaan. In de openbaarheidswet wordt een aantal algemene beginselen opgesomd waarmee het recht op toegang tot publieke informatie is omgeven.⁴⁵ Eén daarvan is de bescherming van persoonsgegevens.⁴⁶ Wat dit betekent wordt niet verder uitgewerkt. Specifieke gronden voor weigering van een verzoek om toegang tot publieke informatie zijn niet in de openbaarheidswet opgenomen. Alleen zeer algemeen is bepaald dat het recht op toegang tot publieke informatie geweigerd wordt als het gaat om informatie die geclas-

39 De Hert 2001, p. 423.

40 De Hert 2001, p. 399 en Schram 2006, p. 145-146.

41 Artikel 1 sub 3 Wet betreffende de openbaarheid van bestuur.

42 Artikel 4 Wet betreffende de openbaarheid van bestuur. De gegevensbescherming in België is geregeld in de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens van 8 december 1992.

43 Artikel 4 lid 1 sub 2 Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

44 Zie voor een kritische analyse van de wet het jaarrapport uit 2003 over toegang tot informatie in Bulgarije dat is opgesteld in het kader van het *Access to Information Programma* dat in 1996 werd gestart en dat wordt gefinancierd door het Nederlandse ministerie van Buitenlandse Zaken, zie http://www.aip-bg.org/L_reports.htm.

45 Artikel 6 Access to Public Information Act van 22 juni 2000.

46 Artikel 6 lid 5 Access to Public Information Act.

sificeerd is omdat het een staatsgeheim is of een ander beschermd geheim.⁴⁷ Over persoonsgegevens of privacybescherming wordt verder niet gesproken.

In artikel 31 zijn regels vastgelegd voor het openbaren van informatie waarvoor toestemming van een derde partij nodig is. Als deze toestemming niet wordt verkregen, kan de informatie niet worden geopenbaard.⁴⁸ Dit vereiste van toestemming zou voor het openbaren van persoonsgegevens kunnen volgen uit de Bulgaarse gegevensbeschermingswetgeving.⁴⁹

In de Bulgaarse gegevensbeschermingswetgeving is een apart artikel gewijd aan het doorgeven van gegevens aan een derde. Dit is toegestaan als de gegevens uit een publiek register afkomstig zijn of als het om publieke informatie gaat die op grond van een wettelijke procedure toegankelijk is.⁵⁰ Hiermee wordt bedoeld op de openbaarheidswetgeving. Uit deze wetgeving valt echter lastig af te leiden wanneer persoonsgegevens als publieke informatie aangemerkt kunnen worden.

In de Bulgaarse gegevensbeschermingswetgeving wordt een afwijkende definitie van het begrip 'persoonsgegevens' gehanteerd. Vóór een amendement uit 2005 viel ook informatie over iemands 'public identity' onder het begrip.⁵¹ Op die grond werd toegang tot informatie over publieke activiteiten van publieke personen geweigerd. Met het amendement werd 'public identity' veranderd in 'social identity'.⁵² Het begrip 'persoonsgegevens' is vervolgens beperkter uitgelegd, waardoor informatie over publieke activiteiten van publieke personen voortaan buiten de reikwijdte van de gegevensbescherming valt.⁵³ In een evaluatierapport over de toepassing van zowel de openbaarheidswetgeving en de gegevensbeschermingswetgeving in Bulgarije wordt geconcludeerd dat door het amendement de mogelijkheid wordt gecreëerd voor

[...] a precise balance between personal data protection and the right of access to information, providing for accountability, transparency and public trust of public authorities and their administrations.⁵⁴

Kennelijk levert de aanpassing van het begrip 'persoonsgegevens' voldoende ruimte voor de praktijk om beide regimes op elkaar af te stemmen. Uit de wetgeving zelf blijkt verder overigens niet hoe moet worden omgegaan met een verzoek om openbaarmaking van informatie die wél onder het begrip

47 Artikel 7 Access to Public Information Act. Zie hierover ook het eerdergenoemde jaarrapport uit 2003 dat is opgesteld in het kader van het *Access to Information Programma*.

48 Artikel 31 lid 4 Access to Public Information Act.

49 Personal Data Protection Act van 1 januari 2002.

50 Artikel 35 lid 1 sub 2 Personal Data Protection Act.

51 Zie hierover het jaarrapport uit 2005 over toegang tot informatie in Bulgarije dat is opgesteld in het kader van het eerdergenoemde *Access to Information Programma*, te vinden op http://www.aip-bg.org/l_reports.htm, p. 16/17.

52 Artikel 2 lid 1 Data Protection Act.

53 Zie het jaarrapport uit 2005 over toegang tot informatie in Bulgarije, p. 16-17.

54 Zie het jaarrapport uit 2005 over toegang tot informatie in Bulgarije, p. 17.

‘persoonsgegevens’ valt. Op het beperken van de reikwijdte van de bescherming van persoonsgegevens kom ik in § 8.4 uitgebreid terug.

- In de *Deense* wetgeving wordt informatie ‘on the private circumstances of individual persons including their finances’ buiten de reikwijdte van het recht op toegang tot overheidsinformatie geplaatst.⁵⁵ Daarnaast kan het recht op toegang beperkt worden als dit essentieel is voor de bescherming van ‘private [...] interests where secrecy is required because of the special nature of the matter’.⁵⁶ In de Deense gegevensbeschermingswetgeving wordt niet gerept over openbaarheid van bestuur. Er wordt wel expliciet verwezen naar de openbaarheidswetgeving in het artikel dat het recht op inzage in de eigen gegevens van het data subject regelt.⁵⁷ Bepaalde uitzonderingen op het algemene recht op toegang tot documenten wordt op deze inzage van toepassing verklaard.
- In *Duitsland* is sinds 1 januari 2006 een federale wet van kracht over toegang tot overheidsinformatie.⁵⁸ In deze wet is bepaald dat informatie die op vertrouwelijke basis aan de overheidsinstanties is verstrekt niet toegankelijk mag worden gemaakt.⁵⁹ De afstemming met de regels over bescherming van persoonsgegevens is duidelijk aangepakt:

(1) Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 des Bundesdatenschutzgesetzes dürfen nur übermittelt werden, wenn der Dritte ausdrücklich eingewilligt hat.

(2) Das Informationsinteresse des Antragstellers überwiegt nicht bei Informationen aus Unterlagen, soweit sie mit dem Dienst- oder Amtsverhältnis oder einem Mandat des Dritten in Zusammenhang stehen und bei Informationen, die einem Berufs- oder Amtsgeheimnis unterliegen.

(3) Das Informationsinteresse des Antragstellers überwiegt das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs in der Regel dann, wenn sich die Angabe auf Name, Titel, akademischen Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und – telekommunikationsnummer beschränkt und der Dritte als Gutachter, Sachverständiger oder in vergleichbare Weise eine Stellungnahme in einem Verfahren abgegeben hat.

55 Artikel 12 lid 1 sub 1 Act 572/1985 on Access to Public Administration Files van 19 december 1985.

56 Artikel 13 lid 1 sub 6 Act 572/1985.

57 Zie artikel 32 Act 429/2000 on Processing of Personal Data van 31 mei 2000.

58 Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz) van 5 september 2005.

59 Artikel 3 lid 7 Informationsfreiheitsgesetz.

(4) Name, Titel, akademische Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und – telekommunikationsnummer von Bearbeitern sind vom Informationszugang nicht ausgeschlossen, soweit sie Ausdruck und Folge der amtlichen Tätigkeit sind und kein Ausnahmetatbestand erfüllt ist.⁶⁰

Uit deze bepaling blijkt dat de Duitse wetgever als uitgangspunt neemt dat de achterliggende belangen tegen elkaar afgewogen moeten worden. Voor gevoelige gegevens is bepaald (dit is de verwijzing naar artikel 3 lid 9 van de Duitse *Bundesdatenschutzgesetz*) dat altijd toestemming van de betrokkene is vereist.⁶¹

In beginsel laat de wetgever de afweging van de achterliggende belangen over aan de uitvoerende instantie. Maar in de leden 2 tot en met 4 is voor bepaalde situaties de uitkomst al gegeven. De wetgever benoemt een aantal gegevens expliciet: de naam, titel, academische graad, beroeps- en functieaanduiding, werkadres en (werk)telefoonnummers. Het belang achter openbaarmaking weegt ten aanzien van deze gegevens zwaarder dan het belang van de betrokken als zij een ambtenaar in de uitoefening van zijn functies betreffen, of een private persoon die in een bepaalde procedure zijn mening heeft gegeven of optrad als expert.

De Federale *Informationsfreiheitsgesetz* wordt vermoedelijk gezien als een wettelijke plicht op basis waarvan gegevensverwerking mag plaatsvinden zonder toestemming van de betrokkene.⁶²

– In de *Estse* openbaarheidswetgeving is één van de uitgangspunten dat het verlenen van toegang tot informatie niet tot een schending van het privé-leven van personen mag leiden.⁶³ Bij de regulering van welke informatie als ‘restricted information’ mag of moet worden aangemerkt, is bepaald dat informatie die privé- of gevoelige persoonsgegevens bevatten als *restricted* moet worden aangemerkt.⁶⁴ Deze bepaling is opgenomen na aanneming van de huidige Estse gegevensbeschermingswetgeving. Daarin wordt namelijk naast de gebruikelijke groep gevoelige persoonsgegevens een groep privé persoonsgegevens onderscheiden. Dit zijn, onder andere, gegevens die details van het privé-leven onthullen, informatie over verzoeken voor sociale bijstand en gegevens met betrekking tot belastingen.⁶⁵ In de Estse openbaarheidswetgeving is verder bepaald dat informatie die persoonsgegevens bevat als *restricted information* mag worden aangemerkt als openbaarmaking het privé-leven van de betrokkene op *significante* wijze schendt.⁶⁶

60 Artikel 5 Informationsfreiheitsgesetz.

61 Bundesdatenschutzgesetz van 20 december 1990.

62 Zie artikel 4 lid 1 Bundesdatenschutzgesetz.

63 Artikel 4 lid 3 Public Information Act van 15 november 2000.

64 Artikel 35 lid 1 sub 10 Public Information Act.

65 Artikel 4 lid 2 Personal Data Protection Act van 12 februari 2003.

66 Artikel 35 lid 1 sub 11 Public Information Act.

In de openbaarheidswetgeving is ook vastgelegd wat *niet* als *restricted information* mag worden aangemerkt, namelijk 'information which damages the reputation of a state or local government official [...] or a natural person, except sensitive or private personal data'.⁶⁷

Tot zover is de Estse openbaarheidswetgeving vrij goed te volgen, hoewel het natuurlijk de vraag is wat onder een significante schending van het privéleven wordt verstaan. De situatie wordt ingewikkelder omdat naast deze bepalingen een apart artikel is gewijd aan toegang tot documenten die persoonsgegevens bevatten.⁶⁸ Toegang tot deze informatie wordt verleend als de gegevensbeschermingswetgeving daarvoor een grondslag biedt. Een analyse van deze gegevensbeschermingswetgeving leert dat het openbaren aan derden van persoonsgegevens die rechtmatig zijn verzameld mogelijk is als toegang tot deze informatie niet *restricted* is.⁶⁹ Vermoedelijk is dat een terugverwijzing naar de openbaarheidswetgeving.

– De *Finse* openbaarheidswetgeving kent geen generieke uitzondering op het recht op toegang tot documenten met betrekking tot privacy of bescherming van persoonsgegevens. Wel is er een uitgebreide lijst van informatie opgenomen die als geheime officiële documenten beschouwd moeten worden.⁷⁰ Bij verschillende categorieën informatie bepaalt de Finse wetgever expliciet wanneer de informatie toch niet als geheim mag worden aangemerkt.

Voor de bescherming van persoonsgegevens zijn verschillende categorieën relevant.⁷¹ Zo blijft een document dat gegevens bevat over het jaarinkomen van een persoon geheim, alsook een document dat informatie over het inkomen en de bezittingen bevat waarop een subsidie is toegekend.⁷² Documenten over vluchtelingen en asielzoekers blijven geheim, tenzij toegangsverlening geen gevaar voor de betrokken persoon met zich meebrengt.⁷³ Gevoelige informatie blijft geheim, tenzij het openbaren van de gegevens noodzakelijk is voor de uitoefening van een publieke taak.⁷⁴ Interessant is het artikellid waarin de volgende documenten als geheim worden bestempeld:

documents containing information on the political convictions or the privately expressed views of a person, or information on a person's lifestyle, participation in voluntary associations, interests, family life or other comparable personal circumstances of the person; however, documents containing information on the activity

67 Artikel 36 lid 1 sub 6 Public Information Act. Vergelijk de eerder beschreven Belgische wetgeving.

68 Artikel 39 Public Information Act.

69 Artikel 14 lid 2 sub 3 Personal Data Protection Act.

70 Zie artikel 24 Act 621/99 van 21 mei 1999 on the Openness of Government Activities.

71 Zie van artikel 24 Act 621/99 de leden 23 tot en met 32.

72 Artikel 24 lid 23 Act 621/99.

73 Artikel 24 lid 24 Act 621/99.

74 Artikel 24 lid 26 Act 621/99.

of a person in political or other elected office, or his/her seeking such office, as well as the participation of a person in the establishment or registration of a political party, or the establishment of an electoral association are in the public domain.⁷⁵

Juist op dit artikellid en het lid waarin het jaarinkomen als geheim wordt aangemerkt, is in de wet een uitzonderingsmogelijkheid opgenomen. Toegang mag toch worden verleend als dit noodzakelijk is 'for the realisation of a private person's or some other authority's statutory duty of information'.⁷⁶ Dit zal een plicht zijn die volgt uit specifieke wetgeving.

De Finse gegevensbeschermingswetgeving is op de openbaarheidswetgeving afgestemd: '[t]he provisions on access to official documents apply to access to information in the personal data files of the authorities and to other disclosure of data therein'.⁷⁷

– In de Franse openbaarheidswetgeving is neergelegd dat bepaalde informatie *alleen* aan de betrokken persoon zelf overhandigd mag worden. Het betreft informatie 'dont la communication porterait atteinte au secret de la vie privée et des dossiers personnels, au secret médical' en ook informatie waarin waardeoordelen over de betrokkene zijn opgenomen of waarin zijn gedrag is beschreven.⁷⁸ In de wet over gegevensbescherming is bepaald dat deze geen afbreuk doet aan de toepasselijkheid van de regels uit de openbaarheidswetgeving.⁷⁹

– Hongarije is de enige lidstaat waarin de algemene regels over toegang tot documenten en bescherming van persoonsgegevens in één wet zijn neergelegd.⁸⁰ In deze wet wordt een onderscheid gemaakt tussen 'personal data', 'data of public interest' en 'data public on grounds of public interest'. In de oorspronkelijke tekst van de wet bestonden alleen de eerste twee categorieën. *Personal data* is wat ook in richtlijn 95/46 onder persoonsgegevens wordt verstaan en *data of public interest* zijn gegevens die niet als persoonsgegevens zijn aan te merken. Voor de eerste categorie gegevens werden regels voor de rechtmatige verwerking gesteld (hoofdstuk II), voor de tweede categorie regels voor de rechtmatige inzage (hoofdstuk III). Door de strikte scheiding tussen de twee categorieën was de toegang tot elk persoonsgegeven (*personal data*) om redenen van transparantie in feite uitgesloten. De derde categorie werd daarom toegevoegd: persoonsgegevens die om redenen van publiek belang

75 Artikel 24 lid 32 Act 621/99.

76 Artikel 26 Act 621/99.

77 Artikel 8 lid 4 Personal Data Act 523/1999 van 22 april 1999.

78 Artikel 6 Loi 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

79 Artikel 37 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

80 Act LXIII van 1992 on the Protection of Personal Data and Public Access to Data of Public Interest.

(toch) openbaar gemaakt moeten worden. Uit artikel 19, een artikel uit hoofdstuk III, blijkt dat het gaat om de volgende gegevens:

Unless otherwise provided for by an Act, personal data relating to the sphere of tasks of a person exercising the sphere of tasks and powers of organs [performing state or local government function], furthermore the personal data relating to the sphere of tasks of a person performing a public function shall be regarded as data public on grounds of public interest. The provisions on access to data of public interest of this Act shall apply to the access to these data.⁸¹

– In de *Griekse* wetgeving over toegang tot documenten vormen documenten die het privé- of familielevens van derden betreffen een absolute uitzonderingsgrond: toegang tot deze documenten wordt geweigerd.⁸² De gegevensbeschermingswetgeving volgt de bepalingen van richtlijn 95/46 nauwgezet. Opvallend is dat aan het artikel over de rechtmatige verwerking van persoonsgegevens een extra artikellid is toegevoegd:

The Authority [for the Protection of Personal Data] may issue special data processing rules for the more usual categories of data processing and files, which do not evidently affect the rights and freedoms of the persons to whom the data refer.⁸³

In de *Griekse* wetgeving wordt gebruik gemaakt van de in hoofdstuk 4 geopperde mogelijk om voor bepaalde situaties soepelere regels te stellen.⁸⁴ De *Griekse Data Protection Authority* (DPA) heeft van de bepaling slechts eenmaal gebruik gemaakt. In een decreet uit 2000 definieerde de DPA een aantal categorieën die onder deze bepaling vallen.⁸⁵ Daar blijft het echter bij. De DPA gaf verder niet aan welke gegevensbeschermingsregels voor de verwerking van deze categorieën gelden. Eén van de categorieën betreft het persoonsdossier van private en publieke rechtspersonen.⁸⁶

– In de *Ierse* openbaarheidswetgeving is een apart artikel gewijd aan toegang tot persoonsgegevens.⁸⁷ Het uitgangspunt is dat toegang tot een document wordt geweigerd als hiermee persoonlijke informatie wordt geopenbaard.⁸⁸ Uitzonderingen hierop zijn de expliciete instemming van de betrokkene of de situatie waarin de betrokkene voorafgaand aan de overdracht van de gegevens aan de overheidsinstantie erop is gewezen dat de gegevens onderdeel

81 Artikel 19 lid 4 Act LXIII.

82 Artikel 5 lid 3 Act 2690/1999, the Administrative Procedure Code van 19 maart 1999.

83 Artikel 5 lid 3 Act 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data van 10 april 1997.

84 Zie § 4.4.2. Zie hierover verder § 9.3.2 en § 10.3.3.

85 Presidentieel Decreet 79/2000.

86 Artikel 4 Decreet 79/2000.

87 Artikel 28 Freedom of Information Act 1997.

88 Artikel 28 lid 1 Freedom of Information Act.

zullen uitmaken van informatie die publiekelijk toegankelijk kan worden gemaakt.⁸⁹ Ook de algemene bekendheid van de gegevens kan ertoe leiden dat persoonlijke informatie geopenbaard mag worden.⁹⁰ Tot slot, is een afwijking van het uitgangspunt mogelijk als:

the public interest that the request should be granted outweighs the public interest that the right to privacy of the individual to whom the information relates should be upheld.⁹¹

De Ierse wetgever voorziet derhalve in een belangenafweging. Opvallend daarbij is dat gesproken wordt over het *publieke* belang bij het eerbiedigen van het recht op privacy. De plicht die uit de openbaarheidswetgeving volgt, valt onder de wettelijke plicht op basis waarvan verwerking van persoonsgegevens rechtmatig is volgens de Ierse gegevensbeschermingswetgeving.⁹²

– In de *Italiaanse* openbaarheidswet wordt de mogelijkheid gecreëerd om een uitzondering op het recht op toegang tot overheidsdocumenten te maken voor de bescherming van de ‘privacy of third parties’.⁹³ In een decreet van de president waarin de openbaarheidswet verder is uitgewerkt, wordt dit nader toegelicht. Volgens het decreet mag toegang worden geweigerd als de documenten gerelateerd zijn aan het privé-leven van een individu en openbaarmaking concreet schade toebrengt aan het belang van de betrokkene.⁹⁴ In de Italiaanse gegevensbeschermingswetgeving wordt expliciet bepaald dat op toegang tot documenten die persoonsgegevens bevatten, de regels van de openbaarheidswetgeving van toepassing zijn:

[...] prerequisites for, mechanisms of, and limitations on exercise of the right to access administrative records containing personal data, and the relevant judicial remedies shall be regulated further by Act no. 241 of 7 August 1990 [...]⁹⁵

Persoonsgegevens die door de overheid op rechtmatige wijze zijn geopenbaard mogen zonder instemming van de betrokkene verwerkt worden.⁹⁶

– De *Letse* wetgeving kwalificeert informatie die betrekking heeft op het privé-leven van natuurlijke personen als ‘restricted access information’.⁹⁷ Deze

89 Artikel 28 lid 2 sub b en d Freedom of Information Act.

90 Artikel 28 lid 2 sub c Freedom of Information Act.

91 Artikel 28 lid 5 Freedom of Information Act.

92 Zie artikel 8 sub e Data Protection Act 1988 en artikel 9 Data Protection (Amendment) Act 2003.

93 Artikel 24 lid 2 sub d Act 241/1990 van 7 augustus 1990.

94 Artikel 8 lid 5 Decreet 352/1992 van 27 juni 1992.

95 Artikel 59 Decreet 196/2003, Personal Data Protection Code van 30 juni 2003

96 Artikel 24 lid 1 sub c Decreet 196/2003.

97 Artikel 5 lid 2 sub 4 Freedom of Information Law van 29 oktober 1998.

informatie is volgens artikel 8 van de openbaarheidswet 'protected by law'. Hiermee wordt vermoedelijk bedoeld op de gegevensbeschermingswetgeving. In deze wetgeving wordt verder niet gesproken over het openbaren van persoonsgegevens om transparantieredenen. Ten aanzien van het doorgeven van gegevens aan een derde geldt dat deze doorgifte, tenzij dit bij wet anders is geregeld, dient plaats te vinden op basis van een schriftelijke overeenkomst waarin het doel van de doorgifte is opgenomen.⁹⁸

– De *Litouwse* wet over informatievoorziening voor het publiek bepaalt dat het recht op bescherming van het privé- en gezinsleven van personen geëerbiedigd moet worden als overheidsinformatie aan het publiek wordt verstrekt.⁹⁹ Informatie over iemands privé-leven mag alleen worden verstrekt als de betrokkene daarmee instemt. Hierop bestaat een aantal uitzonderingen. De eerste is dat de openbaarmaking niet schadelijk is voor de betrokkene ('publication [...] does not cause undue harm to the person').¹⁰⁰ De tweede uitzondering is dat de openbaarmaking helpt om schendingen van de wet te onthullen.¹⁰¹ De derde uitzondering is de volgende:

information concerning the private life of a public figure (state political figures, public servants, heads of political parties and public organisations as well as other persons participating in public or political activity) may be made public without his consent if such information discloses the circumstances of the aforementioned person's private life or personal traits which are of public significance.¹⁰²

In een andere wet, waarin het recht op toegang tot overheidsinformatie nader is uitgewerkt, is vastgelegd dat de overheidsinstantie, in het geval van het niet verstrekken van informatie, er zeker van moet zijn dat dit noodzakelijk is een democratische samenleving, en dat het streven om de belangen van bijvoorbeeld andere personen te beschermen belangrijker is dan het recht van de verzoeker om informatie te verkrijgen.¹⁰³

In de gegevensbeschermingswetgeving is de afstemming met de wet over informatievoorziening voor het publiek expliciet gereguleerd.¹⁰⁴ De bepaling waarin de vereisten voor rechtmatige verwerking van persoonsgegevens zijn neergelegd, is op deze vorm van verwerking niet van toepassing. Het toezicht op de afstemming van beide wetten is toegewezen aan de *Inspector of Journalistic Ethics*.

98 Artikel 13 Personal Data Protection Law van 24 oktober 2002.

99 Artikel 14 lid 1 Act I-1418 van 2 juli 1996 on Provision of Information to the Public.

100 Artikel 14 lid 2 Act I-1418.

101 Artikel 14 lid 3 Act I-1418.

102 *Ibidem*.

103 Artikel 13 Act VIII-1524 van 11 januari 2000 on the Right to Receive Information from State and Local Authorities.

104 Artikel 8 Act IX-1296 van 21 januari 2003 on Legal Protection of Personal Data.

– In de Nederlandse openbaarheidswetgeving (de Wob) is vastgelegd dat verstrekking van informatie achterwege blijft als het gegevens betreft die in de gegevensbeschermingswet (de Wbp) als ‘bijzondere gegevens’ worden aangeduid.¹⁰⁵ Toegangsverlening is toch mogelijk als deze ‘kennelijk geen inbreuk op de persoonlijke levenssfeer maakt’.¹⁰⁶ In de gegevensbeschermingswetgeving zelf is bepaald dat bijzondere persoonsgegevens die betrekking hebben op iemands politieke gezindheid wél verwerkt mogen worden als dit verband houdt met de benoeming in bestuursorganen en adviescolleges.¹⁰⁷ Gedacht kan worden aan burgermeestersbenoemingen.¹⁰⁸

Ten aanzien van niet-bijzondere gegevens wordt geen toegang verleend als het belang van openbaarheid niet opweegt tegen de eerbiediging van de persoonlijke levenssfeer.¹⁰⁹ Deze uitzondering is niet van toepassing als de betrokkene met openbaarmaking heeft ingestemd.¹¹⁰ In de Nederlandse gegevensbeschermingswetgeving is over de relatie met de openbaarheidswetgeving niets bepaald. Beers beschouwt de plicht tot openbaarmaking onder de Wob als een wettelijke plicht waarvoor verwerking noodzakelijk kan zijn.¹¹¹ Uit de memorie van toelichting bij de Wbp blijkt dat de Wob als een *lex specialis* ten opzichte van de gegevensbeschermingswetgeving wordt beschouwd.¹¹²

De genoemde uitzonderingen in de Wob zijn in uitspraken van verschillende rechterlijke instanties nader verduidelijkt. Daalder geeft in zijn dissertatie uit 2005 op basis van een uitgebreid jurisprudentieonderzoek de hoofdlijnen weer van de manier waarop aan de belangenafweging invulling is gegeven.¹¹³ Het uitgangspunt van de Afdeling Bestuursrechtspraak van de Raad van State is dat als de informatie uitsluitend het beroepshalve functioneren van een bestuurder of ambtenaar betreft, een beroep op artikel 10 lid 2 sub e van de Wob, de uitzondering ten aanzien van de niet-bijzondere gegevens, in beginsel

105 Artikel 10 lid 1 sub d Wet openbaarheid van bestuur van 31 oktober 1991, verwezen wordt naar hoofdstuk 2, paragraaf 2 van de Wet bescherming persoonsgegevens van 6 juli 2000.

106 Artikel 10 lid 1 sub d Wob.

107 Artikel 19 lid 1 sub b Wet bescherming persoonsgegevens.

108 Zie T.F.M. Hooghiemstra, *Tekst en toelichting op de Wet bescherming persoonsgegevens*, Lelystad 2001, Koninklijke Vermande, p. 68.

109 Artikel 10 lid 2 sub e Wob.

110 Artikel 10 lid 3 Wob.

111 Zie artikel 8 sub c Wet bescherming persoonsgegevens. A.A.L. Beers, ‘Privacy en Wet openbaarheid van bestuur’, in J.E.J. Prins & J.M.A. Bervkens (eds), *Privacyregulering in theorie en praktijk*, Deventer 2002, Kluwer, p. 197-219, op p. 211-212. Zie over de botsing tussen openbaarheid en privacybescherming eerder T.A. Knoop Pathuis, ‘Openbaarheid en Privacy’, in J.E. Goldschmidt, A.W. Heringa & W.J. Witteveen (eds), *Openbaarheid*, Deventer 1981, Kluwer, p. 53-69.

112 *Kamerstukken II 1997/98*, 25 892, 3, p. 43. Zie hierover Hooghiemstra 2001, p. 31-32 en M.M. Groothuis, ‘Openbaarheid van bestuur en privacy’, in J.M.A. Bervkens & J.E.J. Prins (eds), *Privacyregulering in theorie en praktijk*, Deventer 2007, Kluwer, p. 130.

113 E.J. Daalder, *Toegang tot overheidsinformatie. Het Grensolak tussen openbaarheid en vertrouwelijkheid*, Den Haag 2005, Boom Juridische Uitgevers (diss. Leiden), § 6.11.

niet mogelijk is.¹¹⁴ Deze rechtspraak is doorgetrokken naar de particuliere sector.¹¹⁵ In bepaalde gevallen kan informatie die behoort tot het beroepshalve functioneren wél onder de uitzondering worden gebracht. Dit volgt uit de uitspraak over de zogenaamde 'Peperbonnetjes'. Deze bonnetjes onthulden het declaratiegedrag van minister Bram Peper wat uiteindelijk tot zijn aftreden leidde.¹¹⁶ De Afdeling Bestuursrechtspraak overwoog hierin:

Dat de desbetreffende uitgaven hebben plaatsgevonden in het kader van de uitoefening van een publieke functie, neemt niet weg dat ook van bestuurders in functie de persoonlijke levenssfeer in het geding kan zijn en dat deze levenssfeer bescherming verdient.¹¹⁷

Daalder voegt zelf als voorbeeld toe persoonsgegevens in personeelsdossiers zoals gegevens met betrekking tot het functioneren van een ambtenaar of de met hem getroffen regelingen.¹¹⁸ Een element dat verder een rol kan spelen bij de belangenafweging is het gedrag van de betrokkene; heeft hij of zij afstand gedaan van de bescherming van de persoonlijke levenssfeer?¹¹⁹

In een uitspraak uit 2006 ging de Afdeling Bestuursrechtspraak in op het belang van openbaarheid van bestuur.¹²⁰ In deze zaak had het gemeentebestuur van Nijkerk een extern onderzoeksrapport openbaar gemaakt over de belangenverstrengeling van een gemeenteambtenaar. In het rapport werd deze persoon bij naam genoemd. De Afdeling overwoog dat de betrokken persoon weliswaar een belang had bij het weglaten van zijn naam uit het rapport, maar dat dit niet opwoog tegen het belang van openbaarheid van bestuur.¹²¹ In dit geval was namelijk de integriteit van het openbaar bestuur in het geding en bestond er al een publieke discussie over de vermeende belangenverstrengeling.¹²² Het was daarom van groot belang dat het publiek duidelijkheid werd verschaft.

Uit een evaluatieonderzoek van de Wob uit 2004, dat was uitgevoerd door de Universiteit Tilburg in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, volgt dat de wijze waarop het raakvlak van toegang tot documenten en bescherming wettelijk is vormgegeven en door de rechter

114 Zie Daalder 2005, p. 226 onder verwijzing naar ABRvS 18 december 2002, *JB* 2003/40. Zie ook Groothuis 2007, p. 132-134.

115 Daalder 2005, p. 226.

116 Zie over deze zaak ook L.J.A. Damen, 'Openbaarheid van bestuur in discussie. Hoe verder na de Peperbonnetjes en de voetbalvandalen?', *NJB* 2000, p. 1813-1822.

117 Daalder 2005, p. 227 onder verwijzing naar ABRvS 25 april 2000, *AB* 2000/210.

118 Daalder 2005, p. 227.

119 Daalder 2005, p. 225.

120 ABRvS 31 mei 2006, *JB* 2006/218 m.n. G. Overkleef-Verburg.

121 ABRvS 31 mei 2006, r.o. 2.8.

122 ABRvS 31 mei 2006, r.o. 2.9.

wordt uitgelegd, geen knelpunten oplevert.¹²³ Daarmee is overigens niet gezegd dat de huidige wettelijke vormgeving niet tot discussie leidt. Over de betekenis van het begrip ‘persoonsgegevens’ uit de Wbp bestaat in dit verband bijvoorbeeld de nodige onduidelijkheid. Van recente datum is de discussie over de categorische weigering van de politie op grond van artikel 10 lid 1 sub d van de Wob om processen-verbaal openbaar te maken waarin verslag wordt gedaan van het verhoor van verdachten. De politie beschouwde de inhoud van deze verslagen als identificeerbare (bijzondere) persoonsgegevens. De Afdeling Bestuursrechtspraak vond deze interpretatie te breed.¹²⁴ De verslagen van verhoor bestaan niet allemaal en niet helemaal uit tot een persoon herleidbare informatie.¹²⁵ Volgens de Afdeling moet het mogelijk zijn de processen-verbaal zodanig te schonen, dat daaruit niet meer kan worden afgeleid wie welke verklaring heeft afgelegd over het verloop van de feitelijke gebeurtenissen.¹²⁶

In de Nederlandse gegevensbeschermingswetgeving is het doelbindingsbeginsel, net als in de Belgische wetgeving, op afwijkende wijze neergelegd. In artikel 9 is op bekende wijze bepaald dat persoonsgegevens niet verder worden verwerkt op een manier die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. In het tweede lid wordt echter toegelicht met welke omstandigheden rekening moet worden gehouden bij de beoordeling of sprake is van ‘onverenigbaarheid’. Deze zijn:

- a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- b. de aard van de betreffende gegevens;
- c. de gevolgen van de beoogde verwerking voor de betrokkene;
- d. de wijze waarop de gegevens zijn verkregen;
- e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Door het doelbindingsbeginsel zo vorm te geven, hoeft er geen frictie te bestaan met het verwerken van persoonsgegevens naar aanleiding van een verzoek om toegang tot documenten.

– In de *Oostenrijkse* wetgeving is geen uitzondering voor privacy of bescherming van persoonsgegevens te vinden.¹²⁷ Alleen zeer algemeen geldt dat

123 T. Brandsen e.a., *Over wetten en praktische bezwaren*, onderzoeksrapport Universiteit van Tilburg 2004, te vinden op http://www.minbzk.nl/search/contents/pages/9366/wobevaluatie_eindrapport_060404.pdf (geraadpleegd op 4 december 2006), zie m.n. § 1.5 en § 1.6.

124 ABRvS 31 januari 2007, AB kort 2007/93.

125 ABRvS 31 januari 2007, r.o. 2.2.3.

126 ABRvS, 31 januari 2007, r.o. 2.2.3.

127Zie de Auskunftspflicht-Grundsatzgesetz 268-287/1987 van 15 mei 1987.

toegang tot documenten geweigerd kan worden als dit in het belang van individuen is.¹²⁸

De Oostenrijkse gegevensbeschermingswetgeving kent een benadering die enigszins afwijkt van de gegevensbeschermingswetgeving in andere lidstaten. In de Oostenrijkse gegevensbeschermingsregels wordt meerdere malen de nadruk gelegd op het belang van de betrokkene. Dit blijkt al uit artikel 1 waarin het fundamentele recht op bescherming van persoonsgegevens is neergelegd. Volgens dit artikel heeft iedereen het recht op geheimhouding van zijn persoonsgegevens (in het bijzonder als dit zijn privacy betreft) *voor zover hij hier een belang bij heeft*.¹²⁹ Dit belang is volgens hetzelfde artikel afwezig als de informatie algemeen beschikbaar is.¹³⁰ In een apart artikel is aangegeven wanneer het belang van de betrokkene *niet geschonden* wordt geacht.¹³¹ Hiervan is onder meer sprake als een gerechtvaardigd belang van een derde (of van de verwerker van de gegevens) zwaarder weegt.¹³² Onder verwijzing naar deze bepaling, wordt verderop in hetzelfde artikel een aantal voorbeelden gegeven.¹³³ Verwerking van gegevens die louter de uitoefening van een publieke functie (*öffentliche Funktion*) van het datasubject betreffen, levert in die zin geen schending van het betrokken belang op.¹³⁴ De Oostenrijkse wetgeving maakt hier, net als de Griekse wetgeving, gebruik van de in hoofdstuk 4 geopperde mogelijkheid om voor bepaalde situaties soepelere regels te stellen.¹³⁵

– In de Poolse openbaarheidswetgeving is neergelegd dat het recht op toegang tot overheidsinformatie beperkt wordt door de vereisten die volgen uit de bescherming van de persoonlijke levenssfeer van natuurlijke personen.¹³⁶ Deze beperking is echter niet van toepassing op:

information on persons holding public function, connected with holding such function, including conditions of entrusting and performing the function, and in cases where natural persons [...] waive this right.¹³⁷

In de Poolse gegevensbeschermingswet wordt niet gesproken over de openbaarheidswetgeving. Waarschijnlijk is de openbaarmaking van de gegevens

128 Dit is in artikel 20 lid 3 van de Oostenrijkse Bundes-Verfassungsgesetz terug te vinden.

129 Artikel 1 lid 1 Bundesgesetz über den Schutz personenbezogener Daten van 17 augustus 1999.

130 *Ibidem*.

131 Zie artikel 8 Bundesgesetz über den Schutz personenbezogener Daten.

132 Zie artikel 8 lid 1 sub 4 Bundesgesetz über den Schutz personenbezogener Daten. Vergelijk artikel 7 sub f richtlijn 96/56. Zie § 8.2.2.2.

133 Zie artikel 8 lid 3 Bundesgesetz über den Schutz personenbezogener Daten.

134 Artikel 8 lid 3 sub 6 Bundesgesetz über den Schutz personenbezogener Daten.

135 Zie § 4.4.2. Zie hierover verder § 9.3.2 en § 10.3.3.

136 Artikel 5 lid 2 Act 112/2001 van 6 september 2001 on Access to Public Information.

137 *Ibidem*.

die onder de geciteerde bepaling vallen als een wettelijke verplichting aan te merken.¹³⁸

– In de *Portugese* openbaarheidswetgeving worden documenten die persoonsgegevens bevatten als aparte categorie documenten ('named document') aangeduid.¹³⁹ Onder persoonsgegevens wordt volgens deze wet verstaan: 'any information concerning an identified or identifiable natural person, and containing assessments, or judgments of value, or covered by the clause of respect for private life'.¹⁴⁰ Toegang tot deze categorie documenten is voorbehouden aan de betrokkene of aan derden met schriftelijke toestemming van de betrokkene.¹⁴¹ Ook is verstrekking van de gegevens aan een derde mogelijk als deze een direct, persoonlijk en legitiem belang daarbij heeft.¹⁴² De derde aan wie de persoonsgegevens worden verstrekt mag deze gegevens niet voor andere doeleinden gebruiken dan waarvoor ze zijn overhandigd.¹⁴³ Anders is deze persoon of instantie aansprakelijk voor geleden schade.¹⁴⁴

Niet duidelijk is hoe de bepaling over toegang tot *named documents* zich verhoudt tot wat is bepaald in een eerder artikel, namelijk dat toegang tot 'documents concerning automatically processed personal data' bij aparte wet is geregeld.¹⁴⁵ Hiermee wordt bedoeld op de Portugese gegevensbeschermingswetgeving.¹⁴⁶ Kennelijk is bij *named documents* geen sprake van op geautomatiseerde wijze verwerkte persoonsgegevens. De afstemming tussen beide wetten lijkt gebrekkig, het begrip persoonsgegevens dat in beide wetten gehanteerd wordt is niet identiek. In de gegevensbeschermingswetgeving is verder niets geregeld ten aanzien van toegang tot persoonsgegevens om redenen van transparantie.

– De *Roemeense* wet over toegang tot publieke informatie heeft als uitgangspunt dat toegang tot informatie wordt geweigerd als het om persoonsgegevens gaat, onder de voorwaarden van de wet.¹⁴⁷ Met dit laatste wordt waarschijnlijk bedoeld op de regels uit de gegevensbeschermingswetgeving.¹⁴⁸ In de openbaarheidswetgeving zelf wordt op dit uitgangspunt een uitzondering

138 Artikel 23 lid 2 Act 133/97 van 29 augustus 1997 on the Protection of Personal Data.

139 Artikel 4 lid 1 sub b Act 65/93 van 26 augustus 1993 on Access to administrative documents.

140 Artikel 4 lid 1 sub c Act 65/93.

141 Artikel 8 lid 1 Act 65/93.

142 Artikel 8 lid 2 Act 65/93.

143 Artikel 10 lid 3 Act 65/93.

144 *Ibidem*.

145 Artikel 7 lid 7 Act 65/93.

146 Act 67/98 van 26 oktober 1998 on the Protection of Personal Data.

147 Artikel 12 lid 1 sub d en artikel 2 sub c Act 544 van 12 oktober 2001 on Free Access to Public Information.

148 De regels over gegevensbescherming zijn neergelegd in Act 677 van 21 november 2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of such Data.

gemaakt voor persoonsgegevens die gerelateerd zijn aan de uitoefening van een publieke functie. Deze gegevens worden als publieke informatie beschouwd.¹⁴⁹

De gegevensbeschermingswetgeving is op de openbaarheidswetgeving afgestemd. In § 8.2.2.2 verwees ik bij de bespreking van richtlijn 95/46 naar de mogelijkheid die lidstaten hebben om voor journalistieke, artistieke en literaire doeleinden uitzonderingen op de gegevensbeschermingsregels te maken. In de Roemeense gegevensbeschermingswet is hiervan gebruik gemaakt. Een aantal bepalingen is niet van toepassing op verwerking die voor die doeleinden plaatsvindt.¹⁵⁰ Dit geldt ook als:

the processing regards personal data that were made public in a specific manner by the data subject or which are linked to the quality of public person of the data subject or linked to the public character of the facts he/she is involved in.¹⁵¹

– In de *Slowaakse* openbaarheidswetgeving is een apart artikel gewijd aan de bescherming van personen en persoonsgegevens.¹⁵² Daarin is bepaald dat informatie die gerelateerd is aan de persoon en het privé-leven van natuurlijke personen alleen geopenbaard mag worden met toestemming van de betrokkene of als er een specifieke wettelijke grondslag is.¹⁵³

In de Slowaakse wet over de bescherming van persoonsgegevens worden regels gesteld ten aanzien van het publiek maken van persoonsgegevens.¹⁵⁴ Deze regels zien in de eerste plaats op het openbaren van gegevens door niet-publieke actoren. Over het openbaren van persoonsgegevens door publieke instanties wordt met zoveel woorden niet gesproken. De vereisten voor het publiek maken van persoonsgegevens (zonder toestemming van de betrokkene) zijn dat er een specifieke wet moet zijn waarin het doel duidelijk is vermeld, alsook het soort gegevens en de ontvangende partij(en).¹⁵⁵ Als ondergrens wordt bepaald dat het openbaar maken van de gegevens nooit het recht van de betrokkene op bescherming van zijn privacy kan schenden.¹⁵⁶

– In de *Sloveense* wetgeving over toegang tot overheidsinformatie wordt voor persoonsgegevens een uitzondering gemaakt. Toegang wordt geweigerd als de informatie persoonsgegevens betreft 'the disclosure of which would constitute an infringement of the protection of personal data in accordance with

149 Artikel 14 lid 1 Act 544.

150 Artikel 11 Act 677.

151 *Ibidem*.

152 Artikel 9 Act 211/2000 on Free Access to Information van 17 mei 2000.

153 Artikel 9 lid 1 Act 211/2000.

154 Artikel 4 lid 1 sub d Act 428/2002 on Protection of Personal Data van 1 september 2002.

155 Artikel 7 lid 3 Act 428/2002.

156 Artikel 7 lid 7 Act 428/2002.

the Act governing the protection of personal data'.¹⁵⁷ De gegevensbeschermingswetgeving is echter zeer vaag. Uit de wetgeving blijkt dat voor de verwerking van gegevens door een publieke instantie een wettelijke basis is vereist.¹⁵⁸ Verwerking zonder deze wettelijke basis is mogelijk als dit essentieel is voor de rechtmatige uitoefening van de bevoegdheden en verplichtingen van de overheidsinstanties.¹⁵⁹ De verwerking mag geen afbreuk doen aan de rechtmatige belangen van het datasubject.¹⁶⁰

– *Spanje* kent een vrij algemene uitzondering op het recht op toegang tot documenten voor de belangen van derden.¹⁶¹ Alleen ten aanzien van het openbaren van medische gegevens wordt bepaald dat daarvoor een apart wettelijk regime geldt.¹⁶² In de Spaanse gegevensbeschermingswetgeving is over het openbaren van gegevens door overheidsinstanties niet expliciet iets geregeld. Vrij algemeen wordt bepaald dat het verwerken van persoonsgegevens uit publieke bronnen is toegestaan als dit een legitiem belang dient van de voor de verwerker verantwoordelijke of een derde.¹⁶³ Onder publieke bronnen wordt verstaan:

the publicity register, telephone directories subject to the conditions laid down in the relevant regulations, and the lists of persons belonging to professional associations containing only data on the name, title profession, activity, academic degree, address and an indication of his membership of the association. Newspapers, official gazettes and the media shall also be considered as sources with public access.¹⁶⁴

Ten aanzien van het doorgeven van gegevens aan derden is vastgelegd dat dit alleen mag voor doeleinden die direct gerelateerd zijn aan de legitieme functie van de voor de verwerking verantwoordelijke en met instemming van de betrokkene.¹⁶⁵ Deze instemming is niet vereist als de gegevens uit een publieke bron afkomstig zijn.¹⁶⁶ Het is niet duidelijk of deze bepaling ook voor overheidsorganen geldt.

– Als gevolg van de implementatie van richtlijn 95/46 is in de *Tsjechische openbaarheidswetgeving* een bepaling over de 'protection of personality and

157 Artikel 6 lid 3 Act 9/03 on the Access to Information of Public Character van 25 februari 2003.

158 Artikel 9 Personal Data Protection Act 148/04 van 15 juli 2004.

159 Artikel 9 lid 4 Act 148/04.

160 *Ibidem*.

161 Artikel 37 lid 4 Act 30/92 on Rules for Public Administration and Administrative Procedures van 26 november 1992.

162 Artikel 37 lid 6 sub b Act 30/92.

163 Artikel 6 lid 2 Act 15/1999 on the Protection of Personal Data van 13 december 1999.

164 Artikel 3 sub j Act 15/1999.

165 Artikel 11 lid 1 Act 15/1999.

166 Artikel 11 lid 2 sub b Act 15/1999.

privacy' geschrapt.¹⁶⁷ In plaats daarvan is er een directe verwijzing opgenomen naar de gegevensbeschermingswetgeving.¹⁶⁸ In deze wetgeving is over het openbaren van persoonsgegevens om redenen van transparantie niets bepaald. Wél wordt het begrip 'published personal data' gehanteerd.¹⁶⁹ Dit zijn persoonsgegevens die toegankelijk zijn gemaakt 'by mass media, other form of public communication, or as a part of a public list'.¹⁷⁰ Aan deze toegankelijkheid moet wel een speciale wet ten grondslag liggen.¹⁷¹ Er wordt verwezen naar een wet waarin regels voor de pers zijn neergelegd.¹⁷² Of er ook een speciale wet bestaat waarin voor de overheid regels zijn opgenomen over het publiceren van persoonsgegevens, is niet duidelijk. De openbaarheidswetgeving zelf voldoet daar gezien de verwijzing in elk geval niet aan. De *published personal data* mogen verwerkt worden zonder instemming van de betrokkene, mits dit geen afbreuk doet aan het recht op bescherming van de persoonlijke levenssfeer van het data subject.¹⁷³

– In 2000 werd in het *Verenigd Koninkrijk* openbaarheidswetgeving aangenomen. Twee jaar eerder was gegevensbeschermingswetgeving aangenomen.¹⁷⁴ In de openbaarheidswetgeving is duidelijk rekening gehouden met de interferentie met de bestaande gegevensbeschermingsregels. De inwerkingtreding van de openbaarheidswet vond gefaseerd plaats.¹⁷⁵ Sommige bepalingen waren direct van kracht, andere na twee maanden en een aantal pas na (ruim) vijf jaar. Tot deze laatste behoorden bepalingen die de gegevensbeschermingswet op een aantal punten wijzigden. Vanaf 1 januari 2006 is de regulering van het raakvlak van beide regimes daarmee expliciet in beide wetten vastgelegd. Het is geen eenvoudige opgave om de precieze juridische invulling van het raakvlak te doorgronden. De verhouding tussen beide wetten wordt door Wadham en Griffiths beschreven als 'undesirable over-complex'.¹⁷⁶ Als startpunt van een beschrijving van de regulering kan de definitie van het begrip 'data' in de gegevensbeschermingswet dienen. Deze luidt:

167 Zie artikel 50 Act 101/2000 on the Protection of Personal Data and on Amendments to Some related Acts van 4 april 2000. De inhoud van artikel 8 Act 106/1999 on Free Access to Information van 11 mei 1999 wordt geschrapt.

168 Artikel 2 lid 3 Act 106/1999.

169 Artikel 4 lid 6 sub 1 Act 101/2000.

170 *Ibidem*.

171 Artikel 5 lid 2 sub d Act 101/2000.

172 Act 81/1966 on the Periodical Press and Other Media of Mass Information, trad in werking op 1 januari 1967.

173 *Ibidem*.

174 De Freedom of Information Act van 30 november 2000.

175 Zie artikel 87 Freedom of Information Act 2000. Zie over de geschiedenis van toegang tot overheidsinformatie in het Verenigd Koninkrijk, P. Birkinshaw, *Freedom of information, the law, the practice and the ideal*, Londen 1996, Butterworths.

176 Zie ook J. Wadham & J. Griffiths, *Blackstone's guide to The Freedom of Information Act 2000*, Oxford 2005, Oxford University Press, hoofdstuk 10, p. 142.

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
- (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);¹⁷⁷

Sub e is door de openbaarheidswetgeving aan het rijtje toegevoegd.¹⁷⁸ Als gevolg hiervan is informatie die niet onderdeel uitmaakt van een *relevant filing system* of van een *accessible record* ook binnen de reikwijdte van de gegevensbescherming gebracht. Uit de gegevensbeschermingswet blijkt dat gedacht moet worden aan 'unstructured personal data'.¹⁷⁹ Hiervan is sprake bij informatie die niet onderdeel uitmaakt van 'any set of information relating to individuals to the extent that the set is structured by reference to individuals or by reference to criteria relating to individuals'.¹⁸⁰

In de openbaarheidswetgeving is een afzonderlijk artikel gewijd aan persoonlijke informatie.¹⁸¹ Daarin is bepaald dat het niet mogelijk is om op basis van de openbaarheidswet toegang tot eigen persoonsgegevens te verkrijgen. Daarvoor moet de Britse gegevensbeschermingswet als grondslag dienen. Volgens Pitt-Payne moet hierin de reden worden gezocht voor de uitbreiding van de reikwijdte van het begrip 'data' in de gegevensbeschermingswetgeving. Men wilde er zeker van zijn dat verzoeken om toegang tot eigen persoonsgegevens onder de gegevensbeschermingswet zouden vallen.¹⁸²

Informatie die persoonsgegevens van anderen bevat, is uitgezonderd van het recht op toegang tot documenten als aan één van twee voorwaarden is voldaan. De eerste voorwaarde is dat, voor het geval de gegevens onder één van de in sub a tot en met d genoemde beschrijvingen vallen, het openbaar maken van de gegevens de gegevensbeschermingsbeginselen schendt of schade of ernstig ongemak tot gevolg heeft.¹⁸³ Vallen de gegevens onder de beschrijving van sub e dan kunnen zij niet geopenbaard worden als de openbaarmaking niet voldoet aan de vereisten van de gegevensbescherming die specifiek

177 Artikel 1 lid 1 Data Protection Act 1998. De verwijzing naar artikel 68 van deze wet is, ondanks dat dit op het eerste gezicht anders lijkt, niet relevant. Zie artikel 68 en annex 12 bij de Data Protection Act 1998.

178 Zie artikel 68 Freedom of Information Act 2000.

179 Artikel 9A Data Protection Act 1998.

180 Artikel 9A lid 1 Data Protection Act 1998.

181 Artikel 40 Freedom of Information Act 2000.

182 Zie T. Pitt-Payne, 'Privacy versus Freedom of Information: Is There a Conflict?', *EHRLRev.* 2003, p. 109-119. op p. 115.

183 Artikel 40 lid 3 Freedom of Information Act 2000.

voor deze restcategorie gelden. Deze vereisten zijn soepeler dan voor de gegevens die onder sub a tot en met d vallen. Zo is ten aanzien van deze gegevens het doelbindingsbeginsel niet van toepassing.¹⁸⁴ De Britse *Information Commissioner*, een onafhankelijke autoriteit die zich zowel met openbaarheid van bestuur als bescherming van persoonsgegevens bezighoudt, heeft op de eerste voorwaarde een toelichting gegeven.¹⁸⁵ Volgens hem is de centrale vraag of openbaarmaking van de persoonsgegevens rechtmatig en redelijk is. Daarbij moet rekening worden gehouden met het onderscheid tussen het publieke en privé-leven van personen:

‘Information which is about the home and family life of an individual, his or her personal finances, or consists of personal references, is likely to deserve protection. By contrast, information which is about someone acting in an official or work capacity should normally be provided on request unless there is some risk to the individual concerned.’¹⁸⁶

Dan merkt hij op:

‘An issue that will often arise is whether the Data Protection Act prevents the disclosure of information identifying members of staff. Applying the criteria suggested above, if the information requested consists of the names of officials, their grades, job functions or decisions which they have made in their official capacities, then disclosure would normally be made. On the other hand, information such as home addresses or internal disciplinary matters would not normally be disclosed. While it would be wrong to disclose bank account details of staff, it would be unlikely to be unfair to publish details of expenses incurred in the course of official business, information about pay bands, or, particularly in the case of senior staff, details of salaries’.¹⁸⁷

De tweede voorwaarde is dat een van de uitzonderingen op het recht op toegang tot *eigen* persoonsgegevens uit de gegevensbeschermingswetgeving van toepassing is.¹⁸⁸

In de openbaarheidswetgeving is, tot slot, bepaald dat informatie die op basis van vertrouwelijkheid aan de publieke autoriteiten is overhandigd, niet geopenbaard mag worden.¹⁸⁹ Op de Engelse wetgeving kom ik in § 8.4 terug.

184 Artikel 33A Data Protection Act 1998. Zie voor een overzicht artikel 33A Data Protection Act 1998 en Wadham & Griffiths 2005, § 10.3.

185 Zie de *Freedom of Information Act Awareness Guidance No 1*, te vinden op de website van de Information Commissioner: <http://www.ico.gov.uk> onder ‘guidance’.

186 *Freedom of Information Act Awareness Guidance No 1*, p. 4.

187 *Freedom of Information Act Awareness Guidance No 1*, p. 5.

188 Artikel 40 lid 4 Freedom of Information Act 2000.

189 Artikel 41 Freedom of Information Act 2000.

– In *Zweden* mag toegang tot officiële documenten geweigerd worden als dit noodzakelijk is voor de bescherming van de ‘personal or economic circumstances of private subjects’.¹⁹⁰ In artikel 3 is bepaald dat informatie die is samengesteld uit materiaal dat was vergaard voor geautomatiseerde gegevensverwerking niet als overheidsinformatie kan worden aangemerkt als het persoonsgegevens bevat en de openbaarmaking ervan niet door een bijzondere wet is toegestaan. In de wet over gegevensbescherming wordt apart aandacht besteed aan de relatie met toegang tot overheidsinformatie:

The provisions of this Act are not applied to the extent that they would limit an authority’s obligation under Chapter 2 of the Freedom of the Press Act to provide personal data.¹⁹¹

Dit betekent dat de weergegeven bepalingen over toegang tot persoonsgegevens het juridisch kader vormen. De gezamenlijke lezing van deze twee bepalingen leidt tot de conclusie dat persoonsgegevens die niet de persoonlijke of economische omstandigheden van het data subject betreffen en die niet met het oog op geautomatiseerde verwerking zijn verzameld in beginsel openbaar gemaakt moeten worden.

8.3.3 Tussenconclusie

Het bovenstaande overzicht toont een grote diversiteit in de wijze waarop de openbaarheids- en gegevensbeschermingswetgeving door de lidstaten op elkaar is afgestemd. Het ene uiterste is een totale afwezigheid van enige afstemming van beide wetten, zoals in Oostenrijk en Spanje die in de openbaarheidswetgeving alleen een uitzondering hebben opgenomen voor respectievelijk de belangen van individuen en derden. Het andere uiterste wordt gevormd door landen die de manier waarop met de botsing van beide rechten moet worden omgegaan expliciet hebben gereguleerd en gedetailleerd hebben vastgelegd, zoals Duitsland en het Verenigd Koninkrijk. Tussen beide uitersten verschuift de afstemming van een simpele vermelding van privacy als uitzonderingsgrond op het recht op toegang tot documenten, via een verdere uitwerking van de privacyexceptie tot een uitdrukkelijke afstemming met de gegevensbeschermingswetgeving. De opname van een privacyuitzondering in openbaarheidswetgeving biedt in de meeste gevallen ruimte voor een nadere regulering van het raakvlak van beide regimes. Dat er toch behoefte kan bestaan aan een meer uitgewerkte wettelijke afstemming van beide regelingen

190 Hoofdstuk 2, artikel 2 lid 6 Freedom of the Press Act van 1766 (!). Zie over de Zweedse situatie uitgebreid J. Steele, ‘Data Protection: An Opening Door? The Relationship between Accessibility and Privacy in Sweden in an EU Perspective’, *LLRev.* 2002, p. 19-39.

191 Artikel 7 Personal Data Act (1998:204) van 29 april 1998.

blijkt uit de analyse van De Hert en Schram ten aanzien van de Belgische situatie. De uitzondering op het recht op toegang tot documenten voor 'de persoonlijke levenssfeer' blijkt voor de Belgische praktijk onvoldoende houvast te bieden.

In verreweg de meeste landen is de nadere afstemming van beide rechten in de openbaarheidswetgeving neergelegd. Hierop zijn drie uitzonderingen: in Hongarije zijn beide regimes in één wet vastgelegd, in Roemenië is in zowel de gegevensbeschermingswetgeving als de openbaarheidswetgeving een specifieke bepaling opgenomen en in het Verenigd Koninkrijk is de regulering van het raakvlak in beide wetten gezamenlijk neergelegd.

De eventuele nadere afstemming van beide wetten wordt op verschillende wijzen ingevuld. In Duitsland, Ierland en Nederland is nadrukkelijk sprake van een *belangenafweging* die door de uitvoerende instanties moet worden gemaakt. In de Duitse wetgeving moet het belang van toegang tot documenten afgewogen worden tegen het gerechtvaardigde belang van de betrokkene. In de Ierse en Nederlandse wetgeving moet het belang bij openbaarheid afgewogen worden tegen het belang van de eerbiediging van de persoonlijke levenssfeer.

Daarnaast zijn *verschillende criteria* vastgelegd voor de beslissing over openbaarmaking. In de Estse wetgeving is bijvoorbeeld vastgelegd dat informatie waarvan de openbaarmaking het recht op bescherming van het privé-leven op significante wijze schendt niet mag worden geopenbaard. In Nederland is openbaarmaking van gevoelige gegevens mogelijk als deze kennelijk geen inbreuk op de persoonlijke levenssfeer maakt. Litouwen hanteert de schade voor de betrokkene als beslissend criterium: als openbaarmaking geen schade toebrengt is het toegestaan. De algemene bekendheid van de informatie kan een rol spelen (Ierland) of het gedrag van de betrokkene (Polen).

Ook wordt voor *bepaalde categorieën gegevens* door de wetgever zelf beslist wanneer het belang van openbaarheid zwaarder weegt dan het belang van de betrokkene, en wanneer niet. In zeven landen wordt daarbij aangehaakt op de publieke functie of status van de persoon. Zo wordt in de Duitse wetgeving gesproken over ambtenaren en personen die op een bepaalde manier betrokken zijn bij de overheidsbesluitvorming, in de Estse wetgeving informatie over een 'state or local government official', in de Finse wetgeving is sprake van personen met een politieke of verkozen functie, in Hongarije worden functiegerelateerde gegevens van personen met een publieke functie openbaar gemaakt, in de Litouwse wet wordt over publieke figuren gesproken en in de Poolse wetgeving over personen met een publieke functie. In de Roemeense wetgeving worden persoonsgegevens die gerelateerd zijn aan de uitoefening van een publieke functie als publieke informatie beschouwd.¹⁹² Uit de be-

192 In de Bulgaarse wetgeving is de reikwijdte van het begrip 'persoonsgegevens' zodanig aangepast dat informatie over publieke activiteiten van publieke personen buiten het begrip vallen.

schreven praktijk in Nederland en het Verenigd Koninkrijk blijkt ook dat de publieke functie of status van de betrokkene een doorslaggevende rol kan spelen bij de beslissing over openbaarmaking. In een aantal landen is voor *gevoelige* gegevens beslist dat toegang door derden daartoe niet mogelijk is zonder toestemming van de betrokkene.¹⁹³ In sommige landen wordt toegang tot gegevens expliciet uitgesloten als deze gegevens duidelijk in vertrouwen aan de overheid zijn overhandigd.¹⁹⁴

In hoofdstuk 7 is er naar aanleiding van de situatie op Europees niveau op gewezen dat het openbaren van persoonsgegevens om transparantieredenen lastig is in te passen in de huidige Europese gegevensbeschermingsregels.¹⁹⁵ Omdat veel landen de bepalingen van richtlijn 95/46 letterlijk hebben overgenomen, kunnen de besproken problemen zich ook op nationaal niveau voordoen. Op een aantal manieren is dit voorkomen. In vijf landen (Finland, Frankrijk, Italië, Litouwen en Zweden) is in de gegevensbeschermingswetgeving zelf bepaald dat deze wetgeving geen afbreuk doet aan de rechten en plichten die voortvloeien uit de openbaarheidswetgeving. In de Griekse en Oostenrijkse gegevensbeschermingswetgeving is gebruik gemaakt van de mogelijkheid om voor bepaalde situaties soepelere regels vast te stellen. In Griekenland is de *bevoegdheid* hiertoe gecreëerd, waar tot op heden inhoudelijk geen gebruik van is gemaakt. In de Oostenrijkse wetgeving is bepaald dat het belang van de betrokkene niet geschaad is als het de verwerking van gegevens van personen betreft in de uitoefening van hun publieke functie en daar tegenover een ander gerechtvaardigd belang staat. Hoewel dit niet expliciet ziet op de *openbaarmaking* van deze gegevens, leidt de strikte toepassing van de gegevensbeschermingsregels met gebruik van deze categorie minder snel tot een *onevenredige* beperking van de openbaarheidsregels.¹⁹⁶

Eerder gaf ik aan dat het openbaren van persoonsgegevens vanwege het inwilligen van een verzoek om toegang tot documenten op gespannen voet zou kunnen staan met het doelbindingsbeginsel.¹⁹⁷ Alleen als het openbaren als niet onverenigbaar met het oorspronkelijke doel wordt beschouwd, vormt het beginsel geen obstakel. In België en Nederland is in de gegevensbeschermingswetgeving invulling gegeven aan wat onder *niet onverenigbaar met dit doel* moet worden beschouwd. België haakt daarbij aan op de redelijke verwachting van de betrokkene. Door de gegeven invulling is in beide landen duidelijk dat het openbaren van gegevens om transparantieredenen niet strijdig hoeft te zijn met het doelbindingsbeginsel.

193 Zie Duitsland, Estland en Finland.

194 Zie Duitsland en het Verenigd Koninkrijk.

195 Zie § 7.3.3 en § 8.2.2.2.

196 Zie hierover verder § 9.3.2 en § 10.3.3.

197 Zie § 7.3.3 en § 8.2.2.2.

8.4 EEN ALTERNATIEVE BENADERING: DE ZAAK *DURANT T. FINANCIAL SERVICES AUTHORITY* (VK)

8.4.1 Inleiding

In hoofdstuk 5 heb ik verschillende definities besproken die voor het verdere onderzoek als uitgangspunt dienden. Op de vraag of door aanpassing van deze definities het recht op toegang tot documenten en het recht op bescherming van persoonsgegevens beter op elkaar afgestemd zouden kunnen worden, zal ik verder niet ingaan.¹⁹⁸ Toch wil ik in deze paragraaf kort ingaan op een discussie die momenteel in Europese kringen wordt gevoerd over de definitie van het begrip 'persoonsgegevens'. Aanleiding voor deze discussie is een uitspraak van het Britse *Court of Appeal* van eind 2003, de zaak *Durant t. Financial Services Authority*.¹⁹⁹ Hierin werd overwogen dat bepaalde gegevens, hoewel zij tot identificeerbare personen te herleiden waren, toch niet als persoonsgegevens moesten worden aangemerkt.²⁰⁰ Het *Court of Appeal* beperkte hiermee de werking van de gegevensbeschermingswetgeving (*Data Protection Act 1998*, vanaf nu DPA 1998) in algemene zin door een strikte definitie van de begrippen 'personal data' en 'relevant filing system' te hantieren. De uitspraak leidde tot vragen van de Europese Commissie met het oog op een mogelijke inbreukactie tegen het Verenigd Koninkrijk wegens onjuiste omzetting van richtlijn 95/46. Op het moment van afronding van dit onderzoek, moest de Commissie nog een beslissing nemen over de eventueel te starten inbreukactie tegen het Verenigd Koninkrijk.

Ook de Artikel 29 Groep heeft zich recentelijk over de definiëring van de reikwijdte van de gegevensbescherming gebogen. Aanleiding was een werkdocument van de Artikel 29 Groep over het gebruik van zogenaamde 'RFID-technologie'.²⁰¹ Op een *tag* (een soort microchip) kan bepaalde informatie worden opgeslagen en vervolgens door die *tag* worden uitgezonden. Met gebruik van een speciale *reader* kan deze informatie worden opgevangen en met een computer worden verwerkt. Deze technologie kan bijvoorbeeld gebruikt worden in de supermarkt. Op alle producten in de supermarkt wordt een *tag* bevestigd die op analoge wijze de prijs van het betreffende product

198 Zie § 1.5 en § 5.1.

199 Court of Appeal (civil division) 8 december 2003, *Michael John Durant t. Financial Services Authority*, [2003] EWCA Civ 1746, te vinden op <http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm>. Zie over deze zaak ook: S. Chalton, 'Reflections on Durant v. FSA: The Court of Appeals' interpretation of 'personal data' in Durant v. FSA – a welcome clarification or a cat among the data protection pigeons?', *CLSR* 2004, vol. 20, nr. 3.

200 Vergelijk de beschrijving van de Bulgaarse situatie in § 8.3.2.

201 Working document 105 on data protection issues related to RFID technology van de Artikel 29 Werkgroep van 19 januari 2005 (te vinden via http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm). RFID staat voor *Radio Frequency Identification*.

uitzendt. Door simpelweg met het boodschappenwagentje langs de *reader* te rijden, kan in één keer het totale bedrag van de boodschappen worden bepaald. In het werkdocument ging de Artikel 29 Groep uitgebreid in op de implicaties van de nieuwe technologie voor de bescherming van persoonsgegevens. Naar aanleiding van het werkdocument rees de vraag of de Artikel 29 Groep geen 'overstretched definition of personal data' hanteerde.²⁰² Op het moment van afronding van dit onderzoek, werd binnen de Artikel 29 Groep gewerkt aan een document waarin uitgebreid bij dit punt wordt stil gestaan. Duidelijk is dat dit document relevant zal zijn voor het oordeel van de Commissie over de toepassing van de Britse wetgeving zoals deze blijkt uit de uitspraak in de zaak *Durant*.

Hieronder volgt een beschrijving van de *Durant*-uitspraak en de relevantie ervan voor het onderwerp van het onderhavige onderzoek. Het *Court of Appeal* deed de uitspraak voordat de DPA 1998 door de openbaarheidswetgeving werd geamendeerd.²⁰³ Als gevolg van de amendementen is de uitspraak ten aanzien van de interpretatie van het begrip 'relevant filing system' niet meer relevant doordat het data subject ook het recht op toegang tot ongestructureerde persoonsgegevens heeft gekregen.²⁰⁴ Dit deel van de uitspraak blijft daarom verder onbesproken.

8.4.2 De feiten

Michael Durant was verzeild geraakt in een rechtszaak tegen de Engelse Barclays Bank waar hij klant van was. Nadat hij de zaak in 1993 verloor, probeerde hij inzage te krijgen in verschillende dossiers en documenten die verband hielden met de aanleiding van de rechtszaak. Hij hoopte op die manier feiten boven water te krijgen die een heropening van de zaak zouden rechtvaardigen. Hij zocht hiervoor steun bij de toezichthouder voor de financiële sector in het Verenigd Koninkrijk: de Financial Services Authority (FSA). Nadat de FSA de kwestie had onderzocht, sloot zij de zaak zonder Durant op de hoogte stellen van de uitkomst. Dit was het gevolg van de geheimhoudingsplicht van de FSA. Michael Durant vroeg vervolgens op basis van de DPA 1998 toegang tot de documenten uit het onderzoeksdossier van de FSA omdat deze gegevens over zijn persoon bevatten. Hij vroeg, met andere woorden, om toegang tot zijn eigen persoonsgegevens. Er was volgens Durant in

202 Zie de resultaten van de publieke consultatie over Werkdocument 105, gepubliceerd op 28 september 2005 (te vinden via http://ec.europa.eu/justice_home/fsj/privacy/working_group/index_en.htm), p. 3.

203 Zie de beschrijving van de Engelse wetgeving in § 8.3.2.

204 Dit komt door de toevoeging van sub e aan de definitie van het begrip 'data' en de toekenning van het recht op toegang van het data subject in (het door de openbaarheidswetgeving toegevoegde) artikel 33A Data Protection Act 1998. Zie hierover ook Wadham & Griffiths 2005, p. 152.

de eerste plaats sprake van eigen persoonsgegevens omdat de informatie in het dossier naar aanleiding van zijn klacht was samengesteld en daardoor aan hem gerelateerd was, en in de tweede plaats omdat zijn naam in verschillende stukken moest zijn terug te vinden. Tussen de FSA en Durant ontspon zich vervolgens een discussie over, onder meer, de precieze reikwijdte van het begrip 'persoonsgegeven'. Een discussie die uiteindelijk door de rechter moest worden beslecht.

8.4.3 Het oordeel van de Britse rechter

In § 8.3.2 heb ik bij de weergave van de Engelse wetgeving over toegang tot documenten en bescherming van persoonsgegevens de definitie van het begrip 'data' besproken. In de DPA 1998 is apart bepaald wanneer deze 'data' als 'personal data' zijn aan te merken:

'personal data' means data which relate to a living individual who can be identified
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

Net als in richtlijn 95/46 moet sprake zijn van informatie over een identificeerbare persoon.²⁰⁵ In afwijking van de gebruikelijke praktijk, concentreerde het *Court of Appeal* zich echter voor het antwoord op de vraag wat als persoonsgegeven moest worden aangemerkt niet op de identificeerbaarheid van de persoon, maar op de betekenis van het gebruik van de woorden 'relate to'. Woorden die ook zijn terug te vinden in (de Engelse versie van) richtlijn 95/46. Eén van de Britse rechters, *Lord Justice Auld*, overwoog het volgende:

28. [...] not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act. Mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data. Whether it does so in any particular instance depends on where it falls in a continuum of relevance or proximity to the data subject as distinct, say, from transactions or matters in which he may have been involved to a greater or lesser degree.

In het vervolg van dezelfde overweging gaf deze rechter richtsnoeren voor de toepassing van deze interpretatie:

205 De toevoeging na sub b is overigens niet terug te vinden in de definitie uit richtlijn 95/46.

It seems to me that there are two notions that may be of assistance. The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised. The second one is on focus. The information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest, for example, as in this case, an investigation into some other person's or body's conduct that he may have instigated. In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity.

De toepassing van deze interpretatie van het begrip 'persoonsgegevens' leidde tot de conclusie dat de documenten waar Micheal Durant inzage in wilde geen persoonsgegevens bevatten of niet als persoonsgegevens konden worden aangemerkt.²⁰⁶

Hoewel het in eerste instantie leek alsof Durant zich bij de uitspraak neerlegde, diende hij op de valreep een petitie in voor een nadere behandeling van de zaak door het *House of Lords*.²⁰⁷ In november 2005 werd deze petitie afgewezen, waardoor de uitspraak van het *Court of Appeal* in stand bleef.²⁰⁸ Daarna richtte Michael Durant zijn pijlen op het EHRM in Straatsburg. Hij diende in april 2006 een klacht in die op het moment van schrijven nog op behandeling wacht.²⁰⁹

8.4.4 Een toelichting op de uitspraak door de Britse *Information Commissioner*

In het najaar van 2004 verscheen een rapport van de Britse *Information Commissioner* waarin de impact van de uitspraak voor de toepassing van de DPA 1998 werd geanalyseerd.²¹⁰ In dit rapport herformuleerde de *Commissioner* de *Durant*-uitspraak in toegankelijker bewoordingen en voegde hij er een aantal concrete voorbeelden aan toe. Het uitgangspunt is volgens de *Commissioner* dat '[w]here an individual's name appears in information the name will only be personal data where its inclusion in the information affects the named

206 Court of Appeal, *Durant t. FSA*, r.o. 30. Zie voor een uitgebreide analyse van dit deel van de uitspraak M.J. Taylor, 'Durant in the Court of Appeal: Identifying a Better Approach', *EPL* 2006, p. 461-488.

207 Deze informatie is afkomstig van <http://www.cr-law.co.uk/articles/viewarticle.asp?articleid-1225>.

208 Deze informatie is afkomstig van <http://www.out-law.com/page-6405>.

209 Deze informatie is afkomstig van <http://www.out-law.com/page-6664>.

210 Zie het rapport 'The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998' van 4 oktober 2004 (IC rapport DPA 1998). Te vinden op <http://www.ico.gov.uk>.

individual's privacy'.²¹¹ Als iemands naam vermeld staat in combinatie met zijn adres of telefoonnummer of zijn hobby's, dan is de naam van dit individu wél als persoonsgegeven in de zin van de DPA 1998 aan te merken. De *Commissioner* verwees hierbij naar de eerder besproken uitspraak van het HvJ in de zaak *Lindqvist*, waarin Bodil Lindqvist namen van collega-vrijwilligers in een Zweedse kerkgemeenschap op Internet plaatste in combinatie met bepaalde adresgegevens, hobby's en in een enkel geval zelfs medische gegevens.²¹² In dit verband plaatste de *Commissioner* ook het door het *Court of Appeal* geopperde aanknopingspunt van de *focus* van het betreffende document. Er moet een link bestaan tussen de met naam genoemde persoon en de resterende informatie in het document.²¹³ De *Commissioner* noemde vervolgens een aantal voorbeelden van wat normaal gesproken niet als persoonsgegevens kan worden aangemerkt:

- mere reference to a person's name where the name is not associated with any other information;
- incidental mention in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity; or
- where an individual's name appears on a document or e-mail indicating only that it has been sent or copied to that particular individual, the content of that document or e-mail does not amount to personal data about the individual unless there is other information about the individual within it.²¹⁴

8.4.5 De relevantie van de *Durant*-uitspraak voor het onderhavig onderzoek

De uitspraak van het Britse *Court of Appeal* is, mede gezien de overweging van de Commissie om een inbreukprocedure tegen het Verenigd Koninkrijk te starten, controversieel. Los van het Commissieonderzoek, biedt de interpretatie van de Britse rechters hoe dan ook voer voor een bredere discussie over de vraag of de bestaande regels over de bescherming van persoonsgegevens nog wel volledig geschikt zijn om de huidige verwerking van persoonsgegevens te reguleren.²¹⁵ Door de ruime uitleg van de begrippen 'persoonsgegevens' en 'verwerken' is er in de huidige gedigitaliseerde maatschappij bijzonder snel sprake van een situatie waarin geautomatiseerde verwerking van persoonsgegevens plaatsvindt en waarop de gegevensbeschermingsregels van toepassing zijn.²¹⁶ Als in elk geval strak de hand wordt gehouden aan de verplichtingen

211 Zie IC rapport DPA 1998, p. 2.

212 Zie over de zaak *Lindqvist* ook § 8.2.2.1.

213 Zie IC rapport DPA 1998, p. 3.

214 Zie IC rapport DPA 1998, p. 3.

215 Zie bijv. de eerder genoemde discussie die momenteel wordt gevoerd in de Artikel 29 Werkgroep.

216 Zie hierover ook § 5.2.

die uit deze regels voortvloeien, dan lijken deze regels het maatschappelijke leven eerder te frustreren dan te reguleren.

De *Durant*-uitspraak gaat niet over de botsing tussen toegang tot documenten en bescherming van persoonsgegevens. Toch is de uitspraak relevant omdat een beperking van de reikwijdte van de gegevensbeschermingsregels uiteraard ook tot een verkleining van de overlap van beide rechtregimes leidt.²¹⁷ Dat de uitspraak voor dit onderzoek relevant is, wordt duidelijk geïllustreerd door het tweede voorbeeld dat de *Information Commissioner* naar voren brengt. Een 'Durant'-uitleg van het begrip 'persoonsgegevens' zou ertoe geleid hebben dat de namen van de aanwezigen tijdens de Commissievergadering uit de *Bavaria*-zaak zonder problemen vrijgegeven konden worden aan Andrew Ronnan, de directeur van Bavaria. Immers, de loutere vermelding van de naam wegens aanwezigheid kan niet worden aangemerkt als persoonsgegevens.

Overigens gaat het in de *Durant*-zaak uiteindelijk ook om toegang tot documenten, alleen dan om toegang tot documenten die persoonsgegevens van de verzoeker bevatte. Michael Durant probeerde namelijk toegang tot de documenten te verkrijgen op basis van het recht op inzage in *eigen* persoonsgegevens, zoals dat is neergelegd in de DPA 1998. Omdat zijn naam in bepaalde documenten vermeld stond of omdat de informatie in de documenten aan hem gerelateerd was, claimde hij een specifiek recht op toegang. De beperkte interpretatie van het begrip 'persoonsgegevens' heeft tot gevolg dat toegang tot de documenten als gevolg van het recht op inzage in eigen persoonsgegevens *niet* wordt toegekend: er is in dit geval namelijk geen sprake van persoonsgegevens. Maar uiteraard heeft de beperkte interpretatie net zo goed uitwerking op de andere situatie: de gegevens die buiten de reikwijdte van het begrip 'persoonsgegevens' vallen, zullen automatisch ook buiten de reikwijdte van de uitzondering van de bescherming van persoonsgegevens in openbaarheidswetgeving vallen. Deze gegevens kunnen dan, los van andere redenen voor geheimhouding, geopenbaard worden.

Het verschil tussen de in hoofdstuk 7 weergegeven discussie over de juiste interpretatie van artikel 4 lid 1 sub b van de Eurowob en de interpretatie van het *Court of Appeal*, is dat het hier gaat om een afbakening van de reikwijdte van bescherming van persoonsgegevens *als zodanig* en niet om een beperking van de reikwijdte door de expliciete vermelding dat de privacy van het individu door openbaarmaking aangetast zou moeten zijn.²¹⁸ De *Durant*-benadering heeft consequenties voor *alle* vormen van verwerking van persoonsgegevens, terwijl de discussie over de beperking tot gevallen waarin de privacy in het geding is alleen de openbaarmaking van de persoonsgegevens aan derden betreft omdat dit nu eenmaal in de Eurowob zou zijn vastgelegd.²¹⁹ Om te spreken in de drie situaties zoals beschreven in hoofdstuk 4, de *Durant*-

217 Zie voor een beschrijving van de overlap van beide regimes hoofdstuk 5.

218 Zie § 7.2.

219 Zie ook § 1.5.

uitspraak leidt ertoe dat de reikwijdte van de bescherming van persoonsgegevens beperkt wordt tot de tweede situatie (bescherming van persoonsgegevens is van toepassen én de privacybescherming) en de derde situatie (apart regime van gegevensbescherming is van toepassing alsook de privacybescherming).²²⁰ De eerste situatie (bescherming van persoonsgegevens is van toepassing en privacybescherming *niet*) houdt op te bestaan, omdat het *Court of Appeal* voor de afbakening van de reikwijdte van de bescherming van persoonsgegevens aanhaakt op de privacybescherming. De hele discussie over het onderscheid tussen privacy en bescherming van persoonsgegevens vervalst, omdat de scheidslijn van wat wel en niet onder de gegevensbescherming valt, gelijk wordt gesteld met die van de privacybescherming.²²¹

8.4.6 De *Durant*-uitspraak en de verhouding tussen privacy en de bescherming van persoonsgegevens

De *Durant*-uitspraak geeft een duidelijk uitgangspunt: alleen de vermelding van iemands naam in een document valt niet binnen de bescherming van persoonsgegevens.²²² Het eerste voorbeeld van de *Information Commissioner* betreft de situatie waarin sprake is van een naam zonder extra informatie. Dit voorbeeld is vrij theoretisch. Het zal zelden voorkomen dat een document waarin iemand bij name wordt genoemd, geen enkele extra informatie over deze persoon verschaft. Een vermelding van aanwezigheid tijdens een vergadering maakt duidelijk dat de genoemde persoon op het aangegeven tijdstip op de aangegeven plek was in het kader van een bepaalde vergadering. De *Durant*-uitspraak gaat echter verder door ook eisen te stellen aan deze extra informatie: een naam valt pas binnen de bescherming van persoonsgegevens als door de vermelding in het document de privacy van de betrokkene wordt aangetast. De vraag is wanneer van een dergelijke aantasting sprake is. Het *Court of Appeal* kiest een formulering die lijkt aan te sluiten op een meer klassieke omlijning van het privé-leven: 'information [...] going beyond the recording of the putative data subject's involvement in a matter or an event that has no personal connotations'. De *Information Commissioner* verduidelijkt dit laatste in zijn tweede voorbeeld van wat niet als persoonsgegevens kan worden aangemerkt: de vermelding van iemands naam gekoppeld aan de uitoefening van iemands officiële functie ('official capacity'). Dit sluit aan op de eerder besproken jurisprudentie van het EHRM, met dat verschil dat de

220 Zie § 4.4.

221 Zie § 4.2 en § 4.3.

222 Ter vergelijking, de EDPS hanteert in zijn richtsnoeren eenzelfde uitgangspunt alleen dan in het kader van het *onderscheid* tussen privacy en bescherming van persoonsgegevens. Volgens de EDPS is de privacy van de betrokkene in beginsel niet in het geding en is de uitzondering van artikel 4 lid 1 sub b Eurowob niet inroepbaar als alleen de naam van deze persoon openbaar wordt gemaakt. EDPS-Richtsnoeren 2005, p. 36.

Information Commissioner zich niet beperkt tot personen die politiek actief zijn of een officiële functie namens de staat bekleden.²²³ Het lijkt om iedereen te gaan die vanwege zijn professionele hoedanigheid bij een activiteit is betrokken en in een daaropvolgend document bij name wordt genoemd. Over deze situaties heeft het EHRM geen uitspraak gedaan, wat wellicht aangeeft dat het publiceren of op andere wijze verwerken van iemands naam, gekoppeld aan registrerende informatie over professionele activiteiten, tot nu toe niet tot bezwaren bij de betrokken persoon heeft geleid. Het is hoe dan ook interessant te weten of de klacht van Durant door het EHRM ontvankelijk zal worden verklaard.

Een aanwijzing of het EHRM hiertoe over zal gaan, kan gevonden worden in de ontvankelijkheidsbeslissing in *Smith t. het Verenigd Koninkrijk*, die in hoofdstuk 4 al ter sprake kwam.²²⁴ Ook in deze zaak was iemand toegang geweigerd tot een dossier terwijl zijn naam, uit hoofde van zijn professionele hoedanigheid, in bepaalde documenten voorkwam. Het EHRM verklaarde de klacht kennelijk ongegrond omdat het dossier louter zakelijke informatie bevatte en de verzoeker al bekend was met de inhoud ervan.²²⁵ De beslissing van het EHRM biedt weinig hoop voor Durant, zij het dat een belangrijk verschil is dat Durant niet bekend was met de inhoud van het onderzoeksdossier van de FSA. Mocht Durants klacht worden afgewezen dan is het Britse standpunt niet strijdig met *artikel 8 EVRM*. Daarmee is echter nog niets gezegd over de verenigbaarheid van de Britse interpretatie van het begrip ‘persoonsgegevens’ met richtlijn 95/46. Dit merkt het EHRM in *Smith* ook op, door vooraf te benadrukken dat het niet aan het EHRM is om te beoordelen of de Britse rechters de Europese richtlijn correct hebben geïnterpreteerd.²²⁶

8.4.7 Brede implicatie van de *Durant*-uitspraak wordt buiten beschouwing gelaten

Voor de afstemming van toegang tot documenten en bescherming van persoonsgegevens is de *Durant*-uitspraak duidelijk interessant en relevant. Omdat de Britse *Lords* voor de afbakening van de reikwijdte van de gegevensbescherming aansluiten op de privacybescherming, zijn er sterke overeenkomsten met de wijze waarop de EDPS het raakvlak inkleurt.²²⁷ Uit het overzicht van de wetgeving van de landen die het raakvlak van beide rechten hebben aangepakt, blijkt bovendien meerdere malen dat ten aanzien van gegevens die de Britse

223 Vgl. § 4.3.7.

224 EHRM 4 januari 2007, *Smith t. het Verenigd Koninkrijk* (ontvankelijkheidsbeslissing). Zie § 4.3.3.

225 EHRM, *Smith*, p. 4. Zie over deze beslissing ook § 8.4.6.

226 EHRM, *Smith*, p. 4.

227 Zie EDPS-Richtsnoeren 2005, p. 36-38.

rechters buiten de gegevensbescherming plaatsen, de gegevensbescherming ten gunste van de openbaarheid opzij wordt gezet. Alleen wordt in die gevallen voor een andere systematiek gekozen.

Zoals gezegd, heeft de *Durant*-uitspraak consequenties voor alle vormen van verwerking van persoonsgegevens. Voor het afstemmen van toegang tot documenten en bescherming van persoonsgegevens is de beperking van de reikwijdte van de gegevensbescherming het overwegen waard. Dit geldt alleen niet per definitie voor alle andere vormen van verwerking. Elke vorm van verwerken heeft een verschillende invloed op de privacybeleving van de betrokkene. Om de gegevensbeschermingswetgeving geen onduidelijke reikwijdte te geven, verdient het mijns inziens aanbeveling om, indien gewenst, in wetgeving soepelere regels voor nader gespecificeerde vormen van verwerken van bepaalde gegevens op te nemen. Zo zal dit in het onderhavige onderzoek voor het openbaren van bepaalde persoonsgegevens worden voorgesteld.²²⁸

Hoewel de *Durant*-uitspraak voor het onderhavige onderzoek wat betreft de afbakening van de privacybescherming als inspiratiebron dient voor de afstemming van toegang tot documenten en bescherming van persoonsgegevens, wordt de verstrekkende impact ervan verder buiten beschouwing gelaten.

8.5 CONCLUSIE

In dit hoofdstuk is een overzicht gegeven van de manier waarop de EU-lidstaten toegang tot documenten en bescherming van persoonsgegevens wettelijk op elkaar hebben afgestemd. 24 lidstaten hebben zowel een wet over toegang tot overheidsinformatie als een wet over gegevensbescherming. De afstemming van deze twee wetten varieert sterk. In sommige landen is deze nagenoeg afwezig, en in andere landen zijn beide wetten zeer expliciet en gedetailleerd op elkaar afgestemd. Daar tussenin verschuift de afstemming van een simpele vermelding van privacy als uitzonderingsgrond op het recht op toegang tot documenten, via een verdere uitwerking van de privacyexceptie tot een uitdrukkelijke afstemming met de gegevensbeschermingswetgeving.

De afstemming van beide wetten wordt op verschillende manieren ingevuld. In drie landen laat de wetgever de afweging van de achterliggende belangen uitdrukkelijk over aan de uitvoerende instanties. Verder zijn verschillende criteria te vinden aan de hand waarvan de beslissing over toegang tot persoonsgegevens moet worden genomen: (de mate van inbreuk op) de privacy van de betrokkene, de schade die openbaarmaking voor de betrokkene oplevert, de algemene bekendheid van de informatie en het gedrag van de betrokkene. In veel landen worden bepaalde categorieën persoonsgegevens

228 Zie § 9.4-9.6.

door de wetgever benoemd die wel of niet geopenbaard mogen worden. Zo is bepaald dat gevoelige gegevens niet geopenbaard mogen worden, en is in de wetgeving van zeven landen vastgelegd dat bepaalde gegevens die gerelateerd zijn aan iemands publieke functie of status niet geheim gehouden mogen worden.

Naar aanleiding van de uitspraak van het Britse *Court of Appeal* in de zaak *Durant* heb ik kort gesproken over de definitie van het begrip 'persoonsgegevens'. In deze uitspraak hanteren de Britse rechters een enge definitie van het begrip 'personal data' waardoor de reikwijdte van de bescherming van persoonsgegevens als zodanig wordt beperkt. Deze beperking van de reikwijdte zou leiden tot een verkleining van de overlap van de rechtsregimes van toegang tot documenten en bescherming van persoonsgegevens en is om die reden voor dit onderzoek relevant. De afbakening van de privacybescherming dient als inspiratiebron voor het onderhavige onderzoek, de verstrekkende impact ervan wordt verder echter buiten beschouwing gelaten.